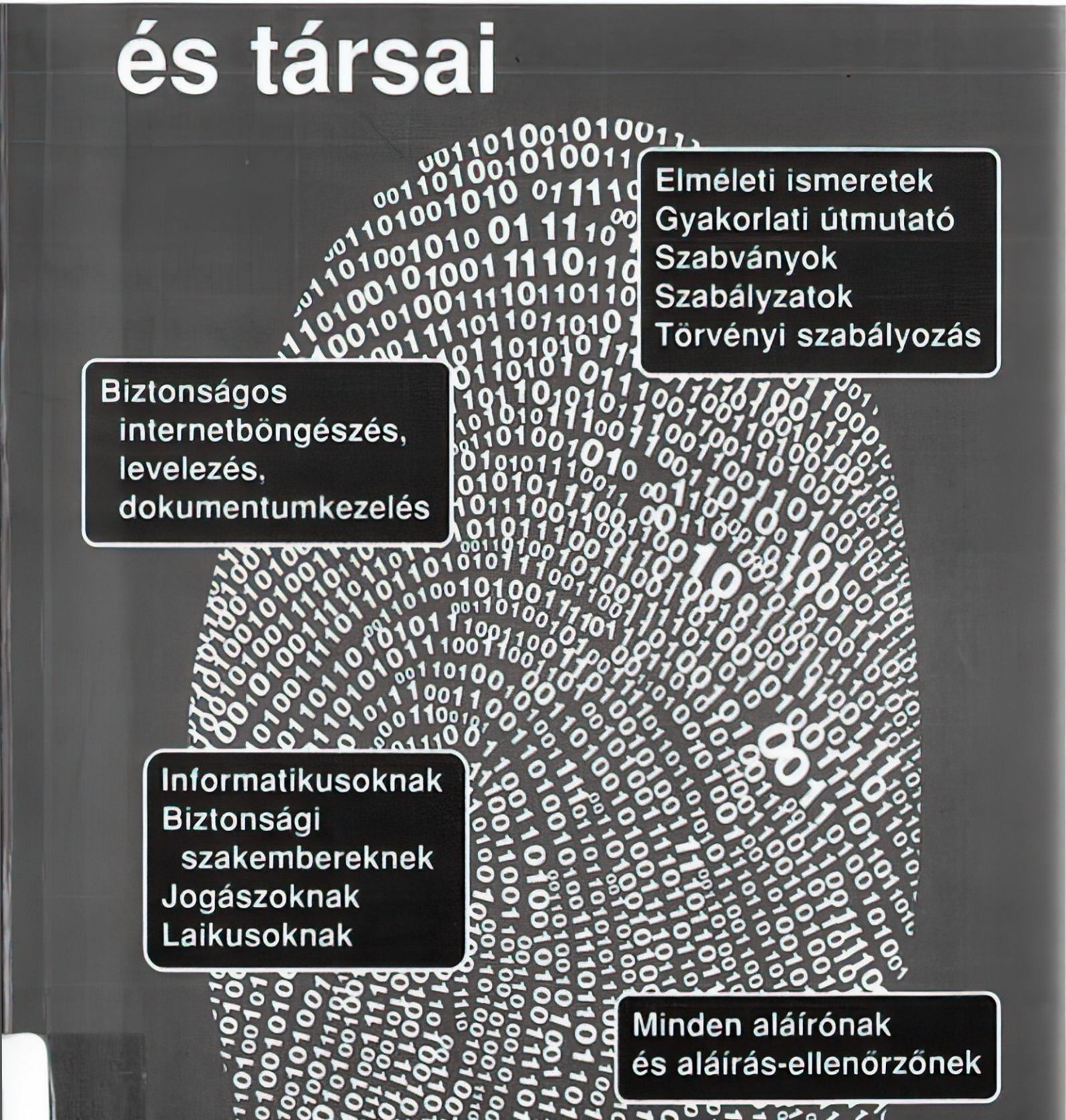
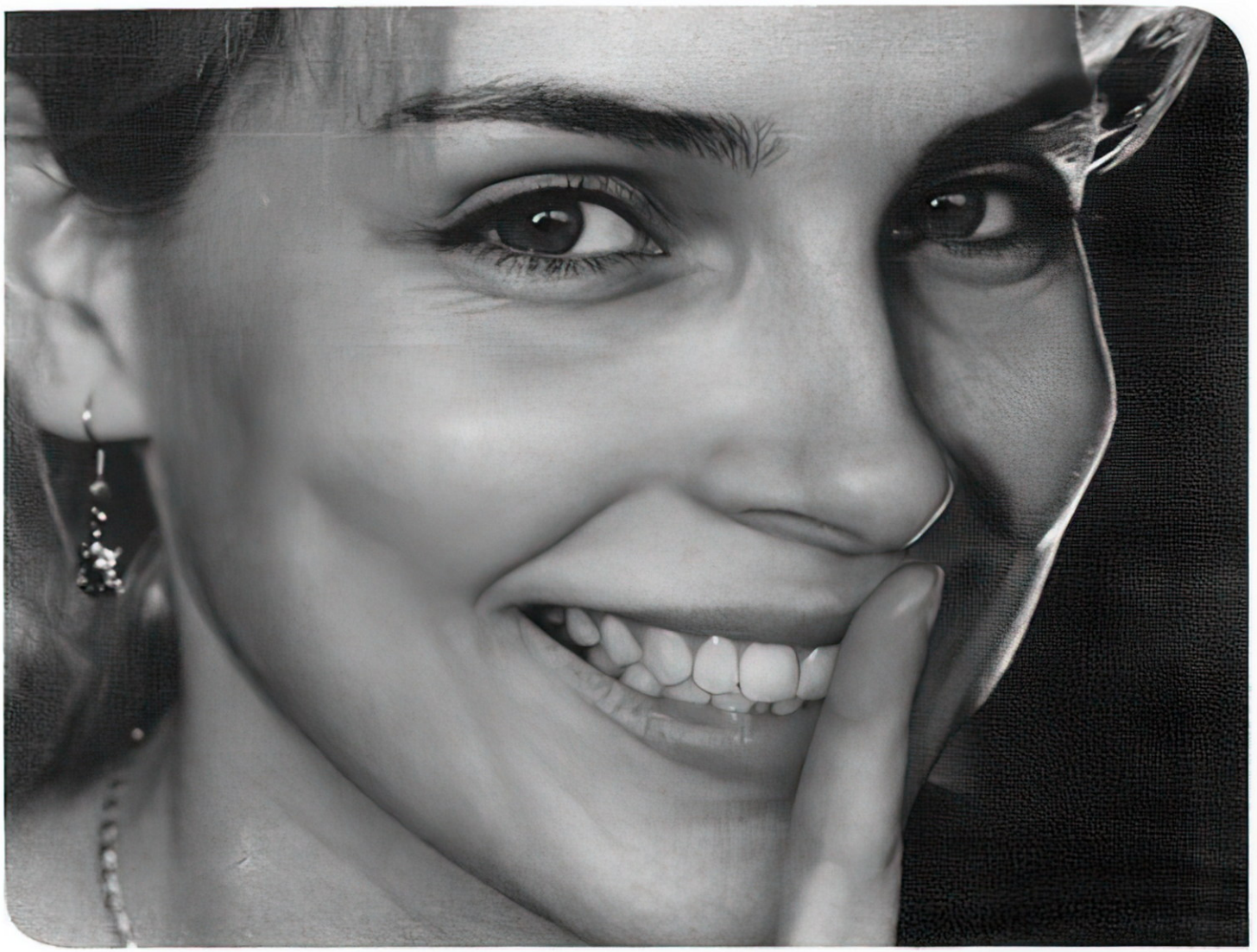
Almási János

Elektronikus aláírás és társai



Hogy a titok titok maradjon



Tegye biztonságossá informatikai rendszerét!

Egy vállalat megbízhatósága nemcsak dolgozóin múlik. A technika fejlődésével egyre nagyobb szerepet kap az informatikai rendszer megbízhatósága. Digitalizált világunkban nem mindegy, hogy egy titkos információ csak az érintettekhez jut el, vagy mások számára is hozzáférhető. Megfelelő védelem nélkül nemcsak a titkok kiszivárgásának nagy a kockázata, de könnyedén avatkozhatnak hálózatába illetéktelenek, így akár meg is béníthatják rendszerét, esetleg pótolhatatlan adatai sérülhetnek. A védekezés hasznos, de mindenképp célszerű szakértőre bízni a problémát, mert a különböző szintű kockázatok különböző megoldást igényelnek!

Keressen fel minket, hiszen mi széles körű, cégre szabott biztonsági megoldást kínálunk Önnek!

SYNERGON
A megoldásszállító.

Synergon Informatika Rt. ▪ 1047 Budapest, Baross utca 91–95.

ISO 9001 UKAS

Elektronikus aláírás és társai

„Aki ellenünk van, az velünk van.”

Sans Serif

A NetLock Kft., mint hitelesítés szolgáltató a következő osztályú és típusú tanúsítványokat kínálja:

Tanúsítvány osztály	"A" osztály Kibocsátás közjegyző által hitelesített adatok alapján. Felelősségbiztosítás 5.000.000 Ft-ig.	"B" osztály Kibocsátás személyes megjelenés során bemutatott eredeti okmányok alapján. Felelősségbiztosítás 500.000 Ft-ig.	"C" osztály Kibocsátás okmányok másolatának (pl. faxon) bemutatása alapján. Felelősségbiztosítás 50.000 Ft-ig.
Személyes tanúsítványok	Természetes személy igényelheti a sajót nevében. Az aláíró tanúsítvány kizárólag elektronikus aláírás előállítására, a titkosító tanúsítvány kizárólag titkosításra használható. Elsősorban magánjellegű kommunikációhoz ajánlott.		
Szervezeti tanúsítványok	Jogi személy, szervezet igényelheti. Az aláíró tanúsítvány kizárólag elektronikus aláírás előállítására, a titkosító tanúsítvány kizárólag titkosításra használható. Elsősorban a szervezet által bonyolított kommunikációhoz ajánlott.		
Meghatalmazásos tanúsítványok	Természetes személy igényelheti, egy adott szervezet munkatársaként. Az aláíró tanúsítvány kizárólag elektronikus aláírás előállítására, a titkosító tanúsítvány kizárólag titkosításra használható. Elsősorban a szervezet munkatársai által a szervezet nevében tett nyilatkozatokhoz, kommunikációhoz ajánlott.		
Technikai eszköz tanúsítványok	Technikai eszközök (szerverek, routerek) számára igényelhető, biztonságos adattovábbítást lehetővé tévő, titkosító tanúsítványok. Az SSL tanúsítvány web szerverekkel történő biztonságos kommunikációhoz, a VPN tanúsítvány LAN-ok nyílt hálózaton történő biztonságos összekötéséhez, a WAP Gateway tanúsítvány biztonságos WAP kommunikáció kialakításához használható.		

NETLOCK
Az Időpecsét Szolgáltató

Új szolgáltatás! Időbélyegzés

A NetLock Kft. legújabb szolgáltatása segítségével bizonyítható, hogy egy adott elektronikus dokumentum egy adott időpontban létezett. A Hírközlési Főfelügyeletnél regisztrált szolgáltatás szabványos eszközök segítségével biztosítja az elektronikus tranzakciók esetében elengedhetetlen fokozott biztonságú időbélyeget.

NetLock Informatikai és Hálózatbiztonsági Kft.
1023 Budapest, Zsigmond tér 10. • Telefon: (1) 345-2255 • Fax: (1) 345-2250
e-mail: info@netlock.net • web: www.netlock.net

Tanúsítványainkról, cégünkről kérjen bővebb információt Ügyfélszolgálatunktól is!

NETLOCK
Az Első Hitelesítés Szolgáltató

Tartalomjegyzék

Előszó 13

A könyvben alkalmazott jelölések 19

1 **Bevezetés** 21
1.1 *A hagyományos aláírás* 23
1.1.1 Az aláírás célja 23
1.1.2 A hagyományos aláírás (és társai) 24
1.2 *Az elektronikus aláírás* 25
1.2.1 Veszélyek az elektronikus világban 25
1.2.2 Mi az elektronikus aláírás? 27
1.2.3 Az elektronikus aláírás eszközei 27
1.2.4 Mi szükség az elektronikus aláírásra? 28
1.2.5 Melyik a jobb aláírás? 28
1.2.6 Az elektronikus aláírás bökkenői 30
1.2.7 Az elektronikus aláírás felhasználási területei 31
1.2.8 Amire az elektronikus aláírás sem jó 31
1.2.9 Mi szükséges az elektronikus aláíráshoz? 32
1.2.10 A társak 33
1.3 *Nyilvános kulcsú infrastruktúra* 34

2 **Elektronikus aláírás (és társai) a gyakorlatban** 37
2.1 *Tanúsítvány igénylése – NetLock* 40
2.2 *Elektronikus levelezés – Outlook 2002* 43
2.2.1 Beállítások 43
2.2.2 Levél aláírása, titkosítása 44
2.2.3 Aláírt levél ellenőrzése, dekódolása 45
2.3 *Elektronikus levelezés – Drótposta* 47
2.4 *Webkommunikáció – Internet Explorer* 48
2.5 *Állományok titkosítása – EFS* 49
2.5.1 Miért kell az állományokat titkosítani? 50
2.5.2 Titkosítás és visszafejtés 50
2.6 *Dokumentumok aláírása – Office XP* 51
2.6.1 Word-dokumentumok aláírása 52
2.6.2 Word-dokumentumok aláírás-ellenőrzése 53

2.6.3 Excel és PowerPoint 53
2.6.4 Dokumentumok titkosítása 54
2.6.5 Makrók aláírása – Office XP 56
2.7 Tanúsítványok lekérdezése 58

3 Az elektronikus aláírás (és társai) fiziológiája 63
3.1 Felhasználási lehetőségek 65
3.2 Alapműveletek 66
3.3 Az elektronikus aláírás működése 66
3.3.1 Elektronikus aláírás készítése 67
3.3.2 Az elektronikus aláírás ellenőrzése 68
3.3.3 Egyéb megfontolások 69
3.3.4 A lenyomatkészítő eljárás 69
3.4 A titkosítás működése 70
3.4.1 A rejtjelezés felhasználása 70
3.4.2 Rejtjelezési módszerek 71
3.4.3 Szimmetrikus kulcsú rejtjelezés 71
3.4.4 A szimmetrikus kulcsú rejtjelezés 72
3.4.5 Üzenetek titkosítása 73
3.4.6 Soros és blokktitkosítás 74
3.4.7 Hogyan lesz a titkosításból elektronikus aláírás 75
3.5 Felhasználói hitelesítés 76
3.5.1 A felhasználói hitelesítés módszerei 76
3.5.2 Jelszó 76
3.5.3 OTP 77
3.5.4 Biometria 77
3.5.5 Kombinált megoldások 78
3.5.6 PKI alapú hitelesítés 78
3.6 Algoritmusok, kulcsméretek és egyebek 79
3.6.1 Algoritmus feltörése 79
3.6.2 És ha mégis? 80
3.6.3 Támadások, kriptoanalízis 80
3.6.4 Nyers erő és egyéb huncutságok 81
3.6.5 Hash- és feltöltő algoritmusok 82
3.6.6 A DES algoritmus 82
3.6.7 Egyéb szimmetrikus algoritmusok 82
3.6.8 AES 83
3.6.9 RSA 84
3.6.10 A faktorizálás 84
3.6.11 DSA 85
3.6.12 ECDSA 85
3.6.13 Kulcshosszak 86
3.6.14 Blokkos rejtjelező algoritmusok üzemmódjai 86

3.6.15 Véletlenszám-generálás 87
3.7 Kriptoprotokollok 88
3.7.1 A protokollok jellemzői 88
3.7.2 A kriptoprotokollok típusai 89
3.7.3 Pár érdekes kriptoprotokoll 89
3.7.4 Néhány földhözragadtabb kriptoprotokoll 90
3.7.5 Diffie-Hellman kulcsegyeztetés 91
3.7.6 Az SSL, TLS és WTLS protokollok 92
3.7.7 Az S/MIME protokoll 93
3.7.8 Az IPSec protokoll 93
3.8 Letagadhatatlanság 94

4 A tanúsítvány 99
4.1 Mi is az a tanúsítvány? 101
4.1.1 Hagyományos világ 101
4.1.2 Elektronikus világ 102
4.2 Nyilvános kulcsú tanúsítványok 102
4.2.1 Mi szükség a tanúsítványra 102
4.2.2 A megbízható harmadik fél 103
4.2.3 Mit tanúsít a tanúsítvány 103
4.2.4 A tanúsítvány tartalma 104
4.2.5 Koncentrált bizalom 104
4.2.6 A tanúsítvány jellemzői 105
4.3 Tanúsítvány és kulcs – érvényességi idő és állapot 105
4.3.1 Az érvényességi idő korlátozása 106
4.3.2 A tanúsítvány érvényességi ideje 106
4.3.3 Tanúsítványok visszavonása 107
4.3.4 Mit jelent az érvényességi idő 108
4.3.5 Kulcshasználat az érvényességi idő után 108
4.3.6 Aláírás érvényességének ellenőrzése 108
4.4 Kulcsmenedzsment 109
4.4.1 Kulcspárgenerálás 109
4.4.2 A magánkulcs tárolása és védelme 110
4.4.3 Különböző kulcsfajták és ezek kezelése 111
4.4.4 Magánkulcs letét 113
4.5 Tanúsítványok osztályozása 114
4.5.1 A rendezés módja 114
4.5.2 Tanúsítványok típusai 114
4.5.3 Tanúsítványok osztályai 115
4.5.4 Osztály és típus viszonya 117
4.6 Tanúsítványok kibocsátása 117
4.6.1 Tanúsítványigénylés 117
4.6.2 Szerepek 118

4.6.3 Azonosító és azonosítás 119
4.6.4 Álnév 121
4.6.5 Adatok ellenőrzése 121
4.6.6 Tanúsítvány elkészítése 123
4.6.7 Kézbesítés 123
4.6.8 Tanúsítvány megújítása 124
4.7 Tanúsítványok szétosztása 125
4.7.1 Az aláíró és titkosító kulcsok terjesztése 125
4.7.2 Nyilvános tanúsítványtárak 126
4.7.3 Könyvtárrendszerek 127
4.8 Tanúsítvány-visszavonás és visszavonási lista 128
4.8.1 Visszavonási okok 128
4.8.2 Visszavonás, felfüggesztés, visszahelyezés 129
4.8.3 A tanúsítvány-visszavonási lista 130
4.8.4 A visszavonási lista generálása 130
4.8.5 A visszavonási lista szétosztása 131
4.8.6 A visszavonási lista ellenőrzése 131
4.8.7 Visszavonási listák típusai 132
4.8.8 Visszavonási időskála, felelősségi kérdések 134
4.8.9 Azonnali érvényesség-ellenőrzés 136
4.9 Az X.509-es szabvány 137
4.9.1 A szabvány 137
4.9.2 A tanúsítvány felépítése 137
4.9.3 Az X.500 egyedinév-formátum 139
4.9.4 Toldalékok 140
4.9.5 Objektumregisztráció 141
4.9.6 A tanúsítvány szabványos toldalékai 141
4.9.7 Az X.509-es visszavonási lista 143
4.9.8 A visszavonási lista szabványos toldalékai 144
4.10 Attribútumtanúsítványok 145
4.11 Találkozások a tanúsítvánnyal 147
4.11.1 Elektronikus levelezés 147
4.11.2 Biztonságos böngészés 148
4.11.3 Aláírt programok 148
4.11.4 Mit nézzünk a tanúsítványon 149

5 A hitelesítésszolgáltató 155
5.1 A hitelesítésszolgáltató feladatai 157
5.2 Hitelesítésszolgáltató-típusok 158
5.3 Közösség 158
5.4 A hitelesítésszolgáltató felépítése 159
5.4.1 Hitelesítőszervezet 160
5.4.2 Regisztrációs szervezet 160

5.4.3 Tanúsítványtár 162
5.4.4 Valós idejű állapotinformációs egység 162
5.4.5 Szabályzószervezet 162
5.5 Hitelesítésszolgáltatások 163
5.5.1 Hitelesítésszolgáltatások felosztása 163
5.5.2 Tanúsítvány-létrehozási szolgáltatás 165
5.5.3 Regisztrációs szolgáltatás 165
5.5.4 Egyedinév-szolgáltatás 166
5.5.5 Tömeges regisztrációs szolgáltatás 166
5.5.6 Adattárolási szolgáltatás 167
5.5.7 Tanúsítványszétosztási szolgáltatás 167
5.5.8 Visszavonás-kezelési szolgáltatás 168
5.5.9 Tanúsítványarchiválási szolgáltatás 168
5.5.10 Állapotinformációs szolgáltatás 168
5.5.11 Valós idejű állapotinformációs szolgáltatás 169
5.5.12 Tanúsítványmegújítási szolgáltatás 169
5.5.13 Kulcsletét szolgáltatás 169
5.5.14 Aláírás-létrehozó eszközzel kapcsolatos szolgáltatások 170
5.5.15 Elérhetőség, rendelkezésre állás 170
5.6 Egyéb bizalmi szolgáltatások 170
5.6.1 Érvényességi információs szolgáltatás 171
5.6.2 Időbélyegzés szolgáltatás 171
5.6.3 Tranzakcióhitelesítő szolgáltatás 172
5.7 Szolgáltatók megbízhatósága 173
5.7.1 Üzleti-jogi biztonság 174
5.7.2 Személyi biztonság 175
5.7.3 Fizikai biztonság 175
5.7.4 Informatikai biztonság 176
5.7.5 Adminisztratív, szervezeti, szabályzati biztonság 177
5.7.6 Audit és minősítés 177
5.7.7 Szolgáltatók típusai, Nagy Testvér komplexus 178
5.8 Struktúrák 180
5.8.1 Regisztrációs struktúrák 180
5.8.2 Hitelesítési struktúrák 181
5.8.3 Tanúsítási láncok 182
5.8.4 Kereszthitelesítés 183
5.8.5 Láncbejárás 185
5.8.6 Hitelesítőegység-tanúsítványok 187
5.8.7 Házi hitelesítő-központ 187

6 Az aláíró eszköz 191
6.1 Kulcstároló és aláíró eszközök 193
6.2 Aláíró eszköz és aláíró környezet 193

6.3 Az aláíró eszközök fajtái 194
6.4 ALE és BALE 195
6.5 Intelligens kártyák 196
6.5.1 Multiapplikációs kártyák 196
6.5.2 Kártyaplatformok 197
6.5.3 Kártyamenedzsment, biztonság 198
6.5.4 Kártyaolvasók 198
6.5.5 Kártyaszabványok 199
6.6 Gyártók, árak 199

7 Szabványok 203
7.1 Mit jelent a szabvány 205
7.2 Szabványok tengere 206
7.3 Szabványosítási szervezetek 206
7.3.1 Nemzetközi, amerikai szervezetek 207
7.3.2 Európa – EESSI 207
7.3.3 Vállalati szabványok 208
7.4 Szabványok, specifikációk, ajánlások 209
7.4.1 A szabványosítás területei 209
7.4.2 A szabványosítás szabványtalansága 210

8 Szabályzatok 213
8.1 A szabályzatok forrásai 215
8.2 A szabályzatok megjelenési formája 216
8.3 A szabályzatok szerepe 216
8.4 Szabályzatok egymás hegyén-hátán 217
8.5 Fontosabb szabályzatok 219
8.5.1 Szolgáltatási szabályzat 219
8.5.2 Hitelesítési szabályzat 220
8.5.3 Aláírási szabályzat 221
8.5.4 Általános szerződési feltételek 222
8.6 Dokumentumok viszonya 222
8.6.1 A hitelesítési szabályzat és a szolgáltatási szabályzat 222
8.6.2 A hitelesítési szabályzat és az aláírási szabályzat 223
8.6.3 Szabályzatok közti ellentétek kezelése 224
8.7 Az RFC 2527 szabvány 224
8.8 Szabályzati tartalomjegyzék 224

9 Az elektronikus aláírás jogszabályi háttere 231
9.1 A szabályozás szintjei 233
9.2 Az EU-irányelv 235
9.3 A magyar elektronikus aláírási törvény 236
9.3.1 A törvény személyi és tárgyi hatálya 236

9.3.2 Az elektronikus aláírás fajtái 236
9.3.3 Az elektronikus dokumentumok fajtái 237
9.3.4 Alapelvek 238
9.3.5 Jogkövetkezmények 238
9.3.6 Elektronikus aláírás szolgáltatások 239
9.3.7 A szolgáltatások nyújtásának feltételei 240
9.3.8 A hitelesítésszolgáltatási tevékenység 240
9.3.9 Adatvédelem 240
9.3.10 A szolgáltató felelőssége 241
9.3.11 Az aláíró jogai és kötelezettsége 241
9.3.12 A felügyelet feladatai 241
9.4 Mitől lesz egy aláírás minősített? 242
9.4.1 A minősített tanúsítvány 242
9.4.2 A fokozott biztonságú tanúsítvány és szolgáltató 242
9.5 A titkosítás szabályozása 243
9.5.1 Titkosítás Eat. módra 243
9.5.2 Adatvédelmi ajánlás 244

10 Az elektronikus aláírás (és társai) lélektana 247
10.1 A magánkulcs védelme 249
10.1.1 Fizikai védelem 249
10.1.2 Aktivizáló adat 250
10.1.3 Jelszó 250
10.2 Fizikai tanúsítvány formátumok 251
10.3 A Windows és az Office 252
10.3.1 Windows tanúsítványtár 252
10.3.2 Tanúsítványok menedzsmentje – Certificates ablak 255
10.3.3 Tanúsítványok menedzsmentje – MMC 256
10.3.4 Microsoft Certificate Server 257
10.3.5 A Certificate ablak 258
10.3.6 Tanúsítványok importálása és exportálása 261
10.3.7 Visszavonási lista 262
10.3.8 Internet Options 263
10.3.9 Internet Explorer 264
10.3.10 A kriptomodul erőssége 265
10.3.11 Aláírt programok 266
10.3.12 Intéző 268
10.3.13 EFS 269
10.3.14 Kártyás bejelentkezés 272
10.3.15 Virtuális magánhálózat 272
10.3.16 IPSec 274
10.3.17 A CryptoAPI és a CSP-k 276
10.3.18 Támogatott kártyák és kártyaolvasók 277

10.3.19 Outlook 2000 és 2002 278
10.4 Hitelesítésszolgáltatók Magyarországon 279
10.4.1 A NetLock Kft. és hitelesítésszolgáltatása 280
10.4.2 Matáv e-Szignó 281
10.4.3 A GIRO hitelesítésszolgáltatása 282
10.5 Aláírás és aláírás-ellenőrzés 282
10.5.1 Az aláíró kötelezettségei 283
10.5.2 Az elektronikus aláírás megtétele 283
10.5.3 Az ellenőrző kötelezettségei 284
10.5.4 Az elektronikus aláírás ellenőrzése 284

Melléklet 289

Fogalomtár 291

Szakirodalom 296

Tárgymutató 298

Előszó

„bizalom az elektronikus kommunikáció alapja", „az internet legnagyobb előnye, a nyitottsága, egyben legnagyobb veszélyforrása is", „a zárt ajtók már nem elégségesek a szervezetek egyik legfontosabb vagyonának, az információnak a védelmére", és folytathatnám még a sort hasonló, immáron közhelyszámba menő kijelentésekkel. Utalhatnék előszavamban a tudás alapú üzletre, ami a legnagyobb értéket termeli, bármely iparágról legyen is szó; a talán végre ténylegesen megvalósuló papírmentes irodára; az elektronikus üzletvitel és kereskedelem kínálta megannyi új lehetőségre; a virtuális világra, ahol az országhatárok értelmüket vesztik; mindezen változások kultúra- és közösségformáló hatásaira; az információs társadalomra mint egyre kevésbé utópisztikus jövőképre, amellyel hol kecsegtetnek, hol riogatnak, pozitívra vagy negatívra festve azt és még sok minden másra is. Én mégis inkább egy régi mondás elferdített változatát választottam könyvem mottójául, mely az elektronikus kommunikációra is könnyen adaptálható: „Aki ellenünk van, az velünk van."

Ebbe a kijelentésbe egyaránt beleérthető a politikai, katonai vagy ipari jellegű kémkedés; a konkurencia üzleti titkokat kutató erőfeszítései; az állam magánszférába hatoló, minden demokratikus alapelvet átlépő kíváncsisága; munkáltatónk privát kommunikációnkat is érintő kontrollja; vagy épp házastársunk érdeklődése az iránt, mit csinálunk, kivel és mit beszélünk akkor, amikor ő azt nem látja, nem hallja. Ugyanígy értelmezhető ügyfeleinkre, üzleti partnereinkre és még inkább saját munkatársainkra, akik információs rendszereinken keresztül készülnek visszaélésre. A passzív fürkészés mellett ide tartoznak az aktív visszaélések is, melyek során adatainkat, üzeneteinket meghamisítják, nevünkkel visszaélnek, vagy megtévesztenek minket.

Mindezen veszélyekkel, mint áthatolhatatlan acélrács és betonfal, szembeállítható a matematika színtiszta ereje, mely algoritmusokon, protokollokon, eljárásokon és alkalmazásokon keresztül materializálódik, és így alkotja azt a tudományt, melyet kriptográfiának nevezünk. Ennek a tudománynak a gyakorlati eredménye az elektronikus aláírás és társai, amiről könyvem szól. Hogy pajzsként vagy fegyverként értékeljük ezeket az eredményeket, csak nézőpont kérdése: attól függ, kinek a kezében látjuk, és mi melyik oldalon állunk. A történelem szigorúan ítélkező tekintetét elkerülendő azt tudom tanácsolni, hogy vegyük minél előbb saját kezünkbe ezeket az eszközöket, és tanuljuk meg élni velük. Annál is inkább, mert visszaélni velük legalább olyan könnyű, mint élni. Minden túlzás és pátosz nélkül hősnek minősíthető kollégáim immár negyed

évszázaddal ezelőtt elkezdett munkájukban azt tűzték maguk elé, hogy ezt a technológiát, ami addig csak szűk tudományos, katonai és államhatalmi csoportok ellenőrzése alatt létezett, széles körben megismertetik, és hozzáférhetővé teszik. E forradalmi tett, melyet a fölbirtokok és termelőeszközök elosztásának modern kori megfelelőjének tekinthetünk, mára egyfajta mozgalommá nőtte ki magát (inicializálva és csatlakozva a nyílt forráskódú fejlesztések eszméjéhez). Magam is e törekvéshez szeretnék csatlakozni könyvemmel, minél szélesebb körrel megismertetve az elektronikus aláírásnak és társainak elvi hátterét és gyakorlati felhasználását.

Éppen ezért igyekeztem – amennyire csak lehetséges volt – amolyan „tudományos ismeretterjesztő" hangvételűre hangolni írásom, érthetővé és – a szó némiképp talán sajátos értelmében – élvezhetővé is tenni azt. Egyszerre szánva a könyvet az elektronikus aláírás és kriptográfia iránt érdeklődő szakembereknek (olyan tervezőknek, fejlesztőknek és tanácsadóknak, akik biztonságos alkalmazásokat kívánnak alkotni) és felhasználóknak (akik ezen alkalmazásokat kívánják tudatosan felhasználni) meglehetősen sok kompromisszum megkötésére kényszerültem, melyek remélhetőleg nem lesznek elviselhetetlenek egyik olvasótábor képviselője számára sem. A szakemberek nem minősítik művem túlságosan könnyűnek vagy populárisnak, a felhasználók pedig bonyolultnak és szárazna k. Kifejezett célom volt, hogy ne csak elméleti kérdéseket fejtegessek, hanem gyakorlati problémákat vessek fel, és az ezekre adott gyakorlati válaszokat mutassam be. Nem elhallgatva a gyakorlat mögötti elméletet sem, de megkímélve mindenkit azoktól a matematikai szörnyűségektől, melyek ismerete nem szükséges az elektronikus aláírás működésének megértéséhez. E nélkül is lesz épp elég elborzasztó rész, melyek voltak azért annyira fontosak, hogy ne maradhassanak ki: szabványok, szabályzatok, jogi kérdések. Másoknak talán az algoritmusok vagy épp az informatikai fejezetek lesznek elrettentőbbek. Bár ezek együttesen alkotják az elektronikus aláírást, nem kell mindenkinek minden vonatkozását teljes mélységében megismernie ahhoz, hogy eredményesen és biztonságosan használhassa azt mindennapi munkájában és magánéletében. Az egyes fejezeteknél ezért jelölni fogom, hogy kinek érdemes megismerni azt, nehogy a kevésbé fontos részeken elfásulva hagyjanak ki lényeges tudnivalókat.* Annál is inkább, mert először magam is csak egy barátságos százötven oldalas könyvet akartam írni, majd ötvenoldalanként revidiáltam elképzelésem: elhatároztam, kétszáz oldal alatt tartom, később, ha törik, ha szakad, kétszázötven oldal alatt, majd megfogadtam a háromszázat. Látják, mi lett belőle. Gyengeségem folytán, mellyel újra meg újra meghajoltam a magukat perdöntőnek beállító tudnivalók előtt, alaposan felhizlaltam a könyvem. És még így sem önthet el az a jó érzés, hogy minden fontosat elmondtam a témáról. A kényszerűségből kimaradt ismereteket, remélem, később lesz alkalmam pótolni. Nem kimon-

* Ezek a jelölések csak iránymutató ajánlások, az átlagosnál érdeklődőbb olvasóim komolyabb mellékhatások veszélye nélkül figyelmen kívül hagyhatják őket.

dottan erre, mint inkább a témával kapcsolatban érkezett fontosabb észrevételek közzétételére, esetleges hibák javítására, kapcsolattartásra szánom a következő weboldalt: sansserif.hu/ealairas és e-mail-címet: info@sansserif.hu. Kérem minden olvasómat, hogy ha bántó hibával vagy fájdalmas hiányossággal találkozik, írjon e-mail-címemre, hogy az információt megoszthassam másokkal is.

Ezúton szeretnék köszönetet mondani családomnak, barátaimnak és barátnőimnek, akik elnéző türelmükkel lehetővé tették a könyv megírását; mindazoknak, akiktől sokat tanultam az elmúlt években, és így elmém pallérozásán keresztül szintén hozzájárultak a könyvhöz; *Sikolya Zsoltnak*, a MEH Informatikai Kormánybiztosság főosztályvezetőjének és *Szabó Istvánnak*, a Hunguard Kft. ügyvezetőjének, akik hozzájárultak az elektronikus aláírás fogalomtár felhasználásához; és speciális köszönettel tartozom azoknak, akik a kéziratot, illetve annak egyes fejezeteit átnézve észrevételeikkel sokat segítettek nekem.

Így *dr. Balázs Istvánnak*, a Hunguard Kft. munkatársának, az egyik legjobb magyarországi elektronikus aláírási szakértőnek; *Patócs Zoltánnak*, aki a PwC Consultingban munkatársam (s aki az egyetlen magyar hitelesítőegység-szoftver vezető tervezőjeként és fejlesztőjeként írta be magát a műszaki legendáriumba); *dr. Rátai Balázsnak*, aki Hírközlési Főfelügyelet Informatikai Szabályozási Osztályán dolgozva elévülhetetlen érdemeket szerzett az elektronikus aláírásról szóló törvény megalkotásában; *Rózsahegyi Zsoltnak*, a NetLock Kft. vezetőjének, aki nemcsak ért hozzá, de műveli is, *Gazsó Gábornak* a SmartCard Kft.-től, a kártyák nagy értőjének, valamint a Microsoft munkatársának, *Gaál Lászlónak*, aki ráadásul több olyan információt is biztosított számomra, amiket magamtól nem sikerült fellelnem.

A könyvben alkalmazott jelölések

A könyv a következő jelöléseket alkalmazza:

Kiemelt szövegrész jelöli az alkalmazásokra s azok menüpontjára, gombjára, fülére és egyéb testrészeire való utalásokat.

Az aláhúzás webcímekre utal.

Az igen sokszor alkalmazott jegyzeteket (minden fejezet végén megtalálhatóak) kis számok jelzik jobb felül,[1] amik nem tévesztendők össze a szintén szerephez jutó hatványkitevőkkel.

A könyv végén felsorolt szakirodalom adott elemére, mint forrásra, szögletes zárójelek közti számok utalnak: [1].

1 A szövegértést nehezítő zárójelek visszaszorítása volt velük a célom.

1 Bevezetés

Ajánlás:

Mindenkinek (a miheztartás végett).

Bevezetésképpen – korunk rohanó világában gyors kielégülést kereső olvasóim örömére – rögtön belevágnék a dolgoknak ha nem is a közepébe, de első harmadába a hagyományos és az elektronikus aláírás összehasonlításával, ami kapcsán az elektronikus aláírás célját, szerepét, felhasználását is tisztázni szándékozom. Az itt olvasottak a későbbiekben még részletesen tárgyalva és magyarázva lesznek, valamint az árnyalásukra és kiegészítésükre is sor kerül.

1.1 A hagyományos aláírás

1.1.1 Az aláírás célja

Talán nem felesleges felidézni azt az evidenciát, hogy az aláírás célja valaminek az igazolása, akár jóváhagyólag, akár tagadólag, például nyilatkozattétel, szerződés vagy kötelezettségvállalás céljából. Ez egyaránt igaz a hagyományos és az elektronikus aláírásra is. Az aláírást tipikusan egy irattal összefüggésben szokás megtenni, s ez esetben az igazolás az irat hitelesítését jelenti: leggyakrabban annak származását, szerzőségét, a tartalom saját véleményünkként való elismerését vagy csak az elolvasását. Az aláírással biztosítani kívánjuk az irat sértetlenségét is, vagyis azt, hogy az iratot az aláírás megtétele után ne lehessen megváltoztatni, illetve ha ilyen mégis történne, az észlelhető legyen[1]. Az aláírás mindezen túl gondoskodik arról is, hogy a megtett igazolást utólag ne tagadhassa le annak megtevője.

A hagyományos aláírás három célja ezek alapján:

- hitelesség: az irat származásának az igazolása,
- sértetlenség: az irat tartalmának biztosítása,
- letagadhatatlanság: az irat jogilag is bizonyító erejének garantálása.

Az aláírás természetesen az irat tartalmától függően ezer dolgot jelenthet, amiket nem célunk elemezni, ugyanúgy, mint a speciális aláírások (ügyvédi ellenjegyzés, közjegyzői hitelesítés, uralkodói kézjegy stb.) témakörében való elmélyedés sem tartozik szorosan a tárgyhoz. E helyett inkább vizsgáljuk meg azt, hogyan teljesíti a kitűzött célokat a hagyományos aláírás.

1.1.2 A hagyományos aláírás (és társai)

A hagyományos aláírás immár több száz évre visszamenőleg a név egyedi formában történő papírra vetését jelenti. Ez az egyedi forma a kézjegy (más szóval szignó)[2], amelyet mindenki maga alakít ki, először valamikor a tinédzserkora elején, körülbelül akkor, mikor az első személyi igazolványát vagy útlevelét kell ellátnia aláírásával. Később folyamatosan változik ez a kézjegy, illetve néha amolyan karbantartó jelleggel változtatás történik rajta az életkor, a divat és az elvárások függvényében. Egy embernek lehet több aláírása is, amiket különböző célokra alakít ki és vesz igénybe, például egy hivatalos forma, amit a hivatalos életben[3], és egy privát forma, amit a magánéletben használ. Az egyedi forma feladata mindegyik esetben a hitelesség biztosítása. Az aláírás megtétele a letagadhatatlanság érdekében eltávolíthatatlan és megváltoztathatatlan módon, azaz tollal és tintával szokott megtörténni, a sértetlenség garantálása végett az irat végére helyezve azt.

A hivatalos felhasználást – annak magasabb biztonsági igényei miatt – gyakran egészítik ki bélyegzőhasználattal is, ami szintén egy egyedi nyomatot jelent, az aláíráshoz hasonlóan eltávolíthatatlan és megváltoztathatatlan módon, az irat végén helyet szorítva számára. A bélyegző, akárcsak korábban használt változata, a pecsét, ugyanakkor az aláíráshoz képest egy plusztulajdonsággal is bír: birtokolni kell. A birtoklás ténye a tulajdonos számára nemcsak biztonságot jelent, de különböző ismérvekkel ruházhatja fel, például az aláírás megtételére való jogosultságot tanúsíthatja. A ma már történelminek nevezhető (viasz)pecsét ezen túl azt is képes volt igazolni, hogy a címzetten kívül más nem olvasta el a dokumentumot (amennyiben a borítékra helyezték).

A hagyományos aláírás megtételének eszközszükséglete a leírtak alapján kimerül egy golyóstollban, s a minimális írástudás képességén kívül további igényeket nem támaszt az aláíróval szemben. Az aláírás ellenőrzéséhez még ennyi se kell: mindössze az aláírás mintájának ismeretét igényli, aminek birtokában az aláírás eredetisége könnyen eldönthető. Vagy nem is olyan könnyen?

A hagyományos aláírás és említett társai, bár évszázadokig működtek, használatuk számtalan nehézséggel és kockázattal is járt. Ezek közül a legkevesebb, hogy a kézzel rajzolt aláírás legtöbbször nem olvasható, vagyis a tulajdonos személyét külön, olvashatóan is jelezni kell. Ennél problematikusabb, hogy a tulajdonossal való összerendelés ennek ellenére sem magától értetődő, hiszen az eredeti aláírásminta ismerete is szükséges ahhoz, hogy az aláírás hitelességéről az elfogadó egyértelműen megbizonyosodhasson. Ez személyes megjelenést igényel az elfogadó előtt minden egyes aláírás megtétele alkalmával vagy előzetesen, egy (banki szóhasználattal) aláíró karton kitöltése apropójából. Ezt minden egyes elfogadó előtt meg kell tenni, ellenkező esetben az aláírás eredetisége csak utólag tisztázható bírósági eljárás keretében, szakértői vélemény kikérésével. Ami nem csak nagyon macerás, de sokszor eső után köpönyeg.

Ezzel együtt is az aláírások legtöbbje meglehetősen könnyen hamisítható, annál is inkább, mert az aláírásminták nem titkosak, sőt kifejezetten könnyen hozzáférhetőek (egy másik aláírt dokumentumból, például a cégek aláírásra jogosult vezetőjének aláírása a nyilvános cégbeszámolóból), s mert nem léteznek általánosan követett biztonsági szabályok a kialakítására vonatkozóan.[4] A biztonságot növelni szándékozó bélyegző ugyanakkor (főleg az elfogadó fél számára) extra kockázatot is jelent, hiszen a bélyegző könnyen ellopható, sokszorosítható, másolható, visszaélni vele még az aláírásnál is könnyebb, vagyis a biztonság nagyon csalóka és csalárd is lehet. Az aláírás változó formája nemcsak az aláírás ellenőrzését, de annak megtételét is megnehezíti, ami mindannyiunk számára ismerős lehet, akinek huszonéves kori aláírását a tizennégy éves korában aláírt személyién szereplő szignóval próbálták összevetni.

Ráadásul a modern vegytan és technika megjelenése egyre inkább kikezdi a hagyományos aláírás bizonyító erejét: Onassis, a híres milliárdos, az első milliót állítólag – többek között – egy idővel nyomtalanul felszívódó vegytintának köszönheti, mely aláírását a gondosan szélbe zárt iratokról is eltüntette. A letagadhatatlanság azonban egyszerűbb módszerekkel is könnyen kikezdhető: ha valaki nem saját általánosan használt aláírását teszi az iratra, később akár eredményesen is tulajdoníthatja azt idegen kéz művének.

1.2. Az elektronikus aláírás

Mielőtt az elektronikus aláírás részletesebb taglalásába belemennénk, rögtön az elején leszögezem az esetleges kétségek csillapítása végett, hogy a hagyományos aláírás három céljának az elektronikus aláírás is eleget tesz. Az elektronikus aláírás egyaránt teljesíti a hitelesség, a sértetlenség és a letagadhatatlanság követelményét az elektronikus iratokkal kapcsolatban.

1.2.1 Veszélyek az elektronikus világban

A hagyományos aláírás kapcsán már említettem, mi ellen kíván védelmet nyújtani az aláírás. Az elektronikussá váló iratkezelés és még inkább az elektronikus kommunikáció kapcsán azonban a már korábban is létező veszélyek sokkal élesebben jelentkeznek, mint előtte. Nemcsak amiatt, mert manapság sokkal több információ áramlik elektronikusan, mint korábban bármikor papíron, hanem mert az adatok továbbításához használt kommunikációs csatorna mind a küldő és a fogadó fél számára észrevétlenül támadható (a küldönccel és postással szemben személytelenné vált információtovábbító rendszer pedig – megfelelő mechanizmusok nélkül – még úgysem észleli a támadást). A már évtizedekkel ezelőtt is létezett egyedi, lokális és zárt hálózatok esetében ez a probléma kevésbé élesen jelentkezett, mert a hálózati forgalom csak a belső felhasználók által volt támadható. A külső „ellenségektől" igen magas műszaki isme-

reteket és kémfilmekbe illő módszereket kívánt ugyanez a feladat. A hálózatok egyre kiterjedtebbé, nyitottá és szabványossá válásával, a WAN, extranet és internet alapú infokommunikációs módszerek elterjedésével ugyanez a támadás már a külső felhasználóktól se kíván James Bond szintű felszerelést és tudást. Sőt az interneten könnyen elérhető kész vagy félkész hackerprogramok amolyan instant „törjük meg könnyen és gyorsan" módszereket kínálnak az egyébként nem profi informatikus, „hobbihackerek" számára is.

De mik is ezek a veszélyek, amik ránk mint az elektronikus kommunikációban részt vevő felekre leselkednek:

FORGALOMELEMZÉS – Forgalomelemzés történik, ha a lehallgató az üzenetváltás tényéből, sűrűségéből, a feladó és címzett ismeretéből (de az üzenet tartalmát nem ismerve) illetéktelen információhoz jut.

SZÍNLELÉS – Színlelés történik, ha valaki (ez lehet mind a küldő, mind a fogadó) más személynek adva ki magát, megtéveszti a kommunikációban részt vevő partnerét.

ÜZENETFELTÖRÉS – Feltörés történik, ha egy harmadik, illetéktelen személy lehallgatja mások üzenetváltását.

ÜZENETMÓDOSÍTÁS – Üzenetmódosítás történik, ha az illetéktelen személy az elfogott üzenetet (akár a tartalom ismerete nélkül is) megváltoztatva juttatja el a címzetthez.

ÜZENETTAGADÁS – Üzenettagadás történik, amikor egy felhasználó az üzenete elküldése után letagadja, hogy az üzenetet elküldte vagy ő küldte el. Ugyanez igaz lehet a másik oldalról is: az üzenet fogadója letagadja, hogy az üzenetet megkapta vagy a küldőtől kapta. A tagadás vonatkozhat az üzenet tartalmára, a küldés, fogadás pontos időpontjára és egyéb attribútumokra is.

VISSZAJÁTSZÁS – Visszajátszás történik, amikor egy eredeti üzenetet valaki elfog s azt megismételve (de módosítás nélkül) újból a címzetthez juttatja.

ÜZENETLOPÁS – Üzenetlopás történik, amikor egy eredeti üzenetet valaki elfog s annak címzetthez jutását megakadályozza.

ÜZENETKÉSLELTETÉS – Üzenetkésleltetés történik, amikor egy eredeti üzenetet valaki elfog s annak címzetthez jutását késlelteti.

ELTÉRÍTÉS – Eltérítés akkor történik, amikor egy üzenetet valaki elfog s azt nem az eredeti címzetthez juttatja el.

Az egyes támadási módszereket megkülönböztetik aszerint, hogy az a kommunikáció tartalmát megváltoztatja-e. Passzív támadásnak nevezik azokat az eljárásokat, amelyek nem változtatják meg az üzenetet, aktívnak pedig azokat, amelyek valamilyen módon beavatkoznak az üzenetküldésbe. Amíg az előbbire példa a forgalomelemzés, üzenetfeltörés és üzenettagadás, addig az utóbbira az üzenetmódosítás. A színlelés, visszajátszás, üzenetlopás, üzenetkésleltetés és eltérítés nem feltétlenül jár az üzenet tartalmának megváltoztatásával, de az üzenetküldés menetébe (a protokollba) való aktív beavatkozást jelentenek.

1.2.2 Mi az elektronikus aláírás?

Az elektronikus aláírás a tágabb körű értelmezés szerint bármi, amivel nevünket egy elektronikus irat végére biggyesztjük. Ebbe belefér az is, ha egy szöveges dokumentum végére egyszerűen odagépeljük a nevünket vagy beszkennelt aláírásunkat odamásoljuk. Ezek bizonyító ereje természetesen nem sokkal több a nullánál.

Könyvem elektronikus aláírásnak a nyilvános kulcsú kriptográfián[5] alapuló elektronikus aláírást nevezi, ami egy matematikai algoritmussal előállított bitsorozat. Ez a bitsorozat nem értelmezhető másképp, kizárólag csak egy másik matematikai algoritmus segítségével. Az így előállított elektronikus aláírást digitális aláírásnak is szokták nevezni, amely értelemben a digitális aláírás az elektronikus aláírás részhalmaza. A jogi terminológia a hitelesség, a sértetlenség és a letagadhatatlanság követelményeinek biztonsággal megfelelő elektronikus aláírást „fokozott biztonságú elektronikus aláírás"-nak nevezi. Mind a digitális aláírásnak, mind a fokozott biztonságú elektronikus aláírásnak – mely fogalmak nem feltétlen fedik teljesen ugyanazt – elviekben több rendszer is megfelelhet, de jelenleg az egyetlen elterjedten használt szisztéma a nyilvános kulcsú elektronikus aláírás módszere. Ezért elektronikus aláírás alatt, hacsak azt külön nem jelölöm, illetve a szövegkörnyezetből nem következik, a nyilvános kulcsú elektronikus aláírást értem.

1.2.3 Az elektronikus aláírás eszközei

Míg a hagyományos aláíráshoz szükséges eszközök (papír, toll, pecsét) olcsók, kis helyigényűek, könnyen hozzáférhetőek, és nem kívánnak bonyolult háttérintézményeket, addig az elektronikus aláírás eszközszükséglete ezzel összehasonlítva meglehetősen drága és bonyolult, ráadásul igen összetett infrastruktúrát kíván. Ennek most csak a felhasználó oldalán minimálisan szükséges alap összetevőit mutatom be.

Az elektronikus aláírás megtételéhez a következők megléte szükséges:
- az aláírandó elektronikus irat,
- személyes aláírás-létrehozó adat (magánkulcs),
- aláíró eszköz és környezet (számítógép, mobiltelefon, intelligens kártya stb.).

Az elektronikus aláírás ellenőrzése csöppet sem egyszerűbb az aláírás megtételénél. Ehhez a következők szükségesek:
- az aláírással ellátott elektronikus irat,
- az aláíróhoz tartozó aláírás-ellenőrző adat (nyilvános kulcs),
- aláírás-ellenőrző környezet (számítógép, mobiltelefon stb.).

S hogy mindez megfelelő módon, egymást értve tudjon együttműködni, szükségesek még algoritmusok, protokollok, alkalmazások, szabványok és intézmények, amint azt a későbbiekben látni fogjuk.

1.2.4 Mi szükség az elektronikus aláírásra?

Bár az elektronikus aláírás sokkal modernebb, mint hagyományos társa, mégsem annak leváltása a célja. A két aláírási módszer a belátható jövőben valószínűleg egymás mellett fog élni, a hagyományőrző egyesületek tanfolyamtára pedig egy ideig még nem gyarapodik manuális aláírási kurzusokkal. Az elektronikus aláírás alapvetően az elektronikus iratok számára készült, a papír alapú iratok világát nem ostromolja. Az elektronikus aláírás arra a problémára ad megoldást, hogy az elektronikus iratok hitelességét, sértetlenségét és letagadhatatlanságát korábban elektronikus módon nem vagy csak nagyon költséges módszerekkel lehetett megoldani. Ezért azon elektronikus iratokat, amelyek ezt a biztonságot megkívánták, ki kellett nyomtatni, hagyományos aláírással ellátni, és ezek után a szokásos manuális módon feldolgozni. Ez a korlát nem csak a korábban beharangozott papír nélküli iroda létrejöttét akadályozta meg, de felesleges párhuzamosságokat teremtett a dokumentumkezelésben, lelassította az ügyvitelt, s végeredményében nyomdagépekké fokozta le az elektronikus irodai rendszereket. Az elektronikus aláírás lehetővé teszi, hogy az elektronikus úton készült iratok teljes életciklusukat elektronikus formában éljék le, a hagyományos iratoknál megszokott biztonsági garanciák megléte mellett. Ez különösen fontos egy olyan világban, ahol az internet térhódításával egyre jobban meghonosodik az elektronikus kommunikáció, gondoljunk akár elektronikus levelezésre vagy a web alapú adatközlésre. A hagyományos aláírás továbbélése így nem az elektronikus aláírás elterjedésének függvénye, hanem a papír alapú iratok fennmaradásáé.

1.2.5 Melyik a jobb aláírás?

Bár a két aláírási módszer valójában nem versenytárs, így ha ebből a szempontból nem is, de az egyezőségek és különbségek megvilágítása végett egy összehasonlítás mindenképp hasznos ismeretekkel gyarapíthatja a tudásunkat.

Az aláírás megtételi módszerek jellemzői:

	Hagyományos aláírás	Elektronikus aláírás
Cél	Hitelesség, sértetlenség, letagadhatatlanság	Hitelesség, sértetlenség, letagadhatatlanság
Eljárás	Szignó lerajzolása	Matematikai algoritmusok
Szükséges eszköz	Toll, tinta	Aláíró eszköz és környezet
Szükséges tudás	Aláírásminta ismerete	Aktivizáló adat (jelszó) ismerete
Szükséges birtok	–	Aláírás-létrehozó adat (magánkulcs)

Mint látható, a két módszer célja megegyezik, a megvalósítás azonban gyökeresen eltérő. Azt, hogy az elektronikus aláírás a hagyományos aláírásnál biztonságosabb tud lenni, elsősorban az aláírás-létrehozó adat és az azt védő aktivizáló adat garantálja: míg a hagyományos aláírás megtételéhez nem szükséges semmilyen birtok, és a szükséges tudás széles körben és könnyen hozzáférhető, az elektronikus aláírás megtételéhez szükséges aláírás-létrehozó és aktivizáló adat megfelelő védelem esetén csak az aláíró által hozzáférhető. A teljesség kedvéért említem meg, hogy az elektronikus aláíráshoz szükséges eszközök és eljárások, ha nem is olyan könnyen, mint a hagyományos aláíráshoz szükséges társaik, de azért különösebb nehézség nélkül beszerezhetők. A magánkulcs biztonsága éppen ezért lényegbevágó az elektronikus aláírás biztonsága szempontjából. Ha valaki rekonstruálja, vagy ami adott esetben egyszerűbb: ellopja, az aktivizáló adatot pedig megismeri, az elektronikus aláírást meg tudja tenni az eredeti tulajdonos nevében. Az oly sokszor és előszeretettel emlegetett algoritmusok és kulcshosszak valójában – közvetlenül – nem az aláírást erősítik vagy gyengítik, hanem a magánkulcsot oltalmazzák. Minél erősebb az algoritmus és hosszabb a kulcs, annál nehezebb a nyilvános kulcs és az aláírások birtokában a magánkulcs rekonstruálása. A magánkulcs persze hagyományos zsebmetsző és bunkósbot módszerekkel is megszerezhető, emiatt azt mindenkinek úgy kell óvnia, mint a szeme fényét. Az elektronikus aláírás előnyei között megemlíthető az is, hogy azt elég csak egyszer megtenni, utána az a kívánt példányban másolható az aláírt dokumentummal együtt.

Eddig nem hozakodtam elő vele, de több dolognak elévágva most mégis kénytelen vagyok: az elektronikus aláírás működéséhez szükség van egy megbízható harmadik félre is, aki a hitelesség biztosítása érdekében az aláírási címpéldány analógiájaként is felfoghatóan igazolja azt, hogy az aláírás ellenőrzéséhez szükséges nyilvános kulcs valóban az illetőé. Ugyanő a letagadhatatlanság érdekében igazolja azt is, hogy az aláírás-létrehozó adat az aláírás megtételekor érvényes (azaz kizárólag az aláíró birtokában) volt.[6] Az elektronikus aláírás a sértetlenség biztosítása kapcsán különösen fejlettebbnek mutatkozik tradicionális társánál. A hagyományos aláírás egy többoldalas iratnak is sokszor csak az utolsó oldalán kap helyet, így semmi sem garantálja, hogy egy oldal nem cserélődik utólag ki, vagy egy sor nem lesz hosszabb (ezek kivédésére némelykor minden oldalt szignóznak, és egyes esetekben, például közokiratoknál, az üresen hagyott sorokat és sorvégeket áthúzzák). Az elektronikus aláírás sértetlenséget garantáló algoritmusa ezzel szemben bármilyen kis mértékű változást is azonnal jelez az iraton, legyen az akár egy 0 karakter O-ra cserélése, vagy egy utólagos vesszőbeszúrás.

	Hagyományos aláírás	Elektronikus aláírás
Eljárás	Szignó eredetivel történő vizuális összehasonlítása Írás utólagos javításainak, törléseinek, kiegészítésének ellenőrzése.	Matematikai algoritmusok
Szükséges eszköz		Aláírás-ellenőrző környezet (például számítógép)
Szukseges ismeret	Eredeti aláírásminta	Aláírás-ellenőrző adat (nyilvános kulcs)
Egyéb követelmeny		Harmadik fél közreműködése

Aláírás-ellenőrzési módszerek jellemzői

1.2.6 Az elektronikus aláírás bökkenői

A szigorúan vett hazugság bűnébe esnénk ugyanakkor, ha elhallgatnánk az elektronikus aláírás hátulütőit. Bár az elektronikus aláírás egészen mobil is tud lenni, akár kis helyet is elfoglalva (például egy mobiltelefonban megvalósítva), még több korlátot is le kell győzni az igazi mobilitás érdekében. A már működőképes megvalósítások ellenére is az igazi integráltság és észrevétlen működés inkább a jövő zenéje, mint a jelené. Mivel a mobiltelefonos aláírás széles körben elterjedt felhasználásáról sehol a világban nem tudok beszámolni, könyvem ezért ezt és az egyéb biztató kezdeményezéseket is a jövőről való fantáziálás mezsgyéjére száműzi. Ma még a hagyományos személyi számítógépekben való felhasználás sem tekinthető megszokottnak, aminek az elsődleges okát abban látom, hogy a jelenlegi gépek még nem rendelkeznek beépített berendezésekkel (aláíró eszközökkel) az elektronikus aláírás biztonságos megtételéhez. Ez pedig annak következménye, hogy jelenleg több szabvány és kezdeményezés is verseng ezen a piacon, amelyek persze egymással nem kompatibilisek. Már többször hittem azt, hogy minden akadály elhárult az elektronikus aláírás felhasználása előtt: először amikor megjelentek a legalapvetőbb szabványok, aztán mikor megszületett a szükséges jogi szabályozás, majd amikor egyre szélesebb körben elterjedtek az aláírást kezelő alkalmazások. Most az aláíró eszközök meghonosodásától várom az áttörést. A közeljövőben várhatóan ez is bekövetkezik, s ekkor véleményem szerint már „csak" a felhasználók tájékozatlansága és bizalmatlansága lesz a kerékkötő. Ennek leküzdésére nemcsak a tájékoztatásnak kell szélesebb körűnek lennie – ami könyvem egyik fő célja –, hanem a teljes aláírási rendszernek is sokkal emberközelibbé kell válnia.

A jövő egyébként – hogy az oly édes álmodozás se maradjon el – véleményem szerint az elektronikus aláírás területén is a ma még hazánkban extrém di-

vathóbortnak számító személyi asszisztenseké (PDA). Azoké az eszközöké, amelyek egy miniatűr rajzasztalként a személyi számítógép és a mobiltelefon jó tulajdonságait egyesítik, s mindennel rendelkezni tudnak, ami az elektronikus aláírás biztonságos megtételéhez és ellenőrzéséhez szükséges.

1.2.7 Az elektronikus aláírás felhasználási területei

Az elektronikus aláírás felhasználásaként szinte kizárólag az elektronikus üzenetküldést, azon belül is a levelezést szokták említeni.[7] Ami abból a szempontból mindenképp jogos, hogy valóban ez a legnyilvánvalóbb és legelterjedtebb fogyasztási mód. Nem az egyetlen azonban, sőt olvasóim valószínűleg többször találkoztak már webszerver-tanúsítványokkal, mint hogy aláírt levelet kaptak vagy elektronikusan írtak volna alá saját kezűleg. Ez talán még az elektronikusan aláírt szoftverekre is igaz, azokra az általában internetről letölthető programokra, amik a program szerzőjét és sértetlenségét igazolják az elektronikus aláírással. Elektronikus aláírást használnak még a virtuális magánhálózatot vagy más biztonságos kommunikációs módszert megvalósító hálózati hardverek is, mint az útválasztók és a tűzfalak. Ezenkívül említésre érdemesek még a kommunikációhoz nem kötődő módszerek is, mint a biztonságos archiválás vagy adatbázis-kezelés, ahol az eltárolt információ hitelességét, sértetlenségét és letagadhatatlanságát egyaránt biztosítja az elektronikus aláírás. Szintén elektronikus aláíráson alapszanak a biztonságos személyazonosítási és beléptetési módszerek, ahol nemcsak a felhasználó kilétéről való, minden korábbinál megbízhatóbb eljárásként használják előszeretettel, de a központosított felhasználó és jogosultságkezelés egyik fontos alkotóelemeként is (például a single sign-on megoldások esetében). Ilyen megoldásoknál szerencsés esetben a felhasználónak a korábban kezelt számtalan jelszó helyett csak egyetlen jelszót (saját aláírás-létrehozó adatának aktivizáló adatát) kell megjegyeznie.

1.2.8 Amire az elektronikus aláírás sem jó

Bár az elektronikus aláírás, ahogy azt a „mellékelt ábra" is mutatja, igen sok dologra jó (majdnem mint egy svájci bicska), mégsem találtuk meg személyében a panaceát. Maradtak még az elektronikus világban veszélyek jócskán, ami ellen hiába próbálnánk meg az elektronikus aláírást mozgósítani.

Így például a korábban felsorolt veszélyek mindegyikére sem nyújt automatikusan megoldást az elektronikus aláírás. A színlelés és az üzenetmódosítás ellen képes védelmet nyújtani, az üzenettagadás összetett problémaköréből azonban csak az adott tartalmú üzenet előállításának letagadhatatlanságát biztosítja (az üzenet – adott személy részére történő – elküldését, megkapásának és elolvasásának tényét vagy mindezek időpontját automatikusan nem). Az üzenetfeltörés ellen a bizalmasságot garantáló titkosítás véd csak. A visszajátszás, az üzenetlopás, az eltérítés, az üzenetkésleltetés és a forgalomelemzés ellen pedig

1.3 Nyilvános kulcsú infrastruktúra

Mielőtt a sűrűjébe vágnánk, van még egy fogalom, amit meg kell magyarázzak. Ez a nyilvános kulcsú infrastruktúra, eredeti angol rövidítésben PKI (publikus kulcsú infrastruktúraként fordítva magyar betűszóként is megállja helyét), amely az elektronikus aláírás működéséhez szükséges háttérintézmények, eszközök, eljárások, szabványok és szabályzatok összefoglaló neve. A „nyilvános kulcsú" kifejezés a nyilvános kulcsú kriptográfiára, az eljárás matematikai alapjaira vonatkozik, az infrastruktúra pedig arra utal, hogy a felsorolt alkotóelemek együttesen nyújtanak egy olyan komplex háttérrendszert a felhasználók számára, amely alapvető, akárcsak az úthálózat a közlekedés számára vagy a kábelhálózat a telekommunikáció részére. A PKI – eredeti jelentésén túlmenően – az utóbbi időben amolyan márkanévvé vált, ami alatt szinte mindent értenek, ami elektronikus aláírással kapcsolatos, ezért amennyire csak lehet, mellőzöm használatát, hogy ne vegyem túlságosan igénybe az olvasó absztrakciós készségét.

A PKI felfogható úgy is, szembeállítva a kitüntetett szerepű harmadik fél (vagyis hitelesítésszolgáltató) nélkül működő elektronikus aláírási megoldásokkal, mint az elektronikus aláírás egyik módszere. Ez a könyv ebben az értelemben kizárólag a PKI alapú elektronikus aláírást tárgyalja, aminek az oka a harmadik félre alapozott megoldás magasabb biztonsági mutatója.[12] Nem véletlen ugyanakkor, hogy a könyv – minden ilyen irányú befolyásolási kísérlet ellenére – nem a „Nyilvános kulcsú infrastruktúra" címet kapta. Ennek oka nemcsak a fogalom szakmai belterjességében és ijesztő voltában keresendő, hanem abban, hogy a könyv fókusza valóban és kimondottan az elektronikus aláírás és annak alkalmazása – a nyilvános kulcsú infrastruktúra és kriptográfia pedig csak mint háttér jelenik meg e mögött.

JEGYZET

1 Bármilyen félelmetes is azonban ennek veszélye (hiszen nem mindegy, hogy 10 000 000 Ft vagy egy nullával nagyobb összeg szerepel egy szerződésen), a hagyományos aláírás erre a célra csak igen korlátozottan felel meg.

2 A kézjegy nem feltétlenül aláírás. Az aláírás csak egy (igen gyakori) szerepe a kézjegynek.

3 A szignó kifejezést szokták a láttamozásra szolgáló rövidített kézjegy értelmében is használni.

4 Szüleink kézjegyét sokszor előbb elsajátítjuk, mint sajátunkat, hisz a szükség gyakran úgy hozza, hogy iskolai ellenőrző füzetünk esetében az önellenőrzés módszere tűnik előnyösebbnek.

5 A kriptográfia a titkosírás tudománya. (Bizonyára olvasóim is sokat gondolkoztak már azon, mi az a kriptokommunista. Kis fantáziával már kitalálhatják: föld alatt bujkáló, titkos kommunista.) Lásd bővebben: Melléklet – I. Fogalomtár.

6 Egyes elektronikus aláírási és ellenőrzési rendszerek harmadik fél igénybevétele nélkül működnek, ezek azonban a biztonságnak csak egy alacsonyabb szintjét garantálják.

7 Az „üzenet" egyébként bármi lehet, ami egy többfelhasználós rendszerben kommunikációval jár, nem csak levél.

8 Az internetes e-mail-megoldások ezeket az elvárásokat nem képesek maradéktalanul teljesíteni.

9 Denial of Service, azaz a szerver rosszindulatú elárasztása adatforgalommal, ami a szolgáltatás lelassulásához, megtagadásához vezethet.

10 Mert a levél elküldés előtti aláírása megfelelő konfiguráció esetén feltétlen küldő általi jóváhagyást igényel (ezzel sok vírus megfékezhető lett volna korábban).

11 Technikailag az elektronikus aláírás a kriptográfiai kódolásra, más néven titkosítás műveletre, az aláírás-ellenőrzés pedig a kriptográfiai dekódolásra, azaz visszafejtés műveletre vezethető vissza, amely eljárásokat egyéb matematikai algoritmusok (például lenyomatkészítés, kulcsgenerálás, prímszámkiválasztás, feltöltés stb.) egészítik ki.

12 A harmadik fél nélküli módszerek legismertebb képviselője a PGP. Bár a PGP rendszernek, véleményem szerint, nincs perspektivikus jövője, minden, az elektronikus aláírás iránt érdeklődőnek ajánlom a vele való megismerkedést. Erre remek lehetőséget ad – a téma szinte végtelen idegen nyelvű szakirodalma mellett – *Ködmön József* Kriptográfia című könyve [4], valamint a PGP honlapja a www.pgpi.org címen.

csak egy összetett, az elektronikus aláírást és titkosítást egyaránt felhasználó, biztonságos üzenetközvetítő rendszer tud védelmet biztosítani, mint ahogy a teljes körű letagadhatatlanságot is csak ez képes megoldani[8].

És akkor még csak a legszűkebben vett kommunikáció területét érintettük. Az elektronikus aláírás és a kriptográfia önmagában nem nyújthat teljes körű védelmet az olyan veszélyek ellen, amilyeneket például a vírusok, trójai falovak, férgek és megannyi undorító cimborájuk jelentenek. A hálózaton keresztül történő betöréstől sem óv meg, így a weboldalak megszentségtelenítésétől és az adatlopástól sem, nem is szólva a DoS[9] támadásokról, és még hosszan lehetne folytatni a fenyegetések sorát. Ugyanakkor az elektronikusan aláírt programok – mivel azok előállítója ismert – sokkal megbízhatóbbak a vírustisztaság szempontjából is; az elektronikusan aláírt levelek sokkal kevésbé valószínű, hogy vírust tartalmaznak, mint aláírás nélküli társaik[10]; s az elektronikus aláírásra alapozott, azonosítást igénylő védelmi rendszereken sem olyan könnyű átjutni, mint az azt nem megkövetelő társaikon. Ezzel együtt is az elektronikus aláírás biztosan nem helyettesíti sem a tűzfalat, sem a vírusirtó szoftvereket; s mindez fordítva még igazabb: a legjobb vírusirtók és tűzfalak sem képesek az elektronikus aláírást kiváltani.

És legvégül egyetlen dolog, amitől mindezek együttesen sem védenek meg minket: a programhibák. Éppen ezért hasznos emlékeztetni arra, hogy az elektronikus aláírási rendszerek is lehetnek hibásak. Akár algoritmikusan is gyengék, vagyis matematikailag (kriptoanalízissel) feltörhetőek. Lehet szoftveres megvalósításuk is hibás, de ami még valószínűbb, hogy a körítés nem megfelelő: a felhasznált protokoll, a felhasználói interfész vagy más csingilingi tartalmaz egy olyan hibát, ami az erős matematikai magot is agyonvágja. Szóval nem árt a körültekintés és az óvatosság, még ha páncélruhát húzunk is magunkra!

1.2.9 Mi szükséges az elektronikus aláíráshoz?

Ha olvasóm lelkesedése nem ismerne határt s úgy érzi, hogy a felvázolt előnyök legyőznek minden nehézséget, azaz az elektronikus aláírással való testközeli megismerkedés tovább nem halasztható, akkor számára a továbbiakat tudom javasolni.

Ha megelégszik egy elektronikus aláírás elfogadásával (vagy elutasításával), akkor keressen fel egy biztonságos weboldalt (a legtöbb magyar bank honlapja ilyen). Ez esetben a webszerver hitelesítése elektronikus aláírással valósul meg, amit a böngésző a státussorban egy sárga lakat megjelenésével jelez is (lásd 2.4 fejezet).

Ha ennél többet akar, vagyis önkezűleg akar elektronikus aláírást megtenni, akkor először is győződjön meg róla, hogy az ehhez szükséges alapvető hardver- és szoftverkellékek rendelkezésére állnak (például **Windows 2000**, **Outlook 2000** és az ezeket futtató számítógép), majd keressen fel egy hitelesítésszolgáltatót, és igényeljen tőle aláírás-létrehozó és ellenőrző adatot, azaz ma-

gánkulcsot és tanúsítványt. Ezek után partnerei körében tegye ismertté tanúsítványát (például küldje el nekik e-mailben), s máris minden készen áll ahhoz, hogy az aláírást ne csak megtenni tudja, de az a gyakorlatban is működőképes legyen (feltéve, hogy partnerei is rendelkeznek a szükséges alkalmazásokkal – lásd 2.2 fejezet). Bár korábban az elektronikus aláírás sokszínű felhasználási lehetőségét hangoztattam, a hétköznapi felhasználás apropói elsősorban valamilyen hálózati kommunikációhoz kötődnek, azon belül is elsősorban az internethez. Hálózati kapcsolat nélkül az egyéni célú felhasználás meglehetősen korlátozott, ezért ezt csak azoknak ajánlom, akik minden szempontból végiggondolták, és megbizonyosodtak az elektronikus aláírás alkalmazásának körülményeiről. Nem csak nekik, de mindenkinek, aki elektronikus aláírásban sántikál, javaslom, hogy olvassa tovább a könyvet, mert igen hasznos tudnivalókkal lehet gazdagabb, olyanokkal, amelyekkel jobb minél előbb tisztába jönni. Ne felejtsék, hogy az elektronikus aláírás megtétele jogilag kötelező erejű kötelezettségvállalásnak minősülhet, s az elektronikus aláírás elfogadása szintén számon kérhető következményekkel járhat. Bár az elektronikus aláírás valóban biztonságosabb tud lenni, mint hagyományos társa, ehhez alapvető feltétel, hogy az azt megtevő és elfogadó felek tudatosan, a szabályoknak megfelelően és a veszélyek ismeretében cselekedjenek. E nélkül nagyobb veszélynek teszik ki magukat, mint eddig papírral és tollal a kezükben bármikor is tették.

1.2.10 A társak

Mivel a könyv a keresztségben a kissé rejtélyes „Elektronikus aláírás és társai" címet kapta, joggal vetődik fel a kérdés – az elektronikus aláírás jelentésének tisztázása után –, hogy melyek is ezek a társak. Nos, mikor a címet kitaláltam, elsősorban a titkosításra gondoltam, amely az elektronikus aláírásnak amolyan édestestvére, legalábbis közvetlen hozzátartozója, hiszen ugyanarról a tőről, a kriptográfiáról, vagyis a rejtjelezés tudományáról sarjadtak[11]. Emiatt az elektronikus aláírás és titkosítás eszközszükséglete jócskán hasonló, s így a két eljárás legtöbbször egymást kiegészítve, együtt szokott működni (még ha ez nem is szükségszerű). A titkosítást mindemellett igyekszem, ahol csak lehet, az elektronikus aláírástól elkülönítve, legalábbis megkülönböztetve kezelni, hiszen a két eljárás alapvetően más célokat szolgál.

Ezen túl ide, a társak közé érthetőek az elektronikus aláírással kapcsolatban kiemelt figyelmet kapó eszközök, mint az intelligens kártyák s az elektronikus aláírás működéséhez elengedhetetlen alapfeltételek, mint a tanúsítványok és hitelesítésszolgáltatók, valamint az elektronikus aláírásból származó egyéb műveletek és szolgáltatások, mint például az időbélyegzés; vagyis minden, ami nem a szó legszűkebb értelmében vett elektronikus aláírás.

2 Elektronikus aláírás (és társai) a gyakorlatban

Ajánlás:

Minden aláírónak
és aláírás-ellenőrzőnek.

A szakkönyvek többsége, mielőtt rátérne a gyakorlati ismeretek és eljárások tárgyalására, végtelen szívóssággal igyekszik az olvasók fejébe tömni a téma elméleti tudnivalóit. Ez sok esetben azzal az eredménnyel jár, hogy a szekvenciálisan haladó olvasó azelőtt megcsömörlik az ismeretektől, mielőtt az élmény beteljesedhetne. A könyv pedig – hacsak nem kötelező tananyagról van szó – visszakerül a szekrény polcára, még mielőtt átadhatná a gyakorlatban is hasznosítható tudást. Ezt megelőzendő én megfordítottam a konvencionális sorrendet: előbb a gyakorlati tudnivalókat mutatom be, csak ezt követően értekezem az elméletről. A tradíciókhoz ragaszkodó olvasóim mindazonáltal nyugodtan fordítsák a visszájáról a rendszert a színére, és ezt a fejezetet átugorva vegyék azt a könyv végére (a 10. fejezet elé).

Az elektronikus aláírás gyakorlati felhasználási lehetőségei, ha nem is végtelenek, de – amint azt már említettem – igen széles körűek. Ezek mindegyikének gyakorlati bemutatására nem vállalkozom, de a legfontosabbakat koncepciózus módon feltétlen kiragadom. A bemutatás eszközeiül olyan alkalmazásokat választottam, amelyek széles körben elterjedtek, és éppen ezért olvasóim is nagy valószínűséggel rendelkeznek velük (vagyis leginkább Microsoft-termékeket). Ha az olvasó mégis egy másik programot használ, annak funkciói nagy valószínűséggel igencsak hasonlítani fognak a bemutatotthoz. Mindazonáltal az alkalmazás dokumentációjának tüzetes áttanulmányozása mindkét esetben ajánlatos, mert jelen esetben csak saját tapasztalataim megosztását irányoztam elő, nem pedig kézikönyvet kívánok a felhasználók kezébe adni. A mai alkalmazások többsége korántsem nevezhető példamutatónak, én legalábbis gyengeségekkel megvertnek tartom őket. De mivel ezek vannak, ezzel kell főznünk, s a legtöbb, amit tehetünk, hogy a meglévő fogyatékosságokról használat előtt megbizonyosodunk.

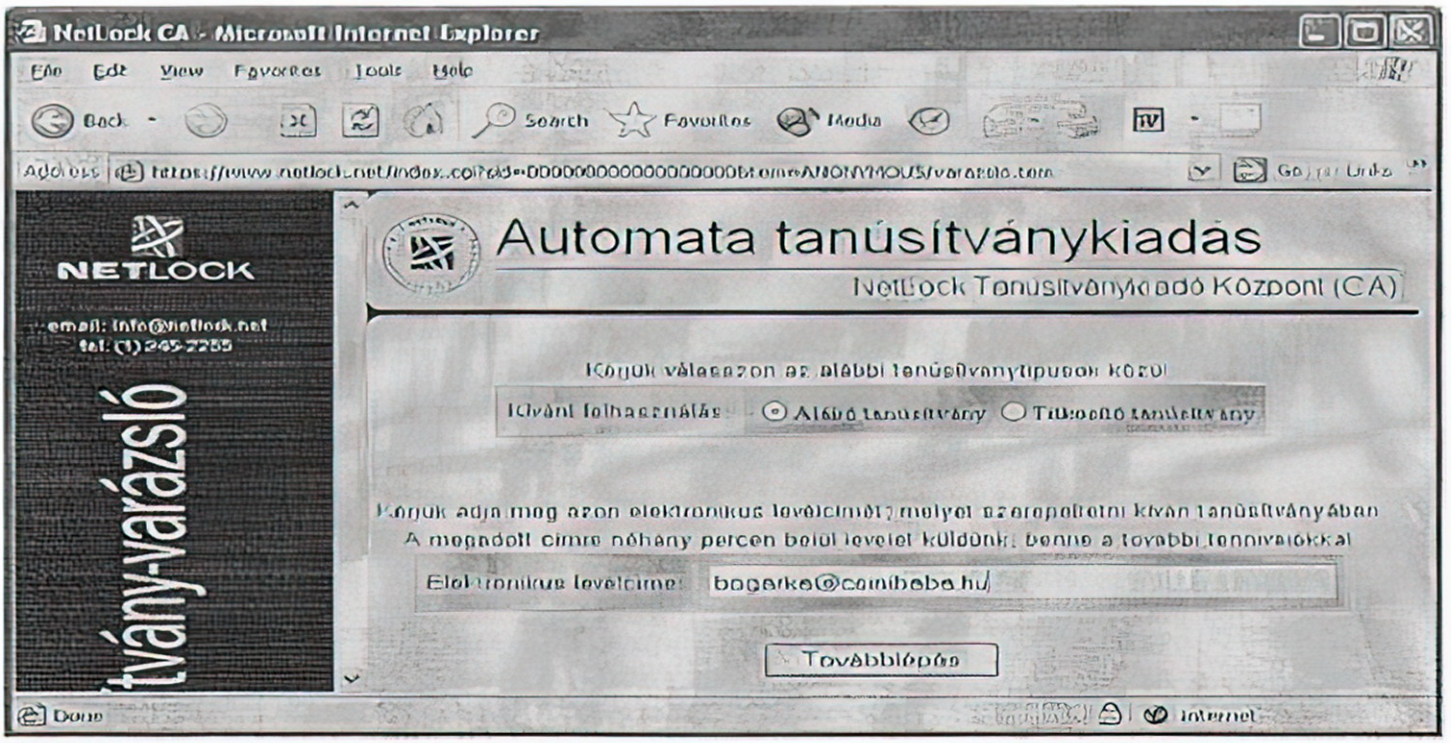
Példaként felhasznált képernyőim némileg szedett-vedettnek tűnhetnek. Ahol csak lehetett, saját angol nyelvű **Windows XP Professional** – magyar nyelvű **Office XP** környezetemből vettem a példákat, mely már önmagában is érdekes bilingvis miliőt teremtett. Néhol azonban még arra is rákényszerültem, hogy (egyaránt angol nyelvű) **Windows NT** és **Windows 2000**-es példákkal is éljek. Az egyes menü- és képernyő-hivatkozásokat is ennek megfelelően használtam: hol angol, hol magyar nyelvű elnevezésekkel élve. Remélem, olvasóim kombinációs készsége és nyelvtudása elégséges lesz ahhoz, hogy egy eltérő összeállítású környezetekben is elboldoguljanak. A legfontosabb műveleteket

az XP mellett 2000-es és NT-s környezetben is ellenőriztem, és ahol lényeges eltérést tapasztaltam, igyekeztem utalni a különbségekre.

2.1 Tanúsítvány igénylése – NetLock

Ha elektronikusan szeretnénk aláírni vagy üzeneteket titkosítani, akkor első lépésként egy tanúsítványt kell beszereznünk magunknak. Ennek legegyszerűbb módja, ha felkeressük valamelyik hitelesítésszolgáltató weboldalát, és ott igénylünk magunknak egyet. Számos hitelesítésszolgáltató üzemeltet olyan szolgáltatást, melynek keretein belül teszt vagy demonstrációs osztályú tanúsítványt ingyenesen biztosít az arra igényt tartóknak. Ilyennel találkozhatunk például a Verisign oldalain[1], vagy a magyar szolgáltatók esetében a NetLocknál. Ez utóbbi nemcsak hogy magyar nyelvű felhasználói felülettel rendelkezik, de példaértékűen egyszerű is a kezelése. Pár perc alatt szert tehetünk egy aláíró és egy titkosítótanúsítványra. Lássuk lépésenként:

1. Keressük fel a http://www.netlock.net/ oldalt, és ott válasszuk a **Tanúsítvány-varázslót.**
2. Irány az **Automata rendszer.**
3. Válasszuk ki az **Aláíró tanúsítvány** felhasználást, és írjuk be e-mail-címünket. A **Továbblépés** gomb hatására kapunk egy levelet a megadott e-mail-címre.[2]

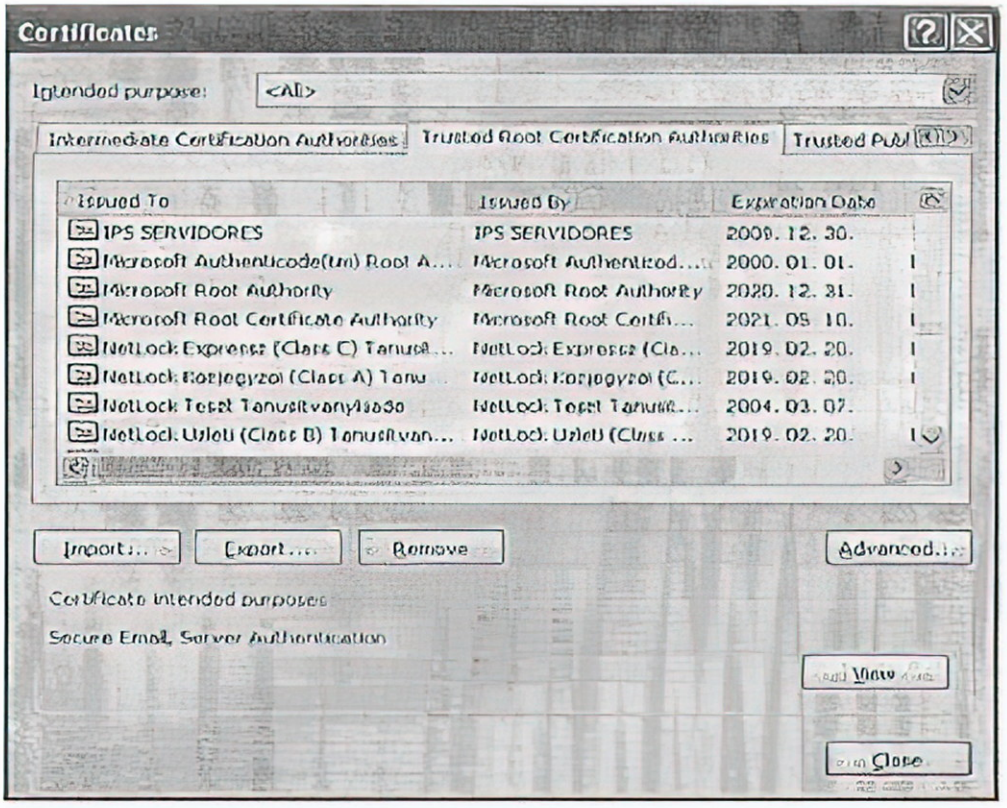


1. ábra Tanúsítványigénylő weboldal

4. Menjünk az e-mailben feltüntetett webcímre, és töltsük le (ne elmentsük, hanem nyissuk meg) a szolgáltató „Teszt tanúsítványkiadójának" saját tanúsítványát.

2. ábra
A tanúsítványkiadó saját tanúsítványa

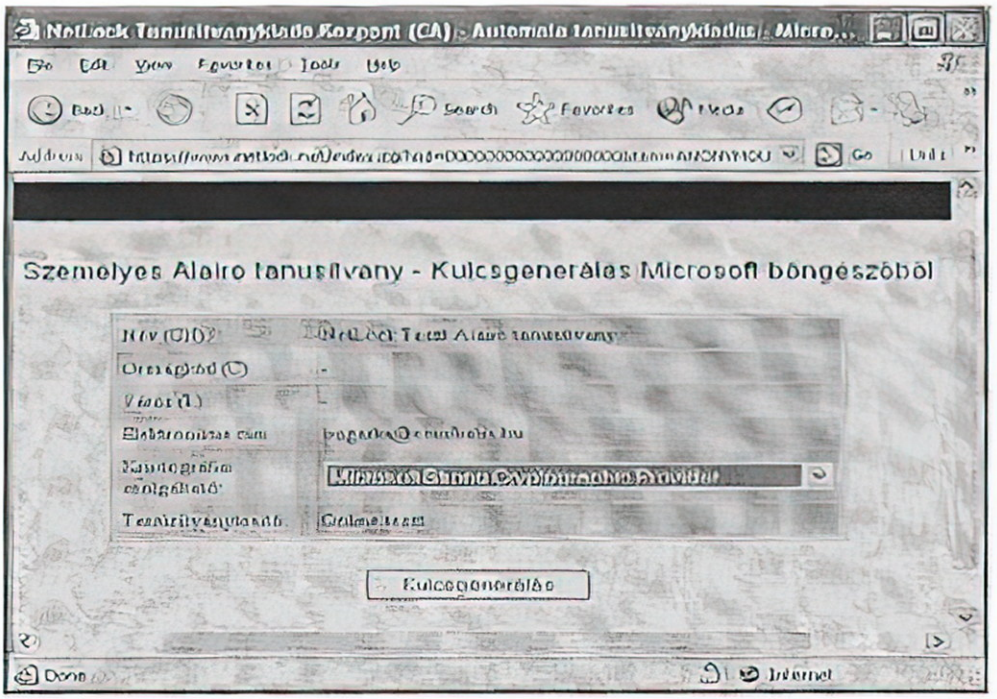
Az **Install Certificate** gomb hatására az importálási varázsló indul el. Az alapértelmezett javaslatok elfogadása után a tanúsítvány a **Trusted Root Certification Authorities** listában fog megjelenni, a többi, a **Windows**-ban már egyébként is szereplő NetLock szolgáltatói tanúsítvány mellett.[3]



3. ábra
Kiadói tanúsítványok listája

5. Keressük fel a levélben feltüntetett weboldalt, és kiválasztva a **kriptográfiai szolgáltató**[4] rendszert, generáljunk magunknak kulcspárt, amiből a szolgáltató tanúsítványt készít számunkra (az ablakban a tanúsítvány leendő adatai látszódnak – 4. ábra).

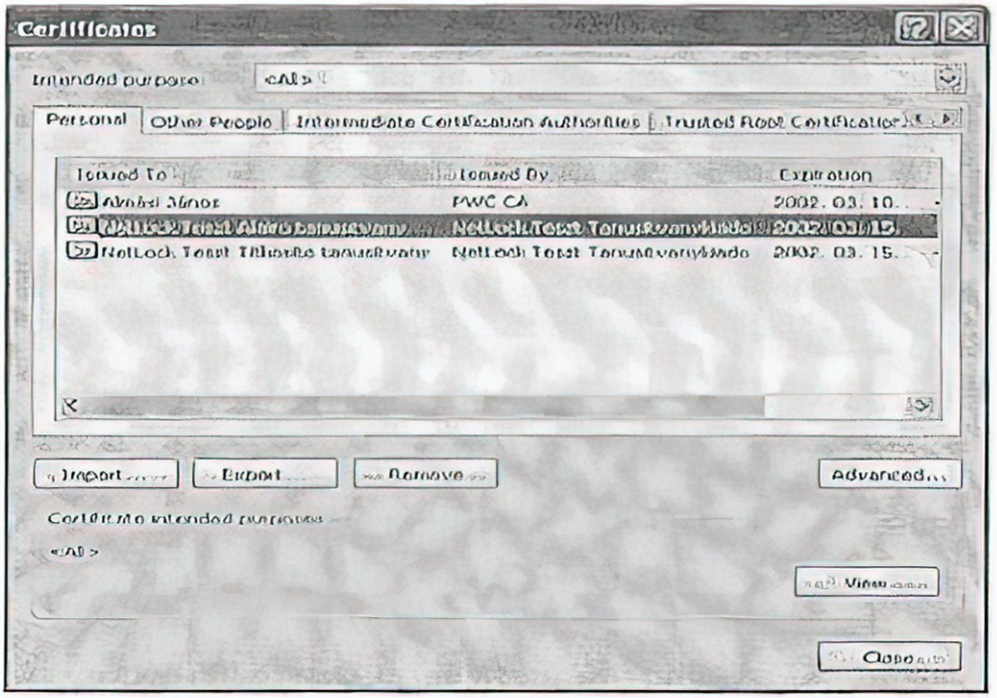
6. Mielőtt elkészülne a kulcs, át lehet állítani a magánkulcs tárolási-védelmi mechanizmusát. Ez azt határozza meg, hogy a magánkulcs felhasználása előtt meg kell-e majd adni a hozzá tartozó jelszót vagy sem – 5. ábra (**Set Security Level**).[5]



4. ábra
Kulcsgenerálás konfigurálása

5. ábra
Kulcsgenerálás

7. A tanúsítvány és a magánkulcs ezek után automatikusan elkészül, és bekerülnek a megfelelő tárolókba. Ez a **Tools – Internet Options – Content – Certificates** menüpontokon keresztül ellenőrizhető.



6. ábra
Tanúsítványok listája

A tanúsítvány tulajdonosaként nem az a személy van megjelölve, aki használja azt (hiszen erre vonatkozóan nem is kért adatot a NetLock), hanem a használat teszt jellegére történik utalás.

8. A 3. lépésre visszatérve válasszuk ki a titkosítótanúsítványt, és ismételjük meg a műveletsort a 4. lépés kihagyásával.

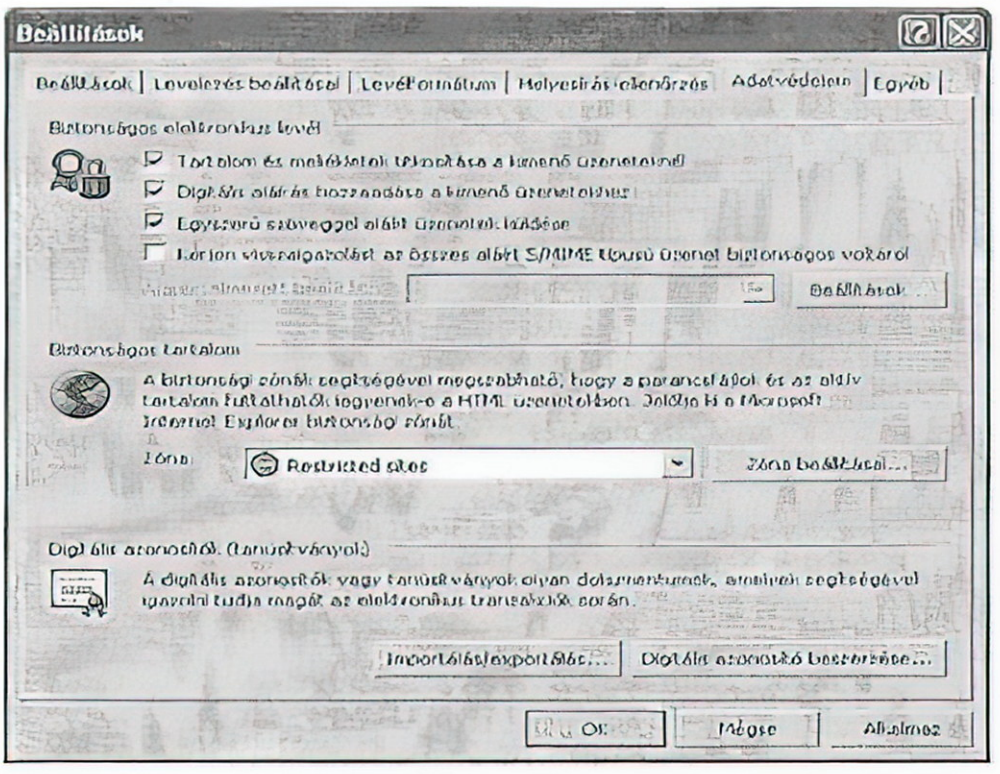
A kommunikáció biztonságos SSL protokollon keresztül valósul meg, de ettől függetlenül sem kell attól tartanunk, hogy a letöltött tanúsítványokba valaki belenyúlhatna. Magánkulcsunk pedig saját gépünkön generálódik, és azt nem is hagyja el.

2.2 Elektronikus levelezés – Outlook 2002

Az **Outlook** 2002-ben[6] továbbfejlesztették a 2000-es és Express változatokban már korábban implementált elektronikus aláírási és titkosítási funkciókat (mielőtt azonban bemutatom ezeket, tisztázzuk, hogy az elektronikus aláírás nem keverendő össze az aláírásnak nevezett művelettel, ami a levelek végéhez automatikusan csatolt szöveges információt jelenti[7]). Az **Outlook** 2002 az S/MIME v3 szabványnak megfelelően kezeli az aláírási és aláírás-ellenőrzési műveleteket.

2.2.1 Beállítások

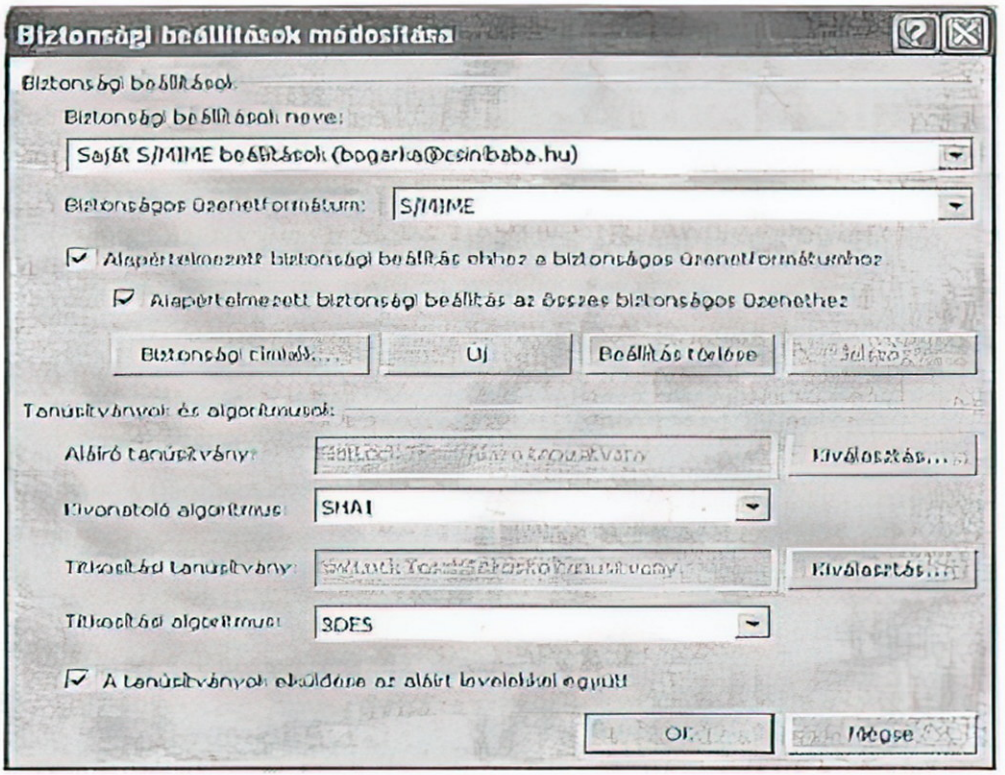
Ha gyakran akarunk aláírt és titkosított leveleket küldeni, érdemes a levelezésre általánosságban vonatkozó beállításoknál az erre vonatkozó konfigurációt elvégezni. Az **Outlook** főmenüjében, az **Eszközök – Beállítások** menüpont alatt, a **Beállítások** képernyő **Adatvédelem** fülénél találhatók az erre vonatkozó beállítási lehetőségek.



7. ábra
Levelek aláírásának és titkosításának beállítása

A biztonságos elektronikus levelezésre vonatkozóan meghatározhatjuk, hogy kimenő leveleink titkosítva legyenek, elektronikus aláírással legyenek ellátva, hogy az S/MIME kódolást nem támogató elektronikus levelezőprogramok is elolvashassák az üzenetet (az aláírás ellenőrzése nélkül), és hogy visszaigazolást kapjunk elküldött üzenetünk aláírás-ellenőrzéséről (ami egyben a levél elolvasására is utal).

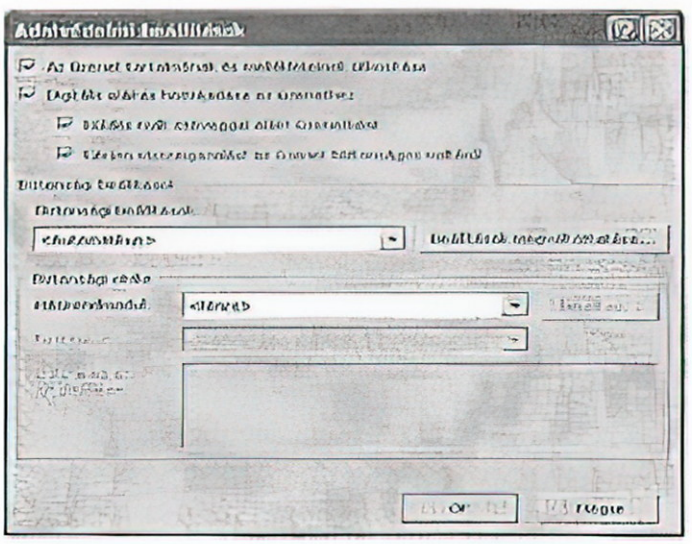
A **Beállítások** gomb mögött az aláíró és titkosítótanúsítványunkat installálhatjuk fel, de erre nincs szükség az előzőekben leírt tanúsítványigénylést követően, mert az **Outlook** automatikusan átveszi az e-mail-címnek megfelelő tanúsítványt az operációs rendszertől. Ha tanúsítványunkat egy másik rendszeren állítottuk elő, akkor ezt az installálást a **Kiválasztás** gombok segítségével kell elvégezni.



8. ábra
Aláíró és titkosítótanúsítvány és algoritmusok beállítása

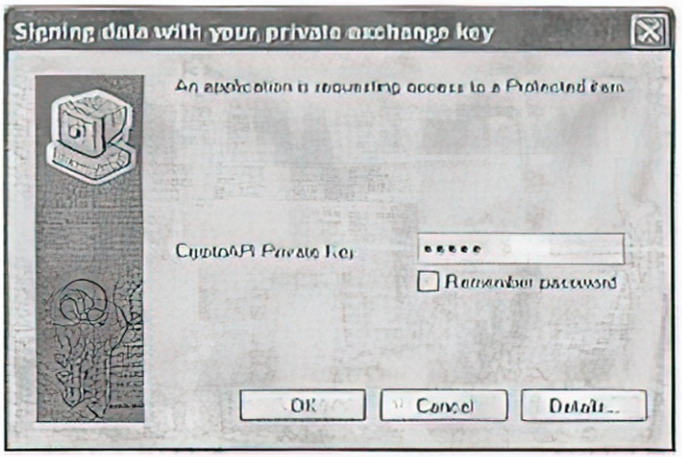
2.2.2 *Levél aláírása, titkosítása*

Ugyanezen üzenetküldési opciókat az egyes üzenetekre vonatkozóan egyedileg is beállíthatjuk, illetve a korábbi beállításainkat egyedileg is módosíthatjuk a levél elküldését megelőzően az **Üzenet beállítások** képernyő – **Biztonsági beállítások** gombjára kattintva (üzenet képernyő beállítások ikonjával érhető el).



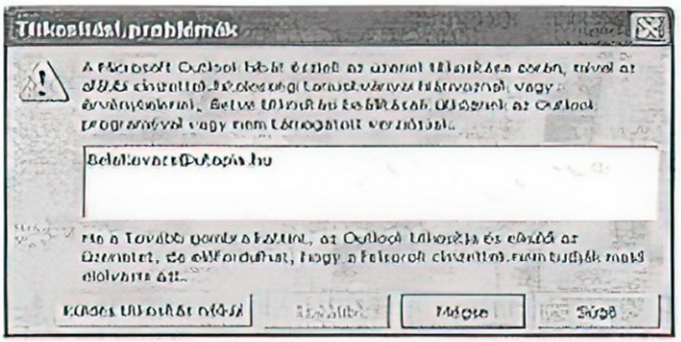
A 9. ábrán látható opciók beállítása után már semmit nem kell tennünk, csak a magánkulcsunkhoz való hozzáférést engedélyezni az aláírás céljára, a biztonsági szinttől függően a jelszó megadásával vagy csak az **Enter** billentyűvel (a **Remember Password** az az opció, amit soha ne állítsunk be).

9. ábra
Üzenet aláírásának és titkosításának beállítása



10. ábra
Magánkulcs elérésének engedélyezése

Az üzenetet titkosítani csak akkor lehet, ha partnerünk titkosítótanúsítványa rendelkezésünkre áll. Ha ezzel nem rendelkezünk, a következő figyelmeztető üzenetet kapjuk:

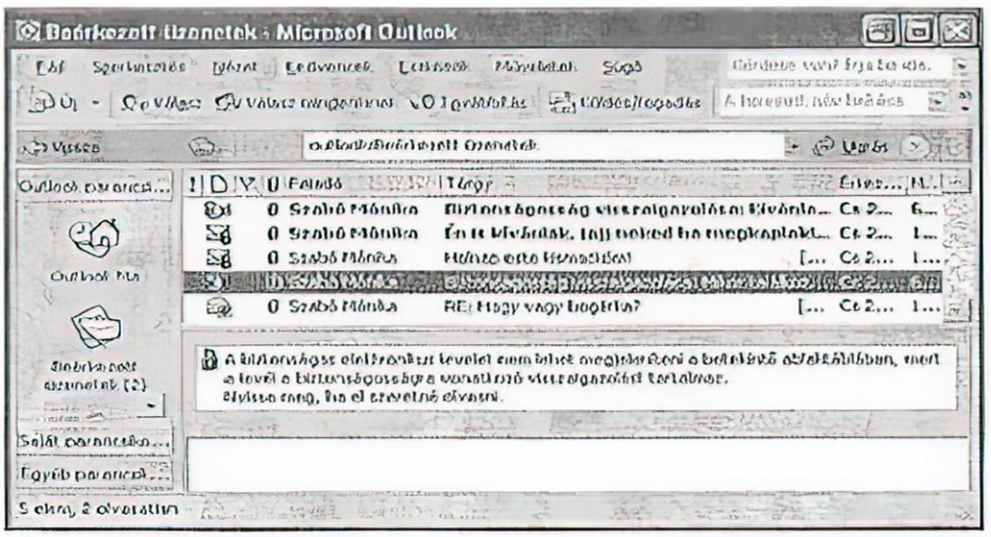


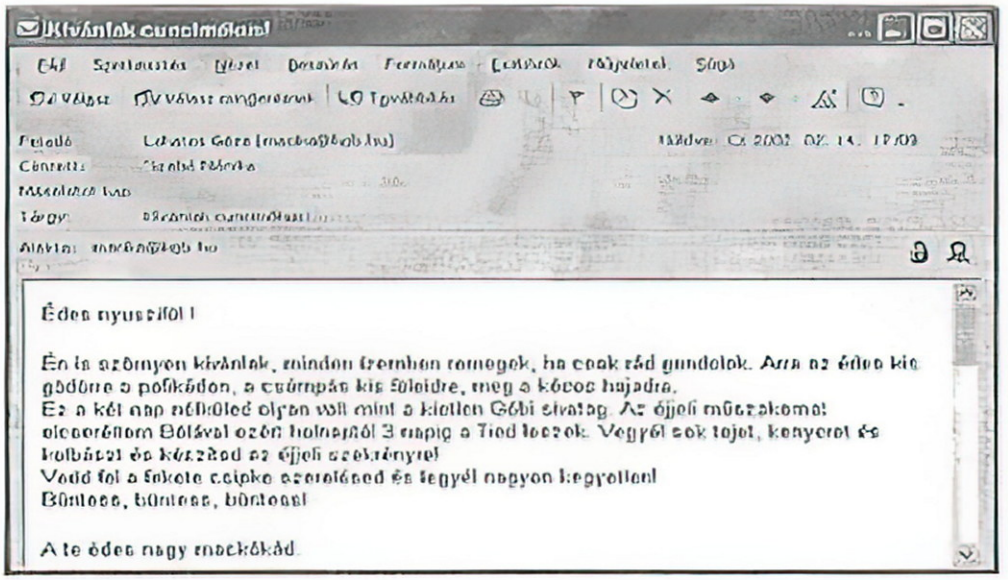
11. ábra
Figyelmeztetés a titkosító kulcs hiányára

Ha levelezőpartnerünknek van titkosítótanúsítványa, akkor csak arra kell megkérnünk, hogy küldje el azt számunkra (ez az **Outlook**-ban automatizálható is a **Biztonsági beállítások** képernyőn). Ezek után a titkosítás automatikusan tud működni.

2.2.3 Aláírt levél ellenőrzése, dekódolása

A beérkezett üzenetek mappában az aláírt és titkosított üzenetek, valamint a visszaigazoló értesítések eltérő szimbólumokkal jelennek meg. A titkosított üzenetek tartalma az ablak alsó felében nem jelenik meg. Ezek megtekintéséhez meg kell adni az engedélyt a visszafejtést végző magánkulcsunkhoz való hozzáférésre (szimplán aláírt levelekkel ilyen macera nincsen).


Beérkezett üzenetek - Microsoft Outlook
Fájl Szerkesztés Nézet Kedvencek Eszközök Műveletek Súgó
Címzettek vagy írja be ide...
Új
Visszaállítás
Címzettek
Címzettek...
Címzettek...
Címzettek...



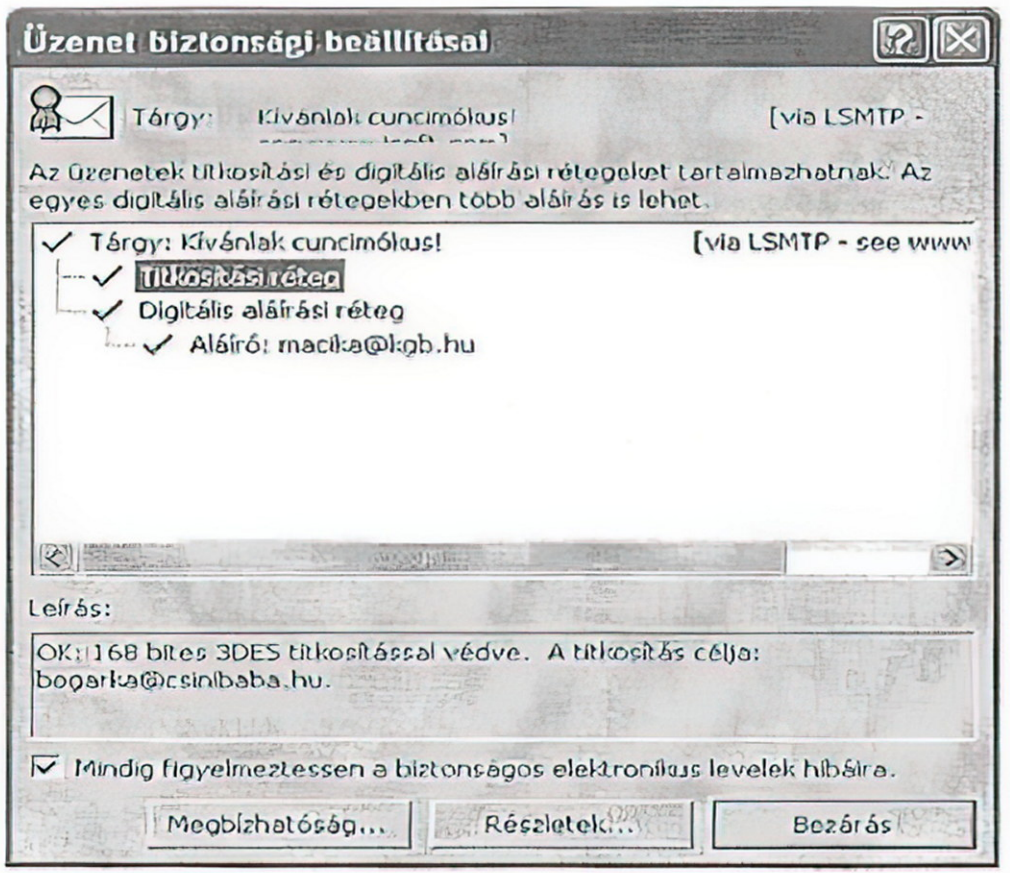
13. ábra
Aláírt és titkosított üzenet megtekintése

A szimbólumok valamelyikére kattintva (vagy **Fájl – Adatlap – Adatvédelem**) megjelennek az üzenet titkosítására és aláírására vonatkozó adatok.

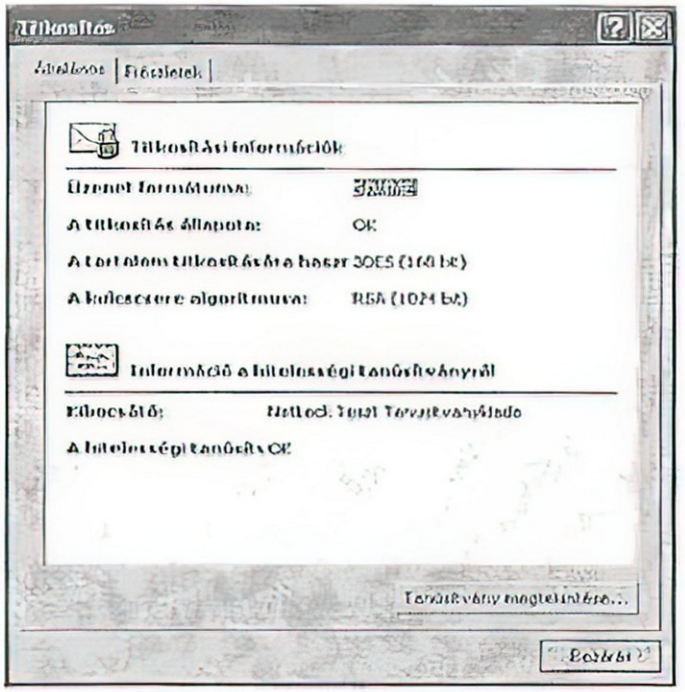
A külön rétegben jelölt titkosítás és aláírás legfontosabb adatai (az adott rétegen állva) a **Leírás** mezőben látszódnak, illetve a **Részletek** gombbal külön ablakban is megjelennek. (14. ábra)

Ekkor láthatóvá válik az üzenet formátuma (S/MIME, Exchange, X.400 stb.), titkosítás esetében a rejtjelező és kulcscsere-algoritmus fajtája és erőssége, aláírás esetében az aláíró e-mail-címe, az aláírás ellenőrzésének eredménye, az aláírás ideje és algoritmusai. Mindkét esetben megjelenik a tanúsítvány kiadója és a tanúsítvány ellenőrzésének eredménye. (15. ábra)

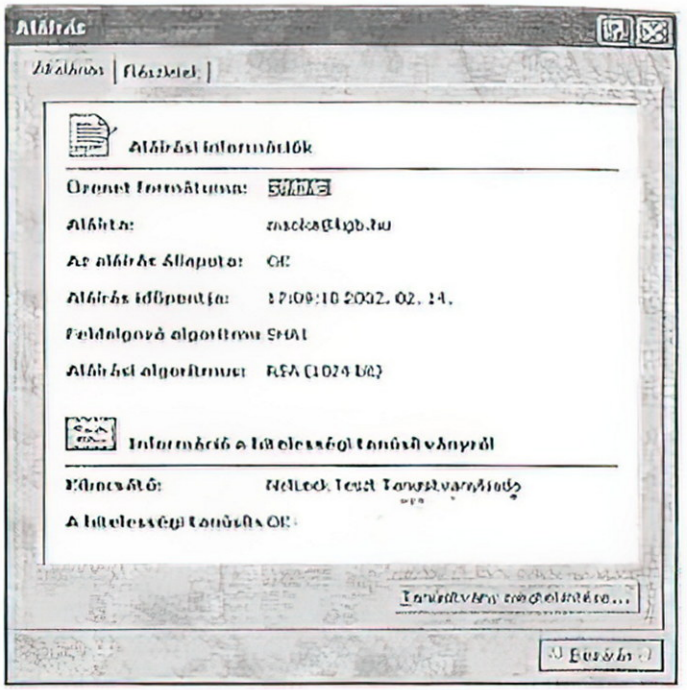
Meg lehet tekinteni a tanúsítványok tartalmát is, valamint a tanúsítványra vonatkozó megbízhatósági beállításokat.



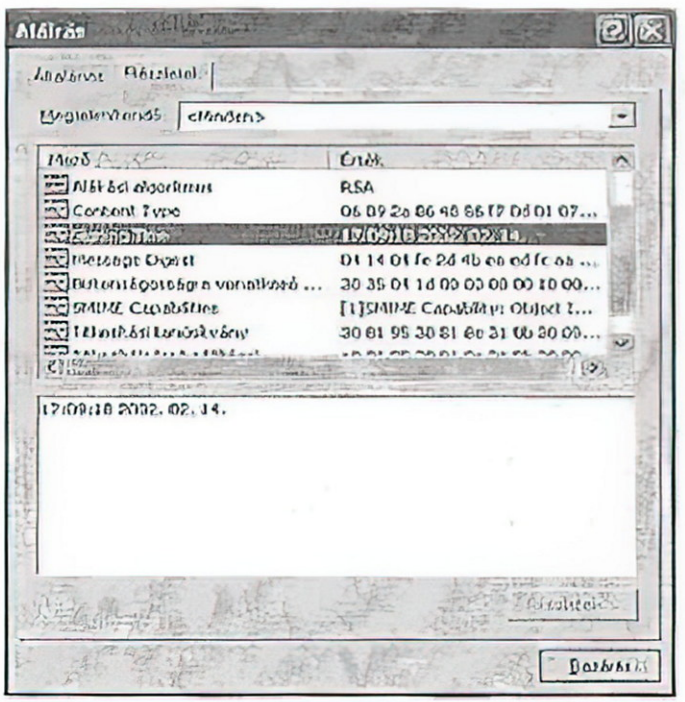
14. ábra
Levél aláírására és titkosítására vonatkozó információk



15. ábra
Levél titkosítására vonatkozó információk



16. ábra
Levél aláírására vonatkozó információk



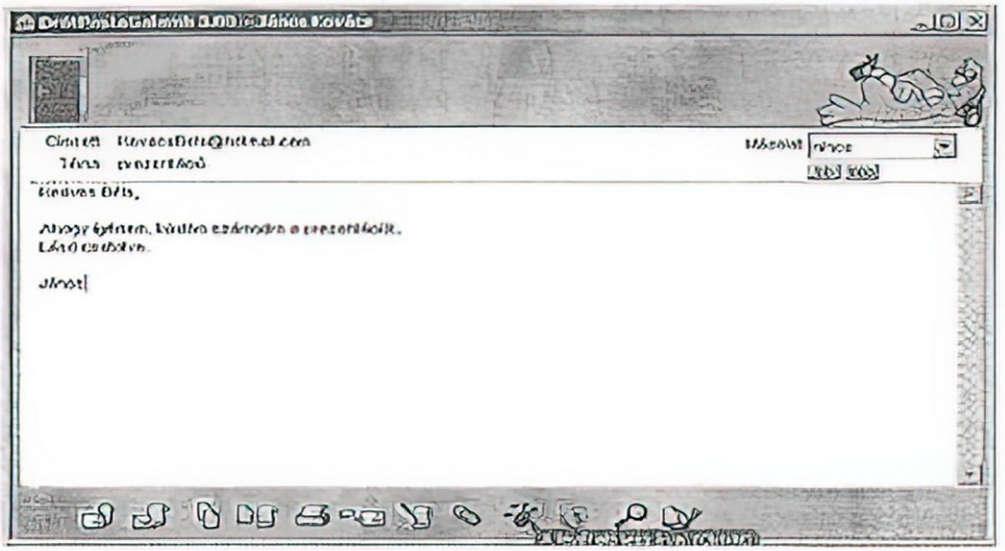
17. ábra
Levél aláírására vonatkozó részletes információk

2.3 Elektronikus levelezés – Drótposta

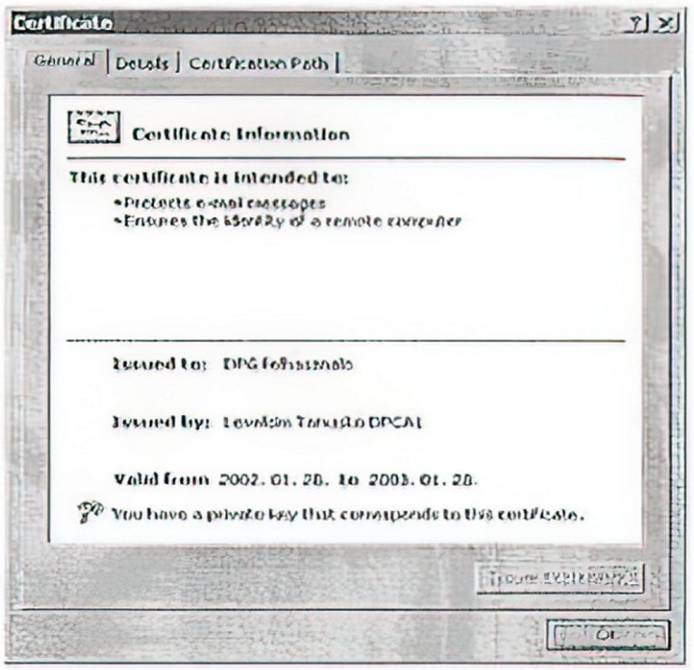
Az **Outlook**-hoz hasonló funkciókat biztosít a DrótPostaGalamb (DPG) levelezőprogram is[8]. Ez egy saját kliensprogrammal rendelkező, szabványos formátumokkal dolgozó levelezőalkalmazás, amely bármely, hasonlóan szabványos internetes levelezőklienssel képes kommunikációra. A kimerítő regisztráció után

a szoftver, az alkalmazás használata (kivéve a telefondíjat) s a tanúsítvány is teljesen ingyenes.

A program a postaláda legyártása után előállítja a felhasználó kulcsait, majd a központilag hitelesített tanúsítványt elküldi a felhasználó részére. Ennek folyamata – csakúgy, mint a levelezés során az elektronikus aláírás és titkosítás használata – teljesen evidens a felhasználó számára (az alábbi képernyőn a **tappancs** és **lakat** szimbólumokkal kapcsolható ki-be).



18. ábra
DPG-levelezés aláírással és titkosítással

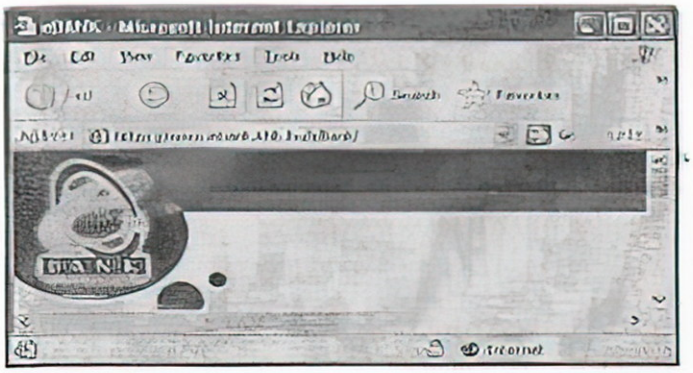


19. ábra
A DPG által generált tanúsítvány

2.4 Webkommunikáció – Internet Explorer

Webes kommunikáció esetében az elektronikus aláírás használata még egyszerűbb, mint a levelezés esetében. Ha felkeresünk egy elektronikus tanúsítvánnyal felszerelt weboldalt, akkor annak tanúsítványa csak akkor jelenik meg, ha

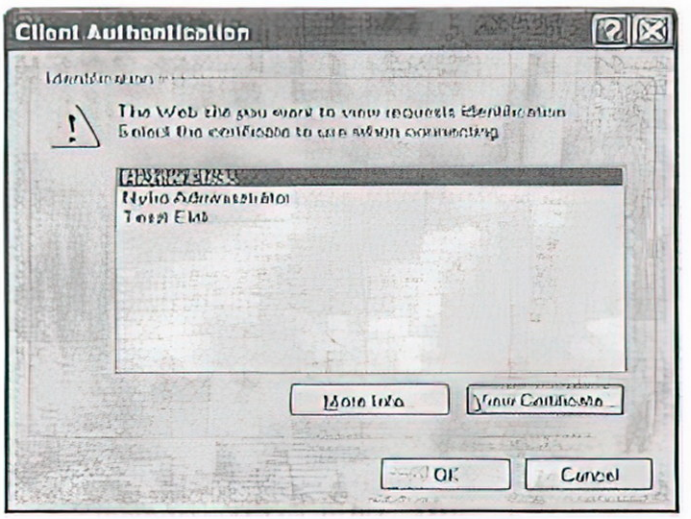
az azt kibocsátó szervezet saját tanúsítványa nem szerepel az elfogadott hitelesítésszolgáltatók listájában. Egyébiránt mindössze annyi utal a kommunikáció biztonságos voltára, hogy a böngésző **Address**-nek nevezett mezőjében az oldal címe https://-rel kezdődik[9] a megszokott http:// helyett, s az ablak alsó sarkában ott terem egy sárga apró lakat (ez nem azt jelenti, hogy foglyok lettünk, hanem azt, hogy biztonságban vagyunk)[10].



20. ábra
Biztonságos internetoldal

Ha ilyenkor a **lakatra** bökünk, megjelenik a webszerver tanúsítványa. Akár össze is hasonlíthatjuk a tanúsítványban szereplő domainnevet a megtekintett oldal nevével (ha az esetleg különbözne, akkor sikítva fussunk böngészőnk gyártójához, amiért a program automatikusan nem figyelmeztetett minket erre).[11]

Ha a webszerver elektronikus aláíráson alapuló kliens oldali felhasználóazonosítást is kér tőlünk, akkor egy ablakban megjelennek a tanúsítványaink (vagy tanúsítványaink közül azok, amelyet a webszerver elfogad), s amelyeket felajánlhatunk az azonosításra.



21. ábra
Kliens azonosítása tanúsítvánnyal

Az ablakban a tanúsítványok tulajdonosainak neve jelenik meg, de a tanúsítvány teljes tartalmát is megtekinthetjük. A tanúsítványt kiválasztva az elektronikus aláírásunkkal együtt a webszervernek elküldésre kerül. A webszerver aláírásunkat a tanúsítvány segítségével ellenőrzi.

2.5 Állományok titkosítása – EFS

A **Windows XP** (sőt elődje, a **Windows 2000** is) NTFS fájlrendszer esetén az Encrypting File System segítségével lehetőséget ad állományaink rejtjelezett módon történő tárolására[12]. Az erre vonatkozó igény a kérdéses állomány vagy könyvtár egy attribútumával állítható be (a tömörítéshez hasonlóan). A rejtjele-

zés ezek után a felhasználó további közreműködése nélkül automatikusan, egy, az operációs rendszer által erre a célra létrehozott kulccsal történik, csakúgy, mint a visszafejtés, melyre az állomány megnyitásakor vagy nyílt módú tárolásra való visszaállításakor van szükség.

2.5.1 Miért kell az állományokat titkosítani?

Sokan abban a tévhitben tengetik mindennapjaikat, hogy az NTFS fájlrendszerben tárolt adataik védettek az illetéktelen kíváncsiskodástól, hiszen beállították azokat a jogosultságokat, amivel mindenki mást kitiltanak a kényes könyvtárakból. Pedig ez még akkor sem elégséges védelem, ha rendszergazdai jogosultságokkal más nem rendelkezik az adott gépen (hiszen annak segítségével e jogosultságok is könnyedén újrakonfigurálhatóak). Ez a védelem ugyanis csak akkor aktivizálódik, ha a kérdéses fájlrendszerre vonatkozó beállításokat az operációs rendszer (a **Windows**) betölti. Ha az operációs rendszert el sem indítjuk, hanem azt megkerülve egy speciális programmal férünk a lemezhez (akár **MS-DOS** vagy **UNIX** alól), akkor ezek a jogosultsági beállítások nem tudnak érvényt szerezni önmaguknak. A lemez tartalma teljesen nyílt formában ott áll az ügyes kezű behatoló előtt.

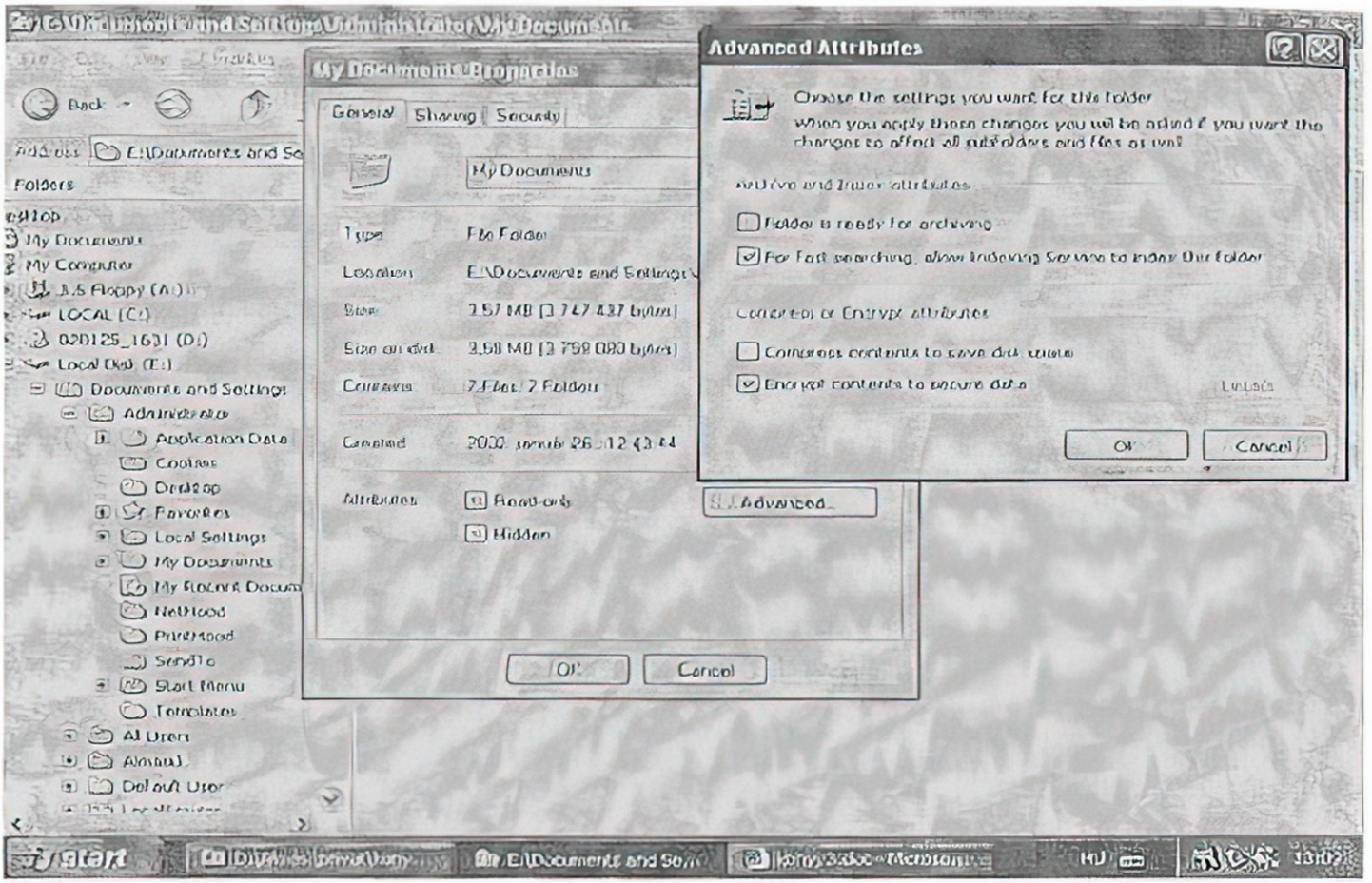
Ehhez még csak el sem kell lopni a gépet (bár ha ellopják laptopunkat, készüljünk fel az adatlopásra is), illetve annak lemezegységét, elég az is, ha egy kis időre magára hagyjuk, és ezalatt a behatoló be tudja bootolni a szükséges programot. Ha viszont titkosítjuk állományainkat, a behatoló csak a rejtjelezett adatokhoz fér hozzá, amiket nem tud értelmezni.

2.5.2 Titkosítás és visszafejtés

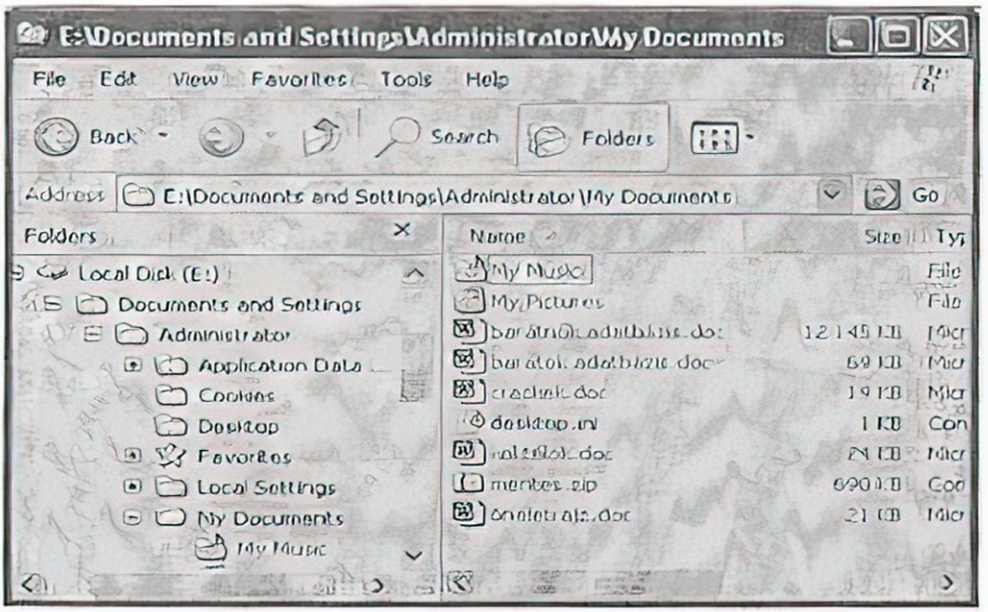
A megfelelő beállításokat követően a felhasználó a feldolgozás lassabb voltán kívül semmit sem észlel az állomány rejtjeles voltából, annál inkább a többi felhasználó, akiket üzenet figyelmeztet arra, hogy nincs jogosultságuk a kérdéses állományhoz való hozzáférésre.[13] Nem engedélyezi számukra az állomány megnyitását, másolását vagy olyan fájlrendszerbe való mozgatását, ahol az állomány további rejtjelezése nem megoldható (például FAT állományrendszer, floppy), de megengedi számukra is az állomány átnevezését és törlését.

A rejtjelezett tárolás attribútuma a könyvtáron vagy állományon állva a **Properties** menüpont (jobb egérgomb) – **Advanced** gomb – **Encrypt contents to secure data** kontrollkocka kipipálásával állítható be.[14]

Igen hasznos ily módon rejtjelezve tárolni minden üzleti és személyes jellege folytán kényes információnkat. Különösen igaz ez a hordozható gépek esetében, amelyek fokozottan ki vannak téve a lopás veszélyének. Nem érdemes ugyanakkor minden adatot titkosítani azok jóval lassabb feldolgozása miatt. Emiatt is ajánlatos kényes adatainkat egy-két könyvtárba szervezni, és csak ezeket titkosítani. Rejtjeles attribútumú állományainkat megfelelő beállítás esetén a többi fájltól megkülönböztető színnel láthatjuk az **Intéző**-ben.[15]



22. ábra Állománytitkosítás beállítása



23. ábra Titkosított és nyílt állományok megjelenítése

2.6 Dokumentumok aláírása – Office XP

A **Word** és az **Excel** eddig is biztosított lehetőséget a dokumentumok titkosítására, de aláírásukra nem. Az **Office XP** verziójától kezdve azonban végre ez a

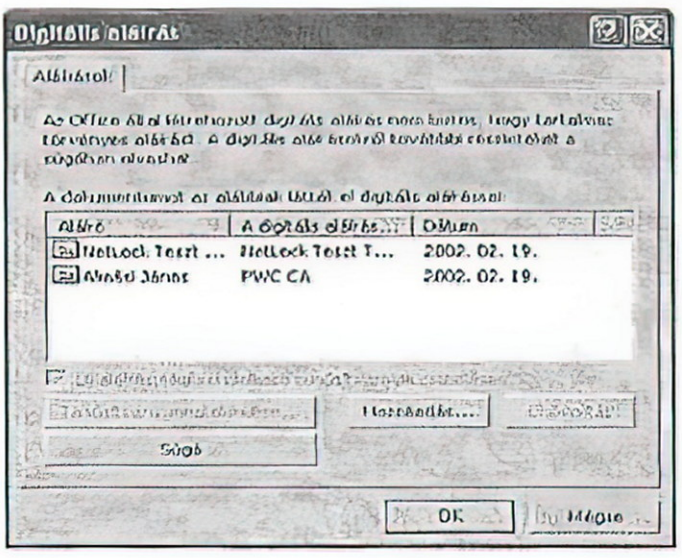
primitív funkció is bekerült az **Office**-programok eszköztárába.[16] Kicsit sután, de azért ott van.

Az aláírási művelet az **Adatvédelem** ablak **Digitális aláírások** gombjára kattintva érhető el a program főablakának **Eszközök – Beállítások** menüpontjain keresztül (mivel alaposan el van dugva, érdemes lehet kirakni az eszközsorba a **Beállítások** funkciót a könnyebb elérhetőség végett)[17]. Figyelni kell arra, hogy ha egy korábban aláírt dokumentumon módosítunk, és azt újra elmentjük, akkor az eredeti aláírás frissítését a programok nem végzik el maguktól (vagy miután rákérdeztek arra). Mentés előtt mindig nekünk kell aláírni a dokumentumot, ellenkező esetben a mentés törli a korábbi aláírásokat. Ennek ugyan megvan az az előnye, hogy az aláírás megtételének szándékossága nehezebben vonható kétségbe, de e bonyolultság miatt az aláírás használata csak azokban az esetekben javasolt, amikor valóban szükség van a dokumentum szerzőjének minden kétséget kizáró azonosítására és a sértetlenség biztosítására.

Az aláírás nem akadályozza meg azt, hogy bárki módosítsa a dokumentumot, és később akár saját aláírásával lássa el. Célja mindössze az, hogy az irat eredetét igazolja, s ezzel elsősorban nem minket véd, hanem a dokumentum felhasználóit. A dokumentumhoz való hozzáférést titkosítással tudjuk korlátozni (lásd: 2.6.4 fejezet), ha pedig szerzői jogainkat akarjuk jogi értelemben is igazolni, akkor független időbélyegzőre van szükségünk (lásd: 5.6.2 fejezet).

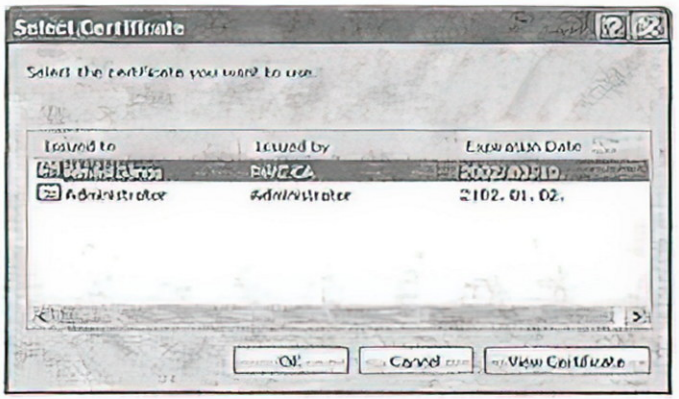
2.6.1 Word-dokumentumok aláírása

A **Digitális aláírás** képernyőt előhívva megjelennek azoknak az aláírásoknak az adatai, amivel korábban ellátták a dokumentumot. Az aláíró személy neve (ahogy a tanúsítványban szerepel), az aláírást hitelesítő szervezet neve és az aláírás ideje. Amennyiben több személy is aláírta ugyanazt a dokumentumot, aláírásaik egymás alatt jelennek meg a listában.



24. ábra
Digitális aláírások egy Word-dokumentumon

Az egyes aláírások ellenőrzésére szolgáló tanúsítványok dupla kattintással tekinthetők meg. Új aláírást a **Hozzáadás** gombbal lehet a dokumentumon elhelyezni. Ekkor megjelenik az összes, erre alkalmas tanúsítvány, amelyek közül választhatunk.[18]

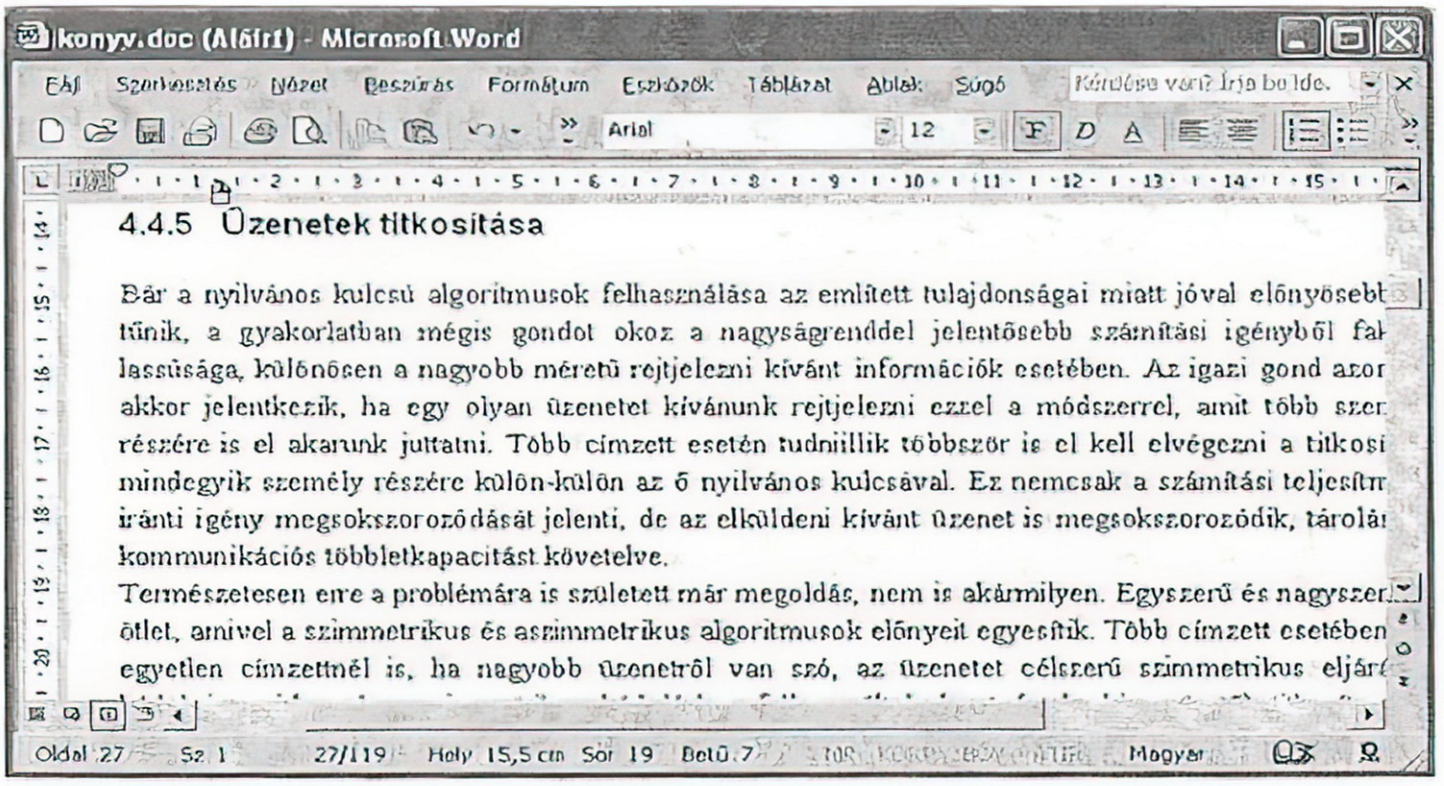


25. ábra
Aláíró tanúsítvány kijelölése

Amennyiben a kontrollkocka be van jelölve a **Digitális aláírás** képernyőn, a tanúsítvány is csatolódik a dokumentumhoz.

2.6.2 Word-dokumentumok aláírás ellenőrzése

Az így aláírt dokumentum aláírt jellegét a szövegszerkesztő ablakának címsorában a fájl neve mellett megjelenő zárójeles „Aláírt" szöveg és az állapotsorban feltűnő **pecsét** szimbólum jelzi. Az aláíró kilétének ellenőrzéséhez a **Digitális aláírások** képernyőt kell előhívni (a menün keresztül vagy a pecsét szimbólumra kattintva).

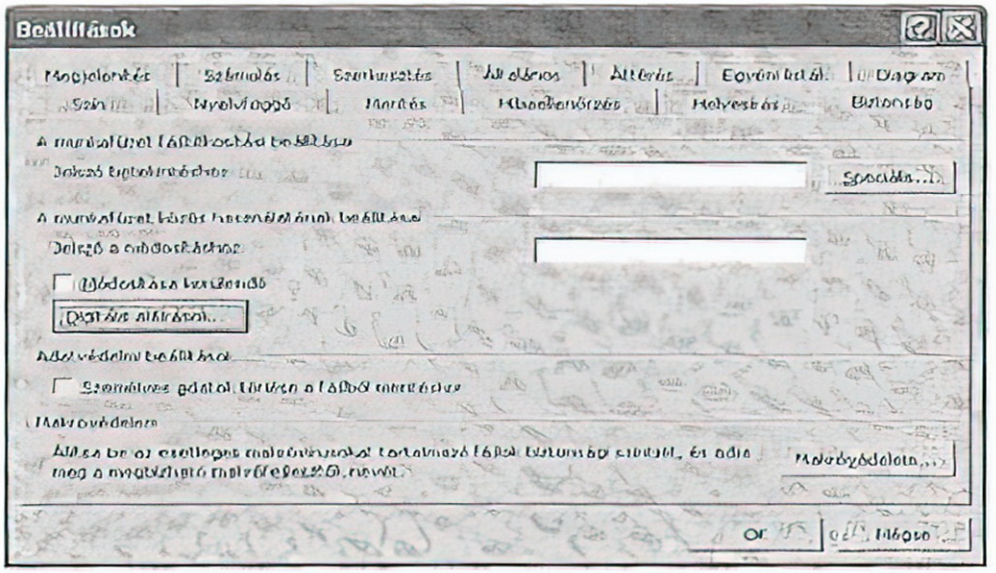


26. ábra Aláírt dokumentum Wordben

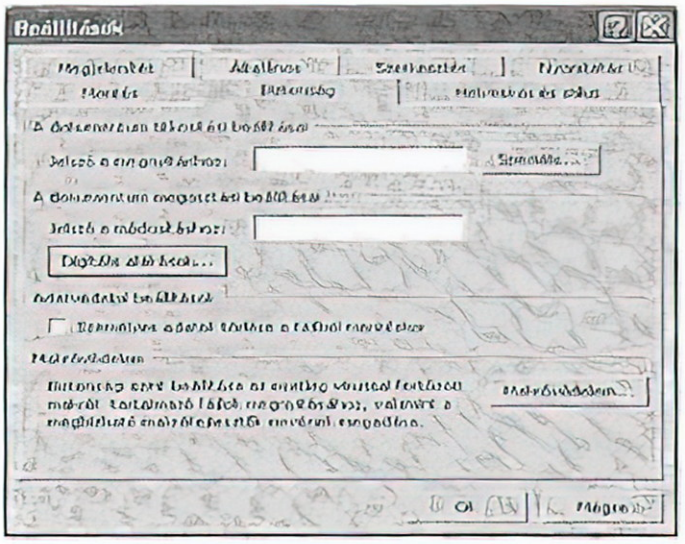
2.6.3 Excel és PowerPoint

Bár az **Excel**-ben és a **PowerPoint**-ban nincs a státussorban kis pecsét, és az ablak címsorában a szöveg kicsit másképp jelenik meg, ezen apró különbségektől eltekintve az aláírás megtételének és annak ellenőrzésének menete megegyezik

a **Word** esetében bemutatottal. A **Beállítások** képernyő ugyan mindkét program esetében másképp néz ki, az aláírási funkcionalitás mögöttük megegyezik a **Word** esetében bemutatottal.



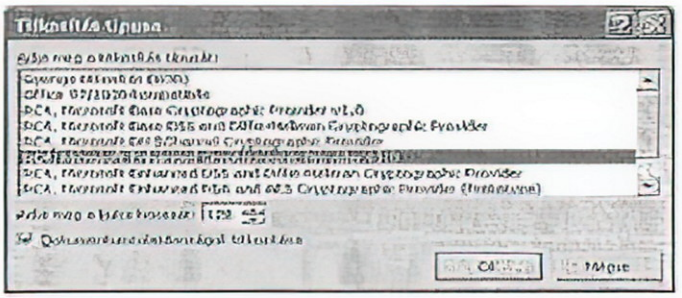
27. ábra
Excel biztonsági beállítások képernyő



28. ábra
PowerPoint biztonsági beállítások képernyő

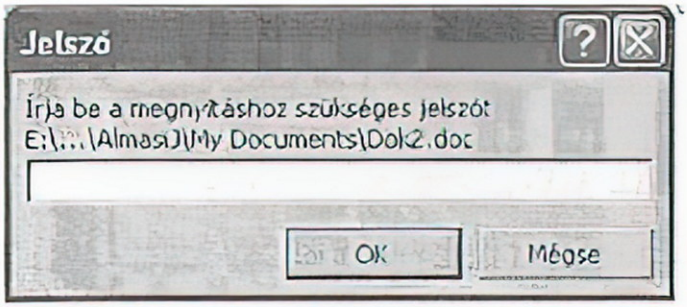
2.6.4 Dokumentumok titkosítása

A dokumentumok titkosítása (jelszóval való levédése az illetéktelen megnyitás ellen)[19] a régebbi **Office**-verziókhoz képest alaposan át lett dolgozva[20]. A funkció az **Adatvédelem** ablakban (az **Eszközök – Beállítások** vagy a **Mentés** ablak **Eszközök – Biztonsági beállítások** menüpontjain keresztül) érhető el. A megnyitási jelszót be kell gépelni a Jelszó mezőbe, majd biztos, ami biztos alapon meg kell ismételni, és a dokumentum elmenthető kódolt formátumban. A jelszó megadásakor a **Speciális** gomb segítségével megadható a titkosítás típusa: választhatunk egy, a korábbiakkal kompatibilis (kevésbé biztonságos) módszert, vagy egy erősebbet a kulcshosszúság megadásával, amely esetben a dokumentum tulajdonságainak titkosítására is mód van (azok az **Intéző**-ben sem fognak megjelenni).



29. ábra
Dokumentum titkosítási módszerének kiválasztása

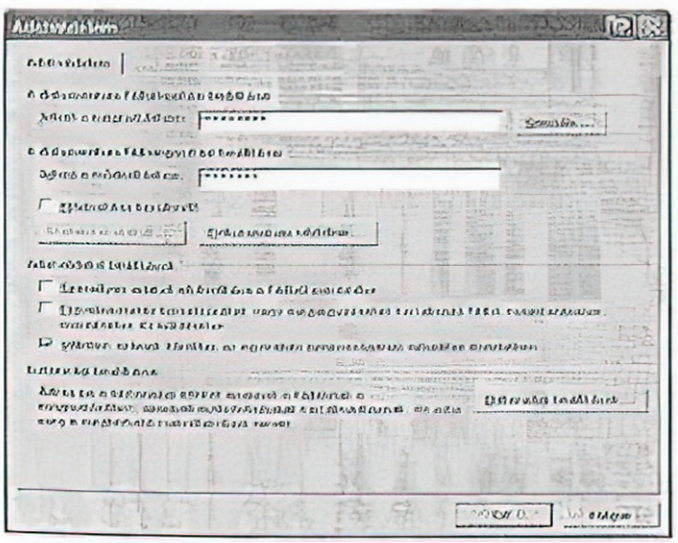
Ezt követően a dokumentum csak a jelszó megadása után tekinthető meg (a dokumentum nyílt tartalma más, **Word**-formátumot ismerő programmal vagy egy bájtszintű nézegetővel nem válik láthatóvá).



30. ábra
Jelszó megadása a dokumentum visszafejtéséhez

A kódolás, illetve a jelszavas hozzáférés annak beállításához hasonló módon szüntethető meg: ugyanazon mezőben, ahol beírtuk a jelszót, törölni kell azt.

A megnyitáshoz hasonlóan védhetjük dokumentumainkat módosítás ellen is, egy másik (a megnyitási jelszótól célszerűen különböző) jelszó megadásával. Megnyitáskor a **Word** a módosítási jelszóra is rákérdez, s ha nem tudjuk azt megadni, akkor a dokumentum csak olvasásra nyitható meg. Ekkor is tudunk azonban a dokumentumon módosítani, de ezek után csak egy másik néven tudjuk elmenteni. Ilyenkor automatikusan bekapcsol a korrektúra, amit nem is enged a **Word** kikapcsolni (igaz, ez a „védelem" könnyen kijátszható). Ez a módszer azonban (önmagában) nem titkosítja a dokumentum szövegét, az akár **WordPad**-del is megnyitható, majd RTF formátumban menthető. Valójában a védelemnek ez a módja nem tudja megakadályozni egy rossz szándékú embertársunkat sem abban, hogy a dokumentumunkat módosítsa, ez a módosítás azonban észlelhetővé válik (a korrektúra által vagy azáltal, hogy az eredeti módosítási jelszó lekerül a dokumentumról).

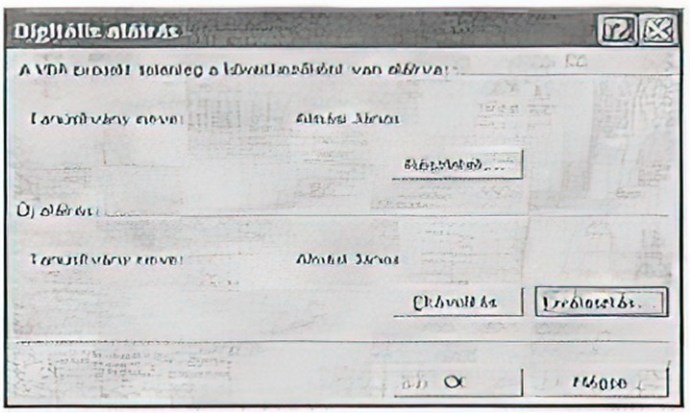


31. ábra
Megnyitási és módosítási jelszó megadása

2.6.5 Makrók aláírása – Office XP

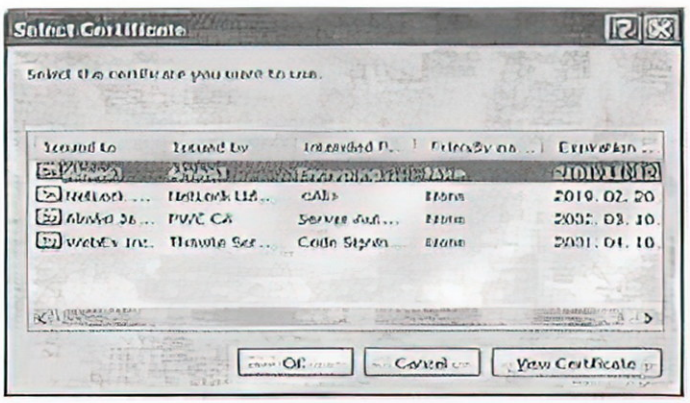
Az **Office**-dokumentumokhoz készített makróinkat a dokumentum aláírásától függetlenül is elláthatjuk elektronikus aláírással.[21] Az így aláírt makróprogramokat aztán annak felhasználói nagyobb bizalommal indíthatják el, mivel készítőjében és változatlan tartalmában biztosak lehetnek. Mivel manapság virágkorukat élik a csekély fejlesztői tudással is létrehozható, igen kártékonnyá szabható makróvírusok, ennek jelentőségét bizonyára senki előtt nem kell bizonygatnom.

Egy elkészült makróprojektet a Visual Basic **Digitális aláírás** képernyőjén (**Tools – Digital Signature**) keresztül írhatunk alá. A képernyőn látszódik a makróprojekten jelenleg szereplő aláírás (a dokumentummal ellentétben itt csak egy aláírás lehet), illetve az, hogy új aláírás megtételére melyik tanúsítványt ajánlja a rendszer (a rendelkezésünkre álló tanúsítványok közül azt, amelyik alkalmas az aláírásra[22]).



32. ábra
Makróprojekt elektronikus aláírása

A **Részletek** gomb segítségével megnézhetjük az aláíró tanúsítvány tartalmát, a **Kiválasztás** gombbal új tanúsítványt választhatunk az aláírásra, az **Eltávolítás** gombbal eltávolíthatjuk a makróprojekten szereplő aláírást.



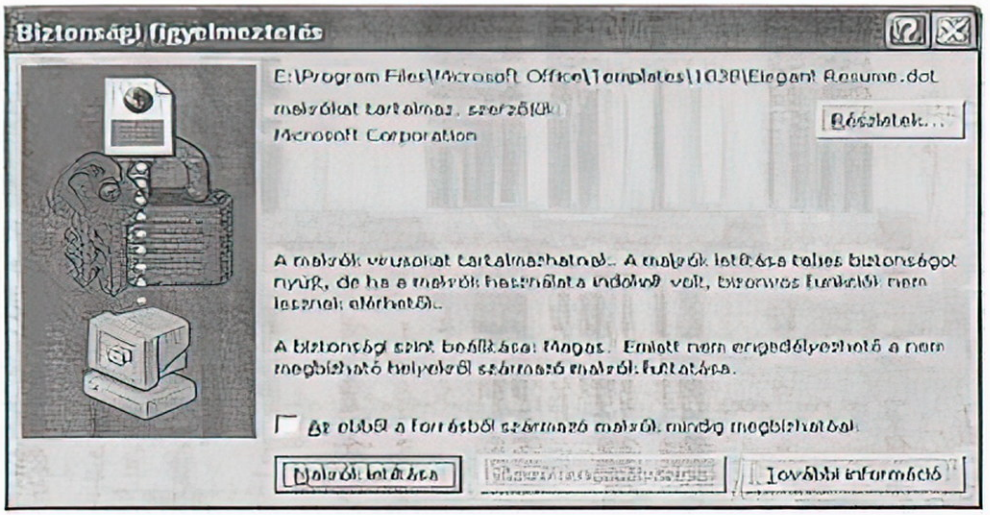
33. ábra
Választás a tanúsítványok közül

A kiválasztás hatására felsorolt tanúsítványok között nem csak azok jelennek meg, amelyek alkalmasak az aláírásra.[23] Ha nem megfelelőt választunk ki, a rendszer figyelmeztet a hibára.

Az egyes makróprojekteket külön-külön kell aláírni (az aláírás a projektböngésző ablakában épp aktuális projektre fog vonatkozni), s erre tetszés szerint használhatunk akár különböző tanúsítványokat is. A dokumentumok aláírásához hasonlóan, ha módosítunk a projekt valamely részletén, az aláírást újra meg kell tennünk. Hogy az ilyen véletlen módosításokat megakadályozzuk, zároljuk a projektünket.[24]

Az **Office**-programok ezek után a biztonsági beállításoktól függően figyelmeztetnek a makró megnyitásakor a makró aláírását ellenőrizve és bemutatva. A figyelmeztető képernyőn a **Részletek** gombra kattintva megtekinthetjük az aláírás és az aláíró tanúsítvány részletes adatait, a **Makrók engedélyezése** gombbal engedélyez-

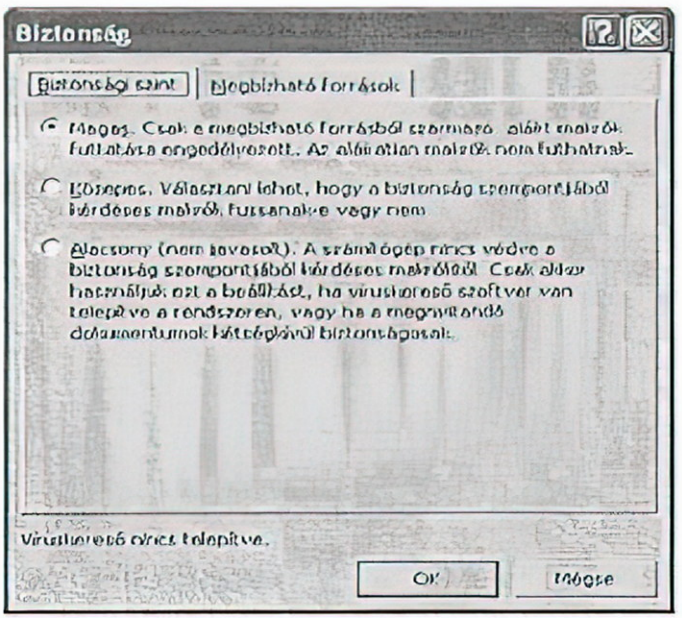
hetjük a makrók futását (magas biztonsági szint esetén csak akkor választható, ha az aláírót megbízhatónak minősítjük), a **Makrók letiltása** gombbal pedig megnyithatjuk a dokumentumot anélkül, hogy a makrók futását engedélyeznénk.



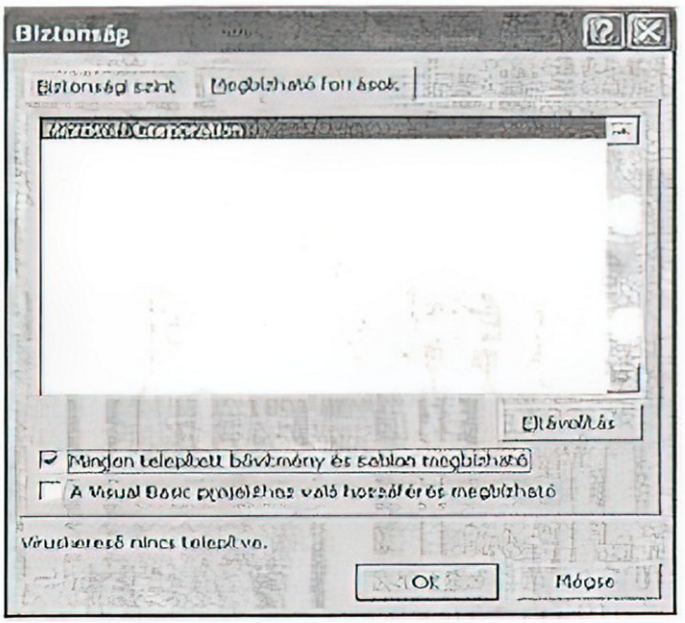
34. ábra
Figyelmeztetés egy makróra az aláíró megjelenítésével

A biztonsági szint az **Eszközök – Makró – Biztonság** útvonalon elérhető **Biztonság** ablakban állítható be. A *Közepes* szint ideális, az *Alacsony* nem javasolt, hiszen így a makrók figyelmeztetés nélkül, automatikusan lefutnak, akkor is, ha rosszindulatú makróvírusról van szó. Gondolom, ma már mindenki tisztában van ennek esetleges következményeivel (35. ábra).

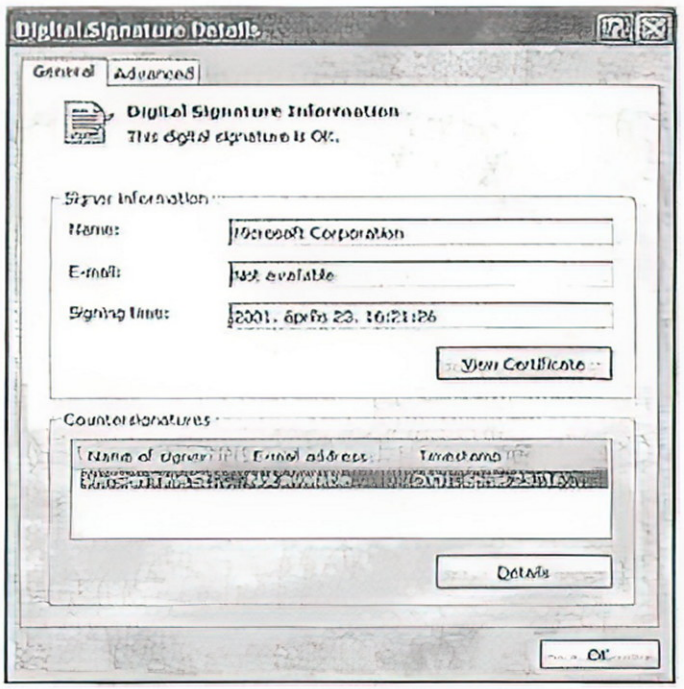
Az **Office XP**-nek minden gyári makrója (a telepített sablonok és bővítmények részeként) el van látva a Microsoft aláírásával és időbélyegzővel is. A **Biztonság** ablak **Megbízható források** füle alatt beállítható, hogy ezeket a program megbízhatónak tekintse-e. Ugyanitt láthatók a korábban megbízhatónak minősített makróaláírók is. Ezeket az **Eltávolítás** gombbal ritkíthatjuk. A gyári makrók megbízhatóságát a sablonokra vonatkozó kontrollkocka kipipálásával vagy a Microsoft felvételével a megbízható források listájába állíthatjuk be.



35. ábra
Makrók ellenőrzésének beállítása



36. ábra
Megbízható makróaláírók listája



37. ábra
Aláírás adatai

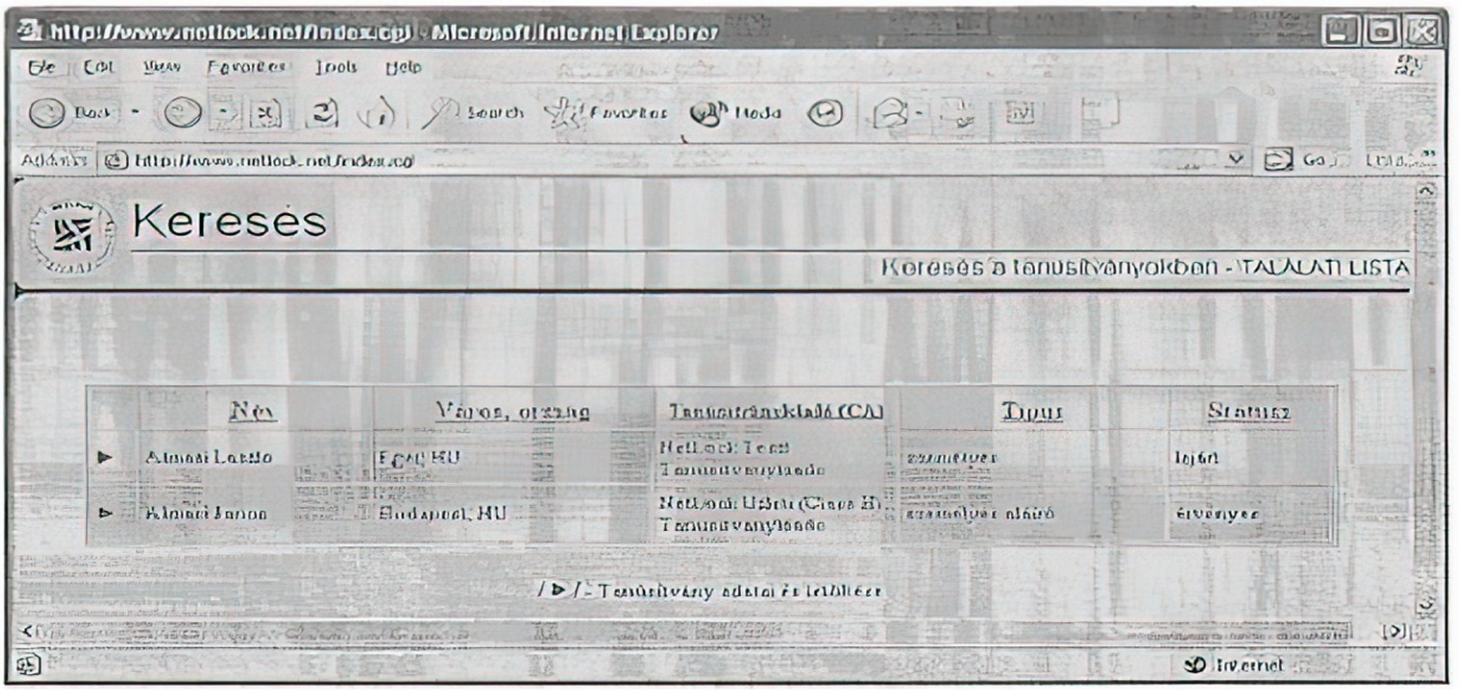
A makróaláírás adatainak megtekintése a dokumentum-aláírástól eltérő ablakban lehetséges. A **Digital Signature Details** ablak az aláírás részletes adatait is bemutatja. Az ablakban látszódik az aláíró neve és e-mail-címe, valamint az időbélyegző adatai. A **View Certificate** gombbal megtekinthetjük az aláíró tanúsítványt, a **Details** gombbal (az időbélyegzőn állva) pedig az időbélyegző adatait.

38. ábra
Aláírás adatai részletesen

2.7 Tanúsítványok lekérdezése

A szolgáltatók az interneten történő tanúsítványigénylés mellett hasonló módon biztosítják a kiadott tanúsítványok lekérdezhetőségét. Webes felületen keresztül kereshetünk a szolgáltató tanúsítványtárában a kiadott és visszavont tanúsítványok között, s a talált tanúsítványokat megtekinthetjük. Erre akkor lehet szükségünk, ha egy aláírt üzenet mellett valamiért nem található meg az ellenőrzéséhez szükséges tanúsítvány, illetve, ha meg akarunk bizonyosodni arról, hogy a tanúsítvány nem lett-e visszavonva a kiadást követően (lásd bővebben a 4.8 fejezetet).

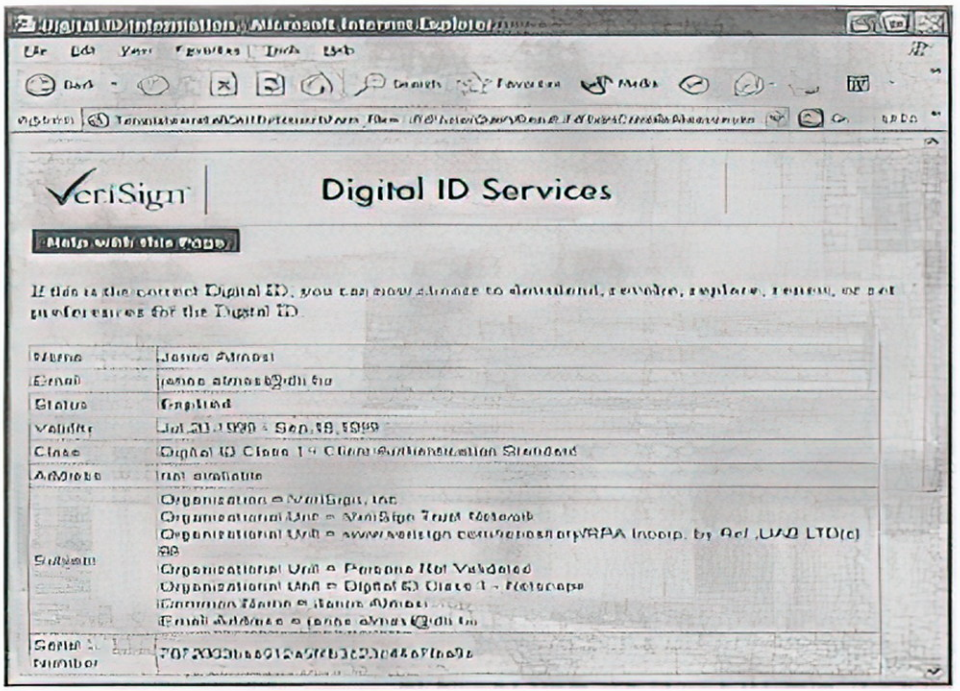
Ez a funkció a NetLock esetében a főoldalon található **Keresés a kiadott tanúsítványokban** menüpont segítségével érhető el. Az **Egyszerűsített keresés** során a tanúsítvány legalapvetőbb mezői alapján, a **Részletes keresés** esetében pedig szinte minden mezőre kereshetünk. A találati listában a keresésének megfelelő tanúsítványok legfontosabb adatait láthatjuk, s lehetőségünk van a tanúsítvány összes adatának megjelenítésére s a tanúsítvány letöltésére is.



39. ábra Keresés eredménye

40. ábra
Tanúsítvány adatainak megjelenítése – NetLock

A Verisign a https://digitalid.verisign.com/query.htm címen biztosít hasonló szolgáltatást. Itt a tanúsítvány sorozatszáma, a tulajdonos neve és e-mail-címe alapján kereshetünk az érvényes, lejárt és visszavont tanúsítványok között. A tanúsítványok részletes adatait megjelenítve módunk van a tanúsítvány letöltésére, visszavonására és megújítására.



41. ábra
Tanúsítvány adatainak megjelenítése – Verisign

JEGYZET

1 www.verisign.hu vagy www.verisign.com

2 Erre a levélre azért van szükség, hogy a szolgáltató biztos lehessen abban, hogy a tanúsítvány valóban az e-mail-cím tulajdonosáé lesz.

3 Más szolgáltatóknál, amennyiben azok nem CER tanúsítványformátumban teszik közzé tanúsítványukat (ld. GIRO), a tanúsítványt előbb el kell mentenünk a winchesterre, majd onnan kell importálnunk (lásd 10.3 fejezet).

4 CSP, azaz Cryptographic Service Provider. Ez voltaképpen a kriptorendszer meghajtóprogramja. Itt a Microsoft saját, különböző erősségű kriptomoduljai mellett a **Windows** által eleve ismert, valamint a felhasználó által korábban installált idegen meghajtóprogramok közül lehet választani. Lásd bővebben: 10.3.14 fejezet.

5 Vegyük a fáradságot, és a jelszavunkat adjuk meg mindig!

6 Bár az **Office** csomag legújabb változatát megilleti az XP elnevezés, tagjainak (**Outlook, Word, Excel, PowerPoint**) hivatalosan csak a 2002-es jelző jár.

7 Ez a hagyományos aláírás a **Beállítások – Levélformátum – Aláírás** útvonalon érhető el.

8 Bővebb információ és letöltés: http://www.drotposta.hu/

9 A HTTPS a HTTP protokoll SSL-lel kombinált változata. Lásd bővebben a 3.7.6 fejezetben.

10 **Netscape** esetében hasonló a helyzet az **Internet Explorer**-hez: A böngésző **Location** mezőjében a https://-rel kezdődő cím szerepel, az ablak alsó felében pedig bezárul egy sárgás **lakat.**

11 Ilyenkor nyilván csak a domainnevet (a :// és / közötti alapcím) kell összehasonlítani, mert nincs minden oldalnak külön tanúsítványa.

12 Korábbra viszont nem mehetünk vissza az időben. A **Windows NT 4**-féle NTFS még nem támogatta az EFS-t.

13 Saját magunk is észlelhetjük ezt, ha több **Windows**-user nevében használjuk gépünket (például lokális rendszer-adminisztrátorként és mezei tartományi felhasználónként).

14 Az EFS funkciói parancssorból is elérhetőek a **cipher** parancs segítségével (paraméterezést lásd: cipher /?).

15 A **Folder Options – View – Advanced Settings – Show Encrypted or Compressed NTFS files in color** kontrollkocka beállításával.

16 Ez sem keverendő össze az **Elektronikus levél aláírása** művelettel, ami a **Beállítások – Általános – Elektronikus levelek beállításai** útvonalon érhető el.

17 Furcsa módon (valószínűleg azért, mert az előzőleg mentett állományból képzi a **Word** az aláírandó lenyomatot) a **Mentés** ablak **Eszközök – Biztonsági beállítások** menüpontjain keresztül az aláírási művelet nem érhető el.

18 Azok a tanúsítványok, melyek magánkulcsa is rendelkezésünkre áll. Érdekes módon használhatók aláírásra az EFS-kulcsok is.

19 A jelszóval védett dokumentumokat a **Word** nem engedi felülírni sem (Save as funkció során), csak a jelszavak megadása után, sőt a másoláshoz az **Intéző** is jelszót kér.

20 A régebbi megoldás biztonsági szintje igencsak kétes volt. A dokumentum szerkesztésekor létrejövő átmeneti állományokat az **Office** nem titkosította, a kulcsot a lapozófájlban tárolta. Az interneten hozzáférhetőek olyan programok, melyek képesek azt a védelmet feltörni. Ugyanakkor az új módszer sem bombabiztos: szótármódszerrel ez is támadható.

21 Ez a lehetőség már az **Office 2000**-ben is szerepelt.

22 Itt az EFS tanúsítvánnyal nem írhatunk alá.

23 A képernyőn a **Windows** tanúsítványtár Personal könyvtárának tartalma jelenik meg.

24 Az ilyen zárolás azonban nem védi meg a projektünket attól, hogy később valaki kicserélje a rajta található aláírást a sajátjára.

3 Az elektronikus aláírás (és társai) fiziológiája

Ajánlás:

Azoknak, akiket érdekel az elmélet.

Az előző fejezet néhány példán keresztül, amolyan kedvcsinálóként is bemutatta, hogy az elektronikus aláírás (és társai) a gyakorlatban egész egyszerűen felhasználhatók. Ez az egyszerűség azonban látszólagos, a felhasználói felület felszíne mögött összetett műveletek zajlanak le, amikkel nem árt tisztában lenni. Ez a fejezet – bízva abban, hogy az olvasó kedve nem megy el olyan könnyen – megmutatja, mik is ezek a műveletek, és hogyan zajlanak le. Mi történik akkor, amikor az alkalmazás felhasználói felületén beikszelünk egy kockát, ráklikkelünk a rendben gombra, vagy például miért kell megadni a jelszavunkat.

3.1 Felhasználási lehetőségek

Az elektronikus aláírás és titkosítás – illetve általánosabb értelemben véve a kriptográfia – legismertebb felhasználási lehetőségei az alábbiak:

- Az elektronikus levelezés biztonságossá tétele a levél aláírásával és/vagy titkosításával.
- Biztonságos internetes szolgáltatások nyújtása (például webáruházak, házibank-rendszerek, tőzsdei szolgáltatások, hírszolgálat stb.) a szolgáltatást nyújtó és igénybe vevő megbízható azonosításával és a szolgáltatott információ hitelességének, sértetlenségének, letagadhatatlanságának és bizalmasságának biztosításával.
- Zárt internetközösségek létrehozása (például orvosi konzílium, ügyvédek fóruma, bármilyen szolgáltatás előfizetői) a felhasználók megbízható azonosításával és a kommunikáció bizalmassá tételével.
- Zárt kommunikációs csoportok kialakítása bármilyen kommunikációs felületen (mobiltelefon, internet, LAN, WAN hálózatok stb.) a csoport tagjainak azonosításával s az adatforgalom aláírásával és titkosításával.
- Biztonságos elektronikus fizetési módszerek kialakítása a felhasználó azonosításával és a kártyaszám titkosításával akár interneten, akár mobiltelefonon keresztül.
- Elektronikus pénztárca és elektronikus pénz megoldások kis összegű vásárlások céljára a „pénz"-kibocsátó általi elektronikus aláírásával.
- Biztonságos archiválás és adatbázis-kezelés, az eltárolt információ elektronikus aláírásával és/vagy titkosításával.
- Felhasználók biztonságos azonosítása és beléptetése informatikai rendszerekbe vagy helyiségekbe.

- Szoftverek származásának igazolása és sértetlenségének biztosítása a programkód aláírásával.
- Bármilyen információ adott időben és formában való létezésének igazolása.
- Különböző elektronikus iratokkal kapcsolatos szolgáltatások.
- Internet alapú szavazási és választási rendszerek.

A fenti felhasználási lehetőségekből kitűnik, hogy az elektronikus aláírást és titkosítást nem csak természetes személyek, de informatikai alkalmazások (például webszerverek) és hardverberendezések (például tűzfalak, útválasztók, mobiltelefonok) is alkalmazzák.

A felhasználásban világszerte élen járó iparágak a pénzügyi szolgáltatások, a telekommunikáció és az egészségügy, amelyek mellé egyre inkább felzárkóznak a közszolgáltatások. Ha ki lehet emelni bármelyik funkcióját, akkor a pénzügyi szolgáltatások esetében a letagadhatatlanság (a pénzügyi tranzakció bizonyíthatósága), a telekommunikáció számára a sértetlenség (az adatcsomagok eredeti formában történő továbbítása), az egészségügy számára a bizalmasság (a bizalmas személyes adatok védelme), a közszolgáltatások részére pedig a hitelesség (az eljáró felek pontos azonosítása) a legfontosabb.

3.2 Alapműveletek

A bemutatott felhasználási lehetőségek mögött a következő műveletek állnak:

- elektronikus üzenetek és adatok aláírása és az aláírás ellenőrzése,
- elektronikus üzenetek és adatok titkosítása és visszafejtése,
- felhasználó-azonosítás,
- kulcsok aláírása és az aláírás ellenőrzése,
- kulcsok titkosítása és visszafejtése,
- időbélyegzés és az időbélyegző ellenőrzése.

Ezek a műveletek is két eljárásra vezethetők vissza: a felhasználó-azonosítás és az időbélyegzés az aláírásra, a kulcsok pedig felfoghatók speciális adatként, melyek aláírása vagy titkosítása algoritmikusan semmiben nem tér el egyéb adatok aláírásától és titkosításától.

Míg az időbélyegzés és a kulcsok aláírása (tanúsítvány előállítása) tipikusan hitelesítésszolgáltató által kereskedelmi tevékenységként végzett műveletek, addig az összes többi műveletet a felhasználók is elvégezhetik a szolgáltatótól kapott tanúsítvány és magánkulcs segítségével, amennyiben a szolgáltató erre feljogosítja őket.

3.3 Az elektronikus aláírás működése

Mint azt már említettem, az elektronikus aláírás egyaránt eleget tesz a hitelesség, sértetlenség és letagadhatatlanság követelményének. A hitelesség érdekében biztosítja az aláíró egyértelmű azonosíthatóságát, a sértetlenség garantálá-

sa végett azt, hogy az elektronikus irat az aláírás óta nem változott, továbbá gondoskodik arról, hogy az irattal kapcsolatban tett elektronikus aláírást utólag ne lehessen letagadni.

De hogyan képes minderre:

Sértetlenség	– Az információról lenyomatot készít.
Hitelesség	– A lenyomatot az aláíró magánkulcsával kódolja.
Letagadhatatlanság	– Biztosítja azt, hogy a lenyomat csak az adott információra, a magánkulcs pedig csak az aláíróra legyen jellemző.

Az aláíró magánkulcsával kódolt lenyomat maga az elektronikus aláírás, amely együttesen jellemző az adott információra és annak előállítójára. Az eredeti információt ezek a műveletek nem módosítják, az ezek után szabadon kiegészíthető az elektronikus aláírással, vagy kezelhető a nélkül is, ahogy az adott művelet kívánja.

Ebből persze magam sem érteném meg elsőre, miről van szó, így lássuk mindezt lépésenként részletezve.

3.3.1 Elektronikus aláírás készítése

Hozzávalók: Az elektronikus aláírás készítéséhez venni kell egy darab tetszőleges hosszúságú nyílt szöveget – amit alá akarunk írni –, egy magánkulcsot – az aláíró magánkulcsát –, valamint lenyomat- és aláírás-készítő eljárásokat.

Tennivalók: Ha mindezek megvannak, akkor a lenyomatkészítő eljárásba bedobjuk az eredeti nyílt szöveget, majd az ennek eredményeként előálló szöveglenyomatot és a magánkulcsot óvatosan belehelyezzük az aláírás-készítő eljárásba, amely a lenyomat kódolásával előállítja az elektronikus aláírást[1].

	Paraméterek	Művelet	Eredmény
1. lépés	Nyílt szöveg	*Lenyomatkészítő eljárás*	Lenyomat
2. lépés	Lenyomat, aláíró magánkulcsa	*Aláírás-készítő eljárás*	Aláírás

Programozóknak mindez így írható le:

Aláírás := aláírás-készítő eljárás (lenyomatkészítő eljárás (nyílt szöveg), aláíró magánkulcsa);

Magyarázat:

A nyílt szöveg voltaképpen akármilyen, nem titkosított digitális információt jelenthet, nem csak szöveg, de akár kép, zene vagy bármely más adat is lehet. A lenyomat- és az aláírás-készítő eljárások szempontjából akár titkosított is lehetne az aláírásra szánt információ, más okok miatt azonban titkosítás használata esetén is általában a nyílt szöveg kerül aláírásra. Az aláírás-készítő eljárás gyakorlatilag egy nyilvános kulcsú kódoló algoritmus, amely a lenyomatot az aláíró magánkulcsával kódolja.

3.3.2 Az elektronikus aláírás ellenőrzése

Az elektronikus aláírás ellenőrzése voltaképpen az elektronikus aláírás során végrehajtott lépések visszajátszását jelenti.

Hozzávalók:

Az elektronikus aláírás ellenőrzéséhez szükség van az eredeti vagy eredetinek titulált (korábban aláírt) nyílt szövegre, az aláírás készítéséhez használt magánkulcs nyilvános párjára, magára az aláírásra, valamint az aláírás-ellenőrző és lenyomatkészítő eljárásokra.

Tennivalók:

Az ellenőrzés tennivalói igen hasonlatosak az aláírás-készítéshez. Az első lépés itt is a nyílt szöveg lenyomatának előállítása, mely ugyanazon a módon történik, ahogy az aláírás készítésénél. Ezek után az aláírást a nyilvános kulccsal együtt az aláírás-ellenőrző eljárásba tápláljuk, és ennek eredményéből is kapunk egy lenyomatot[2] (azt a lenyomatot, amit az aláírás során készítettünk). Ha a két, így előállt lenyomat megegyezik, akkor az aláírást elfogadhatjuk, mert az aláírást minden bizonnyal a nyilvános kulcs magán párjával készítették, és biztosak lehetünk abban, hogy a szöveg az aláírás készítése óta nem változott.

	Paraméterek	**Művelet**	**Eredmény**
1. lépés	Nyílt szöveg	*Lenyomatkészítő eljárás*	Lenyomat 1
2. lépés	Aláírás, aláíró nyilvános kulcsa	*Aláírás-ellenőrző eljárás*	Lenyomat 2
3. lépés	Lenyomat 1, Lenyomat 2	*Összehasonlítás*	Aláírás valódi/nem valódi

Programozóknak:

Valódi := aláírás-ellenőrző eljárás (aláírás, aláíró nyilvános kulcsa) = lenyomatkészítő eljárás (nyílt szöveg);

Magyarázat:

Az aláírás-ellenőrző eljárás gyakorlatilag egy nyilvános kulcsú dekódoló algoritmus (az aláírás elkészítésére használt nyilvános kulcsú kódoló algoritmus párja), amely az aláírást az aláíró nyilvános kulcsával fejti vissza. Amennyiben az aláírás-ellenőrző eljárás nem képes az aláírás visszafejtésére, az azt jelenti, hogy az aláírás nem az ellenőrzés során felhasznált nyilvános kulcs párjával készült, vagyis a valódi aláíró nem az, akinek kiadja magát (vagy az elfogadó valamilyen hibát vétett az ellenőrzés során, például nem megfelelő nyilvános kulcsot alkalmazott). Amennyiben a két lenyomat nem egyezik meg, az azt jelenti, hogy az aláíró ugyan az, akinek kiadja magát, de a nyílt szöveg nem egyezik meg azzal, amit ő eredetileg aláírt. A változás mértékét és helyét ezek az eljárások nem mutatják meg.

3.3.3 Egyéb megfontolások

Ahhoz, hogy az előbbiekben bemutatott elektronikusaláírás-készítő és -ellenőrző módszerek a gyakorlatban is működőképesek legyenek, s valóban kielégítsék az említett biztonsági követelményeket, még további feltételeknek is teljesülniük kell:

- Az aláíró magánkulcsának egyedinek kell lennie, és egyedül az aláíró befolyása alatt kell állnia. A nyilvános kulcsnak kizárólag a magánkulcshoz tartozónak kell lennie, és az aláírás ellenőrzőjének biztosnak kell lennie abban, hogy a nyilvános kulcs az aláíróé.
- A felhasznált aláíró és lenyomatelj árások mögött több különböző algoritmus is állhat (például RSA, DSA, ECDSA, illetve SHA-1, MD5, RIPEMD-160), de az aláíráskor és annak ellenőrzésekor csak ugyanazon algoritmusok alkalmazhatók. Ennek érdekében az aláíró és az elfogadó feleknek előzetesen meg kell egyezniük az alkalmazott algoritmusok típusáról, paraméterezéséről, vagy ezeknek az információknak az aláírással együtt kell utazniuk az elfogadó félhez.
- Az elfogadónak tudnia kell azt is, melyik nyilvános kulcsot kell alkalmaznia az ellenőrző eljárás során, vagyis tudnia kell, hogy ki az aláíró, és rendelkeznie kell annak nyilvános kulcsával (a nyilvános kulcs is utazhat az üzenettel vagy kicserélhető korábban is, de a kulcs aláíróhoz tartozását valamilyen módon biztosítani kell).
- A letagadhatatlanság érdekében az aláírásnak szándékosnak kell lennie, vagyis az alkalmazott módszereknek biztosítania kell azt, hogy aláírásra csak „megfontolt" és szándékos döntés nyomán kerülhessen sor.

3.3.4 A lenyomatkészítő eljárás

A lenyomatkészítő eljárás egy egyirányú hash-függvényen alapszik. A hash-függvény tetszőleges hosszúságú szövegből olyan, fix hosszúságú bitsorozatot állít elő, amely egyértelműen jellemző az adott szövegre (adott szöveg lenyomata mindig ugyanaz lesz). Ez a fix hosszúságú bitsorozat a lenyomat, más néven üzenetkivonat[3]. Az alkalmazott hash-algoritmusok egyirányúak, ütközésmentesek és lavinahatásúak. Mit jelent ez:

Egyirányúság	– A lenyomatból képtelenség az eredeti dokumentumot visszaállítani vagy annak tartalmára következtetni. Lehetetlen egy adott lenyomathoz olyan dokumentumot konstruálni, amelyikhez a transzformáció ugyanazt a lenyomatot rendeli.
Ütközésmentesség	– Lehetetlen két olyan dokumentumot konstruálni, amelyek azonos lenyomatot eredményeznek
Lavinahatás	– Ha egy bitet megváltoztatunk a dokumentumban, akkor a lenyomat értéke (bitjei) közel a felében különbözni fog.

A hash-függvény egyirányú volta miatt szükséges az elektronikus aláírás ellenőrzésénél újra előállítani a lenyomatot, és lavinahatása miatt nem lehet következtetni az eredeti dokumentum tartalmára, ha ellenőrzéskor a két lenyomat közt eltérés fordul elő.

A lenyomat igen rövid, fix hosszúságú adatsorozat, az alkalmazott algoritmustól függően tipikusan 128 vagy 160 bit méretű[4], s ennek megfelelően $1:2^{128}$, illetve $1:2^{160}$ valószínűséggel jellemző az eredeti szövegre (a lehetetlen és képtelenség jelzők ennek megfelelő gyakorlati korlátozással értendők).

A hash-függvények felhasználási lehetőségei jóval szélesebb körűek, mint az elektronikus aláírás céljára történő lenyomatképzés. Az egyes szoftverek, így az operációs rendszerek is, előszeretettel használják a felhasználói hitelesítésre alkalmazott jelszó kódolására (vagyis a jelszó valójában nem visszafejthető titkosító eljárással kerül kódolásra). Itt egyirányúsága nemhogy hátrány, de előny, hiszen a jelszó dekódolására nemcsak hogy nincs szükség (ha a felhasználó elfelejti, az egyszerűen lecserélhető), de ennek lehetősége kifejezett kockázatot is jelent[5]. Széles körben használják a hash-függvényeket sértetlenség ellenőrzésére az elektronikus aláíráson kívül is: egy adott adathalmazról történő ellenőrző kód generálásával később az adathalmazban bekövetkező bármilyen véletlen változás észlelhető. Igaz, ennél több nem is mondható meg róla (mikor, hol, milyen típusú volt a változás), így ez a módszer hibajavításra nem alkalmas.

3.4 A titkosítás működése

3.4.1 A rejtjelezés felhasználása

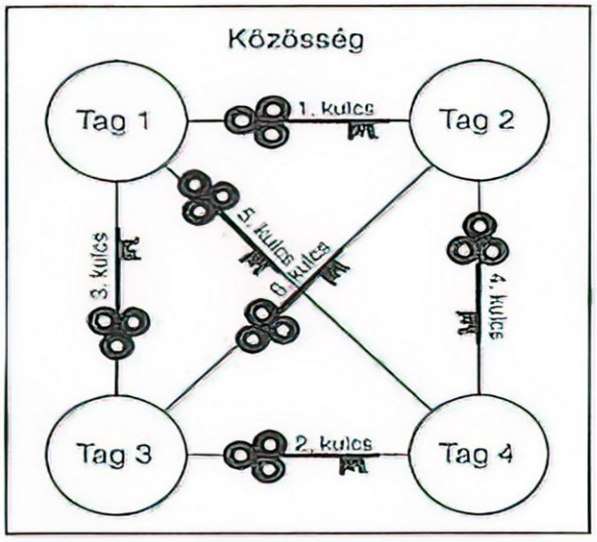
A titkosítás feladata a bizalmasság garantálása, vagyis annak biztosítása, hogy egy információhoz csak azok férhessenek hozzá, ismerhessék meg tartalmát, akik arra jogosultak. A rejtjelezés és rejtjelfejtés korántsem az elektronikus kommunikáció szülötte, sőt valószínűleg nem sokkal fiatalabb, mint maga az írásbeliség és az üzenettovábbítás[6]. A rejtjelezés a kommunikáció módszereivel együtt változott, a papír alapú, majd a különböző elektronikus üzenettovábbítási módszereknek mind megvolt a maguk titkosítási megoldásai. Napjainkban sokkal elterjedtebben és széleskörűbben használnak rejtjelezést, mint bármikor korábban, nemcsak a kommunikáció megsokasodásának köszönhetően, de mert a polgári életben is egyre inkább közkeletűvé válik szerepe. Hogy mennyire így van ez, csak két példával élnék mindennapjainkból: az egyik a szatellit tévé- és rádióadások, ahol a jelet a kalózvevők ellen kódolják, a másik pedig a mobiltelefónia, ahol az egyes beszélgetéseket az illetéktelen lehallgatások ellen védik rejtjelezéssel.

3.4.2 Rejtjelezési módszerek

Manapság az elektronikus kommunikációban a szimmetrikus és aszimmetrikus kulcsú titkosítást használják elterjedten. Mindkét módszerre jellemző, hogy a korabeli rejtjelező eljárásokkal ellentétben – ahol a kódfejtő algoritmust szigorúan titokban tartották – ezen eljárások bárki, de legalábbis sokak számára hozzáférhetőek. Csak a visszafejtéshez szükséges kulcs értéke titkos. A módszerek erősségét az adja, hogy a kulcs ismerte nélkül a kódfejtésnek hatalmas az időszükséglete, ami az eljárás alapjául szolgáló matematikai problémákból és a rendelkezésre álló variációk (kulcsok) óriási számából adódik. Az algoritmusok nyilvánossága a nyílt kódú szoftverfejlesztéshez hasonlóan matematikusok és szoftverfejlesztők százezrei számára teszi lehetővé szerte a világon, hogy az eljárásokat tesztelje. A szimmetrikus és aszimmetrikus kulcsú rendszerek közti fő különbség az, hogy míg a szimmetrikus algoritmus esetében a kódolás és dekódolás ugyanazon kulccsal történik, az aszimmetrikus algoritmus esetében ehhez két különböző (de összetartozó, egy nemzésből származó) kulcsra van szükség. Az aszimmetrikus eljárások sokkal lassabbak, mint a hasonló algoritmikus biztonságot képviselő szimmetrikus eljárások, de több előnyük is van, ami a kulcsok menedzseléséből adódik.

3.4.3 Szimmetrikus kulcsú rejtjelezés

A szimmetrikus (vagy más néven titkos) kulcsú rejtjelezés azon a feltételen alapul, hogy a kódoló és a dekódoló egyaránt ismer valamilyen információt, amelyet mások előtt titokban tartanak. Ennek a titkos információnak a birtokában a kódoló rejtjelezni tudja a nyílt üzenetet, a dekódoló pedig vissza tudja azt fejteni. Harmadik fél a titkos információ hiányában sem megérteni nem tudja a rejtjelezett üzenetet, sem pedig rejtjelezni nem tud hamis üzenetet. A titkos információ a kulcs, amelyből egy adott, „n" főt tartalmazó közösség esetében (ha a közösség minden tagja rejtjeles adatcserét kíván folytatni úgy a másikkal, hogy azt a közösség többi tagja ne legyen képes visszafejteni), a lehetséges összes kapcsolat számára külön kulcsot kell generálni. Ha valakivel adatot kívánunk cserélni a közösségben, akkor a rejtjelezéshez az adott felhasználóval való kapcsolattartáshoz rendelt kulcsot kell felhasználni. Amíg a közösség kicsi, ez nem jelent nagy problémát, de mihelyst nagyobbá válik, a kulcsok száma is kezelhetetlenné növekszik [összesen $n\times(n-1)/2$ számosságúvá, ami tagonként $n-1$ kulcsot jelent]. Az sem evidens, hogy a kulcsot kinek kell generálnia (melyik félnek), és mivel ugyanaz a kulcs közös kezelésben van, két vagy több fél között (akik közös titkot kezelnek), annak biztonságáért is közösen felelnek. Ez nemcsak egymásra utaltságot jelent, de így ha egy kulcs kitudódik, annak felelőse is nehezen megállapítható. Ha minden kulcs csak két fél között van megosztva, a címzett ugyan (majdnem) biztos lehet benne, hogy az üzenetet feladó állította elő és kódolta, de harmadik fél számára ez nem egykönnyen bizonyítható (hiszen a címzett éppúgy képes le-



42. ábra
Szimmetrikus kulcsok egy közösségben

hetett erre). Ha ugyanazon kulcsot több fél között osztjuk meg, hogy csökkentsük a közösségen belüli számukat, akkor a másik ujjunkba harapunk: nemcsak az előbbi bizonyosságot veszítjük el a kódoló személyét illetően, de a kulcsok menedzselését is jelentősen megnehezítjük.

Gondot jelent az is, hogy a kulcsban annak felhasználóinak előzetesen meg kell egyezni. Ez valamilyen kommunikációs folyamatot igényel, méghozzá biztonságosat, hiszen ellenkező esetben a kulcs hozzáférhetővé válna más számára is, vagyis a rejtjelezés későbbi biztonsága sérülne. Mivel a módszer pont egy biztonságos csatornának a megteremtésére irányul, a legtöbb esetben ilyennel nem számolhatunk, tehát a feleknek valamilyen más módon (például személyesen) kell kulcsot cserélniük.

3.4.4 Aszimmetrikus kulcsú rejtjelezés

A szimmetrikus eljárásokkal szemben az aszimmetrikus eljárások esetében minden egyes felhasználónak két kulcsa van, a közösség számától függetlenül. Az egyik kulcsot magánkulcsnak, a másikat nyilvános kulcsnak nevezzük, amely elnevezés a kulcskezelés mikéntjére is utal. A két kulcs ugyanazon kulcsgenerálási eljárásból származik, egy az egyben összetartoznak, de egyik a másikból nem következtethető ki. A magánkulcsot minden felhasználónak titkosan kell kezelnie, nem megismertetve, megosztva azt bárkivel is. A nyilvános kulcsot pont ellenkezőleg, meg kell ismertessük mindenkivel, akivel kommunikálni akarunk (az aszimmetrikus algoritmikusokat éppen ezért nevezik nyilvános kulcsú algoritmikusoknak is). Ha valamely adatot titkosítani akarjuk, úgy, hogy azt csak adott személy legyen képes elolvasni, akkor az ő nyilvános kulcsával kell a rejtjelezést elvégeznünk. Az így kódolt információt ezek után csak a címzett magánkulcsával lehet visszafejteni (ha nem magunk vagyunk az – s így a kulccsal nem rendelkezünk –, akkor mi sem vagyunk képesek erre).

Az előbbi *n* fős közösségnél maradva így összesen n×2 kulcsra van szükség közösségi szinten. Ez azt jelenti, hogy öt felhasználó alatt a szimmetrikus kulcsú rendszer kulcsigénye alacsonyabb (öt felhasználó esetében egyaránt tíz-tíz kulcsra van szükség), de e felett a helyzet az aszimmetrikus eljárások javára egyre előnyösebbé válik[7]. A nyilvános kulcsrendszer legnagyobb előnye mégsem ez, hanem az, hogy a titokért mindig csak egy személy felel, a magánkulcs tulajdonosa. A felek ezért nincsenek egymásra utalva, nem kell megbízniuk a

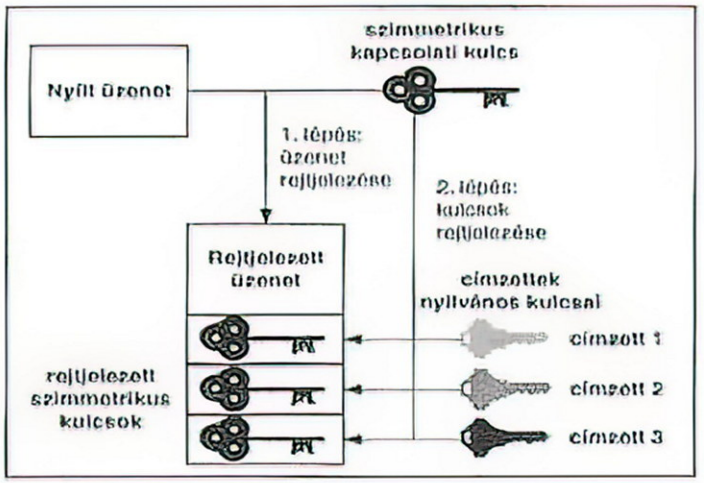
43. ábra
Aszimmetrikus kulcsok egy közösségben

közösség többi tagjában, illetve nincsenek kiszolgáltatva egy, a kulcsot ismerő másik félnek. Ebből következik a módszer másik hatalmas előnye, hogy a magánkulcsok megosztására nincs szükség, a nyilvános kulcsok pedig, következően nyilvánosságukból, hagyományos, kommunikációs módszerekkel is szétoszthatók. A feleknek így nincs szükségük megbízható csatornára vagy előzetes személyes találkozásra, „csak" a kulcs hitelességét, pontosabban az állítólagos tulajdonosához való tartozását kell garantálni.

3.4.5 Üzenetek titkosítása

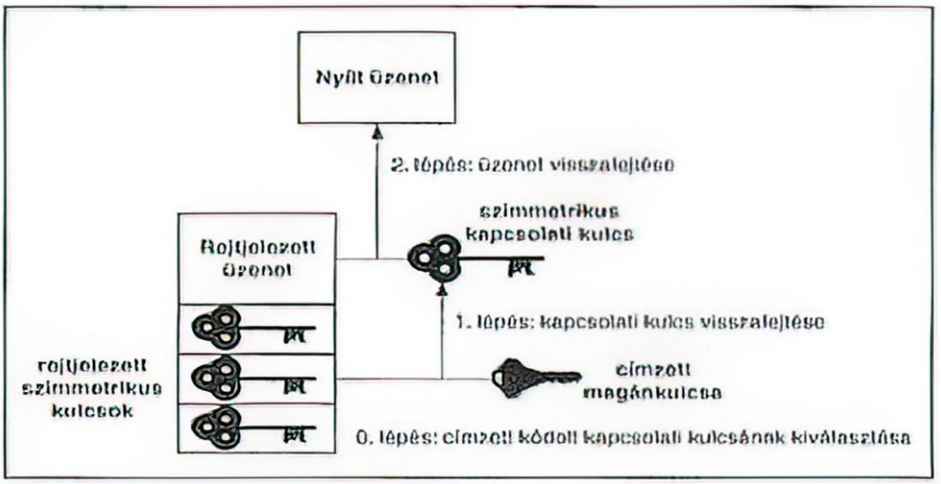
Bár a nyilvános kulcsú algoritmusok felhasználása az említett tulajdonságai miatt jóval előnyösebbnek tűnik, a gyakorlatban mégis gondot okoz a nagyságrendekkel jelentősebb számítási igényből fakadó lassúsága, különösen a nagyobb méretű rejtjelezni kívánt információk esetében. További gond akkor jelentkezik, ha egy olyan üzenetet kívánunk rejtjelezni ezzel a módszerrel, amit több személy részére is el akarunk juttatni. Több címzett esetén ugyanis többször is el kell elvégezni a titkosítást: mindegyik személy részére külön-külön az ő nyilvános kulcsával. Ez nemcsak a számítási teljesítmény iránti igény megsokszorozódását jelenti, de az elküldeni kívánt üzenet is megsokszorozódik, tárolási és kommunikációs többletkapacitást követelve.

Természetesen erre a problémára is született már megoldás, nem is akármilyen. Egyszerű és nagyszerű az ötlet, amivel a szimmetrikus és aszimmetrikus algoritmusok előnyeit egyesítik. Több címzett esetében, sőt egyetlen címzettnél is, ha nagyobb üzenetről van szó, az üzenetet célszerű szimmetrikus eljárással kódolni, majd csak a szimmetrikus kódoláshoz felhasznált kulcsot (mely kisméretű) titkosítani az aszimmetrikus eljárással annyi példányban, ahány címzettünk van. A titkosított kulcs példányai ezek után hozzácsatolhatók az üzenethez, csak annyit kell jelölni, hogy melyik változatot kinek szánjuk (az, hogy a kulcsot minden címzett több példányban is kódolva megkapja, nem okoz biztonsági problémát és jelentős vízfejet). A titkosításra használt szimmetrikus kulcsról így előzetesen nem szükséges megállapodni, az a borítékolásnak is nevezett eljárás keretében kódolt formában az üzenet részévé válik. Gyakorlatilag ezt a módszert használja szinte mindegyik alkalmazás manapság, a címzettek számától és az üzenet méretétől függetlenül.



44. ábra
Üzenet titkosítása több címzett részére

Ez az eljárás (feltételezve, hogy az üzenet hosszabb, mint egy kulcs mérete) nemcsak sokkal gyorsabb, mint a teljes üzenet nyilvános algoritmussal történő rejtjelezése[8], de mivel az üzenet csak egy példányban kerül titkosításra, jóval kisebb méretet is eredményez. Az üzenet titkosítására felhasznált szimmetrikus kapcsolati kulcs (session kulcs) minden üzenetváltás esetében véletlenszerűen kerül kiválasztásra (a küldő által), így ez tovább növeli a rejtjelezés biztonságát.



45. ábra
Több címzett részére titkosított üzenet visszafejtése

Azt szokták mondani, hogy legokosabban akkor járunk el, ha a teljes üzenetforgalmunkat rejtjelezzük, ellenkező esetben csak magával a titkosítás tényével felhívjuk a kommunikáció érzékenységére a figyelmet. A gyakorlatban ennek többlet számítási kapacitása miatt csak ritkán van lehetőség.

3.4.6 Soros és blokktitkosítás

Az információk kódolását végző szimmetrikus rejtjelező algoritmusok két módszer szerint működhetnek: az egyik a soros, a másik a blokktitkosítás módszere. Míg az előbbi folyamatosan, bitenként vagy bájtonként kódolja a nyílt információt, az utóbbi meghatározott méretű (általában 64 bites) szeletekre vágja azt, és az így előállt darabokat külön-külön kódolja. Mivel az utolsó darab mérete eltérhet az egyébként alkalmazottól, azt feltöltő (padding) algoritmusokkal szokták a kívánt méretűre növelni kódolás előtt. A dekódolás a kódolásnak megfelelően ugyanígy blokkonként vagy folyamatos módon történik. A blokktitkosítás esetében a megegyező tartalmú blokkok (ugyanazon kulccsal történő) kódolása ugyanazt a kódolt adatot (kriptoszöveget) eredményezi, a soros titko-

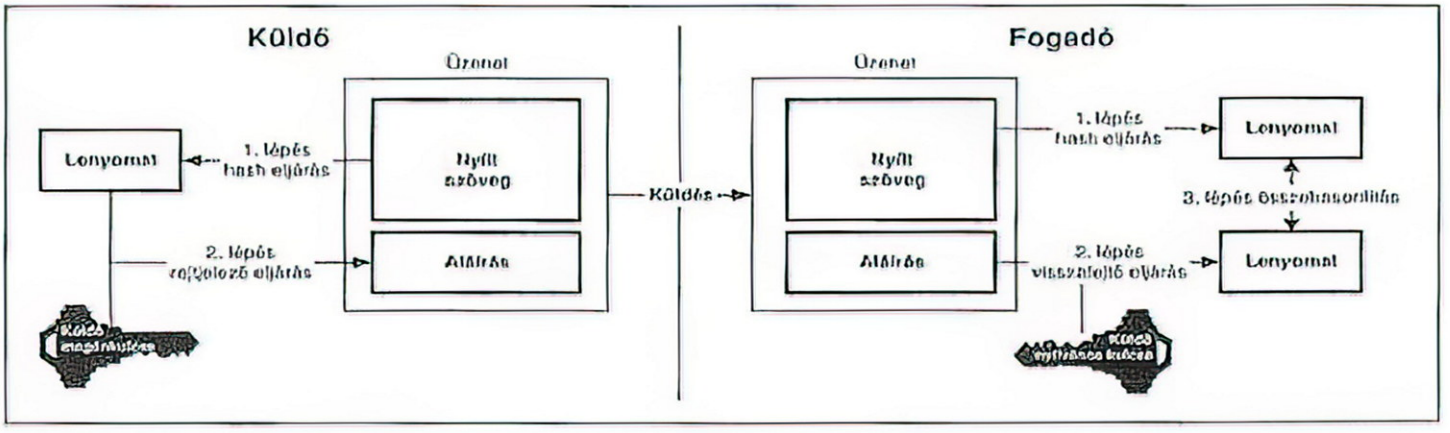
sítás esetében ugyanazon bit vagy bájt kódolása eltérő eredményt ad az egyes alkalmakkor. Míg a soros titkosítást általában kommunikációs hardverberendezésekben alkalmazzák, a blokktitkosítás általánosan elterjedt a különböző szoftverek esetében.

A titkosítást gyakran kombinálják tömörítéssel, ami a még nyílt szöveg rejtjelezést megelőző, előzetes zömítését jelenti (a rejtjelezés megtartja a kódolt szöveg hosszát, míg a rejtjelezett szöveget utólag már nem lehet hatékonyan tömöríteni).

3.4.7 Hogyan lesz a titkosításból elektronikus aláírás

A csattanót, miszerint az elektronikus aláírás maga sem más, mint titkosítás (pontosabban rejtjelezés, hiszen itt a cél nem az amúgy is értelmezhetetlen lenyomat eltitkolása), sajnos már lelőttem korábban. Egy pár gondolat erejéig azonban nem árt visszatérni erre a dologra. Elektronikus aláírás céljára kizárólag az aszimmetrikus, azaz nyilvános kulcsú rejtjelező algoritmusok megfelelőek. A nyilvános kulcsú algoritmikusokat az a tulajdonságuk teszi az elektronikus aláírásra történő felhasználásra alkalmassá, hogy a kulcsok mindig adott személyekhez dedikáltak.

Amikor az algoritmust titkosításra használjuk fel, a kódolást bárkinek végbe kell tudni vinni, de csak a címzett lehet képes annak visszafejtésére. Elektronikus aláírás esetében a cél pont ennek a fordítottja: az aláírást mindenkinek képesnek kell lennie visszafejteni, viszont csak egyvalaki követheti el. A megoldás kézenfekvő: míg a titkosításhoz a címzett nyilvános kulcsát használtuk, a visszafejtéshez pedig a címzett saját magánkulcsát hívta segítségül, addig az elektronikus aláírásnál ennek is a „fordítottját" kell tenni. Az aláíráshoz saját magánkulcsunkat kell felhasználni, az aláírás ellenőrzéséhez pedig a bárki számára hozzáférhető nyilvános kulcsunkat. Mivel a magánkulcsa felett mindenki egy személyben rendelkezik, ezért az elfogadók biztosak lehetnek az aláíró személyében. Ettől válik a magánkulcs aláírás-létrehozó adattá, a nyilvános kulcs pedig aláírás-ellenőrző adattá.



46. ábra Üzenet elektronikus aláírása és ellenőrzése

3.5 Felhasználói hitelesítés

3.5.1 A felhasználói hitelesítés módszerei

A felhasználói hitelesítés célja egy személy vagy egy jogosultság hiteles, kétséget kizáró meghatározása. Erre informatikai rendszerek esetében különböző erőforrások igénybevétele előtt szokott szükség lenni. Az igénylő csak az azonosítását követően használhatja az adott erőforrást (lokális számítógép, kiszolgálógép, nyomtató, internet stb.), illetve annak szolgáltatásait. De nemcsak informatikai rendszereknél van rá igény, hanem például helyiségekbe történő beléptetéskor, szavazáskor, bankszámlanyitáskor és sok más esetben.

Az azonosítás különböző megvalósításai közös alkotóelemekre épülnek:

Tudás alapú:	Ilyen például a jelszó és a hagyományos aláírás stb.
Birtok alapú:	Belépőkártya, párttagkönyv, BKV-bérlet és -jegy stb.
Tulajdonság alapú:	Biológiai jellegzetesség, mint például ujjlenyomat, retina, hang.

Mindhárom azonosítási módszer évezredes múltra tekinthet vissza. A tulajdonság alapú hitelesítést alkalmazzuk nap mint nap, amikor ismerőseinket arcuk, hangjuk alapján felismerjük, a birtok alapján történőt, amikor személyi igazolványunkkal vagy más azonosító okmányunkkal igazoljuk magunkat, vagy mikor lakáskulcsunkkal ajtót nyitunk, és a tudás alapút, amikor PIN-kódunkat megadva mobiltelefonunkba belépünk. A példákból jól látszódik, hogy a legtöbbször nem személyazonosságunkat kell igazolnunk, mindössze jogosultságunkat valamilyen szolgáltatás igénybevételére.

Az egyes rendszerek az említett módszereknek a legkülönbözőbb kombinációit használják. A személyi igazolvány például mindhármat egyszerre: az igazolvány tulajdonlása a birtok alapú azonosítás alapja, a benne lévő fénykép egy biológiai jellegzetesség bizonyítéka, az aláírás pedig egy tudásé (a fénykép összehasonlítása evidens, az aláírás megerősítése pedig szükséges lehet). Nincs általánosan megfelelő módszer, az adott helyzethez optimális megoldás mindig egyedileg határozandó meg. Az optimum keresésében különböző elvek vezérelhetnek a kényelemtől, a költségeken keresztül, a rendelkezésünkre álló rendszerek képességéig.

3.5.2 Jelszó

Az informatikai rendszerek esetében a legelterjedtebb a jelszó alapú hitelesítés. Előnyei közé tartozik az egyszerűsége (egyszerű a kezelése a felhasználók számára), könnyű megvalósíthatósága, elterjedtsége és az, hogy az elfelejtett jelszó könnyen cserélhető. Számos hátránya miatt azonban önálló használata sok esetben nem elégséges. A jelszó könnyen átadható másnak (jó- vagy rosszhiszeműen), könnyen leleshető (például billentyűzetről begépeléskor), ellopható (például trójai faló segítségével vagy az átviteli csatornák monitorozásával), könnyen megfejthető (találgatással, összes változat végigpróbálásával vagy

szótár módszerrel). Statikus jellege miatt a jelszó visszajátszható, újra felhasználható, s mivel a különböző rendszerekben sokszor azonos jelszó kerül felhasználásra, a leggyengébb rendszer feltörésével az erősebb rendszerek is könnyen prédává válhatnak. A felhasználók oktatásával, tudatosságuk kialakításával, különböző szabályok érvényesítésével és kódolással a jelszó biztonsága valamelyest növelhető, de számos veszély így sem zárható ki.

3.5.3 OTP

Az OTP-ről persze mindenkinek a legnagyobb magyar bank jut eszébe, pedig van ennél érdekesebb megfelelője is a rövidítésnek, méghozzá a One Time Password. Ez egy folyamatosan változó jelszót takar, ami a „szimpla" jelszó statikussága mellett annak több más hátrányát is képes kiküszöbölni. Ez működhet úgy is, hogy a felhasználó egy listát kap az általa felhasználható jelszókról, amiket egymás után vagy az időpont függvényében kell megadnia, és a másik oldalon a lista ismeretében ellenőrzik azt. Ugyanennek kicsit modernebb változata, amikor a felhasználót egy kis tokenkalkulátorral szerelik fel, amely a jelszót egy eljárás és a pontos idő függvényében generálja, és kijelzi a képernyőjén. A felhasználónak ezt kell leolvasnia az eszközről, és akárcsak egy hagyományos jelszót begépelnie. A rendszer az eljárás és annak paramétereinek ismeretében szintén legenerálja a jelszót, és összehasonlítja a megadottal (az eljárásnak természetesen paramétere a kérdéses token is, így a generált jelszó nem egyezik meg az egyes felhasználók esetében). Ez a módszer ugyan a hagyományos jelszónál jóval biztonságosabb (nem visszajátszható, ellenáll a szótártámadásnak stb.), annak mobilitását sem korlátozza, ugyanakkor jóval kényelmetlenebb és/vagy költségesebb is. Az eljárás (vagy a jelszavak listája) ismeretében ugyanakkor egy illetéktelen bárkinek kiadhatja magát a tokenhez való hozzáférés nélkül is.

3.5.4 Biometria

Egyre népszerűbbé válnak, és egyre elérhetőbbek a különböző biometrikus azonosítási módszerek. A már nagy múltra visszatekintő ujjlenyomat alapú azonosítás mellett, amit elsősorban bűnözők azonosítására alkalmaznak, a bűnügyi technikusok, orvosok, halottkémek és régészek régóta ismernek egyéb módszereket is. Így például a fogsor vagy DNS[9] alapú azonosítást, amely utóbbit – férfitársaim figyelmébe ajánlom – apasági tesztek ügyében is be szoktak vetni. Ezek az eljárások azonban kevéssé automatizálhatók, és meglehetősen kényelmetlenek (még életben lévő) páciensek számára. Mostanra megjelentek azonban olyan arcfelismerő rendszerek (stadionokban nálunk is használják garázda szurkolók kiszűrésére), retina és hang alapú azonosítást végző megoldások is, amelyek minden kellemetlenség nélkül pillanatok alatt megállapítják valaki kilétét (a felsorolt megoldások természetesen nem személyazonosságot állapíta-

nak meg, csak egy adott mintát hasonlítanak össze adatbázisban szereplő minták halmazával). A biometrikus azonosítás ugyan kiemelkedően megbízható és biztonságos, két nagy hátrányát is meg kell említsem: az első az ára, amely még mindig jóval magasabb, mint más azonosítási módszerek költsége, a másik pedig a felhasználók idegenkedése.

3.5.5 Kombinált megoldások

Amennyiben a felhasználói hitelesítést nagy biztonsággal kívánjuk megvalósítani, akkor a legokosabb, amit tehetünk, hogy különböző módszereket együtt alkalmazunk. Nem mindegy azonban, hogy milyen módszereket párosítunk. Amennyiben az alkalmazott megoldások egymás komplementerei, akkor növelik a hitelesítés megbízhatóságát, de ha a megoldások egymás szinonimái, a megbízhatóság nem feltétlenül emelkedik. Nem lesz erősebb az a rendszer például, amely egy jelszót, majd egy PIN-kódot kér, vagy amely egy személyi és egy tb-kártya felmutatását (mindkettő egyszerre ellopható, vagy egyik a másik birtokában beszerezhető). Ugyanígy nem nyújt valódi (többlet)biztonságot az a weboldalak és telefonos ügyfélszolgálatok által bevett módszer, hogy minél több adatot elkérünk az ügyféltől.

Nemcsak a különböző típusú módszerek lehetnek komplementerek: két biometrikus azonosítás, amely két, alapvetően eltérő módszert használ (például ujjlenyomat és retina), növeli a biztonságot. A legmegbízhatóbb komplementer módszernek azonban mégis a kétkomponensű (más szóval kétfázisú) azonosítás számít, amely az említett három módszer közül kettő különbözőt használ egyszerre. Erre azért van szükség, mert önmagában egyik módszer sem nyújt tökéletes védelmet. A tudás könnyen átadható, a birtok gyakran másolható, a tulajdonság pedig nem teljesen állandó, s ellenőrzése ma még nem elég elterjedt. A kétkomponensű módszerek közül a legelterjedtebb a tudás és birtok párosára alapozott módszerek, például a bankkártya esete, amikor a birtokként bemutatott bankkártya mellé még a PIN-kód ismeretét is bizonyítanunk kell (van háromkomponensű hitelkártya is, amin fénykép is szerepel).

3.5.6 PKI alapú hitelesítés

A kicsit hosszúra nyúlt bevezető után végre következik a lényeg, ami miatt szükségesnek láttam a felhasználói hitelesítés elméletének ezt a nagyon rövid összefoglalását.

A nyilvános kulcsú rejtjelezés (ezért van a címben PKI, és nem elektronikus aláírás), mint egyike a kétfázisú módszereknek, a felhasználói hitelesítésre is kitűnően felhasználható. Optimális biztonságot nyújt, megfizethető költségek mellett. Működése nagyon egyszerű: a személy, aki azonosítani kívánja magát, a magánkulcsa és egy nyilvános kulcsú algoritmus segítségével rejtjelez egy nyílt adatsort (a visszajátszás ellehetetlenítése érdekében általában az azonosí-

tást végzőtől kapott véletlenszerű adatot). Az ellenőrző fél ezt a rejtjelezett adatsort megpróbálja visszafejteni a személy nyilvános kulcsával. Ha a dekódolás sikerül, akkor az bizonyíték a magánkulcs birtoklására. A módszer esetében ez a birtoklás a két komponens egyike. A másik komponens az aktivizáló adat ismerete, ami a magánkulcs használatához szükséges.

A módszer előnye, hogy egyszerűen felhasználható, kényelmes (a sok jelszó helyett csak egy megjegyzésére van szükség), mobilis tud lenni (a magánkulcs hordozhatósága megoldható), dinamikus (a visszajátszásos betörések ellen jól védett), biztonságos (jelszó nem utazik a kommunikációs csatornákon), a biológiai azonosításnál olcsóbb, és hogy jogilag elfogadott. Legnagyobb hátránya, hogy az elvesztett magánkulcs pótlása némi időbe telhet, amely időre a felhasználó hozzáférése az erőforrásokhoz nem megoldható, vagy vissza kell térni egy kevésbé megbízható hitelesítési módszerhez. A PKI alapú hitelesítés kombinálható más módszerekkel is, mint például a Kerberosszal, melyet a **UNIX**-rendszerek mellett a **Windows** is használ a **Windows 2000** operációs rendszertől kezdve, vagy az attribútumtanúsítványokra alapozott módszerekkel. Ezek ismertetésétől megkímélem az olvasót, de egy példát mindenképp megemlítek a PKI alapú hitelesítésre, méghozzá a webszerverek esetét. Az internet esetében a webszerverek hitelesítésére (és az SSL 3-tól a kliensek azonosítására is) ez a PKI alapú módszer az egyetlen alkalmazott. Mivel a hiteles kommunikáció egyre inkább elengedhetetlen, főleg olyan esetekben, ahol fontos és érzékeny információk vándorolnak, mind szélesebb körben terjed a PKI alapú hitelesítések használata.

3.6 Algoritmusok, kulcsméretek és egyebek

Ha kriptográfiáról beszélünk, akár elektronikus aláírással vagy rejtjelezéssel összefüggésben, akkor a legnépszerűbb téma az algoritmusok és a kulcsok erősségének kérdése. Az algoritmusok a kriptográfia sztárjai. Könnyen megjegyezhető, tekintélyt és tudományosságot sugárzó nevük van, a kulcsméretekkel pedig úgy tudjuk egymást überolni, mint más teszi az autójával és a motor löktérfogatával: a BMW 750 helyett itt RSA 1024-et kell mondani, és máris mindenki tudja, mihez tartsa magát. Bár az algoritmusok kétségkívül az eljárások lelkei, s a kulcsméretnek valóban igen nagy jelentősége van, fontosságukat nem szabad eltúlozni. A titkosítási és elektronikus aláírási rendszerek ugyan támadhatók az algoritmus oldaláról is, de adott esetben sokkal egyszerűbb és több eséllyel kecsegtető módszerek is kínálkozhatnak a visszaélésre.

3.6.1 Algoritmus feltörése

Az algoritmus feltörése sok mindent jelenthet. Egy szimmetrikus eljárás esetén például azt, hogy az üzenetet a kulcs ismerete nélkül is képesek vagyunk visszafejteni. Az aszimmetrikus eljárások esetében pedig azt, hogy a magánkulcsot

képesek vagyunk reprodukálni a nyilvános kulcs és egyes üzenetek segítségével. Egy feltörés akkor tekinthető igazán sikeresnek, ha az csekély számítási teljesítményt igényel (azaz nem kíván hatalmas befektetést), viszonylag gyorsan eredményt ad, s bármikor megismételhető egy másik rejtjelezett üzenettel vagy magánkulccsal. Egy ebben az értelemben sikeres feltörés az algoritmus egészének alkalmazhatóságát sárba döntheti, de ehhez a kódoláshoz felhasznált matematikai probléma inverzére kéne hatékony aritmetikai megoldást találni. Mivel a kriptográfiában felhasznált matematikai problémák évszázadok óta ismertek, s eddig minden matematikusnak beletört a bicskája a megfejtésbe, kevéssé valószínű, hogy egyik pillanatról a másikra azzal kellene szembenéznünk, hogy valaki felfedezte azt, amit talán jobb lett volna nem felfedezni.

3.6.2 És ha mégis?

Ha egy erre vonatkozó felfedezés mégis megszületne, és napvilágra kerülne, az szerfelett nagy galibát okozna. Nem is az lenne a legnagyobb gond, hogy a kérdéses eljárást alkalmazó szoftverek és hardverek hirtelen hasznavehetetlenné válnának (legalábbis biztonságuk lenullázódna), hanem az, hogy a korábban a velük védett adataink egy pillanat alatt ott állnának pőrén, illetve lemeztelenít-hetően a világ szeme előtt. A titkosított adatokat az analízis ismerője visszafejthetné, az aláírások valódiságát pedig bárki megkérdőjelezhetné, megtételüket bárki letagadhatná. Ez sem jelentené azonban a nyilvános kulcsú kriptográfia halálát. Mind szimmetrikus, mind aszimmetrikus eljárásból több is ismert, így az egyik algoritmus kiesése esetén pótolható lenne egy másik algoritmussal. Szándékosan nem alkalmaztam a „problémamentesen" jelzőt, mert ez azért nem lenne egy sétagalopp: a meglévő szoftvereket azok fejlesztőinek át kellene alakítani, a felhasználóknak a frissítést le kellene tölteniük, a meglévő kulcsok helyett újakat kéne előállítani, azokat újra teríteni kéne a partnerek között, és a korábban titkosított és aláírt dokumentumokat újra titkosítani és aláírni lenne szükséges, immár az új eljárással. Elsősorban nem emiatt, hanem a széles körű kompatibilitás és a többféle elvárásnak való megfelelés miatt egyes szoftverekbe eleve több szimmetrikus és aszimmetrikus algoritmust is beépítenek, vagy alkalmassá teszik őket algoritmusok utólagos (plug-in-szerű) betáplálására. Az ilyen megoldások egy algoritmus szomorú elhalálozása esetén – a gyászidőszakot mellőzve – azonnal képesek átállni egy másik módszerre.

3.6.3 Támadások, kriptoanalízis

Léteznek ugyanakkor más, az algoritmus egészére ugyan kevésbé veszélyes, de egyes megvalósításokat ugyanígy fenyegető módszerek. Ismertek például szinte minden algoritmus ellen sikeres támadások, amelyek az algoritmus bizonyos gyengeségét, sajátosságát használják ki. Ezek sokszor csak különleges helyzetekben, bizonyos együtthatók együttállásakor működnek, és ami még fonto-

sabb: lehet ellenük védekezni. Az algoritmus, illetve annak szoftveres megvalósítása ezeket a gyenge helyzeteket automatikusan ki tudja zárni. Léteznek azonban olyan támadások, amelyeket nem lehet előre kizárni, például azok, amelyek a nagyon sok titkosított üzenet elemzésén alapszanak. Védekezni azonban ezek ellen is lehet, mint azt látni fogjuk.

A kriptoanalízis a kriptográfia azon része, amely tudományos elemzéseket végezve ilyen gyenge pontok felderítésével foglalkozik (nemcsak az algoritmusok, de a protokollok, szoftverek és hardverek esetében is), s azok ellen támadásokat dolgoz ki. A kriptoanalízis ugyanakkor nem a kriptográfia ellensége, annak eredményeit megismerve a kriptográfusok (akik egyébként sokszor csak nappal kriptográfusok, éjjelre átalakulnak „kriptoanalitikussá") új módszereket tudnak kidolgozni az algoritmus megerősítésére. Így ha új támadási módszerre derül fény, jó eséllyel annak megoldására se kell sokat várni.

3.6.4 Nyers erő és egyéb huncutságok

Az egyes felhasználókat és felhasználásokat s a rejtjelezett információkat így nem a kriptoanalízis fenyegeti a legjobban, hanem egyéb, nem algoritmikus támadási módszerek, amelyek közül egy, a machósága folytán legtöbbet emlegetett nyers erő módszere. A nyers erő azt jelenti, hogy „ész nélkül" nekimegyünk a rejtjelezett szövegnek, és minden egyes lehetséges kulcsot végigpróbálva megkíséreljük visszafejteni azt. A módszer előbb-utóbb eredményt hoz. Kisebb méretű kulcsok, azaz kevesebb variációs lehetőség esetén hamarabb, nagyobb méretű kulcsok esetében utóbb[10]. A manapság használt, biztonságosnak tekinthető kulcsméretek esetében ez az utóbbi a világ legerősebb számítógépe számára is évmilliókat, ha nem évmilliárdokat jelent.[11] Nem szabad azonban figyelmen kívül hagyni, hogy a technika fejlődik. Bár a számítási kapacitások törvényszerű másfél évenkénti duplázódásával[12] az évmilliárdok még sokáig nem csökkennek elérhető közelségbe, egy esetleges felfedezés[13], amely a jelenleg rendelkezésünkre álló számítási kapacitást nagyságrend(ekk)el meghaladja, itt is alapvetően új helyzetet teremthet.

Ahogy a bankoknak sem szabad elfeledkezni a megannyi új szofisztikált megkopasztási módszer mellett a falbontás és a robbantás ősi, de hatékony technikáiról, ugyanígy a kriptográfia felhasználói sem téveszthetik szem elől a kriptoanalízisnél kevésbé kifinomult, de a nyers erőnél kevesebb befektetést igénylő módszereket. Meglehetősen kezdetleges, de igen célravezető módszer lehet például a kulcs ellopása vagy egyéb, fondorlatos módon történő megszerzése. Az ez ellen való védekezésről a későbbiekben még ejtünk egy-két szót.

Mindent összevéve és összevetve, ha egy már régóta használt és kifinomult algoritmust megfelelő kulcsmérettel használunk, s algoritmusunk megvalósítása tudományos igénnyel, az ismert gyenge pontok kizárásával történt, nincs mitől félnünk. De azért résen lenni, mint a jó cserkésznek, ilyenkor sem árt!

3.6.5 Hash- és feltöltő algoritmusok

A hash-algoritmusok esetében a visszafejtéstől nemigen kell félni, hiszen a függvény egyirányúsága elég könnyen biztosítható. Az egyszerű logikai XOR (kizáró vagy) művelet[14] például kitűnően megfelel ennek a követelménynek. A hash-algoritmusok esetében elsősorban nem is ez, hanem az ütközésmentesség és a lavinahatás együttes és hatékony megvalósítása szokott fejtörőt jelenteni a matematikusoknak.

Jelenleg két hash-algoritmust használnak elterjedten: az MD5-öt[15], amely egy 128 bites kódot generál az üzenethez és a 160 bitet generáló SHA-1-et, amely a Digital Signature Standard része. Az MD5 eljárásnak ismertek olyan teoretikus gyengeségei, ami miatt az SHA-1 algoritmus felhasználása egyre inkább előtérbe került.[16] Nem használják széles körben, de érdemes megemlíteni még az európai szabvány[17] RIPEMD-160 eljárást, melynek bithossza a nevébe van foglalva.

A feltöltő algoritmusokra akkor van szükség, ha az aláíró algoritmus hosszabb adatsoron végez műveletet, mint amit a lenyomatolás eredményez. Az alkalmazott módszerek jobbára a PKCS #1 (RFC 2313), illetve az ISO/IEC 9796-2 szabványokban leírt ajánlásokat követik.

3.6.6 A DES algoritmus

A DES algoritmus a szimmetrikus algoritmusok nagy öregje. Az IBM kutatólaboratóriumaiban még a '70-es évek elején Lucifer néven kifejlesztett eljárás továbbfejlesztett változata a keresztségben a sokkal kevésbé fantáziadús Data Encryption Standard nevet kapta. Az 1977-es USA-beli szabványosítás és az amerikai kormányzat által „hivatalos" rejtjelező eljárásként való elismerés gyakorlatilag egyeduralkodóvá avatta az algoritmust. A módszer a Feistel-féle transzformáción alapul – ha ez bárkinek is mond valamit. Az 56 bites kulccsal[18] dolgozó DES blokktitkosító algoritmus (64 bites blokkokat kódol 64 bites kódokká), de mivel igen gyorsan működik mind a kódolás, mind a dekódolás során – különösen hardveres megvalósítás esetén –, eredményesen használják soros titkosítás céljára is, például kommunikációs berendezésekben. Bár évtizedekig használták eredményesen[19], a DES algoritmus mára kifáradt. Az egyre nagyobb számítási teljesítmények megjelenésével és olcsóbbá válásával az 56 bites kulcsméret feltörése reális lehetőséggé vált (elérhető számítási kapacitás aktivizálásával). A kulcsméret növelésével ez az időszak jelentősen megnövelhető[20].

3.6.7 Egyéb szimmetrikus algoritmusok

A DES algoritmus használata éppen ezért ma már senkinek sem ajánlható jó szívvel, legalábbis eredeti formájában nem. Van viszont a DES algoritmusnak számos továbbfejlesztett változata, egy egész takaros fészekaljravaló, amelyek

többé-kevésbé orvosolják ősük gyengeségeit: CRYPT(3), DESX, GDES, RDES, kulcsfüggő S-dobozos DES, alternatív S-dobozos DES, DES-EDE stb. (lásd bővebben: [4]). A gyakorlatban nem ezek a tudományos, hanem az izomból dolgozó úgynevezett 3DES (triple-DES) módszer terjedt el, amely egyszerűen csak megtöbbszörözi az algoritmus használatát, három különböző kulccsal egymás után rejtjelezve az eredeti nyílt szöveget, illetve az előző rejtjelezés eredményeként előálló kódolt szöveget (a visszafejtés ennek a fordítottja, háromszori dekódolás visszafele a megfelelő kulcsok felhasználásával)[21]. Sokkal kevésbé terjedtek el a szimmetrikus rejtjelezés egyéb módszerei, azok erősségei ellenére is. Az 1992-ben kifejlesztett 128 bites kulcsot alkalmazó IDEA (International Data Encryption Algorithm) algoritmus sokak szerint a legbiztonságosabb ezek közül. A 64 bites kulcsot alkalmazó, 1993-ban Kanadában kifejlesztett CAST algoritmus eddig szintén ellenállt minden feltörési kísérletnek. Az RSA cég által kifejlesztett RC2 és RC4 eljárásokat használja többek között a **Netscape** böngészője. Az RC2 egy blokktitkosító eljárás, az RC4 soros titkosítási algoritmus.[22]

A szimmetrikus algoritmusokról általában is elmondható, hogy 40 bites változatait kifejezetten gyengének, 128 bites változatait pedig megbízhatónak tartják. Nem véletlenül, hiszen a 128 bites kulcs generálásakor 2^{128} számú lehetséges eredmény létezik.[23] Ez nagy szám. Nagyon nagy szám. Még pontosabban: irdatlanul baromi nagy szám. Annyira nagy, hogy nyers erő alkalmazásával a feltöréshez (a helyes kulcs megtalálásához) több időre volna szüksége a világ ma rendelkezésre álló összes számítógépének, mint a világegyetem eddigi léte.[24]

3.6.8 AES

Az amerikai National Institute of Standards and Technology (NIST) e módszerek ellenére 1997 szeptemberében pályázatot írt ki a DES leváltására alkalmas titkosítási szabvány kidolgozására. Olyan algoritmus kidolgozása volt a cél, amely újabb évtizedekre meghatározhatja a biztonságos kommunikáció kriptográfiai alapjait. Az Advanced Encryption Standard (AES) címért folyó viadal döntőjébe öt megoldás jutott: az IBM által benyújtott Mars, az RSA által kidolgozott RC6, *Bruce Schneier*[25] Twofish algoritmusa, az internacionális koprodukcióban előállt Serpent, valamint *Joan Daemen* és *Vincent Rijmen* közös munkája, a „Rijndael" algoritmus. Három évvel a pályázat kiírása után, kivédve a világ minden tájáról próbálkozó kriptoanalitikusok, hackerek és titkosítási szakértők valamennyi támadását, ez utóbbi lett a győztes.[26] A pályázati kiírás követelményeinek megfelelően az algoritmus támogatja a 128, a 192 és a 256 bites kulcsok alkalmazását. A NIST a Rijndaelt amerikai adatfeldolgozási szabványnak javasolta, s 2001 nyarától az eljárás az USA-ban szabványos algoritmus polgári felhasználásra. Az új eljárást felhasználó szoftverek és hardverek azóta már kereskedelmi forgalomban is elérhetők.

3.6.9 RSA

A messze földön legismertebb nyilvános kulcsú algoritmus az RSA[27], mely a feltalálók (*Ronald Rivest*, *Adi Shamir* és *Leonard Adleman*) nevének kezdőbetűiből kapta elnevezését, Az urak a Massachusetts Institute of Technology munkatársaiként 1978-ban dolgozták ki az eljárást, mely a faktorizáció problémáján alapul. Az eljárás, amely az első nyilvános kulcsú algoritmus volt, azóta de facto szabvánnyá vált a világon. 1991-ben de jure is szabvány lett ISO 9796 néven, 2000. szeptember 20-án pedig lejárt a szabadalmi védettsége, így bárki legálisan írhat az RSA algoritmusokra alapuló titkosítási szoftvereket és digitális aláírást generáló programokat. A módszer lényege a prímtényezőkre bontás (más néven faktorizálás) nehézsége: míg prímszámok szorzása meglehetősen egyszerű feladat, addig az így előállt szorzatból, annak prímtényezőit visszaszámolni már korántsem[28]. Ha mindez elég nagy prímszámokkal történik, akkor gyakorlatilag lehetetlen[29], márpedig a gyakorlatban 10^{100}-nál nagyobb prímszámokat alkalmaznak (az eljárás igazi nehézsége éppen ez, a megfelelő nagyságú és erősségű prímszámok megtalálása). Az algoritmus a kulcspár előállításához használja a prímszámokat (nem a kódoláshoz és dekódoláshoz), s ezért a magánkulcs visszafejtéséhez, vagyis az eljárás feltöréséhez faktorizálás szükséges[30]. Bár az eljárás ellen több támadás is ismert, ezek ellen lehet védekezni a prímszámok és a kulcsgenerálás egyéb paramétereinek gondos kiválasztásával. Az eljárás blokkok rejtjelezésével működik, kulcs- és blokkméretként többnyire kettő hatványait felhasználva (512, 768, 1024, 2048 bit)[31]. Az 1024 bit hosszú kulcsot akár katonai célokra is megfelelőnek tartják. Az RSA algoritmus mintegy ezerszer lassabb, mint a DES.

3.6.10 A faktorizálás

Az RSA algoritmus esetében a hagyományos nyers erő módszer, az összes lehetséges kulcsvariáció végigpróbálása reménytelen feladat a kulcs jóval nagyobb méretéből fakadóan. A nagyobb kulcsméretre éppen azért van szükség, mert az összes kulcs végigpróbálása felesleges is lenne: a nyilvános kulcs és a magánkulcs között fennálló matematikai összefüggések kihasználásával a keresés jelentősen egyszerűsíthető.

Itt is van azonban mód brutalitásunk kiélésére, de a nyers erő módszere itt a faktorizálást jelenti. Nem csekély számítási teljesítményt és memóriát kell azonban felmutatni annak, aki például egy 1024 bites számot akar prímtényezőkre bontani. Ugyan 1999-ben sikerült az 512 bites RSA kulcs faktorizálása egy elosztott számítógépes rendszer segítségével[32], ugyanezen számítási teljesítménnyel az 1024 bites kulcs faktorizálása – becslések alapján – ennél mintegy hétmilliószor több időt és 2650-szer több memóriát igényelne[33]. A másik oldalról megközelítve: ha az 512 bites faktorizálás idejét akarnánk megismételni, akkor mintegy 1,4 milliárd számítógépre lenne szükségünk az elosztott hálózat-

ban úgy, hogy mindegyik gép egyenként 170 gigabájt memóriával rendelkezzen, és a hálózat áteresztőkapacitása a ma elérhető sokszorosa legyen. Ha ez meglenne, akkor már csak egy szuperszámítógépre van szükség, mintegy hat terabájt memóriával és hetvenmillió szabad munkanappal. Ragozhatnánk még ezt egy darabig, de úgy érzem, felesleges. Akárhogy is variálunk a processzorokkal és memóriákkal, nem jutunk valódi esély közelébe[34]. Az 1024 bites kulcs faktorizálása – remélem, meggyőző voltam – ma még képtelen vállalkozás[35].

3.6.11 DSA

A DSA algoritmus az RSA legnagyobb konkurense a digitális aláírás-területén (az eljárás titkosításra és kulcsszétosztásra nem alkalmas). A módszert a National Security Agency[36] fejlesztette ki, és az NIST törzskönyvezésével 1994-ben vált az USA digitálisaláírás-szabványává[37]. A módszer az RSA-hoz hasonlóan prímszámokkal operál, de vele ellentétben nem a faktorizálás, hanem a diszkrét logaritmus problémáján alapul. A módszert az NSA szabadalma védi, de nem is ez a legnagyobb „probléma" vele, hanem maga a fejlesztő szervezet kiléte. Vannak, akik attól tartanak, hogy a szervezet ismer olyan módszert, vagy beleépített olyan kiskaput az eljárásba, mellyel – ha érdeke úgy kívánja – vissza tud élni. Mivel az ügynökség elsődleges célja a lehallgatás, s az aláírás hamisításához nem fűződhet valódi nemzetbiztonsági érdek még az USA-ban sem, én a kétkedőket a módszer használatára bátorítanám. Egyesekben aggályokat kelthet az is, hogy a módszer túl új, és még időre van szükség a biztonságáról való meggyőződéshez. A kevésbé óvatosak inkább azt hangsúlyozzák, hogy bár a módszer mintegy huszonötször lassabb az ellenőrzés területén az RSA-nál (az aláírás közel egyforma sebességű), annál kevesebb (ismert) támadható pontja van, s így megbízhatóbbnak tekinthető. Mindezek ellenére és miatt az algoritmus szakmai körökben általánosan elfogadott. A DSA-t kezdetben 512, manapság egyre inkább 1024 bites kulcsmérettel használják.

3.6.12 ECDSA

Az ECDSA algoritmus a DSA algoritmus egyik variánsa, mely az elliptikus görbék (innen az EC, azaz Elliptic Curve) esetében fellépő diszkrét logaritmus problémáját hasznosítja. Az ECDSA algoritmus legnagyobb előnye a DSA-val és RSA-val szemben, hogy kisebb kulcsok felhasználásával is elérhető ugyanaz a biztonsági szint, s ezen eljárásoknál gyorsabb mind az aláírás elkészítése, mind ellenőrzése terén. Ezért megvalósítása könnyebb és eredményesebb lehet limitált memóriával rendelkező eszközök és nagy aláírási teljesítményt felmutatni képes hardverek esetében. Az IEEE és az ANSI a pénzügyi szervezetek részére szabványosította ezt az eljárást ANSI X9.62 néven. Az eljárás, ellentétben nem elliptikus rokonával, titkosításra is alkalmazható.

3.6.13 Kulcshosszak

Az algoritmusok leírásánál említettem, hogy az alkalmazott kulcshosszak az algoritmus nyers erővel történő visszafejtése tekintetében határozzák meg az algoritmus erősségét. Ez voltaképpen mindegyik algoritmusra igaz, azok különbözőségei ellenére is. Azt is látni kell éppen ezért, hogy a kulcshossz növelése csak ettől véd, egyéb támadásoktól nem! Nem evidens azonban, hogy milyen kulcshossz milyen erősséget képvisel, különösen nem az egyes módszereket összehasonlítva.

Az alábbi táblázat ezért álljon itt példaként az egyes eljárások esetében alkalmazott kulcshosszak „egyenerősségére". A táblázat a szimmetrikus kulcsú, az elliptikus görbére és az RSA eljárásra alapozott rejtjelezés erősségét hasonlítja össze, abból kiindulva, hogy a feltörésre tízmillió amerikai dollár áll rendelkezésre (megadott alapvetésekkel, szigorúan elméleti esetőségeket is számításba véve, a visszafejtés költséghatékonysága alapján)[38]:

Szimmetrikus	Elliptikus görbe	RSA	Időszükséglet	Töréshez szükséges erőforrás
56 bit	112 bit	430 bit	5 perc	100 000 PC
80 bit	160 bit	760 bit	50 év	4300 munkaállomás egyenként 4,4 gigabájt memóriával
96 bit	192 bit	1020 bit	3 millió év	Ha lennének 170 gigabájt memóriával rendelkező PC-ink + egy 6 TB memóriás szuperszámítógépünk
128 bit	256 bit	1620 bit	10^{16} év	Ha 120 TB-ra elég lenne a tízmillió dollár

3.6.14 Blokkos rejtjelező algoritmusok üzemmódjai

Előfordulhat, hogy figyelmesebb olvasóim előbb-utóbb, termékleírásokban, szabványszövegekben találkoznak a CBC, ECB, CFB, OFB stb. kifejezések valamelyikével (leginkább az elsővel, például Triple DES-CBC mód, 168-bit; RC2-CBC mód 128-bit). Ezek kriptográfiai technikákat (más szóval: üzemmódokat) jelentenek, vagyis azt, hogy a blokktitkosító algoritmus miképp működik a nyílt szöveg egyes blokkjain. Az ECB (Electronic Code Book) eljárás a legkézenfekvőbb, legegyszerűbb módszert használja: az egyes blokkokat egymástól függetlenül, ugyanazzal a kulccsal képzi le. Ennek a módszernek számos gyengesége van, legfőképpen az, hogy a kódolt szöveg könnyen manipulálható (az egyes blokkok kicserélhetők, elhagyhatók, beszúrhatók úgy, hogy

azt a visszafejtő eljárás nem észleli). Az elektronikus kódkönyv kifejezés maga is arra utal, hogy elviekben összeállítható egy olyan kódkönyv, ami az összes lehetséges nyílt és titkosított szövegblokk összerendelését tartalmazza. Noha ez 64 bites blokkméretnél 2^{64} számú variációt jelent[39], ami merőben elméletivé alakítja ezt a lehetőséget, a gyakorlatban is lehetséges ezt a gyengeséget kihasználva, mindössze pár ismert nyílt és titkos blokkpárra alapozva észrevétlenül átalakítani a titkos szöveget.

Ezt az Achilles-sarkot orvosolja a többi üzemmód, amelyek mind valamilyen visszacsatolást alkalmaznak, azaz az egyes blokkok kódolása során mindig felhasználnak valami olyan információt is, ami az adott blokktól független, vagyis ugyanazon blokk többször történő kódolása mindig más eredményt ad. A CBC (blokkláncolás) technikájánál ez az információ az előzőleg kódolt blokk maga, ami megakadályozza, hogy az egyes blokkokat észrevétlenül manipulálják.

3.6.15 Véletlenszám-generálás

Van abban valami diszkréten perverz, hogy a véletlenszám-generálás témája az algoritmusok fejezetben kap helyet, hiszen hogyan lehetne bármi is véletlen, ha aritmetikai algoritmus állítja elő? De mielőtt erre válaszolnánk, tisztázzuk, miért is van szükség véletlenre a kriptográfiában.

A rejtjelező algoritmusoknál már utaltam rá, hogy „választunk" egy prímszámot, vagy „választunk" valamilyen más értéket. De hogyan választunk? Természetesen véletlenszerűen, hiszen ellenkező esetben, vagyis ha a választás bármilyen elv szerint történne, az elv ismeretében a rejtjelező algoritmus annyit érne, mint halottnak a csók. Márpedig a mi algoritmusunknak úgy kell működnie, hogy az elv ismeretében is biztonságos legyen, sőt pont attól biztonságos, hogy az elvet ismerik, és annak biztonságáról véres fejjel visszavonult matematikusok hada tanúskodik.

Itt jön be a véletlen szám generálásának jelentősége, amelyet természetesen algoritmikus úton nem lehet produkálni. Vannak ugyan véletlenszám-függvények (a programozók bizonyára jól ismerik őket), de ezek csak álvéletlen számok állítására képesek[40]. Ez azt jelenti, hogy csak közelről nézve véletlenek, ha megfelelő távolságról nézzük a véletlennek nevezett számok sorozatát, akkor felfedezhető bennük az ismétlődés. Bármilyen sztratoszférikus magasságba kell is emelkedni ezért a felismerését, egy komoly kriptográfiai rendszernek ez a megoldás smafu[41].

A kriptográfiai biztonság minimum azt követeli meg, hogy az álvéletlen számot előállító algoritmus kezdőértéke legyen valódi véletlen. Aki használt már valamilyen titkosító- vagy aláírórendszert, és maga generálta a kulcsait, az emlékezhet arra, hogy a program érthetetlen módon valamilyen különleges produkciót kért tőle: vagy azt, hogy ész nélkül húzogassa az egerét föl-alá, vagy hogy összevissza csapkodja a billentyűzetét. Ez azt a célt szolgálta, hogy ebből a cselekvéssorozatból a rendszer előállítson egy valódi véletlent, általában egy álvéletlen algoritmus kezdőértékeként (a program ilyenkor nemcsak a lenyo-

mott billentyűk értékét vagy az egér mozgásának irányát figyeli, de a mozgatás sebességét is, illetve a nyomva tartás és a szünetek pontos idejét is). Ennek a módszernek az eredménye nemcsak statisztikailag (annak a jó álvéletlen algoritmus is ellenáll), de bármilyen furmányos elemzéssel sem jósolható meg.

Az igazi, kőkemény kriptográfusok azonban csak a valódi véletlenben bíznak. Ha valódi véletlen számok bármilyen hosszú sorozatát vesszük, nem találunk benne ismétlődést, nézzük azt akár a világegyetem másik feléből is. A sorozatnak ugyanis egyik tagja sem következik a másikból, köztük semmilyen oksági vagy algoritmikus kapcsolat nincsen. Valójában ilyen valódi véletlen sorozatot előállítani nem is annyira nehéz, mindössze valamilyen analóg bizgentyű kell hozzá. Ott van például minden számítógépben a hálózati tápfeszültség, aminek a változásai teljességgel esetlegesek, de felhasználható bármelyik tranzisztor termikus zaja is. Sajnos ezek egy átlagos PC esetében szoftveresen, bármilyen mélyre ereszkedjünk is a gépi kódok dzsungelében, nem elérhetők.

3.7 Kriptoprotokollok

A protokoll szó eredeti jelentése szerint diplomáciai képviselők egymással való hivatalos érintkezését rögzítő szabályok összessége[42]. Az informatikusok szerint a protokoll a hálózati kommunikáció szabályait írja le. A kriptológusok szerint viszont a protokoll olyan, szigorúan szabályozott lépések sorozata, amelyet betartva az alkalmazó két vagy több fél biztonságban tudhatja kommunikációját. A kriptoprotokollok rendszerint kriptográfiai algoritmusokat használnak ennek teljesítésére. Vagyis a kriptoprotokoll algoritmusokból építkezik, és komplexebb biztonsági igényeket képes kielégíteni, mint az algoritmusok önmagukban. Hogy egy egyszerű példával éljünk erre: a titkosított levelezés egy protokoll, mert megmondja, hogy az egyik félnek kódolni, a másik félnek pedig dekódolni kell, hogy mi e műveletek sorrendje, és milyen kulcsokat kell alkalmazni hozzá. Ennél persze számtalan összetettebb protokoll is létezik, amelyek egész bonyolult mechanizmusokat, cselekvéssorokat is biztosítani képesek, több résztvevő között is.

A kriptográfiai protokollok sokkal kevésbé ismertek, mint az algoritmusok, pedig protokoll nélkül nem hasznosítható egyetlen algoritmus sem, s a protokoll hibája éppúgy romba döntheti a biztonságot, mint az algoritmusé. A kriptoprotokollokat, akárcsak az algoritmusokat, matematikusok, kriptográfusok dolgozzák ki, az elméletek ajánlásokként és szabványokként öltenek testet, majd végső soron szoftverekbe építve materializálódnak.

3.7.1 A protokollok jellemzői

A protokoll – mondhatni – olyan, mint a szerelem: legalább két résztvevő szükséges hozzá (ezért nem nevezzük az elektronikus aláírást önmagában protokoll-

nak, bár több algoritmust használ fel). Ennél több hasonlóság azonban a lelkivilággal nincsen. Ellentétben például a szerelemmel, a protokoll több résztvevővel is könnyedén megbirkózik (amihez az érzelmi életben elég erős tehetség kell). A protokollok lépésekből állnak, amely lépéseknek jól definiáltnak, egyértelműnek, ismertnek és elfogadottnak kell lenni minden résztvevő oldaláról. A jó protokoll ezenkívül teljes, azaz minden elképzelhető helyzetre tartalmaz hathatós intézkedést.

3.7.2 A kriptoprotokollok típusai

A kriptográfiai protokolloknak három fő típusa ismert, amelyek eltérő helyzetekben alkalmazhatók.

A döntőbírós protokoll esetében a részt vevő felek mellett egy döntőbíró is helyet kap, aki a protokoll során valamit garantál. Az életben azok a helyzetek hasonlíthatók hozzá, amikor közjegyzőt vagy ügyvédet veszünk igénybe. Tulajdonképpen a mégoly szimpla vásárlás művelete is igényelhetne döntőbírót (mint ahogy nagyobb összegek, jelentősebb ügyletek esetében igényel is): ha vásárolni akarok, mondjuk, egy bajuszkötőt, bemegyek a vegyesboltba, és kiválasztom a pult mögötti megfelelőt, rámutatok s azt mondom a pénztárosnak, hogy ezt kérem. Mire a pénztáros azt mondja három pengő. Ha ebben a helyzetben elkezdenénk vitatkozni azon, hogy ki adja oda előbb azt, ami még jelenleg az övé: én a három pengőmet vagy a boltos a bajuszkötőjét, akkor lenne szükség egy döntőbíróra, akiben mindketten megbízunk. Mindketten odaadnánk neki a cserealapunkat, én a három pengőt, a boltos meg a bajuszkötőt, a döntőbíró pedig a kettőt megcserélné, és kiosztaná mindenkinek a megfelelőt. Letéti számlák alkalmazásával a bankok hasonló szerepet látnak el az üzleti életben.

Az igazságosztó (némiképp bevettebb formában: ítélkező) protokoll az, amelynek a valós életben a bíróság alkalmazása felel meg. Ebben az esetben a protokoll azt biztosítja, hogy ha a részt vevő felek között vita merülne fel, akkor utólag képes tisztázni azt, hogy kinek van igaza.

A leghasznosabb protokoll az önműködő, amelyik esetében a protokoll ítélkező vagy döntőbíró bevonása nélkül automatikusan garantálja a biztonságot. Ebben az esetben a „döntőbíró" maga a kriptográfiai rendszer, amely a részt vevő felek előtt egyértelművé teszi, ha a protokollba valaki beavatkozna vagy az nem fejeződne be.

3.7.3 Pár érdekes kriptoprotokoll

Az egyes algoritmusok kapcsán a legalapvetőbb kriptoprotokoll már meg lett említve, amikor az algoritmus felhasználását demonstráltam. Ez az üzenetküldés protokollja, aminek három típusát is vettük már: a szimmetrikus és aszimmetrikus algoritmusokon alapuló protokollokat és az ezek kombinációjára épü-

lő hibrid protokollt. Egyszerűségük folytán mindenki ezeket szokta használni demonstrációs célra, s ezért a tapasztalatlan olvasónak az az érzése támadhat, hogy az elektronikus aláírás és rejtjelezés másra nem is alkalmas, mint üzenetküldés biztosítására. Pedig dehogy.

Létezik protokoll például pókerezéshez, ahol a feladat az, hogy az osztó és az egyes játékosok ne ismerhessék meg a többi játékos lapjait (csak akkor, amikor a tétek megtétele után felfedik azokat), s a játékosok biztosak lehessenek abban, hogy a felfedett lapok valóban azok, amik kiosztásra kerültek. Ez persze csak játék, de létezik protokoll biztonságos választási rendszer kialakítására is, ami biztosítja, hogy csak a választásra jogosultak szavazhassanak, ők is csak egyszer, minden szavazó ellenőrizhesse, hogy a szavazata bekerült-e az eredménylistába, senki se állapíthassa meg, hogy az egyes szavazók kire szavaztak, s természetesen senki fia ne változtathassa meg másnak a szavazatát, de mindenki megtudhassa, hogy ki szavazott és ki nem. Vagyis mindent tud, amit egy jó szavazási vagy választási rendszernek tudni kell.

Szintén különböző protokollok biztosítják a nem biztonságos hálózaton keresztül történő biztonságos fizetés lehetőségét. Nem a bankkártya számának titkosítására gondolok itt, hanem azokra a módszerekre, amik lehetővé teszik, hogy a számlatulajdonos bankom ne tudja meg, mit vásárolok, a boltos pedig ne ismerje meg a bankkártyám számát, mégis a kereskedő megkapja a pénzét a bankomtól, én pedig megkapjam az árumat (lásd a VISA és MasterCard által kidolgozott SET protokollt). Még ennél is nagyobb adatvédelmet garantál a digitális pénz, illetve pénztárca protokollja, ami kis összegű vásárlásokra lett kifejlesztve, s teljesen anonim fizetést tesz lehetővé.

3.7.4 Néhány földhözragadtabb kriptoprotokoll

Bár az előzőekben említett protokollok felhasználására is akadnak példák, főleg a biztonságos fizetést illetően, vannak ezeknél földhözragadtságuk folytán jobban elterjedt protokollok is. Itt van mindjárt a mindenki által legalább hallomásból ismert SSL (Secure Socket Layer) protokoll, melyet a Netscape dolgozott ki a weben keresztül történő biztonságos adatcserére (vagy ennek vetélytársa az S-HTTP), valamint az S/MIME, ami a biztonságos levelezés alapja. Ezek a protokollok elektronikus aláírást és titkosítást alkalmaznak, az egyes célokra akár több algoritmust is, a helyzettől (például a partner rendszerétől) függően. A szimmetrikus kulcsok biztonságos szétosztására és cseréjére is létezik számos, a gyakorlatban is alkalmazott protokoll.

Vannak helyzetek, amikor bizonyos titkos információt több személy között kell szétvágni vagy megosztani. Ez azt jelenti, hogy az adott titkos információt vagy annak bármilyen, önállóan is értelmes piciny részletét nemcsak hogy a külvilág nem ismerheti meg, de azok sem ismerhetik meg önállóan, akikre rá lett bízva. A titkos információ csak úgy fedhető fel, ha annak gazdái összerakják, amilyük van. A szétvágás esetében ez azt jelenti, hogy az összes személy

szükséges a felfedéshez. A megosztás esetében nem az összes, hanem az összes ember közül előre meghatározott minimum számú jelenlévő. Egy nagyon perverz, de sajnos létező példával élve ilyen (vagy ilyesmi) a szuperhatalmak atomfegyverzetének indítására szolgáló rendszer is: az elnök és más felek titokszeletje együttesen képesek felfedni egy aktivizáló adatot. Ez persze nem igazán földhözragadt, így még egy példát hoznék a titokmegosztó protokollra: a hitelesítésszolgáltatók magánkulcsa általában senki előtt nem ismert módon tárolódik egy hardver kütyüben, amiből nem is jöhet ki másképp, biztonsági másolat készítése céljából, csak darabokban, méghozzá n titokszeletben, amiből m ($m<n$) darab együttes megléte esetén lehet csak a magánkulcsot reprodukálni. A n és m számok az igényeknek megfelelően, bizonyos szabályokat és korlátokat betartva, szabadon megválaszthatók. Arra kell tekintettel lenni, hogy m szám elég nagy legyen ahhoz, hogy m fél rosszhiszemű összejátszása kevéssé legyen valószínű; n ne legyen sokkal nagyobb, mint m; de szükség esetén $x=n-m$ személy akadályoztatása esetén is lehetséges legyen a titok felfedése.

3.7.5 Diffie-Hellman kulcsegyeztetés

A Diffie-Hellman kulcsegyeztetés (kulcscsere) protokollja szimmetrikus kapcsolati kulcsokban történő megegyezésre használható, a „hagyományos" nyilvános kulcsú titkosítás alternatívájaként[43] (olyankor például, amikor elektronikus aláírásra nincs szükség, vagy azt DSA algoritmus végzi). A protokoll a következőképpen működik: *A* és *B* fél generál két véletlenszerű értéket, x-et és y-t, amit titokban tart, majd egy algoritmussal (mely a protokoll egyik lelke) kiszámolja x és y nyilvános párját, X-et és Y-t. A nyilvános kulcsokat a felek kicserélik majd egy másik algoritmussal (mely a protokoll másik lelke), s itt jön a lényeg: a két fél a rendelkezésükre álló titkos és nyilvános értékkel legenerálja ugyanazt a kulcsot. Azaz *A* fél saját x és a megkapott Y értékkel létrehozza a K kulcsot, s *B* is legyártja saját y-jából és a megkapott X-ből a K kulcsot. Lássuk ezt még egyszer lépésenként, az alkalmazott algoritmusokkal együtt, tekintettel azok egyszerűségére.

Lépés	*A* fél	Kommunikációs közeg	*B* fél
0.	z, p	<->	z, p
1.	titkos x generálása		titkos y generálása
2.	nyilvános X számolása: $X = z^x \bmod p$		nyilvános Y számolása: $Y = z^y \bmod p$
3.	X küldése	X-> <-Y	Y küldése
4.	Kulcs kiszámolása $K = Y^x \bmod p$		Kulcs kiszámolása $K = X^y \bmod p$

A módszerhez szükség van egy p prímszámra, valamint egy (p-ből származó) z számra, amelyben a két félnek előzetesen meg kell egyezni. A megegyezés történhet akár nyílt kommunikációval is. Ez a megegyezés nem integráns része a protokollnak ezért 0. lépésként, jelzésértékkel tüntettük fel.

Mint látható, a függvény emlegetett algoritmusai mindössze a hatványozás és a modulus, azaz maradékképzés. A felhasznált értékeknek, x-nek, y-nak, p-nek, és z-nek különböző meghatározott tulajdonságokkal kell rendelkezniük, hogy a protokoll biztonságosan működjön.[44]

A protokollnak ez a változata a felhasználói hitelesítést nem oldja meg (újabb verziói ezt a feladatot is kezelik), azaz abban nem lehetek biztos, hogy kivel is kommunikálok titkosan.

3.7.6 Az SSL, TLS és WTLS protokollok

Az SSL protokoll kliens–szerver kommunikáció biztosítására lett kifejlesztve, s legtöbbször (de nem kizárólag) a böngésző és webszerver viszonyában használják. A szállítási protokoll (például TCP/IP) felett és az applikációs protokoll (például HTTP, FTP, LDAP) alatt helyezkedik el, így használata igen széles körű lehet.

A biztonság négy fontos sarokköve közül hármat biztosít: a bizalmasságot, a sértetlenséget és a hitelességet (1.0-s verziója még a hitelességet sem támogatta, 2.0-s verziója a kiszolgáló hitelesítését, 3.0-s verziója a kliens hitelesítését oldotta meg[45], a letagadhatatlanságot azonban ez sem biztosítja). Manapság az SSL 3.0-s a legelterjedtebb internetes biztonsági protokoll, amit szinte valamennyi webszerver és böngésző támogat. A TLS (Transport Layer Security) protokoll az SSL 3.0-s verziójának továbbfejlesztett változata (a 3.1-es verzióval megegyezik)[46]. A WTLS protokoll pedig a TLS protokoll alacsony sávszélességű kommunikációra (például mobiltelefónia) optimalizált változata.

Az SSL protokoll két protokollból áll: az SSL Handshake és az SSL Record protokollból. Az utóbbi négyfajta üzenettípust kezel: az adat, a kézfogás, a figyelmeztetés és a titkosítás beállítása üzenettípusokat. Az üzenetek egy úgynevezett üzenetblokkban utaznak titkosítva és opcionálisan tömörítve, amely tartalmazza az üzenet HMAC (Hash-Message Authentication Code) kódját. Ez a kód az elektronikus aláíráshoz hasonlóan védi az üzenet sértetlenségét. Értéke a nyílt üzenet, a kulcs és a visszajátszási támadások ellen védő egyedi üzenet azonosító közös lenyomata. E kód generálása sokkal egyszerűbb, mint egy igazi elektronikus aláírásé (sokkal kevesebb számolgatnivaló van vele), viszont az egyes üzenetek hitelesítését és letagadhatatlanságát nem oldja meg. Az üzenetek hitelességét a protokoll közvetve mégis garantálja a kezdeti kézfogási fázison keresztül. A kézfogás az SSL Record protokollra épülő SSL Handshake protokoll segítségével valósul meg. Ez a protokoll a kliens- és szerverhitelesítésért, továbbá a protokoll által használt szimmetrikus algoritmus és kulcs kiválasztásáért felelős. Itt a hitelesítés valódi elektronikus aláírással történik.

A protokoll használata a fejlesztők számára kényelmes, mert alsóbb szinteken definiált, így nem kíván az alkalmazás szintjén fejlesztéseket. Ugyanez egyben hátránya is: mivel a biztonság nem az applikáció szintjén definiált, az ott nem is felügyelhető. Gyengesége, hogy a biztonságos SSL csatorna a legtöbbször csak a webszerverig tart, az információk ott kiesnek egy nem teljesen biztonságos közegbe, valamint hogy a sértetlenség és hitelesség utólagos ellenőrzése, bizonyítása – különösen a kliens oldalon – nem támogatott. Az SSL által alkalmazott rejtjelezési módszerek egyúttal több adatot és adatcsomagot is generálnak, így lassítják a kommunikációt a kliens és a szerver között.

3.7.7 Az S/MIME protokoll

A valamennyi internetes levelezőprogram által támogatott MIME protokoll azt határozza meg, hogy az elektronikus leveleket hogyan kell kezelni-feldolgozni. Az S/MIME (Secure Multi-Purpose Internet Mail Extensions) protokoll[47] a MIME protokollra épülve, a PKCS szabványkészlet hasznosításával teszi lehetővé az üzenet titkosítását és aláírását, továbbá rejtjelezési és aláírási információk üzenetbe foglalását. Fontos tudni, hogy az S/MIME protokoll csak az üzenet tartalmát biztosítja, annak attribútumait, fejlécét (például küldő, címzett) nem.

Az S/MIME protokoll az üzenetek rejtjelezésén és digitális aláírásán túl lehetővé teszi, hogy a küldő az üzenethez csatolja tanúsítványát, és hiteles visszaigazolást kérjen az üzenet címzettjétől, valamint biztonsági címkék alkalmazásával hozzáférési kontrollt is meghatároz a rejtjelezett üzenethez. Az üzenethez csatolt tanúsítvány hiján azt az ellenőrző a nyilvános tanúsítványtárból is lekérdezheti (lásd bővebben a 4.7.2 fejezetet). Az S/MIME protokollt valamennyi elterjedtebb levelezőrendszer támogatja.

3.7.8 Az IPSec protokoll

Az IPSec (IP Security) protokoll az SSL protokollhoz hasonló szolgáltatásokkal rendelkezik, de alacsonyabb kommunikációs rétegekben (a hálózati vagy a csomagkapcsolási szinten) történhet a megvalósítása. Célja, hogy számítógépek és hálózati eszközök (útválasztók, gatewayek) közötti fizikai kapcsolat biztonságát megoldja. A bizalmasság és sértetlenség ellátásán túl tanúsítványok felhasználásával a hitelességet is biztosítani képes. A rejtjelezésnek két módját ismeri: szállítási módban csak az IP-csomagok adatrészét titkosítja, csatorna módban a csomagok fejlécét is. A biztonság szolgáltatása két módszerrel lehetséges: AH (Authentication Header) módban csak a küldő hitelesítése történik meg, ESP (Encapsulating Security Payload) módban az adatok rejtjelezése is (a módszerre vonatkozó információk az IP-csomag IPSec fejlécébe vannak foglalva, közvetlen az IP fejlécet követően). Mindkét módszer biztosítja a sértetlenséget, és ismétlés elleni védelmet is nyújt, az IP fejléc sértetlenségét azonban csak az AH mód biztosítja. A két módszer együtt is használható. A kulcsok cse-

réje Diffie-Hellman-eljárással, a sértetlenség biztosítása lenyomatképzéssel történik, ami ez esetben a kapcsolati kulcs kombinálásával valósul meg.

Mivel alacsony hálózati rétegben implementált, igen gazdaságos a használata: köszönhetően annak, hogy az alkalmazási réteg számára teljesen átlátható, az alkalmazásokban való módosítás nem szükséges. Ez a tulajdonsága elsőrendű eszközzé avatja VPN[48]-megoldások és biztonságos dial-up-protokollok megvalósításakor. A Cisco által kifejlesztett IPSec protokoll az Internet Protocol 6-os verziójának része.

3.8 Letagadhatatlanság

Ha az elektronikus aláírásról beszélünk, letagadhatatlanság alatt általában csak azt értjük, hogy egy bizonyos információ előállítója nem tudja letagadni azt, hogy az információt ő állította elő, ha az a magánkulcsával alá lett írva (arra hivatkozhat, hogy magánkulcsa kompromittálódott[49], de az az ő felelőssége). Ehhez természetesen az aláírt információt a hozzá tartozó aláírással a (bizonyításban) érdekelt félnek meg kell őriznie. Bármennyire is evidens ez a feltétel, a gyakorlatban sokszor nem teljesül. Például egy biztonságos webszerverrel történő adatcsere eredményeként nem keletkezik olyan adathalmaz, amit el lehetne menteni, s később bizonyítékként fel lehetne használni.

A kommunikáció letagadhatatlansága azonban ennél összetettebb probléma. Két fő típusra bontható: a származás letagadására és az átvétel letagadására. Mindkét esetben megkérdőjelezhető a kommunikáció résztvevőinek személye, a kommunikáció tartalma, szándékossága és időpontja.

A származás letagadása ennek megfelelően a következő eseteket jelentheti:

- A címzett azt állítja, hogy egy bizonyos üzenetet kapott, de a gyanúba kevert küldő tagadja, hogy a neki tulajdonított üzenetet valaha is előállította volna.
- A címzett azt állítja, hogy egy bizonyos üzenetet kapott, de a gyanúba kevert küldő tagadja, hogy az üzenetet valaha is elküldte volna bárkinek is.
- A címzett azt állítja, hogy egy bizonyos üzenetet kapott, de a gyanúba kevert küldő tagadja, hogy az üzenetet a címzett számára elküldte volna.
- A címzett azt állítja, hogy egy bizonyos üzenetet kapott, de a gyanúba kevert küldő azt állítja, hogy a neki tulajdonított üzenettől különbözőt küldött a címzett részére.
- A címzett azt állítja, hogy egy bizonyos üzenetet kapott egy bizonyos időpontban, de a gyanúba kevert küldő tagadja, hogy az üzenetet a jelzett időpontot (közvetlen) megelőzően állította volna elő, illetve küldte volna el.
- A címzett azt állítja, hogy egy bizonyos időpontban előállított üzenetet kapott, de a gyanúba kevert küldő tagadja, hogy az üzenetet a jelzett időpont előtt állította volna elő.

Az átvétel letagadása a következő eseteket jelentheti:

- A küldő azt állítja, hogy egy bizonyos üzenetet küldött, de az általa megnevezett címzett tagadja az üzenet megérkezését.

- A küldő azt állítja, hogy egy bizonyos üzenetet küldött, de az általa megnevezett címzett azt állítja, hogy a kérdéses üzenettől különbözőt kapott.
- A küldő azt állítja, hogy egy bizonyos időpontban egy bizonyos üzenetet küldött, de a címzett tagadja, hogy az üzenetet a jelzett időpontot (közvetlen) követően kapta volna meg.

A fentieknek van még három „minősített" esete, melyeket a küldés letagadásaként olykor megkülönböztetnek az átvétel letagadásától:

- A küldő azt állítja, hogy egy bizonyos üzenetet küldött, de az általa megnevezett címzett nemcsak az üzenet megérkezését tagadja, de azt is állítja, hogy a küldő nem küldte azt az üzenetet.
- A küldő azt állítja, hogy egy bizonyos üzenetet küldött, de az általa megnevezett címzett tagadja, hogy azt az üzenetet a küldőtől kapta volna meg.
- A küldő azt állítja, hogy egy bizonyos üzenetet küldött egy bizonyos időpontban, de az általa megnevezett címzett nemcsak az üzenetnek az adott időpontban való megérkezését tagadja, de azt is állítja, hogy a küldő abban az időpontban nem küldte azt az üzenetet.[50]

A tagadások mögött különböző tényezők állhatnak (akár együttesen is):

- Lehet, hogy a küldő hazudik/téved.
- Lehet, hogy a címzett hazudik/téved.
- Lehet, hogy az alkalmazott protokoll hibás.
- Lehet valamilyen hardver-, szoftver-, kommunikáció- vagy más hiba (például az órák közötti nagy eltérés).
- Lehet valamilyen félreértés (például az időzónák figyelmen kívül hagyása, névazonosság stb.).
- Valamilyen behatoló a bolondját járatja a felekkel.

A letagadhatatlanság kezelésére a következő típusú kötelezettségvállalások szolgálhatnak.

Előállítás igazolása: az aláíró készítette az üzenetet (de nem feltétlen hagyta jóvá és küldte el azt). A jóváhagyás igazolása: az aláíró jóváhagyta az üzenetet (de nem feltétlen küldte el azt). A küldés igazolása: az aláíró küldte el az üzenetet (de nem feltétlen készítette és hagyta jóvá azt). A származás igazolása: az aláíró elismeri, hogy ő készítette, hagyta jóvá és küldte az üzenetet. A kézbesítés igazolása: a szolgáltató jelzi, hogy az üzenetet egy a címzett által hozzáférhető lokális tárolóba (tipikusan annak postaládájába) eljuttatta. Az átvétel igazolása: az aláíró elismeri, hogy átvette az üzenetet.

Ezek a kötelezettségvállalások egymásra épülnek (egyre magasabb bizonyosságot jelentenek). Az aláírási szabályzat ezek közül többet is elismerhet, s az aláíráskor jelölni lehet, melyik alkalmazható az adott esetben.

Ebben az értelemben az elektronikus aláírás önmagában csak az előállítás igazolásául szolgálhat automatikusan, a többi szempont bizonyításához az alkalmazott protokollnak is hozzá kell járulnia. Az időbeliség bizonyításához egy külső, megbízható időbélyegzés-szolgáltató közreműködésére van szükség.

JEGYZET

1 A lenyomatot az RSA algoritmus esetében az aláírás előtt az aláíró algoritmusnak megfelelő méretűvé hizlalják egy feltöltő algoritmussal.

2 Az esetlegesen alkalmazott feltöltő algoritmusból kinyerve.

3 Angolul: Message Digest

4 Megjelentek már 256, 384, illetve 512 bit méretű hash-függvények is.

5 Nem állom meg, hogy el ne „dicsekedjem" azzal, hogy tizen-pár évesen magam is ilyenfajta jelszókódoló hash-algoritmust fejlesztettem sejtgenerátor algoritmusra alapozva, mely mind az egyirányúságnak, mind a lavinahatásnak egész jól megfelelt, egyedül az ütközésmentesség követelményével akadtak gyenge pillanatai. Vállalkozó kedvű matematikustanoncoknak ajánlom, hogy hírnevük megalapozása, de legalább szellemük pallérozása végett ilyen eljárásokat fejlesszenek, mellyel az egyébként sokszor túl elméleti matematikának egy gyakorlati, kézzelfogható alkalmazására nyílik mód. De vigyázzanak, mert sokkal bonyolultabb a feladat, mint elsőre látszódik!

6 Azoknak, akiket a titkosítás története érdekel, ajánlom a következő könyveket: [1], [2]

7 200 felhasználó esetében az aszimmetrikus rendszer kulcsigénye 400 kulcs, a szimmetrikus rendszeré viszont 19 900!

8 A szimmetrikus eljárások mintegy százszor-ezerszer gyorsabbak, mint aszimmetrikus párjaik, így sokszor – az üzenet méretétől függően – a kulcs visszafejtése lassabb, mint az egész üzeneté.

9 Elvetemültebb informatikusok tájékoztatásául: itt dezoxiribonukleinsav.

10 A kulcs méretének növelésével exponenciálisan nő a nyers erő módszer időigénye. „m" kulcsméret esetén a kulcsvariációk száma 2^m, azaz 8 bites kulcs esetén 256, de 40 bites kulcs esetén már több mint egybillió.

11 Különösen népszerűek azok a kulcstörő próbálkozások, melyeket az algoritmusok kifejlesztői által felajánlott díjak elnyerésével járó hírnév is motivál. Ezekre külön csapatok alakulnak, amelyek több ezer, sokszor több tízezer személyi számítógépet mozgatnak meg, s ezek erejét, számítási kapacitását egyesítve esnek neki a töréssel járó feladatnak.

12 Moore törvénye.

13 Például egy már jelenleg is tanulmányozott gyökeresen új módszer (pl. sejtszámítógépek, kvantumszámítógépek) termékben történő materializálódása.

14 Általános iskolai tananyag! Ki emlékszik rá?

15 A Message Digest algoritmus 5. verziója. Korábbi változataival az MD2 és MD4 algoritmusokkal szintén lehet találkozni.

16 Az MD5 eredetileg az RSA algoritmus segédje volt, az SHA pedig a DSA szekundánsa. Ma már mindkét aláíró algoritmus esetében az SHA-1 számít közel egyeduralkodónak.

17 Ez a sokszor túlontúl elméleti alapokon álló európai szabványokkal sajnos sokszor előfordul.

18 Bár 56 bites a kulcs, általában 64 biten tárolják, minden 7 bit mellé egy ellenőrző bitet rendelve.

19 Érdekességként: az algoritmus képességeire jellemző, hogy ha a kulcs és a nyílt szöveg egyaránt csupa nulla, akkor a rejtjelezett szöveg: 8CA64DE9C1B123A7.

20 Az IBM eredeti terveiben is 128 bites kulcshossz szerepelt, amit az NSA kérésére csökkentettek 56 bitre. Kis fantáziával ennek oka kitalálható.

21 Két kulccsal is használják az eljárást: az első és harmadik lépésben ugyanazt a kulcsot alkalmazzák. A 3DES nyilvánvalóan háromszor lassabb, mint a DES, ereje azonban nem az általa alkalmazott 168 bites kulcséval ekvivalens, hanem inkább egy 112 bites kulcs erejének megfelelő. A módszer nagy előnye, elterjedtségének legfőbb oka, hogy használatához nem kell lecserélni az egyszer már bevált DES hardvereket és szoftvereket, csak többször meg kell futtatni őket.

22 RC: Rivest's Cipher, vagyis az RSA-s Ron Rivest titkosító eljárása. Bár az anno gyenge titkosításként koncul dobott 40 bites változatai percek alatt nádszálként roppantak meg a nyers erő hatására, nagyobb kulcshosszt alkalmazó változatai megbízhatóak. Az RC4 mintegy kétháromszor gyorsabb, mint a DES, gyengesége viszont, hogy az ugyanazzal a kulccsal kódolt különböző üzenetek között ismert összefüggések vannak, amik megkönnyíthetik az üzenetek megfejtését.

23 Ahogy olvastam egy újságírótól: nagyjából 340×10^{36}. Kicsire nem adunk: a 2^{128} és 340×10^{36} közti különbség mindössze pár százbilliárdszor pár százbilliárd. És ez arányaiban tényleg elhanyagolható!

24 A világegyetem fennállása „mindössze" 15×10^{9} év.

25 Bruce Schneier neves biztonsági szakértő, anyátlan-apátlan fiatal kriptológuspalánták első számú példaképe, érett kriptológusok megfellebbezhetetlen hivatkozási alapja.

26 Az igazsághoz hozzátartozik, hogy ez az utolsó fordulóba bejutott öt algoritmus mindegyikének sikerült (ami azért jelzi, hogy nagy baj esetén azért van még tartalék).

27 Az RSA egy cégnek is a neve, melyet az algoritmus kidolgozói alapítottak a módszer piaci termékként való kialakítására és kereskedelmi értékesítésére. A cég több más kriptográfiai algoritmus kidolgozója, szabványok gazdája és szoftverek gyártója.

28 Egy egyszerű példa erre: Bárki kipróbálhatja mennyi ideig tart számára a 713 prímtényezőinek megtalálása. Ha esetleg „szégyenszemre" idő előtt feladná, a megfejtés 23 és 31, amiknek az összeszorzása még kalkulátor nélkül is pillanatok alatt sikerülne.

29 A prímtényezős felbontásra jelenleg nem áll rendelkezésre hatékony algoritmus, bár az sem bizonyított, hogy ilyen algoritmus nem létezik. A százjegyű (decimális) számok a jelenlegi technológiával még könnyen faktorizálhatóak.

30 Bár a módszer tényleg nem bonyolult, annak ismertetésétől megkímélem olvasóimat. Ha valakit érdekel, számos helyen megtalálja az interneten, illetve fordulhat első kézből a feltalálókhoz [14].

31 A kulcsok a modulusból és exponensekből állnak: a magánkulcs a modulusból és privát exponensből, a nyilvános kulcs a modulusból és a publikus exponensből. A kulcshossz alatt a modulus hosszát szokták érteni, bár a modulus önmagában nem a kulcs.

32 Az eljárás mintegy 8000 MIPS-év teljesítményt igényelt a szűrésnek nevezett fázishoz, amit mintegy 300 PC ereje képviselt, több mint két hónapig reszelve, majd egy Cray C90-es szuperszámítógépet is csatasorba kellett állítani 2,3 gigabájt memóriával a szűrés eredményeként előállt mátrix feldolgozásához.

33 Három számjegyenként (nem bittel) növelve a kulcsméretet mintegy megduplázódik a faktorizálás bonyolultsága.

34 Forrás és bővebb információ: [15].

35 Azoknak, akik a képtelennel dacolnak, vagy egy kisebb kulccsal próbálnának szerencsét, merem javasolni, hogy az RSA cég által meghirdetett több százezer dollár összdíjazású faktorizálási versenynek ugorjanak neki. Ennek keretén belül több, különböző méretű számot kell faktorizálni. A legkisebb szám 174 jegyű, vagyis 576 bit hosszúságú, a legnagyobb 617 jegyű, vagyis 2048 bites. Az előbbi faktorizálásáért tízezer dollár jár a megfejtőnek, az utóbbiért pedig 200 ezer, amivel nem sokat kockáztat a cég.

36 Az USA egyik titkosügynöksége, amely nem mellesleg a lehallgatást végző „húsevő" alkalmazása néven híresült el informatikai és kommunikációs berkekben.

37 A szabvány (FIPS PUB 186) a Digital Signature Standard nevet viseli, melynek a DSA algoritmus egy része.

38 Forrás és bővebb információ: [15].

39 Ha valaki ismeri a mesét, amelyben a királyt sakkban legyőző legény annyi búzaszemet kér, amennyit meg tud duplázni a sakktábla mezőin, akkor az sejtheti, hogy ez igen nagy szám.

40 Az egyik legismertebb véletlenszám-algoritmus a Blum Blum Shub. Lásd: [16]

41 A véletlen számok véletlenségének teszteléséről lásd: http://www.ciphersbyritter.com/news2/testsbbs.htm

42 Bakos Ferenc: Idegen szavak és kifejezések szótára

43 Nyilvános kulcsú eljárásnak tekintik ezt is. A hagyományossá fokozott nyilvános kulcsú titkosítással szemben viszont itt a kulcsok generálása és szétosztása közvetlenül kapcsolódik a kódolási és dekódolási lépésekhez.

44 Bővebb információ: [12]

45 A webszervernek ehhez megbízhatónak kell tartania az ügyfélt hitelesítő szolgáltatót.

46 Az IETF RFC 2246 néven szabványosította 1999-ben.

47 Az S/MIME protokoll 3. változata IETF szabvány.

48 Virtuális magánhálózat. Sokan hallották már ezt a kifejezést, de kevesen tudják, hogy ez is a nyilvános kulcsú kriptográfián, kulcsok és tanúsítványok felhasználásán alapszik.

49 Illetéktelen tudomására jutott, illetéktelen megszerezte.

50 Ezen eseteknek bizonyára ki lehet találni még különböző variánsait és alfajait, de ezek már nem különösebben változtatnak a probléma lényegén és kezelési módján.

4 A tanúsítvány

Ajánlás:

Mindenkinek.

Ki ne hallott volna már a tanúsítványról, az elektronikus aláírás alapvető kellékéről, a nyilvános kulcsú infrastruktúra legfőbb képviselőjéről és egyben legismertebb termékéről? Valószínűleg nem sokan vannak, akik ne találkoztak volna még tanúsítvánnyal, de kevesen vannak, akik az előbb felsoroltaknál sokkal többet tudnának róla. Lássuk hát, miből is lett a cserebogár, és mivé lehet még.

E fejezetben sok olyasmi megjelenik majd, hogy az aláírónak vagy ellenőrzőnek ezt vagy azt kell tennie. Ezektől nem kell megrémülni, mert nagy részüket az alkalmazások automatikusan elvégzik, így e részek inkább ismertetőnek tekinthetők, amelyek a belső mechanizmusokat tárják fel. Nem minden lépés ilyen azonban, találhatók lesznek olyan információk is, amelyek a felhasználók kétkezi, egyagyi tennivalóit írják le. Olyanokat, amelyekkel ajánlatos tisztában lenni.

4.1 Mi is az a tanúsítvány?

4.1.1 Hagyományos világ

Téved, ki azt hiszi, hogy a tanúsítványok a kriptográfia termékei. Szó sincs róla. Ha fellapozzuk a neves Webster szótárt, azt találjuk benne, hogy az angol certificate szó, amelyet a szigetországbeliek kínjukban a „tanúsítvány" helyett használnak, a késő latin certificatus szóból származik. Jó esély van arra, hogy már a római jogban is ismert volt a kifejezés, mely azóta is folyamatosan használt. A szó több specifikus jelentése közül számunkra az általános érvényű a legérdekesebb: a tanúsítvány olyan dokumentum, mely egy hiteles állítást tartalmaz valaminek az igazolására.

Ilyen tanúsítványokkal van tele életünk és mellényzsebünk. Itt van mindjárt a személyi igazolványunk, lakcímigazoló kártyánk, útlevelünk, jogosítványunk, tébékártyánk és egyéb nélkülözhetetlen hivatalos okmányaink, amik tanúsítják, hogy létezünk, lakunk, utazhatunk, szabad autót vezetnünk és fogat húzatnunk. Ezek mind tanúsítványok: dokumentumok, amik állítást tartalmaznak valaminek az igazolására s valamilyen fontos hivatal hitelesíti őket hatósági mivoltában. De tanúsítvány az érettségi bizonyítvány és a diploma is. Ezek azt állítják, hogy elvégeztünk valamilyen fejtágító iskolát, tanfolyamot, gyorstalpalót, amit az iskola pecsétje s az iskolaigazgató aláírása is igazol.

4.1.2 Elektronikus világ

A tanúsítványnak természetesen – mint oly sok mindennek – megvan az elektronikus világban is a megfelelője. E világban azonban egy némileg specifikusabb definícióval élhetünk: a tanúsítvány elektronikus irat, amelyet egy hozzá csatolt elektronikus aláírással igazol egy intézmény, mely intézményben a tanúsítványt felhasználók közössége megbízik. Ezt az intézményt szokták nevezni megbízható harmadik félnek is.

4.2 Nyilvános kulcsú tanúsítványok

Az előbbi definíció jóval általánosabb, mint amire én most determinált agyammal ki akarok lyukadni. Belefér az időbélyegző, a visszavonási lista és akár egy elektronikus személyi igazolvány is. Az elektronikus aláírás kapcsán, ha tanúsítványról beszélünk, valami sokkal konkrétabbra szoktunk gondolni. Ezentúl én is így teszek: ha tanúsítványról beszélek, a nyilvános kulcsú tanúsítványra gondolok.

4.2.1 Mi szükség a tanúsítványra

Az elektronikus aláírás egyik alapvető célja a hitelesség biztosítása. Ezt a nyilvános kulcsú kriptográfia biztosítja is, de csak egyetlen feltétellel: ha biztosak vagyunk abban, hogy az aláírás ellenőrzésére használt nyilvános kulcs valóban ahhoz tartozik, aki azt magáról állítja. Erről meggyőződhetünk úgy, hogy egy füstös kocsmában személyesen összefutunk partnerünkkel, és egy korsó sör mellett kicseréljük nyilvános kulcsainkat (aztán gondosan felcímkézve vigyázunk arra, hogy össze ne keverjük, el ne hagyjuk). Esetleg úgy, hogy az elektronikus cserebere után felhívjuk az illetőt, és bájtról bájtra felolvasva neki a teljes tartalmát (vagy lenyomatát) egyeztetjük vele a nyilvános kulcsot, esetleg kisebb méretű kulcsoknál mindezt SMS-ben is lezavarhatjuk.[1] Ilyen alkalmakkor arról sem árt meggyőződni, hogy az illető nem csap be minket, valaki más nyilvános kulcsát magáénak titulálva. Ennek módja az lehet, hogy egy véletlenszerű adat kódolását kérjük tőle, amit a nyilvános kulccsal visszafejtünk.

Hála a kriptográfusok védőszentjének, a kulcselosztás eme problémájára van ennél egyszerűbb, biztonságosabb és automatikusabb módszer is, ami ráadásul még akkor is működik, ha kommunikációs partnerünket korábban nem is ismertük. A megoldás alapelve annyira egyszerű, hogy valóban isteni sugallatot kell keresnünk a háttérben: ha az elektronikus aláírás biztosítja a hitelességet, hát írjuk alá a nyilvános kulcsot is!

4.2.2 A megbízható harmadik fél

Ha például én egyszer már összefutottam Bélával egy személyes kulcscserére, akkor Béla aláírásában megbízom. Amennyiben Béla ezek után aláírva elküldi részemre Ottó nyilvános kulcsát, akivel ő futott össze személyesen, akkor ezentúl Ottó nyilvános kulcsában is megbízhatom. Ehhez persze Béla személyében is meg kell bíznom, hogy nem ver át, ami kisebb közösségekben még működőképes is lehet. Minél hosszabb azonban egy ilyen bizalmi lánc, annál kevésbé megbízható, és annál babrásabb az ellenőrzése, kezelése: Béla sem ismeri Ottót, ő Gézától kapta Ottó nyilvános kulcsát, aki Géza unokahúgának a titkos szeretője, de igazándiból Géza se látta még, neki a ledér unokahúg felszarvazott férje küldte (aki persze mit sem tud a titkos kapcsolatról), miután mesélte Gézának, amikor Béla is ott volt, hogy Ottó, aki civilben az ő ügyvédje, foglalkozik cégek eltüntetésével, amire neki most pont szüksége lenne, hogy ne kelljen az adótartozásait rendeznie.[2] Még ennél is nagyobb problémát jelent a bizalmi hálós modellnél az, hogy nehéz bizonyítani bárkinek is az igazát, ha utólag valamelyik fél letagadja az aláírását. Azt ugyan nem lehet letagadni, hogy a kérdéses aláírás egy adott nyilvános kulcs magánkulcs párjával történt, de azt igen, hogy a kérdéses magánkulcsot mi birtokolnánk. Azt birtokolhatja egy rosszindulatú fél is, aki egyszer megtévesztve valakit elhitette azt, hogy az ő nyilvános kulcsa valójában valaki másé. Ehhez elég a közösség leggyengébb tagját megkeresnie (például a ledér unokahúgot, aki nem szeretné, ha a házasságtörő parázna kapcsolatra fény derülne, vagy Ottót, aki mellesleg lóversenyadósságokkal küszködik, vagy a felszarvazott férjet, aki egyébként sem egy nagy lumen), és őt megzsarolnia, lefizetnie, megtévesztenie.

Ha létezne egy megbízható harmadik fél, akiben megbíznék én is, meg Béla, Géza, Ottó, a ledér unokahúg és annak felszarvazott férje, s mindenki, akivel elektronikus aláírással akarok kommunikálni, s nézeteltérés esetén mindannyian elfogadnánk az aláírását bizonyító erőként, akkor elegendő lenne, hogy mindannyiunk számára ez a fél igazolja a nyilvános kulcsok adott személyhez tartozását. A gyakorlatban ez a megbízható harmadik fél a hitelesítésszolgáltató.

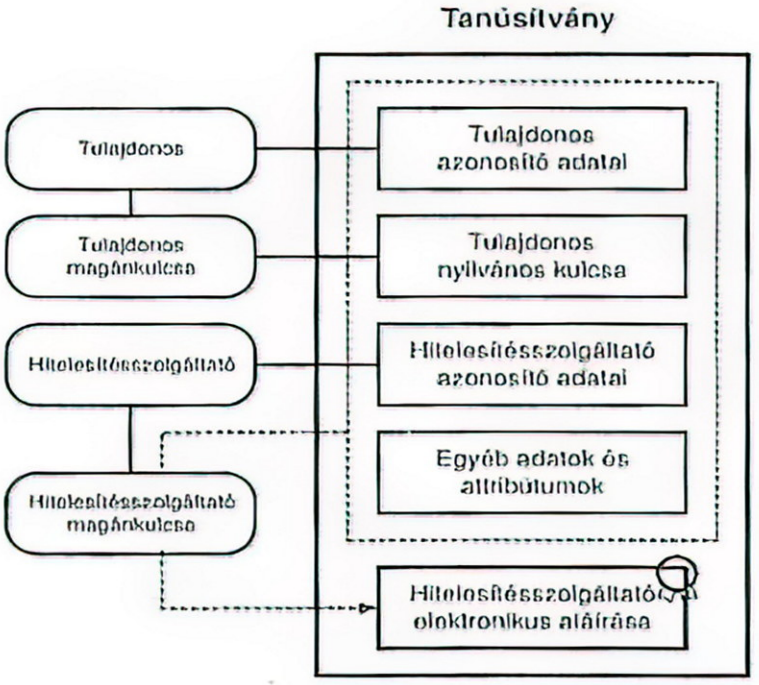
4.2.3 Mit tanúsít a tanúsítvány

Végre kimondom – ha valaki még nem jött volna rá a rétestésztává nyújtott bevezetőből –, a tanúsítvány az elektronikusan aláírt nyilvános kulcs. Jelen esetünkben a hitelesítésszolgáltató által aláírt nyilvános kulcs. Illetve ennél egy kicsivel még több is. Ha csak ennyi lenne, akkor egy másik nyilvántartásnak kellene tartalmazni, hogy melyik tanúsítvány kié. Ennél sokkal egyszerűbb magában a tanúsítványban feltüntetni, hogy az kinek a nyilvános kulcsát tartalmazza. Így lesz a tanúsítvány igazolás valaminek az állítására. És ha már frogatunk bele, miért ne frogatnánk bele egyéb hasznos dolgokat is. Nemcsak azt, hogy ki a nyilvános kulcs tulajdonosa, de, mondjuk, azt is, hogy melyik hitelesítőszervezet adta azt ki.

Meg azt, hogy a nyilvános kulcs milyen algoritmussal készült, illetve hasznosítható (lehetővé téve a közösség tagjai számára, hogy különböző algoritmusokat is felhasználjanak). Így lesz a tanúsítvány egy elektronikus irat, amely különböző adatokat tartalmaz, nemcsak egy szimpla állítást, de annak attribútumait is, mint, mondjuk, a már említett diploma, amin szintén fel van tüntetve a kiadó tanintézet neve, a kiadás dátuma, az elért eredmény és még sok minden más is.

4.2.4 A tanúsítvány tartalma

A tanúsítvány tartalma négy fő szekcióba sorolható. Az első szekció a nyilvános kulcs tulajdonosának azonosítására szolgáló adatok, a második a hitelesítésszolgáltató azonosítására szolgáló adatok, a harmadik maga a nyilvános kulcs, a negyedik pedig minden más, vagyis az attribútumok.



47. ábra
A tanúsítvány tartalma és adatainak kötődése

A tulajdonos azonosítására leginkább annak neve szokott szerepelni, de az elvileg lehet bármilyen más, a közösség által a tulajdonos felismerésére alkalmas adat is, így például egy focicsapat esetében a játékos száma, vagy „életszagúbb" példaként egy titkosszolgálat esetében az ügynökök fedőneve. A hitelesítésszolgáltató azonosítása hasonló a tulajdonoséhoz: itt is szerepelhet annak becsületes neve vagy bármilyen azonosító, amiből a közösség összes tagja tudja, hogy ez a hitelesítésszolgáltató (egy bizonyos hitelesítésszolgáltató). Az attribútumok közt helyet szokott kapni a tanúsítvány érvényességi ideje, osztálya, típusa, egyedi sorszáma, valamint egyéb adatok és a hitelesítésszolgáltató megjegyzései, sőt lehetőség van akár a tulajdonos fotójának és egyéb biometrikus azonosítónak a beillesztésére is.

Mindez a hitelesítésszolgáltató magánkulcsával alá van írva (ez az aláírás szintén a tanúsítvány része), s így ezek az adatok megbonthatatlanok és megváltoztathatatlanok.

4.2.5 Koncentrált bizalom

A nyilvános kulcsok elosztása így egyszerűen megoldódik. Tanúsítvány formáját öltve nyilvános kulcsomat partnereimnek közvetlen magam is elküldhetem,

akár első, elektronikusan aláírt üzenetváltásunk alkalmával is, még akkor is, ha a kommunikációs csatorna nem biztonságos, azon vandál hackerek, idegen hatalmak ügynökei, gonosz terroristák és kíváncsi üzleti konkurenseim nyüzsögnek. Hát nem fantasztikus?

Csakhogy ennek a csodavilágnak komoly ára van. Ami az egyik oldalon egyszerűséget jelent, a másik oldalon komoly erőfeszítéseket kíván. Hitelesítésszolgáltatónak lenni strapás feladat, komoly befektetést, infrastruktúrát, szakértelmet és munkát kíván. A bizalom centralizálása végeredményét tekintve a közösség számára mégis előnyös, hiszen azt egy hozzáértő, megbízható félnél helyezheti el, így nemcsak kényelemhez, de nagyobb biztonsághoz is jutnak tagjai.[3]

4.2.6 A tanúsítvány jellemzői

Mivel a tanúsítvány tartalma nyilvános a közösség számára, így maga a tanúsítvány is egy nyilvános információ (igaz, a tanúsítvány tulajdonosa rendelkezhet annak bizalmas kezeléséről is). A különböző információk tanúsítványba foglalása által a tanúsítvány önhordozóvá, az elektronikus aláírás által pedig önvédelmezővé válik (az aláírás nemcsak a hitelességet és a letagadhatatlanságot, de a sértetlenséget is biztosítja). Ezért szükségtelenné válnak a kulcsszétosztás során egyébként alkalmazandó drága biztonsági megoldások és egyéb ügyeskedések.

Mivel a kriptográfiai rendszer önvédelmező, a tanúsítvány biztonságát innentől fogva alapvetően két, nem műszaki, illetve matematikai tényező határozza meg. Ezek:

- a tulajdonos (személy)azonosságának egyértelmű, teljes bizonyossággal történő meghatározása,
- valamint annak biztosítása, hogy a tanúsítvány párjaként használt magánkulcshoz csak a tulajdonos férhessen hozzá.

Az első tényező a hitelesítésszolgáltató felelőssége (hogy miként történik ez, majd később kerül sorra, egyelőre mondjuk azt, hogy a tanúsítványt a gólya hozza), a második pedig a tanúsítvány és az ahhoz tartozó magánkulcs tulajdonosáé.

Jelmondatszerűen összefoglalva a tanúsítvány: nyilvános, önvédelmező és önhordozó.

4.3 Tanúsítvány és kulcs – érvényességi idő és állapot

A tanúsítványoknak és a kulcsoknak érvényességi ideje és érvényességi állapota van, ami a felhasználás elsősorban jogi értelemben vett korlátozását jelenti. Ez a jogi értelem arra utal, hogy ha nem helyesen, annak érvényességi korlátozásait figyelembe véve járunk el a kulcsunkkal és a tanúsítványokkal (sajátunkkal és másokéval), akkor tevékenységünk utólag a bíróságon támadhatóvá vá-

lik. Az érvénytelen kulccsal kötött szerződések például szintén érvénytelenekké válhatnak, így nem árt odafigyelni arra, hogy magunk és mások milyen kulcsokat és tanúsítványokat használnak. Mindez annak ellenére így van, hogy az aláírás nyújtotta algoritmikus biztonság nem sérül az érvényességi idő lejártával (legalábbis azonnal és automatikusan nem).

Nem evidens ugyanakkor – bár elsőre annak tűnik –, hogyan kell értelmezni az érvényességi időket és állapotokat, s erre vonatkozóan a felhasználók legtöbbször semmilyen útmutatót nem kapnak. Mivel a tanúsítvány érvényessége számtalan dologtól függ – nemcsak az érvényességi idejétől és érvényességi állapotától –, így az „érvényesség" kifejezést önmagában igyekszem kerülni (ha mégse sikerülne – illetve más szerzőknél, dokumentációknál –, legyenek óvatosak ezzel, mert nem nyilvánvaló, mire vonatkozik[4]).

4.3.1 Az érvényességi idő korlátozása

Az aláírásra és rejtjelezésre használatos kulcsokat nem szabad a végtelenségig használni. Ennek egyrészt oka, hogy a technika fejlődése véges időn belül elavulttá tesz korábban még biztonságos megoldásokat, másrészt túl hosszú felhasználás esetén a kriptoanalízis veszélye is jelentősen megnő. Ezért a kulcsok élettartamát be szokták határolni, aminek több előnye is van:

- Hatásosan lehet csökkenteni a kriptoanalízissel járó veszélyeket.
- A kulcsok algoritmusa, erőssége rendszeresen változtatható a kriptográfia eredményeinek megfelelően.
- Az esetlegesen kompromittálódott kulcsokkal okozható veszteségek csökkenthetők.
- A tanúsítvány-visszavonási lista mérete csökkenthető.

A kulcsok érvényességi idejének korlátozása ugyanakkor nem védi a már egyszer megtett aláírásokat, illetve rejtjelezett dokumentumokat. A sikeres kriptoanalízishez ugyan már nem kínál többletinformációt a kulcs felhasználása, de a nyers erővel való támadástól semmi sem menti meg őket. Azok az idők végezetéig ki vannak téve ennek a veszélynek. Éppen ezért olyan aláírást vagy rejtjelezést, amelynek biztonsága évtizedekig szükséges, csak különleges körültekintéssel szabad megtenni, a rejtjelezés és az aláírás időszakonkénti felfrissítésével (újbóli aláírással és rejtjelezéssel).

4.3.2 A tanúsítvány érvényességi ideje

A kulcspár érvényességi idejéhez igazodóan a tanúsítványok érvényességi idejét is korlátozni szokták. A tanúsítványban ennek megfelelően feltüntetik annak érvényességének kezdeti és végdátumát, melyeken túl a tanúsítvány nem megbízható. A kezdeti dátum általában a kiadás dátuma, a végdátum pedig ezt egy-két évvel haladja meg (ettől persze vannak eltérések és kivételek is szép számmal, a hitelesítőegységek saját tanúsítványa például akár tíz–harminc évig is ér-

vényes lehet). Az említett műszaki okok mellett a tanúsítvány érvényességi idejének korlátozása a hitelesítésszolgáltatónak üzlet is, hiszen így egy-két évente rendszeresen „megvághatja" ügyfeleit.[5]

A tanúsítvány érvényességi ideje egyfelől azt jelenti, hogy a hitelesítésszolgáltató aláírása addig érvényes a tanúsítványon, utána már nem igazolja a benne foglalt adatok valódiságát, sértetlenségét, összetartozását, másfelől a nyilvános kulcs érvényességi idejét is jelenti. Nem, vagy nem feltétlenül jelenti viszont a magánkulcs érvényességi idejét, ami ettől rövidebb is (ilyen esetekben azt külön feltüntetik a tanúsítványban), ezzel megegyező, vagy akár korlátlan is lehet.

Arra vonatkozóan, hogy az érvényességi idő ténylegesen mit jelent, azt hogyan kell értelmezni, vannak „általános értelemben vett" szabályok (mondjuk, egy szabványból, egy törvényből vagy csak a szokásjogból származók), és lehetnek a hitelesítésszolgáltatónak vagy a közösségnek is ezt felülbíráló vagy ezt kiegészítő előírásai. Az alkalmazások ugyanakkor ezeket a szabályokat nem mindig követik helyesen, így a felhasználónak különös felelőssége, hogy ezeket betartsa.

4.3.3 Tanúsítványok visszavonása

Bár a tanúsítványoknak előre behatárolt érvényességi időtartama van, szükség lehet arra is, hogy ezen időtartamon belül visszavonják egy tanúsítvány érvényességét. Ennek számos oka lehet, amiket most nem veszünk sorra,[6] csak ennek módszerét tekintjük át.

Ha egy tanúsítványt idő előtt vissza kell vonni, akkor annak érdekében már nem módosíthatjuk az egyszer kiadott tanúsítványt, felülírva benne az érvényesség végdátumát, s az sem megoldás, ha a tulajdonostól visszakérjük azt. Egy papír alapú tanúsítványnál még megoldható, mert értelmezett az eredeti példány fogalma (amit elég átírni vagy tűzre vetni), de egy elektronikus iratnál az eredeti és a másolat nem megkülönböztethető. A tanúsítványból akárhány is keringhet a világban, és azt se tudhatjuk, kinél, merre vannak. Így egészen más megoldással kell élni. Ha van egy hitelesítésszolgáltatónk, aki kiadta számunkra a tanúsítványt, akkor az vezethet egy nyilvántartást azokról a tanúsítványokról, amik időközben visszavonásra kerültek. Ez a nyilvántartás – mert természetesen van ilyen – a tanúsítvány-visszavonási lista, mely a tanúsítványhoz hasonlóan egy elektronikus irat, amit a hitelesítésszolgáltató elektronikusan aláír, biztosítva annak hitelességét, sértetlenségét és letagadhatatlanságát. Ezt a nyilvántartást a szolgáltató rendszeresen karbantartja és nyilvánosságra hozza, így abban bárki ellenőrizheti, hogy egy tanúsítvány nem lett-e idő előtt visszavonva. Ez az információ a tanúsítvány állapota: ha a tanúsítvány szerepel a tanúsítvány-visszavonási listában, akkor a tanúsítvány állapota érvénytelen, ha pedig nem, akkor érvényes.[7]

Kulcsot nem lehet külön visszavonni, csak tanúsítványt (a kettő ez esetben egyre megy), s ezért a tanúsítvány állapotának érvénytelensége úgy értelmezendő, mintha mind a tanúsítvány, mind a magánkulcs érvényességi ideje a visszavonás pillanatában véget ért volna (a visszavonás időpontját a lista tartalmazza).

4.3.4 Mit jelent az érvényességi idő

Lássuk, mit jelentenek azok az „általános értelemben vett" szabályok a tanúsítvány érvényességi idejére vonatkozóan. Az érvényességi idő első közelítésben azt jelenti, hogy a tanúsítvány és a kulcsok addig felhasználhatók, amíg tart az érvényességi idejük, utána már nem. S bár fizikailag ezután is alkalmazhatók, a használat tiltott (szóval a lehet, de nem szabad tipikus esetével állunk szemben). Ez persze túl nyilvánvaló lenne ahhoz, hogy maradéktalanul igaz legyen, s mint látjuk majd, ez alól is vannak kivételek.

Amit biztosan jelent, az az, hogy a hitelesítésszolgáltató csak az érvényességi időn belül lévő tanúsítványokra fogad el visszavonási kéréseket és ad róluk állapotinformációt (a visszavonási listából törlődnek a lejárt tanúsítványok). Többször azt is jelenti, hogy a hitelesítésszolgáltató „normál módon" csak az érvényes tanúsítványokról ad információkat, a régiekről legfeljebb valamilyen archív nyilvántartást vezet, s abból lehet érdeklődni.[8]

A tanúsítvány lejártára az alkalmazások általában figyelmeztetni szoktak (de sokszor lehetővé teszik, hogy a felhasználó ennek ellenére mégiscsak használja őket), a magánkulcs lejáratára viszont csak akkor képesek figyelmeztetni, ha annak tanúsítványpárját is ismerik, s a magánkulcs érvényességi idejére vonatkozó korlátozásokat helyesen értelmezik. Ez sajnos nincs mindig így. És ami még ennél is kétségbeejtőbb, az az, hogy az alkalmazások egy része a tanúsítvány érvényességi állapotát sokszor még lekérdezni sem képesek.

4.3.5 Kulcshasználat az érvényességi idő után

Valójában a kulcsok felhasználása az érvényességi idő leteltével (illetve állapotának érvénytelenné válásával) sem tiltott teljesen, csak erősen korlátozott. Lássuk, mik ezek a korlátok „általában véve".

A titkosításra vonatkozóan:

- A nyilvános kulcs titkosításra már nem használható.[9]
- A magánkulcs visszafejtésre még használható.[10]

Az aláírásra vonatkozóan:

- A magánkulcs aláírás megtételére már semmiképpen nem használható.[11]
- A nyilvános kulcs aláírás ellenőrzésére még használható.[12]

A felhasználónak a tanúsítvány érvényességi idejének lejáratát követően, illetve visszavonás után az aláíró magánkulcsot meg kell semmisítenie[13].

4.3.6 Aláírás érvényességének ellenőrzése

Amikor az érvényességi idő és állapotok tekintetében ellenőrizzük egy aláírás érvényességét (az érvényesség teljes ellenőrzése ettől összetettebb), akkor a legtöbb esetben a tanúsítvány korabeli érvényességére vagyunk kíváncsiak. Vagyis arra, hogy a tanúsítvány érvényességi ideje még nem járt le, állapota

még érvényes volt akkor, amikor az aláírást megtették. Vannak azonban olyan esetek is, amikor a korábban aláírt információ ellenőrzésénél nem (vagy nem csak) erre, hanem az aláírás ellenőrzéséhez használatos tanúsítvány jelenlegi érvényességének megállapítására van szükség.

Az első esetben nem érdekel minket, hogy a tanúsítvány vagy a magánkulcs érvényességi ideje lejárt-e, illetve a tanúsítványt visszavonták-e az aláírás megtételét követően. A második esetben viszont az is érdekel minket, hogy még mindig, az aláírás ellenőrzésekor is érvényességi idején belül van-e a tanúsítvány, és még inkább az, hogy a tanúsítvány állapota érvényes-e.

A második esettel összefüggésben, azonban van egy kis probléma. Említettem, hogy tanúsítványt visszavonni csak annak érvényességi ideje alatt lehet. Utána a hitelesítésszolgáltató már nem fogad el rá visszavonási kérést, és nem is ad róla állapotinformációt. Ha a lejárat után derül ki, hogy a tanúsítványt vissza kellett volna korábban vonni (mert hamis volt), akkor hiába minden, azt már nem lehet megtenni jelen dátummal sem.[14] Még ennél is nagyobb gond, hogy az érvényességi idő leteltével a tanúsítvány és annak állapotinformációi esetleg törlődhetnek a hitelesítésszolgáltató nyilvántartásaiból, s így azok lekérdezésére nincs mód.[15] Így aztán aki utólagosan, a tanúsítvány lejártát követően kíváncsi ezekre az adatokra, az könnyen hoppon maradhat.

Ezek valójában nem is esetek szoktak lenni, hanem bizonyos típusú tanúsítványok esetében van igény az egyik vagy a másik típusú lekérdezésre.[16] Azoknál a tanúsítványoknál, ahol az utóbbira van szükség, a magánkulcs érvényességét a tanúsítvány érvényességénél jóval rövidebbre szokták venni, amit a tanúsítványban is jelölnek. Ez azt jelenti, hogy az ilyen kulccsal aláírni, mondjuk, egy évig lehet, de tanúsítvány párját az aláírás ellenőrzésére akár két évig is fel lehet használni, s a hitelesítésszolgáltató két évig fogad el visszavonási kérelmeket a tanúsítványra.[17]

4.4 Kulcsmenedzsment

A nyilvános és magánkulcsok menedzsmentje a tanúsítványok kezelésével szorosan összefüggő terület, azonban attól mégis megkülönböztetendő.

4.4.1 Kulcspárgenerálás

A nyilvános és magánkulcsokat különféle helyeken lehet előállítani, melyeknek különböző előnyei és hátrányai vannak. Ezt nem úgy értem, hogy a nyilvános kulcsot különböző helyen lehetne előállítani, mint magánkulcs párját, hiszen a kettőt egy és ugyanaz a matematikai algoritmus generálja azonos helyen és időben. Ez a kulcspárgenerálás azonban több helyen is bekövetkezhet, amely helyeket két nagy csoportba lehet sorolni.

A hitelesítésszolgáltatónál:
- a hitelesítésszolgáltató központi rendszerében (hitelesítőegységnél),
- a hitelesítésszolgáltató kihelyezett rendszerében (a regisztrációs egységnél).

A felhasználási és őrzési helyen:
- szoftveres úton a felhasználó számítógépében,
- a felhasználó aláíró (hardver) eszközében.

A hitelesítésszolgáltatónál történő kulcsgenerálás előnye, hogy az így előállított kulcs magasabb biztonsági követelményeknek tud megfelelni a szolgáltatónál rendelkezésre álló erőforrások, szakértelem és kialakult szabályrendszer következtében. Hátránya azonban, hogy ez esetben a magánkulcs őrzési helyre juttatásáról gondoskodni kell, méghozzá biztonságos módon, úgy, hogy az más számára ne legyen felderíthető. Hátránya még az is, hogy így a szolgáltató tudomással bírhat a magánkulcsról. Ha azt meg is semmisíti a szabályai szerint, a lehetőség fennáll az ezzel való visszaélésre, s így a felhasználók bizalma korlátozott lehet.

A felhasználási és őrzési helyen történő kulcsgenerálás előnye, hogy ezen a módon a magánkulcsnak soha nem kell elhagynia a felhasználás zónáját (különösen a hardvermodulok esetében), s így arról a szolgáltató sem bír tudomással. Nem hátrány, de feladat az, hogy ilyen esetben a nyilvános kulcs szolgáltatóhoz történő juttatásáról kell gondoskodni, s bizonyítani kell azt, hogy a kérdéses nyilvános kulcs magánkulcs párja valóban a rendelkezésünkre áll (nem valaki más nyilvános kulcsát nyúltuk le)[18].

A legjobb az a módszer, amikor a generálás a felhasználó aláíró eszközében, de a szolgáltató helyszínén történik (ez nem a kettő kombinációja, hiszen nem helyszínekről beszéltünk eddig) a szolgáltató és a felhasználó közös ellenőrzése mellett[19]. Ez esetben ugyanis érvényesülhetnek a szolgáltató biztonságot garantáló szabályai, s a magánkulcsnak nem kell elhagynia az aláíró eszközt, de a nyilvános kulcs szolgáltatóhoz juttatása és a kulcspár összetartozásának bizonyítása sem probléma. Az az igazság, hogy a kulcspárgenerálás olyan bizalmi dolog (hiszen ez az egyetlen pillanat, amikor az algoritmus sebezhető[20]), hogy jobb, ha mindenki ott van, és figyel. Még akkor is, ha tulajdonképpen nem lát semmit.

4.4.2 A magánkulcs tárolása és védelme

Mivel a magánkulcs védelme alapvető fontosságú a védelmi rendszer szilárdsága szempontjából, ezért biztonságos tárolására különböző módszereket fejlesztettek ki. A tárolás alapvetően két módon történhet: állományban vagy hardvermodulban (néha tévesen szokták szoftveres és hardveres tárolásnak is nevezni, valószínűleg a kulcsgenerálással keverve).

Az állományban történő tárolás alatt általában egy hajlékonylemezt vagy az aláírásra felhasznált számítógép háttértárolóját kell érteni, s bár a kettő közül az

előbbi a biztonságosabb, az alkalmazások legtöbbje pont azt támogatja kevésbé. A hardvermodul legtöbbször egy intelligens kártya, de lehet az egy token vagy HSM-modul[21] is, illetve elvileg bármilyen, adattárolásra és aláírásra alkalmas szerkentyű.

Az állományban történő tárolás legnagyobb hátránya, hogy így a kulcs könnyen és észrevétlenül másolható. A számítógép háttértárolója ráadásul nem eltávolítható az aláíró környezetből, és így a magánkulcs könnyen hozzáférhető mindazok számára, akik a géphez hozzáférnek. A hajlékonylemez a felhasználás idejét követően egyszerűen kivehető a számítógépből, és így másik helyszínen is felhasználható (igaz, ez meg a hagyományos „elemelem" módszerrel egyszerűen meglovasítható).[22] Így az aláírás elvégzése nem kötődik egy adott géphez.

A hardvermodulok legtöbbje (azok, amelyek a hétköznapi felhasználóknak vannak szánva) a hajlékonylemezhez hasonlóan hordozhatók, s van egy nagy előnyük az állományban történő tároláshoz képest: az, hogy nem másolhatók. Olyan könnyen legalábbis egyikük sem, mint egy hagyományos állomány. A hardvermodulok nagy része képes arra is, hogy maga generálja a kulcsokat, és a magánkulcs modulból való kiolvasását megakadályozza.

Akármelyik módon történik is a tárolás, a magánkulcs védelmét ki szokták egészíteni egy másodlagos módszerrel is. Ez általában a kulcs titkosítását jelenti, amely titkosítást egy aktivizáló adat (jelszó vagy PIN-kód) megadásával lehet feloldani. Kevésbé hagyományosabb esetben ez a másodlagos védelem személyi azonosítás is lehet, akár biometrikus jellemzőket alapul véve.

4.4.3 Különböző kulcsfajták és ezek kezelése

Mind elviekben, mind gyakorlatilag lehetséges, hogy ugyanazon kulcspárt különböző célokra használjuk, például ugyanazon kulcspárral titkosítsunk, mint amellyel megejtjük az elektronikus aláírást (ugyanazon magánkulccsal írjunk alá, mint amivel a titkosított elektronikus iratokat visszafejtjük; s ugyanazon nyilvános kulccsal tegyük lehetővé a számunkra történő titkosítást, mint amelyikkel az aláírásunk ellenőrzése lehetséges). Van azonban néhány olyan szempont, elsősorban kulcsmenedzsmenttel kapcsolatos körülmények és követelmények, amelyek annyira eltérőek e két felhasználás esetében, hogy emiatt nem ajánlott ugyanazon kulcspárt több különböző célra alkalmazni. Ez egyre kevésbé is van szokásban, helyette inkább külön kulcspárokat adnak ki minden egyes felhasználási célra a kulcs tipizálásával (vagyis a tanúsítványban jelölik, hogy a kulcspár milyen célra lett kibocsátva).

De melyek ezek az eltérő menedzsmentkövetelmények a nyilvános és a magánkulcsra vonatkozóan? Az alábbi táblázat különböző szempontok szerint hasonlítja össze az aláírás és a titkosítás céljára kibocsátott kulcsokat.

	Aláíró kulcs	Titkosító kulcs
Nyilvános kulcs		
Archiválás	Régebbi aláírások ellenőrzését lehetővé téve archiválandó	Általában nincs szükség az archiválására[23]
Magánkulcs		
Tárolás	Kizárólag a tulajdonos személyes hozzáférése engedélyezett	Meghatározott kör számára a tulajdonoson kívül is elérhetővé kell tenni (akikkel megosztja a titkos ügykezelést)
Biztonsági mentés	Nem mentik, szükség esetén újragyártják[24]	Mentés szükséges lehet a titkosított dokumentumok visszafejtése érdekében
Meg-semmisítés	Lejárat után megsemmisítendő	Nem semmisítik meg, hogy lejárata után is visszafejthetőek legyenek a titkosított információk

A kulcsmenedzsment-szempontokon túl egyéb megfontolások miatt is különbséget tehetünk a két felhasználás között. Bár egyre kevésbé jellemző, legalábbis hazánkkal szemben, de például eltérő exportkorlátozási tilalmak lehetnek érvényesek a titkosító algoritmusoka, és megint mások az aláírókra (a titkosításra általában szigorúbbak). Üzleti, műszaki és biztonsági szempontok is szükségessé tehetik, hogy különböző célokra különböző algoritmusokat, eltérő kulcsméreteket vegyünk igénybe (választhatunk akár az egyik célra egy teljesen más megoldást, mint a másikra, lehet az egyik például egy licencköteles megoldás, a másik meg egy szabad felhasználású[25]). Egyes, kötelezően betartandó közösségi előírásoknak, szabványoknak vagy akár törvényeknek is lehetnek olyan előírásai, amelyek direkt vagy indirekt különböző kulcsfelhasználást tehetnek szükségessé[26].

Bár elviekben lehetséges volna, hogy ugyanazon tanúsítványban több nyilvános kulcs is helyet kapjon, ez azonban bonyodalmakat okozna. A gyakorlatban erre nincsen példa, a magánkulcsok és tanúsítványok kizárólag egy az egyben párosodnak: egy magánkulcs egy tanúsítvány, másik magánkulcs másik tanúsítvány. Arra ugyan továbbra is van lehetőség, hogy a tanúsítványban szereplő egyetlen kulcsot több célra is használjuk (ez esetben az összes használati cél fel van tüntetve a tanúsítványban), de ha különböző célokra eltérő kulcsokra van szükségünk, akkor ez több tanúsítványt is jelent.

A „szimpla" aláíró és titkosító kulcsokon kívül egyéb felhasználások, illetve e felhasználásoknak egyéb alfajai is léteznek.[27] Ezek kulcsmenedzsment-követelményeit és egyéb megfontolásait most nem veszem sorra, de annyit röviden is mondhatok, hogy a végeredmény hasonló lesz.

Vannak ugyanakkor olyan alkalmazások, amelyek nem foglalkoznak azzal, hogy a kulcs milyen célra lett kibocsátva, s nem is kezelnek csak egyetlen kulcspárt. Ezek az aláírás és a titkosítás céljára ugyanazt a kulcspárt használják. Irányukban kár mindenfajta jóakarat, csak reménykedni lehet, hogy előbb-utóbb érkezik egy következő verzió, ami ezt a kérdést is megnyugtatóan megoldja.

4.4.4 Magánkulcs letét

Mivel hosszú magyarázatot igényelt volna, az előbbiekben szándékosan nem említettem a magánkulcs letét kérdését, bár szintén különbségtételt követel a kulcstípusok kezelésében. Egy külön fejezetben azonban nem tudok ellenállni a kísértésnek.

A magánkulcs letét – talán nem lesz nagyon meglepő – a magánkulcs letétbe helyezését jelenti. A letétbe helyezésnek a biztonsági megőrzés a célja, de nem ugyanarról a biztonsági mentésről van szó, mint az előbb. A biztonsági mentést általában a felhasználó maga oldja meg, a magánkulcs letét pedig egy szolgáltatás, amit a hitelesítésszolgáltató nyújt. A cél mindkét esetben hasonló: másolat biztosítása a magánkulcsról arra az esetre, ha az eredeti kulcsebek harmincadjára jutna. Ez utóbbi esetben azonban a magánkulcs másolatának tárolása egy központi rendszerben történik. Ez biztonsági szempontból előnyösebb lehet a felhasználó számára is (hiszen saját másolata könnyen juthat az eredetivel azonos sorsra), bár a kisördög végig benne lehet amiatt, hogy rejtjelezett dokumentumaihoz így esetleg más is hozzáfér. Annál is inkább, mert ez utóbbi esetben a magánkulcshoz rendszerint deklaráltan más is hozzáférhet. Igaz, ez a más mindig csak egy meghatározott szűk kör lehet, fizikailag csak a szolgáltatót jelenti, logikailag pedig a munkáltatót s esetleg különböző hatóságokat. Bár minden ilyen hozzáférésről elviekben értesíteni szokás a felhasználót, vannak, akiket ez nem nyugtat meg. Még az sem, hogy a szolgáltató rendszere az ilyen adatokat (normális esetben) rejtjelezve tárolja, s a hozzáféréseket szigorúan szabályozza és naplózza.

Lehetnek azonban olyan helyzetek, amikor a felhasználónak nincs választási lehetősége, eszi, nem eszi, nem kap mást. Vagy mert a szolgáltató így működik, vagy mert a közösségnek ilyenek a szabályai, vagy mert olyan országban él, ahol ez törvényi előírás[28].

Akármi is az ok, a letét kivétel nélkül és kizárólag csak a titkosítás és kulcsegyeztetés céljára szolgáló magánkulcs letétbe helyezésére vonatkozhat. Aláírás céljára szolgáló magánkulcsra semmilyen körülmények között sem. Éppen ezért olyan esetekben, ahol a titkosító magánkulcs letétbe helyezése szükséges, az aláíró kulcsot mindenképpen külön kell választani titkosító kulcstól.

4.5 Tanúsítványok osztályozása

Már utaltam arra, hogy a kulcsok felhasználásától függően különböző kulcstípusokat és ehhez igazodóan különböző tanúsítványokat bocsátanak ki. Ennek megfelelően mondhatjuk azt például, hogy léteznek aláíró és titkosítótanúsítványok. De messze nem ez az egyetlen osztályozási lehetősége a tanúsítványoknak. A tanúsítványok különböző szempontok szerint, különböző „rendekbe" szerveződnek, s nem is olyan könnyű az ennek megfelelő rendszerezés. A két legfőbb „rend" az osztályoké és típusoké, amely fogalmakat még a hozzáértők sem kezelik mindig egységesen és helyesen.

4.5.1 A rendezés módja

Ha szükségünk van egy tanúsítványra, akkor nem mondhatjuk meg részletesen a szolgáltatónak, hogy az milyen adatokat tartalmazzon, milyen jellemzőkkel bírjon (például legyen benne a nevem, de más adatom nem, aláírásra legyen jó, DSA algoritmussal működjön, 1024 bites kulcsmérettel stb.). A szolgáltatók legalábbis ilyen jellegű kiszolgálásra nincsenek felkészülve. Ha az összes attribútum szerint lehetne tanúsítványt igényelni (úgy, mint az autóknál motort, festést, kárpitot, extrákat), az nagyon sok variációt jelentene. Ez több szempontból sem lenne előnyös. Leginkább abból a szempontból nem, hogy így az egyes tanúsítványok nem lennének összehasonlíthatók, aminek következtében az aláírás elfogadója se tudná hova tegye (mennyire bízhat meg benne) az adott aláírást. Viszont a mégisesak eltérő igények miatt az se lenne jó senkinek, ha mindössze egyetlen fajta tanúsítványt lehetne kapni.

Ezért a hitelesítésszolgáltató inkább különböző csomagokat állít össze, és ezzel biztosítja az arany középutat a választék és egyszerűség között. Vagyis a tanúsítványok ugyanazon szolgáltatón belül is különböző osztályokba és típusokba szerveződnek (olyan ez, mint a távközlési cégek előfizetési csomagjai). De hogy ne legyen olyan egyszerű az élet, itt is több szolgáltató van, melyek korántsem egységesen alakítják ki a csomagokat, így az egyes gyártóknál alkalmazott tanúsítványosztályok és -típusok sokszor még csak nem is hasonlítanak egymásra.

4.5.2 Tanúsítványok típusai

A tanúsítványokat a felhasználás módja és célja, valamint a tulajdonos jellege szerint szokták típusokba sorolni. Így például aszerint, hogy magánember, szervezet vagy valamilyen hardverberendezés (webszerver, tűzfal, útválasztó stb.) a felhasználó, vagy aszerint, hogy a tanúsítvány elektronikus levelezés, internetes áruház, időbélyegzés, szoftveraláírás, netán hitelesítésszolgáltatás céljára készül. Ez összefüggésben lehet azzal, hogy mi a kulcs típusa, de nem ugyanarról van szó (bár az időbélyegzés és a szoftveraláírás csak aláíró kulcsot igé-

nyel, az elektronikus levelezés és az internetes áruház pedig mind az aláíró, mind a titkosító kulcsot igényli). Így aztán van példa bőven arra, hogy ugyanazon tanúsítványtípuson belül adnak ki kulcstípusában eltérő tanúsítványokat.

Bár a típusba sorolás sokféle elv szerint történhet, annyi mégis összeköti őket, hogy valamilyen formában meghatározzák a lehetséges felhasználókat és a felhasználás módját. Hogy ez pontosan micsoda, az nem feltétlen nyilvánvaló (sőt a legtöbbször nem az), így ezt a hitelesítésszolgáltató részletesen le szokta írni.[29] A szolgáltató maga is eltérő módon kezelheti az ilyen tanúsítványokat, így a leírásból ez sem szokott hiányozni.

Hogy kissé világosabb legyen mindez, összeállítottam egy lehetséges, képzeletbeli típustáblázatot a felhasználó és felhasználás megnevezésével (ez a nagyon leegyszerűsített táblázat kimondottan csak demonstrációs célokat szolgál):

Típus	Felhasználó típusa	Felhasználás célja
Magán	Magánszemély	Biztonságos levelezés és böngészés
Céges	Természetes személy mint a cég alkalmazottja	Biztonságos levelezés és böngészés
Eszköz	Hálózati eszköz magánszemély vagy cég tulajdonában	Biztonságos webszolgáltatások, VPN kialakítása
Szoftver-aláírás	Magánszemély vagy cég	Szoftverek származásának biztosítása

A tanúsítvány típusa és a felhasználás célja jelölhető a tanúsítványban is, de az erre vonatkozó részletes szabályozást csak a szolgáltató előírásai tartalmazhatják szöveges formában.

4.5.3 Tanúsítványok osztályai

A tanúsítványtípussal ellentétben osztályba sorolni nem a felhasználó vagy a felhasználás jellege szerint szokták a tanúsítványokat, hanem erősség szerint. Az erősség a tanúsítványok esetében biztonsági szintet jelent, de messze nem csak az algoritmikus biztonságot értve alatta. Sőt elsősorban nem azt, hanem a már említett két másik tényezőt, ami a tanúsítvány biztonságát meghatározza: a felhasználó azonosításának módszerét és a magánkulcs biztonságát. A kulcs algoritmusánál és méreténél fontosabb tényezőként ide értik továbbá a hitelesítésszolgáltató által a tanúsítvány és kulcsok biztonságára foganatosított egyéb intézkedéseket is.

Tanúsítvány és tanúsítvány között ezek kombinálásával olyan különbségek tudnak kialakulni, mint, mondjuk, egy VW Polo és egy Passat között[30] (hogy ugyanannál a gyártónál maradjunk). Vannak tanúsítványok, amelyek gyakorlatilag sem-

mit sem érnek, mert, mondjuk, a kibocsátó egyáltalán nem kezeskedik azért, hogy a tulajdonos valóban az, aki fel van benne tüntetve. Vannak viszont olyanok is, amelyekhez nagyon komoly garanciák kapcsolódnak. A probléma ott van, hogy míg rápillantva az autóra rögtön tudjuk, mivel is van dolgunk, addig a tanúsítványon nem látszódik, vagy ha látszódik, nem könnyen értelmezhető az osztálya.

A tanúsítványosztályokat általában betűjelek (A, B, C) vagy számok (1, 2, 3) különböztetik meg egymástól (az autós hasonlatot tovább gondolva, mint a Mercedes és a BMW esetében). Az egyes osztályok közötti különbségek mint ég és föld, de arra, hogy melyik jel jelöli a magasabb értékű tanúsítványt, nincs általánosan elfogadott vagy kötelező erejű szabvány, megállapodás arra még kevésbé, hogy a különböző osztályokhoz milyen biztonsági eljárásoknak és garanciáknak kell kapcsolódni. Így az egyes hitelesítésszolgáltatók azonos vagy hasonló elnevezésű tanúsítványosztályai véletlenül sem feleltethetők meg egymásnak automatikusan a jelölés alapján. Az egyetlen dolog, amit tehetünk, ha valóban meg akarunk bizonyosodni arról, hogy a kezeink közé került tanúsítvány milyen biztonsági szintet testesít meg, a szolgáltató dokumentációinak fellapozása.[31]

Ez a feladat azonban egy átlagos felhasználó számára több mint kétségbeejtő, így nem véletlen, hogy az európai szabályzás – és azt követve a magyar is – megalkotta a minősített tanúsítvány fogalmát. Ez bizonyos mértékig megoldja a problémát azáltal, hogy a minősített tanúsítványt mint egy „szuperosztályt"[32] definiálja, és számtalan előírással szabályozza a rá vonatkozó követelményeket. Ugyan ezenkívül (és akár ezen belül is) a szolgáltató definiálhat különböző osztályokat, a minősített és nem minősített jelző lámpásként a sötétben utat mutathat (bár a nem minősített nem jelenti azt, hogy az nem minőségi).

A típustáblázathoz hasonlóan álljon itt egy képzeletbeli osztálytáblázat az osztály és annak jellemzőinek bemutatására (a jellemzők szigorúan csak kiragadottak, ennél sokkal több és részletesebb elemzést kívánó különbség szokott lenni).

Osztály	Jellemzők
Minősített „A" osztály	Szigorú felhasználóazonosítás Intelligens kártya kulcshordozó, hardveres kulcsgenerálás Aláíró kulcs: DSA 1024 bit, titkosító kulcs: RSA 1024 bit Érvényességi idő: 1 év
Fokozott biztonságú „B" osztály	Szigorú felhasználóazonosítás Token kulcshordozó, szoftveres kulcsgenerálás Aláíró és titkosító kulcs: RSA 1024 bit Érvényességi idő: 1 év
Teszt „C" osztály	Felhasználóazonosítás nélkül Floppy kulcshordozó, szoftveres kulcsgenerálás Aláíró és titkosító kulcs: RSA 512 bit Érvényességi idő: 1 hónap

A különböző osztályú tanúsítványokat a legtöbbször különböző hitelesítőegységek adják ki, melyek gyökér szinten sem találkoznak, annak érdekében, hogy a tanúsítási láncok se találkozzanak egymással. Így az alkalmazások a gyökér hitelesítőegységgel tudják azonosítani az osztályt, s aszerint képesek automatizálni annak elfogadását, illetve visszautasítását (elképzelhető, milyen zavart okozhatna, ha a fenti „A" és „C" osztályt ugyanaz a hitelesítőegység adná ki)[33].

4.5.4 Osztály és típus viszonya

Az osztályok és típusok együtt egy mátrixot alkotnak, vagyis megadható, hogy milyen típusból milyen osztályt kérek. A kulcs típusával együtt ez a mátrix nem is két-, de háromdimenziós. Nem biztos ugyanakkor, hogy a mátrixnak minden kockája „él", egyes típusok lehet, csak erősebb osztályban állnak rendelkezésre, vagy fordítva.

Mint ahogy előbb-utóbb több bankkártyája lesz az embernek, ugyanúgy valószínűsíthető, hogy különböző célokra más-más tanúsítványt fog igényelni. Minden egyes szerepköréhez egy újat (magánemberként, egy cég alkalmazottjaként, egy szervezet képviselőjeként stb.), amelyek eltérő műszaki és garanciális jellemzőkkel rendelkezhetnek, más adatokat tartalmaznak.

4.6 Tanúsítványok kibocsátása

Lassan eljutottunk oda, hogy ildomos tisztázni, miként is lesz a tanúsítvány. A gólyamese lassan kezd gyermeteg lenni a sok zavaró utalás miatt, s már-már egyenesen bántó az igazság hiánya. Azt már tisztáztuk, hogy a tanúsítványt hitelesítésszolgáltatók bocsátják ki, ha azt a felhasználó igényli. Ilyen esetekben a hitelesítésszolgáltató megállapítja az igénylő (személy- és egyéb) azonosságát, felveszi annak adatait, majd legyártja a tanúsítványt, és eljuttatja azt a részére. Egyszerű – ahogy ezt mondani szokták –, mint az ágybavizelés. Majdnem olyan egyszerű.

4.6.1 Tanúsítványigénylés

A tanúsítványigénylés egy üzleti művelet, melynek elsősorban jogi és adminisztratív vonatkozásai vannak. A tanúsítvány igénylése – akárhogy is nézzük – végül is egy áru (és az ahhoz tartozó szolgáltatások) megrendelését jelenti. Ez a tanúsítvány kibocsátásának első mozzanata: a leendő felhasználó jelzi a hitelesítésszolgáltató felé, hogy hőn áhítozik egy tanúsítvány után. Ezt az igénylő leggyakrabban egy erre rendszeresített tanúsítványigénylő formanyomtatvány (űrlap) segítségével teheti meg. A formanyomtatvány ölthet papír alakot vagy elektronikus formát, s ennek megfelelően az igénylés történhet papíron vagy elektronikus úton (e-mailben, webes űrlap kitöltésével, egy erre alkalmas szoft-

verrel, esetleg WAP-on stb.). Egyes esetekben történhet az igénylés explicit módon is, a felhasználó által elrejtve annak részleteit, egy összetettebb tranzakció részeként vagy automatikusan, amikor egy szervezet, cég tagjává válik a felhasználó.[34]

Az űrlapon kell megadni az igénylő és a felhasználó azon adatait, amiket a tanúsítvány tartalmazni fog s azokat, amiket a hitelesítésszolgáltató belső használatra tart meg. Ha a kulcspárt a felhasználó gyártotta le, akkor az igényléshez csatolnia kell saját nyilvános kulcsát és a magánkulcs tulajdonlását bizonyító aláírását is. Az űrlapon közölheti az ügyfél különböző óhajait-sóhajait is a tanúsítvány osztályával, típusával és „felszereltségi csomagjával", azaz kulcstípusával, kulcshordozójával és egyéb választható paramétereivel kapcsolatban.

Az igénylés előtt vagy azzal egyidejűleg az ügyfél tájékoztatást szokott kapni a felhasználás különböző kondícióiról, a szerződéses feltételekről, saját jogairól és kötelezettségeiről és mindenfajta egyéb körülményről, beleértve az alapvető üzleti, műszaki és biztonsági vonatkozásokat. A formanyomtatvány aláírásával az ügyfélnek nyilatkoznia kell különböző dolgokról, például arról, hogy megfelelő tájékoztatást kapott, a szolgáltató szerződéses feltételeit, szabályzatait megértette és elfogadja, hogy minden nagyon szép, mindennel meg van elégedve, és legfőképpen arról, hogy hozzájárul tanúsítványa közzétételéhez. Ezzel jogi értelemben egy szolgáltató–ügyfél kapcsolat, azaz szerződés jön létre a két fél között.

Előfordulhat, hogy a szerződés aláírására csak a tanúsítvány kiadásakor kerül sor, például ha igényléskor elektronikus formanyomtatvány lett kitöltve, sőt olyan helyzet is előfordulhat (elsősorban nem üzleti alapon működő szolgáltatóknál), hogy ilyenre nincs szükség. Elektronikus formanyomtatványok esetében arra is szokott lehetőség nyílni, hogy azt elektronikus aláírással lássa el az ügyfél, ha már rendelkezik tanúsítvánnyal (bár erre a szolgáltatók csak saját, esetleg egy „baráti" szolgáltató által hitelesített tanúsítványt szoktak elfogadni).[35]

Tanúsítvány igénylésére új tanúsítvány kibocsátásakor vagy lejárt tanúsítvány megújításakor szokott szükség lenni. Tanúsítvány frissítésekor az igénylés egyszerűsített változatára szoktak sort keríteni a szolgáltatók.

4.6.2 Szerepek

Mielőtt továbbmennénk, nem árt tisztázni a különböző szerepeket – amelyek a tanúsítvánnyal kapcsolatban felmerülhetnek – és a könyv erre vonatkozó szóhasználatát. Eddig olyan szavakat használtunk a tanúsítvánnyal kapcsolatba hozható személy jelölésére, mint tulajdonos, felhasználó, igénylő, aláíró, ügyfél stb. Ezek alatt általában ugyanazt a valakit értettük, csak máshonnan megközelítve személyét. Az „igénylő" annyiban lóg ki egy kicsit a sorból, hogy ő még nem kapta meg a tanúsítványt, csak reménybeli tulajdonos. A „tulajdonos" kifejezés ugyanakkor nem a leghelyesebb, mert ez egy jogi kategória, s tulajdonképpen nincs olyan előírás vagy általános érvényű szabály, amely megmon-

daná, hogy a tanúsítvány tulajdonjoga kié (az esetleg maradhat a szolgáltatónál). Az „aláíró" gyengesége, hogy titkosítótanúsítványokra csak megfelelő absztrakciós készség birtokában értelmezhető (ezért ilyen esetekben kerülni is próbáltuk). A „felhasználó" egész jó, az „ügyfél" pedig kicsit sarkosan az üzleti szolgáltató szemszögéből nézi emberünket. Az „ellenőrző", „elfogadó" és „érintett fél" kifejezések (néha a „felhasználó" is) viszont egy másik személyre vonatkoznak, arra a valakire, aki a másik oldalon állva az aláírást és a tanúsítványt ellenőrzi, illetve a titkosítást visszafejti.

Nem csoda ez a kis zavar, hiszen több személy is kapcsolatba hozható a tanúsítvánnyal. A tanúsítványnak mindenesetre biztosan lennie kell egy azonosítójának, ami megmondja, hogy ki számára lett az kiadva. Ez az azonosító azonban megnevezhet egy magánszemélyt, egy szervezetet annak szervezeti egységeivel együtt, egy eszközt annak valamilyen azonosítója alapján, vagy mindezeket egyszerre valamilyen összefüggésben és még mást is. Ráadásul a tanúsítvány igénylője eljárhat megbízás alapján is (ami gyengíti a biztonságot), vagyis nem biztos, hogy ő a tanúsítványban megnevezésre kerül. Az egyszerűség kedvéért az összes ilyen bonyolult variációval nem foglalkozom, csak egyes tipikus és gyakori eseteket gondolok végig.

4.6.3 Azonosító és azonosítás

Elnézést, hogy megint ilyet mondok, de a tanúsítvány azonosítójának a célja nem olyan nyilvánvaló, mint ahogy az elsőre látszik. Azt gondolhatnánk, arra való, hogy mindenki számára egyértelműen megmondja, kié a tanúsítvány. Ez azonban korántsincs mindig így. Egy kisebb (vagy nagyobb, de jól szervezett) közösségben ez még lehetséges, például egy cégen belül megmondhatjuk, hogy ez a tanúsítvány Kovács Béláé, aki a gazdasági igazgatóság számviteli osztályának bérszámfejtő csoportjában dolgozik, és így mindenki tudni fogja, körülbelül kiről van szó. Legalábbis a cégen belül, s így ez az azonosítás kiválóan megfelelhet arra a célra, hogy Kovács Béla a cég munkatársainak elektronikusan aláírva küldje el bérszámfejtési fvüket. Ha viszont Kovács Béla történetesen az adóhivatallal és a nyugdíjfolyósítóval is elektronikusan aláírva akar kommunikálni, akkor már nem biztos. Ha Kovács Béla magánszemélyként akar eljárni, biztosan nem. Ahhoz viszont, hogy Kovács Béla magánszemélyként azonosítható legyen, azaz meg lehessen mondani, hogy a kétezer, világszerte élő Kovács Béla közül melyik Kovács Béláról van szó, más módszerek szükségesek. Ha lenne egy általánosan használt hivatalos egyedi azonosítója mindenkinek (mint a személyi szám volt), akkor a probléma részben megoldódna[36]. Részben azért, mert az egyedi azonosító alapján csak a hatóságok képesek megállapítani, kiről van szó, az egyszeri emberek nem (ők csak hatósági segédlettel). A második módszer lehetne az, hogy az azonosítóba beleírjuk Béla pontos címét, születési idejét és helyét, anyja nevét, leánykori nevét stb. Ez ugyan sokat segítene, de kinek kellene egy ilyen tanúsítvány? Ki akarná azt, hogy ezekhez az

adatokhoz bárki hozzáférjen? Nem is szólva arról, hogy a cím nem egy állandó adat. Egy elektronikus személyi igazolványban szerepelhetnek ezek az adatok (bár a lakcímet már most is külön cédulázzák), de nem egy tanúsítványban. Olyanról is hallottam már, hogy a tanúsítványba fényképet raknak, de ennek ritkán lehet értelme, hiszen pont az arctalan elektronikus kommunikációhoz szükséges a tanúsítvány.

De akkor mi a megoldás? Nos, nincs igazándiból általánosan érvényes megoldás (főleg nem olyan, ami kardcsapással megoldaná a csomót), azt mindig a felhasználás módjától, az alkalmazói közösségtől és egyéb körülményektől függően kell kiválasztani. Ez már korántsem műszaki probléma, s a technikai megoldások kevéssé segíthetnek. A gyakorlatban nagyon sok esetben az azonosító mindössze a felhasználó neve, amit egyes esetekben kiegészítenek cégnévvel (céges tanúsítványok esetében) vagy a lakóhely szerinti várossal. Jogos a kérdés, hogy ezzel mit lehet kezdeni, de a helyzet azért nem annyira zűrös, mint amilyennek látszódik.

A magánéletben történő felhasználás esetén eddig is jól megvoltunk azzal, hogy egy adott e-mail-címről kaptunk levelet, most legfeljebb ha kétkedésre okot adó körülményt találunk, egy baráti telefonhívással tisztázzuk a tanúsítvány azonosítójának értelmezését. Legalább nem idegenedünk el egymástól, és hallhatjuk barátunk, kolléganőnk csengő hangját. Az üzleti életben tipikus tanúsítványok esetében a cég nevének feltüntetése általában megoldja a problémát (hacsak nincs két ugyanolyan nevű kolléga a cégen belül), így ezt tovább nem is ragozom. Az államigazgatással való kommunikáció azonban már érdekesebb feladvány. Itt két módszer kínálkozik.

Az egyik a minden fontosabb hatóságnál alkalmazott egyedi azonosító (adóazonosító jel, taj-szám, személyi szám, esetleg személyiigazolvány-szám) belefoglalása a tanúsítványba. Ez esetben persze minden hivatalhoz külön tanúsítvány szükséges, mert ezek az azonosítók nem találkozhatnak sehol, főleg nem egy nyilvános tanúsítványban. A másik megoldás, mely kissé takarékosabb, egyetlen tanúsítvánnyal oldja meg a problémát, minden hatósági azonosító felhasználása nélkül. Ez esetben ezt a tanúsítványunkat el kell juttatnunk minden olyan hivatalhoz, amivel elektronikus aláírással akarunk kommunikálni, úgy, hogy az bizonyítsa a tanúsítvány személyünkhöz tartozását. Ezt meg lehet oldani egy személyes megjelenéssel, de akár egy levél küldésével is, amit kis kezünkkel még hagyományos úton írunk alá[37].

Sokszor előfordul az is, hogy az azonosítóban a név mellett a tulajdonos adott szervezetben betöltött szerepkörét (finánceführer, fődirektor, atyaúristen) is fel kell tüntetni. Ez az információ legtöbbször fontosabb, mint maga a név, mert a tulajdonos jogosítványairól sokkal többet elárul.

Az azonosító természetesen tanúsítványtípusonként változhat, egy webszerver vagy tűzfal esetében ez például az eszköz domainneve (például www.hotbabes.hu) vagy IP-címe szokott lenni, amelynek értelmezése sokkal kevesebb problémát vet fel.

Az azonosító másik szerepe – a felhasználó azonosításán túl – az egyediség biztosítása a szolgáltató nyilvántartásában. Mivel a nyilvántartásban az azonosító alapján lehet keresni, így az azonosítónak egyedinek kell lennie.[38] Ezért, akármilyen hülyén is néz ki, de számos példa akad arra, hogy azonos nevű felhasználók neve után egy számot írnak. Valahogy így: Kovács Béla 1 és Kovács Béla 394. Erre akkor van szükség, ha az azonosító egyéb (nem név) mezői az egyediséget nem biztosítják. Szerencsés esetben azért akadnak ennél kevésbé idétlen módszerek is.

Az azonosító ráadásul nem szabadul fel a tanúsítvány megújítás nélküli lejáratakor, visszavonásakor, mert arra még jóval később is lehet hivatkozás. Így egy egyszer kiadott azonosítót a szolgáltató soha többet nem használhat fel újra, egy másik tanúsítványban.

Pontot téve az azonosításra, már csak annyi megjegyzést szeretnék hozzátenni a témához, hogy a szolgáltató általában a felhasználónak több adatát tárolja, mint ami a tanúsítványban fel van tüntetve, vagyis a felhasználó egyértelmű azonosítására azért van lehetőség, ha az nagyon szükséges. Ezekről az adatokról azonban a szolgáltató nem ad felvilágosítást egyszerű földi halandóknak[39].

4.6.4 Álnév

Meg kell említeni azt is, hogy a tanúsítványban az igazi név helyett gyakran álnév is feltüntethető, amennyiben az nem megtévesztő. Ilyen tanúsítvány persze üzleti célra csak korlátozottan alkalmas, de olyan esetekben, mikor a kriptográfia nyújtotta biztonságot privátszféránk sérülése nélkül akarjuk élvezni, nagyon is hasznos. A rejtjelezésre például kimondottan jellemző lehet, hogy úgy van rá szükség, hogy inkognitóban kívánunk maradni, valódi énünket még partnerünk előtt sem kívánjuk felfedni. Valódi adatainkat a szolgáltató ilyen álneves tanúsítvány igénylésekor is elkérheti, de azt nem hozza nyilvánosságra. Egyes esetekben azonban – és itt tulajdonképpen csak a hatósági megkeresésre vagy saját magunk ilyen irányú kérelmére tudok gondolni – ezeket a valódi adatokat kiadhatja.[40]

4.6.5 Adatok ellenőrzése

A szolgáltató a tanúsítványigénylő űrlapon felvett adatokat természetesen nem szokta elfogadni bemondásra, hanem azokat különböző módszerekkel ellenőrzi. Méghozzá minden fontos adatot, minden szereplőt és a szerepek jogosságát, azok összefüggéseit is, ha megfelelő gondossággal jár el. A „megfelelő gondosság" azonban sok mindent jelenthet, az egyes szolgáltatóktól, és még inkább az egyes tanúsítványosztályoktól függően. Egyes tanúsítványosztályoknak egészen gyenge azonosítási és ellenőrzési módszerek is megfelelhetnek (különösen tesztelési célra), másoknak pedig (például minősített tanúsítványnak) csak a le-

geslegerősebb. Első esetben elégséges lehet az adatok elektronikus úton való beküldése (elektronikus aláírás nélkül), a másodikban csak a személyes megjelenés elfogadható.

Nézzünk pár leegyszerűsített példát erre:

Ellenőrzés szintje	Adatok forrása	Azonosítás
Gyenge	Weben elküldve	Feltüntetett e-mail-cím létezésének ellenőrzése
Közepes	Faxon elküldve aláírással	Adategyeztetés telefonon
Erős	Személyes megjelenés azonosító okmányokkal	Azonosító okmányok megvizsgálása
Nagyon erős	Személyes megjelenés azonosító okmányokkal és egyéb iratokkal	Azonosító okmányok és iratok megvizsgálása, nyilvános adatbázisokban történő ellenőrzés

A nagy biztonságot garantáló tanúsítványosztályok esetében egy sor személyes adatot fel szoktak venni a felhasználóról, s ezeket a felhasználónak mind igazolni kell. Ilyen esetekben a személyi igazolvány, az útlevél és egyéb okmányok és dokumentumok bemutatása elengedhetetlen. Ekkor természetesen az okmányban szereplő fénykép és aláírás ellenőrzésére is sor szokott kerülni, így a személyes megjelenés ritkán úszható meg. Az e-mail, a fax és a megbízott itt nem segíthet. A szolgáltató a felvett adatokat és a bemutatott okmányokat különböző hatósági nyilvántartásokban is ellenőrizheti (például lakcímnyilvántartás, okmánynyilvántartás stb.), akár minden igénylésnél vagy csak a kétesebb eseteknél[41].

Bonyolítja a helyzetet, ha emberünk egy szervezet nevében kér tanúsítványt, mert ekkor személyes identitásán túl a szervezet azonosságát is igazolnia kell (például alapító okirat), s a szervezet a tanúsítvány kiadásához való hozzájárulásáról is fel kell mutatnia egy meggyőző dokumentumot (mondjuk, egy aláírásra jogosult vezető szívhez szóló levelét).

Felmerülhet a gondolat olvasómban, hogy mit ér az a tanúsítvány, ahol ezek az ellenőrzések nem történnek meg. Sokat nem ér, de azért több célra is megfelelhet. A már említett teszt- és demonstrációs célokon kívül alkalmas lehet például privát levelezésre. Vigyázni kell azonban e tanúsítványok elfogadásával komolyabb ügyletek során. Ezek legfeljebb olyasmit igazolnak, hogy van esély arra, hogy a levelet a tanúsítványban feltüntetett e-mail-cím felhasználója küldte, vagy valaki, aki a feltüntetett telefonszámot felvéve elismerte igényét, amit egy ismert faxszámról küldött a szolgáltatónak. Ezek persze akárkik is lehetnek, hogy valójában kik, azt még a szolgáltató sem tudja. Hogy mennyire egyszerű ezzel visszaélni, bizonyára nem szükséges bizonygatnom.

Akármennyire is furcsa, de egy álneves tanúsítvány, amelynek felhasználóját a szolgáltató akkurátusan ellenőrizte, sokkal nagyobb biztonságot nyújt egy ilyen „valódi nevet" feltüntető tanúsítvánnyal szemben. Ha nagy galiba van, annak utána lehet menni, és meg lehet tudni, ki van valójában mögötte.

4.6.6 Tanúsítvány elkészítése

Az adatok felvételét és ellenőrzését együttesen szokták regisztrációnak nevezni. Ha a regisztráció után az igénylés megkapta a zöld fényt, a szolgáltató elkészíti a tanúsítványt. Egy tanúsítvány elkészítése és az ide tartozó egyéb műveletek nagyjából a következő lépésekből állnak:

- Az űrlap tartalmát a szolgáltató rögzíti belső rendszerében.
- A szolgáltató kulcspárt generál (ha nem a felhasználó biztosította azokat).
- A szolgáltató összeállítja a tanúsítványt, és aláírja saját magánkulcsával.
- A szolgáltató saját adatbázisába elmenti a tanúsítványt.
- A szolgáltató letétbe helyezi a magánkulcsot (titkosító kulcs esetében, opcionálisan).
- A szolgáltató a tanúsítványt nyilvánosan közzéteszi.
- A szolgáltató számlát készít (opcionálisan).

Az egyes műveleteket a szolgáltató informatikai rendszere (az igény rögzítését követően) automatikusan szokta végezni, s azokat naplózza. A műveletek sorrendisége némileg más is lehet, de ez a lényeget nem befolyásolja.

4.6.7 Kézbesítés

Miután elkészült a tanúsítvány, azt a szolgáltató a felhasználónak közvetlenül is át szokta adni a magánkulccsal együtt, a kettőt együtt elhelyezve a magánkulcs hordozóján (floppy, intelligens kártya stb.). Erre azokban az esetekben, mikor a magánkulcs a felhasználó aláíró eszközén generálódott, nem feltétlen van szükség, hiszen a tanúsítványt a szolgáltató nyilvános címtárából a felhasználó maga is letöltheti. Ellenkező esetben gondoskodni kell a magánkulcsot védő aktivizáló adat felhasználóhoz történő eljuttatásáról is. Mindezek átvétele a legbiztonságosabb, ha személyesen történik, a felhasználó személyazonosságának igazolásával. Mivel a tanúsítvány az igénylés ellenőrzése után pillanatok alatt elkészülhet, az egyszerűen megvárható a helyszínen. Ha erre valamiért nincs mód (például központosított kártyamegszemélyesítés miatt a magánkulcs csak napokkal később vehető át), a szolgáltató a legyártott magánkulcsot annak hordozójával és az aktivizáló adattal postán keresztül is kézbesítheti. Ilyenkor azonban a bankkártyák esetében is alkalmazott biztonsági megoldások elengedhetetlenek: biztonságos borítók, kizárólag személyes átvétel, s a magánkulcsnak és az aktivizáló adatnak külön úton vagy időben kell utaznia, úgy, hogy sehol se találkozhassanak, csak a felhasználónál.

Előfordulhat az is, hogy a személyes megjelenésre, az adatok ellenőrzésére s a szolgáltatói szerződés aláírására nem az igényléskor kerül sor, hanem a kézbesítést közvetlen megelőzően. Ezzel a megoldással a szolgáltató némi kockázatot vállal, mert nincs igazi garancia arra, hogy az elektronikus igénylés után a személyes megjelenés, a magánkulcs átvétele és a fizetés megtörténik.

4.6.8 Tanúsítvány megújítása

A tanúsítvány érvényességi idejének végén mód van a tanúsítvány megújítására. Nem mindegy azonban, hogy erre pontosan mikor kerül sor: az érvényességi idő lejárta előtt vagy után. Ha csak egy nappal is utána, akkor az igénylési és ellenőrzési eljárást többnyire ugyanolyan módon le szokták folytatni, mintha a felhasználónak nem is lett volna korábban tanúsítványa. Ha viszont csak egy fertályórával is a lejárat előtt, amikor a tanúsítvány ugyan már a végét járja, de még érvényes, akkor a szolgáltatók legtöbbje módot szokott adni egy egyszerűsített elektronikus tanúsítványigénylésre. Ezt a műveletet szokták nevezni tanúsítványfrissítésnek (mint a megújítás egyik módja).

Ilyen esetben nincs szükség személyes megjelenésre, a még érvényes magánkulcs[42] birtokában az igénylés elektronikusan aláírható. A felhasználónak ilyenkor általában nyilatkoznia kell arról, hogy a tanúsítványban feltüntetett adatai, meg egyáltalán minden adata, amit az eredeti igénylésben megadott, azóta is változatlan és érvényes. A tanúsítvány elkészítése nagyjából a normál módon történik ilyenkor is, de az új nyilvános kulcs és magánkulcs kézbesítése már elektronikus módon, aláírt és rejtjelezett üzenetváltással szokott megtörténni. Ha a tanúsítványosztály biztonsági előírásainak megfelelően a magánkulcsot a felhasználó készíti el, akkor ő küldi el a nyilvános kulcsát a szolgáltatónak, ellenkező esetben a szolgáltató küldi el a generált magánkulcsot a felhasználónak. Nem biztos azonban, hogy ilyenkor új kulcspárt generálnak. Elképzelhető az is, hogy marad a régi kulcspár az új tanúsítványban (ebben az esetben a megújítás értelme kimerült az adatok újbóli ellenőrzésében). Akárhogy is történik, a tanúsítvány megújítását érdemes összekötni az aktivizáló adat egyidejű cseréjével is. A megújított tanúsítvány kibocsátása után a régi (még nem lejárt) tanúsítványt vissza szokták vonni.

A frissítést azonban nem lehet a végtelenségig eljátszani, bizonyos időközönként[43] mindenképp meg szokták követelni az újbóli személyes megjelenést. Ennek gyakoriságát befolyásolhatja az is, hogy a tanúsítvány igénylésekor a személyazonosság és egyéb adatok igazolásához felhasznált okmányok vajon meddig érvényesek (elképzelhető, hogy a tanúsítvány nem lehet tovább érvényben, mint a személyi igazolvány, amely alapján kiadták).

Mint ahogy a tanúsítvány igénylésekor is előfordulhat, hogy az a felhasználó elől rejtve, a háttérben történik, a frissítéskor ez még inkább megtörténhet. Ha a felhasználó rendszere „szuperfejlett", akkor észreveszi a tanúsítvány lejártát, és automatikusan újat igényel a szolgáltatótól úgy, hogy azt a felhasználó

csak a számla érkezéséből veszi észre (jobb esetben azért szól előtte). A szolgáltatónak is lehetnek ilyen szolgáltatásai, amivel nyomon követi, és automatikusan frissíti a tanúsítványokat.

Tanúsítvány megújítására azonban nem csak az érvényességi idő lejártakor lehet szükség, hanem voltaképpen minden olyan esetben, amikor a tanúsítvány visszavonásra kerül. Ilyen esetben azonban nincs mód frissítésre, hiszen épp azért szükséges a visszavonás, mert valami gond van. Így például ha a visszavonás oka a felhasználó adatainak a megváltozása, akkor az eredeti tanúsítványt visszavonják, és helyette egy új lesz kiállítva. Ha az új tanúsítvány azonosítója ugyanaz marad, mint az eredetié volt, akkor ezt a műveletet is megújításnak nevezhetjük.

Bár a szolgáltató saját tanúsítványának érvényessége jóval meghaladja a hétköznapi felhasználói tanúsítványok érvényességét, sokszor tíz-húsz éves vagy még hosszabb élettartamával, előbb-utóbb annak megújítására is sor kell kerüljön (annál is inkább, mert a szolgáltatói magánkulcs ennél sokkal rövidebb ideig szokott érvényes lenni). Ennek kezelésére külön eljárást kell kidolgozni, hiszen ilyen alkalommal a régi szolgáltatói tanúsítvánnyal igazolt felhasználói tanúsítványokat is mind meg kell újítani.[64] Tervezett módon erre a szolgáltató hatékonyan fel tud készülni a felhasználói tanúsítványok előzetes kifuttatásával, de ha a megújítás nem tervezetten következik be, akkor a felhasználói tanúsítványok rövid időn belül történő újbóli legyártása, azok nagy száma esetén, különös problémát jelenthet a szolgáltató számára. A szolgáltató magánkulcs-kompromittálódása például egy ilyen, nem könnyen kezelhető feladatot teremt, hiszen ebben az esetben a nulláról kell újra felépíteni az egész hitelesítési struktúrát.

4.7 Tanúsítványok szétosztása

4.7.1 Az aláíró és titkosító kulcsok terjesztése

Nyilvános aláíró és titkosító kulcsainkat (azaz tanúsítványainkat) el kell juttatnunk azok számára, akikkel elektronikus aláírással és rejtjelezve akarunk kommunikálni. Nyilvános aláíró kulcsunkat azért, hogy ellenőrizhesse aláírásunkat, nyilvános titkosító kulcsunkat pedig azért, hogy üzenetét titkosítani legyen képes számunkra. Mi sem egyszerűbb ennél, gondolhatnánk, hiszen amikor megkapjuk a tanúsítványainkat, küldünk ismerőseinknek egy körlevelet, amiben elküldjük számukra azokat. Ha valaki olyannal akarunk biztonságosan kommunikálni, aki nincs a listában, akkor számára utólag is bármikor elküldhetjük.

De ha ilyen egyszerű lenne az élet, én sem írnék könyveket. Gondolom, már mondanom se kell, hogy ez sem csak ennyiből áll. És nem csak azért, mert nem elég a saját tanúsítványomat, de a szolgáltató tanúsítványát is el kell küldenem, hogy a tanúsítványon lévő aláírás is ellenőrizhető legyen (és ha a tanúsítási lánc ennél hosszabb, akkor annak összes tanúsítványát el kell küldeni), vagy mert ez a

módszer az elektronikus levelezésen kívül nem is igen járható. Nagyobb hátránya ennek az egyéni kézbesítéses módszernek, hogy egy idő után nagyon elbonyolódhat a különböző tanúsítványok és tanúsítási láncok nyilvántartása és kezelése, nem is szólva ennek kommunikációs, nyilvántartási és adminisztrációs erőforrásigényéről. Nem oldja meg a módszer a tanúsítvány visszavonásával és frissítésével járó igényeket sem, azaz ezen a módon nem tudom bizonyítani, hogy tanúsítványom még mindig érvényes, hiszen azzal a visszavonás után is rendelkezem.

4.7.2 Nyilvános tanúsítványtárak

E problémák megoldása érdekében a szolgáltatók egy nyilvános telefonkönyvhöz hasonló funkciójú nyilvántartásba, az úgynevezett nyilvános tanúsítványtárba szokták helyezni a tanúsítványokat, amely egyben hivatalos nyilvántartásként is funkcionál: a benne található információk a tanúsítványok aktuális és valódi állapotát tükrözik. A nyilvánosság általában az adott közösségre vonatkozik, vagyis nem feltétlenül a teljes emberiségre és az univerzum összes életformájára. A tanúsítványtárba bele szokták írni az összes kiadott tanúsítványt (kivéve azokat, melyek nyilvánosságra hozatalához a háklis tulajdonos nem járul hozzá), valamint a visszavont tanúsítványok adatait.

A nyilvános tanúsítványtár céljára – s ez a nyilvános kulcsú kriptográfia fantasztikus érdeme – elégségesek a hagyományos „védelem nélküli" fájlszerverek, címtármegoldások, hálózati protokollok.[45] A gyakorlatban a címtárszolgáltatások váltak egyeduralkodóvá ezen a területen, melyek jelentősen többet tudnak, mint amire a tanúsítványok kapcsán feltétlenül szükség van. A címtárakban például megadott hierarchiába rendezetten a felhasználók egyéb, a tanúsítványba nem belefoglalt adatai is tárolhatók (például foglalkozás, beosztás, telefon, cím stb.), amik különböző jogosultságokkal visszakereshetők és lekérdezhetők (ez általában zárt közösségek esetén különösen hasznos). Nem szabad azonban arról megfeledkezni, hogy ezek az adatok már nem védettek hasonlóképpen, mint a tanúsítványban szereplők.

A nyilvános tanúsítványtáraknak egyetlen hátulütője van, méghozzá az, hogy hálózati kapcsolat kell az elérésükhöz. Feltételezve, hogy elektronikus kommunikáció esetében ez többnyire rendelkezésre áll, e nagyszerű megoldás útjába már csak egyetlen dolog állhat: az alkalmazások nem mindig képesek kezelni. Elsősorban azért nem, mert nincs arra általánosan elfogadott módszer, hogy elektronikus aláírásommal miként mondjam meg azt, hogy hol kell keresni azt a tanúsítványtárt s azon belül tanúsítványomat, mely igazolja aláírásomat.[46] Mivel nem bonyolult feladatról van szó: mindössze egy LDAP/internet cím és egy egyedi név vagy sorozatszám megadásáról, így várható, hogy hamarosan elterjednek az erre vonatkozó szabványok.

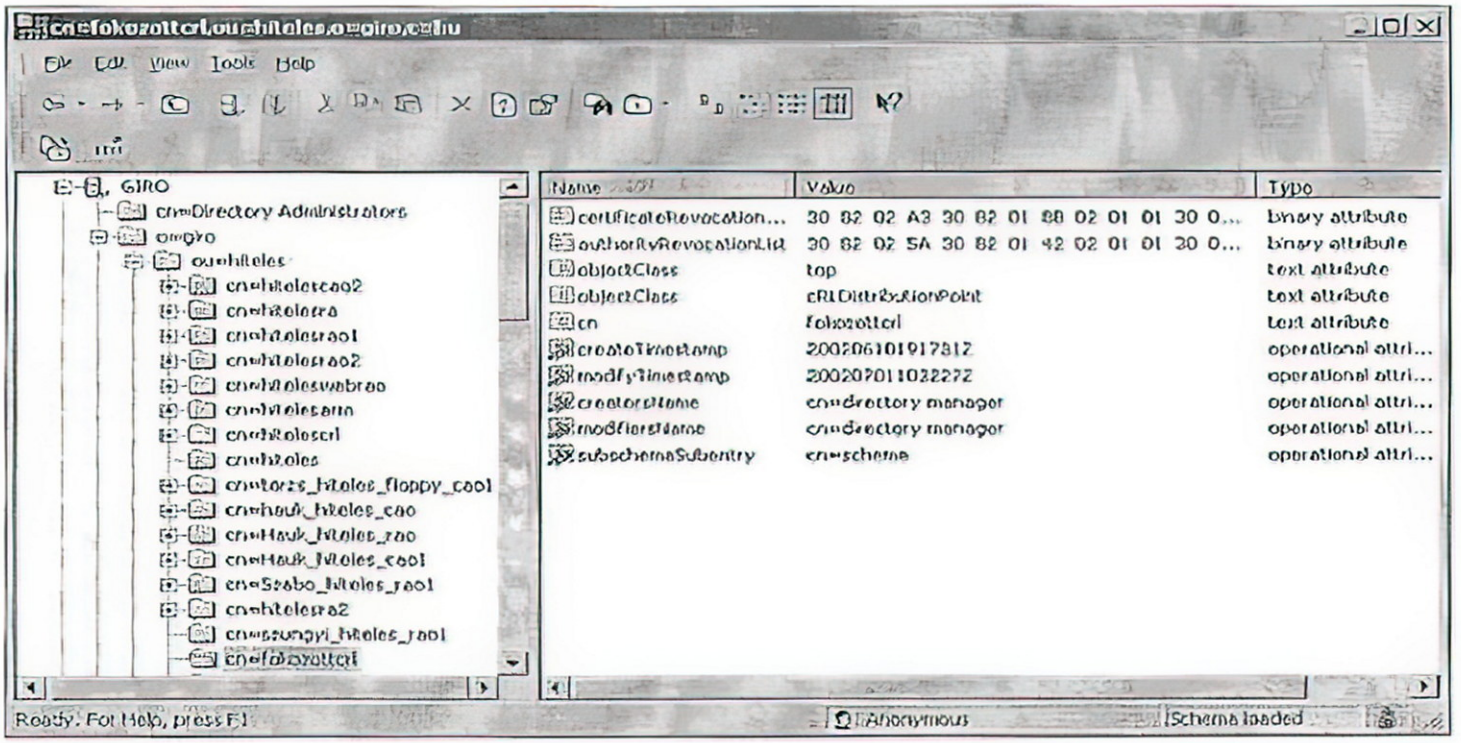
Ez a megoldás mindössze a szolgáltató (gyökér) tanúsítványának közzétételére nem megfelelő. Annak a tanúsítványnak, amit már nem igazol másik tanúsítvány. Ezt a tanúsítványt szokás szerint újságokban szokták nyilvánosságra

hozni[47], a nevesebbeket beépítik az operációs rendszerekbe, illetve zárt közösségben valamilyen más biztonságos módszerrel is teríthetik.

4.7.3 Könyvtárrendszerek

Az említett címtárszolgáltatás (más szóval: könyvtárszolgáltatás) első szabványos megvalósítása anno az X.500-as szabvány kidolgozásával kezdődött meg, amit a technológia összetettsége és a felhasználók érdektelensége folytán csak jóval később követtek létező és működő megoldások (sokkal korábban és nagyobb jelentőséget kapott, hogy az X.500-as szabványhoz kapcsolódóan a tanúsítványok felépítésének részleteit is kidolgozták, mely szabványnak a X.509-es nevet adták). Vagyis az X.500-as könyvtárrendszer, mely kissé megelőzte a korát, sokkal több mindenre alkalmas, mint tanúsítványok tárolására, de a téma szorításában e képességekre most nincs alkalmunk kitérni.

Az X.500-as könyvtármegoldások fejlesztése helyett a nagyobb gyártók saját modelleket dolgoztak ki (bízva abban, hogy elterjesztve az kvázi szabványként egyeduralkodóvá válik), így a Novell, a Lotus és a Microsoft is. Végül is nem ezek, hanem egyszerűsége folytán egy könyvtár-hozzáférési protokoll vált széles körben elfogadottá, ami az X.500 szabvánnyal és könyvtármegoldásokkal kompatibilis. Az LDAP[48] – merthogy arról van szó – azonban, mint neve is mutatja, nem egy könyvtárszabvány, csak egy elérési módszer (ez is egy protokoll), mely mögött bármilyen könyvtárszerver alkalmazás állhat, amely ezt az elérési felületet biztosítja[49]. Még akár a Microsoft Active Directoryja is, ami a **Windows 2000** megjelenése óta egyre elterjedtebb (bár ennek LDAP felülete hagy kívánnivalókat maga után). Az LDAP előnye, hogy sokkal egyszerűbben



48. ábra Visszavonási lista lekérdezése LDAP böngészővel

implementálható, mint az X.500-ban definiált DAP párja. Az egyszerűség ára, hogy az LDAP funkcionalitása szűkebb, például replikációs képességei valamivel fejletlenebbek. Internetes környezetben viszont előny az, hogy az LDAP közvetlenül a TCP/IP protokollra épül.

Ez a kis történelmi visszatekintés, remélem, mindenkit eligazított a könyvtárrendszerek között. Ha mégsem, elég, ha az LDAP-ot megjegyzi, és a tanúsítványtárral azonosítja. Amennyiben valaki a gyakorlatban is meg akar ismerkedni az LDAP-pal, akkor akár az **Internet Explorer**-ben is begépelheti egy LDAP kiszolgáló címét, vagy ha professzionálisabb böngészőre vágyik, hát letölthet egyet az internetről[50]. Ezek után csak gépelje be, mondjuk, a GIRO tanúsítványtárának címét (LDAP://tar.giro.hu), és máris kedvére böngészhet.

4.8 Tanúsítvány-visszavonás és visszavonási lista

Nem rejtettem véka alá eddig sem, hogy speciális esetekben sor kerülhet a tanúsítvány érvényességi idejének lejártát megelőző visszavonására. De melyek ezek az esetek, amelyek talán nem is annyira speciálisak? És mi történik egy visszavonás után? És mi van, ha a visszavonást akarjuk visszavonni? És persze: mi az a visszavonási lista? Ezekre a kérdésekre igyekszik választ adni a következő pár passzus, elsősorban az elektronikus aláírás szemszögéből (a titkosításra szolgáló tanúsítványok esetében a helyzet nem sokban tér el).

4.8.1 Visszavonási okok

Egy tanúsítvány visszavonáshoz számtalan ok vezethet. Különböző jogcímeken a visszavonást kérheti a felhasználó, a tanúsítványban feltüntetett szervezet vagy esetleg más harmadik fél, és a szolgáltató saját hatáskörében is intézkedhet arról. A teljesség igénye nélkül lássunk pár tipikus indokot, a kezdeményező fél szerint rendezve.

A felhasználó kezdeményezése alapján:
- magánkulcs kompromittálódása vagy a gyanú árnyéka,
- magánkulcs aktivizáló adatának kompromittálódása vagy ennek a gyanúja,
- magánkulcs megsemmisülése, aktivizáló adat elfelejtése,
- kulcshordozó eszköz elvesztése, eltulajdonítása, megrongálódása,
- a tanúsítványban feltüntetett hibás vagy megváltozott felhasználói adatok,
- a felhasználó más osztályú/típusú tanúsítványra akar áttérni,
- a felhasználó visszavonási kérelme (akár indoklás nélkül is).

A tanúsítványban feltüntetett szervezet kezdeményezése alapján:
- a felhasználó és a szervezet kapcsolatának megszűnése,
- a szervezet adatainak megváltozása,
- a szervezet megszűnése.

A szolgáltató kezdeményezése alapján:
- a szerződéses feltételek megszegése a felhasználó által,
- a felhasználó kötelezettségeinek be nem tartása,
- a felhasználó nem fizeti az esedékes díjakat,
- a szolgáltató tudomására jutott tény a felhasználó adatainak valótlanságáról,
- a tanúsítványban feltüntetett szolgáltatói adatok megváltozása,
- a szolgáltató magánkulcsának kompromittálódása,
- a hitelesítésszolgáltatás megszűnése.

Harmadik fél kezdeményezése alapján:
- bármely harmadik fél által szolgáltatott bizonyíték a fentiek valamelyikére,
- felügyeleti szerv kötelező erejű döntése,
- bíróság kötelező erejű döntése,
- a felhasználó tartós megbetegedése vagy halála[51].

Azt, hogy pontosan ki milyen indokok alapján és milyen feltételekkel vonhat vissza egy tanúsítványt, a szolgáltatónak pontosan dokumentálnia kell (a felhasználónak pedig érdemes ezt áttanulmányozni). Azokban az esetekben, mikor a visszavonás nem a szolgáltató saját elhatározásából született meg, az igényléshez hasonlóan ellenőrizni kell a kérelmező azonosságát és jogosultságát az adott tanúsítvány visszavonására[52]. A szolgáltatónak mindig pontosan dokumentálnia kell a visszavonás körülményeit.

Lejárt tanúsítvány visszavonása már nem lehetséges, még akkor sem, ha a lejárat után fedezzük fel a magánkulcs lejárat előtti vagy utáni (ha nem lett korrektül megsemmisítve) kompromittálódását.

4.8.2 Visszavonás, felfüggesztés, visszahelyezés

A tanúsítvány visszavonása végleges, irreverzibilis cselekedet, azt visszacsinálni (mert „bocsi, tévedtünk") nem lehet. Ha mégis ilyen történik, új tanúsítványt kell igényelni, és viselni kell a tévedés anyagi konzekvenciáit. Előfordulhatnak azonban olyan körülmények, amelyek esetében a visszavonás túlságosan drasztikus, az életben hagyás viszont indokolatlan könnyelműség. Ilyen esetekre lett kitalálva a felfüggesztés intézménye, amit sajnos nem minden szolgáltató támogat. Ha egy tanúsítványt felfüggesztek, arról a visszavonáshoz hasonlóan értesítés jelenik meg a visszavonási listában, de jelölve azt, hogy ez egy felfüggesztett állapot. Mint ilyen, ideiglenes, és addig tart, míg a felhasználó vissza nem állítja a tanúsítvány érvényességét, vagy véglegesen vissza nem vonja azt. A felfüggesztés és a visszahelyezés (más szóval újraérvényesítés) műveletét, annak kezdeményezőjét – a visszavonáshoz hasonlóan – ellenőrizni és adminisztrálni kell.

Olyasmit általában egyetlen szolgáltató sem támogat, hogy előre megmondjam, mennyi ideig akarom felfüggeszteni a tanúsítványt, ami felfüggesztett állapotban sokszor csak meghatározott rövid ideig lehet. A tipikusan egy-két hetes időtartam után, ha közben más intézkedés nem történik, a tanúsítvány auto-

matikusan visszavonásra vagy újraérvényesítésre kerül, a szolgáltató szabályzatainak megfelelően.

Emiatt olyan helyzetekre, hogy elutazok két hónapos honolului nyaralásra vagy féléves kamcsatkai kiküldetésre, ahol számítógépet nem akarok vagy nem tudok látni, s ezért felfüggeszteném a tanúsítványom, ez a lehetőség nem igazán alkalmas. De nem is erre van kitalálva. Hanem arra az esetre, ha a tanúsítvány biztonságával kapcsolatban olyan kételyek merülnek fel, amik az azonnali visszavonást nem indokolják, de további vizsgálatokig a tanúsítvány érvényességének felfüggesztését tehetik szükségessé. A vizsgálatok lezárását követően, ha kiderült az igazság, annak eredményétől függően a tanúsítvány visszahelyezhető előző érvényes állapotába vagy véglegesen visszavonható.

4.8.3 A tanúsítvány-visszavonási lista

Bár első látásra úgy tűnhet, hogy egy tanúsítvány visszavonása egyszerű feladat, valójában technikailag sokkal bonyolultabb, mint a tanúsítvány legyártása. Az első probléma ott jelentkezik, hogy a tanúsítvány nem mindig törölhető a nyilvános tanúsítványtárból, hiszen a régebbi aláírások ellenőrzéséhez szükség lehet rá a visszavonás után is. Még kevésbé jó megoldás a törlés azért, mert ez esetben nem utalna semmi arra, hogy mikor és mi történt a tanúsítvánnyal, s fennállna az a veszély is, hogy valaki a tanúsítványt rosszhiszeműen visszahelyezi a tanúsítványtárba, illetve az (LDAP protokollt megbuherálva) a címtárlekérdezés tranzakcióba.

Emiatt fejlesztették ki a tanúsítvány-visszavonási listának (CRL[53]) nevezett módszert, ami a visszavont bankkártyák esetében korábban alkalmazott módszerhez hasonló (de automatizált és elektronikus) módon egy listában közzéteszi azon tanúsítványok egyedi azonosítóját (sorszámát), amelyek többé nem megbízhatóak. A listában az összes visszavont és felfüggesztett tanúsítványra van hivatkozás. A listából a tanúsítvány csak úgy kikerülhet ki, ha újraérvényesítik vagy érvényességi ideje lejár (visszavont tanúsítvány esetében csak az utóbbi módon). A lista a tanúsítvány sorszáma mellett tartalmazza a visszavonás/felfüggesztés tényét és idejét, a visszavonás okát s egyéb információkat is, amelyek a lista kibocsátási adataival együtt (kibocsátó hitelesítőegység neve, kibocsátás ideje stb.) a szolgáltató által aláírásra kerülnek, a tanúsítványokhoz hasonló módon.

A lista egyedül a gyökér hitelesítőegység tanúsítványának visszavonására nem alkalmas, mivel ez esetben nincs, aki aláírja a visszavonási listát. Ilyen esetben, akárcsak a gyökér tanúsítvány létrehozásakor, a közzététel hagyományos módszerei közül kell választani.

4.8.4 A visszavonási lista generálása

Kulcsvisszavonási listát minden szolgáltató (pontosabban annak hitelesítőegysége) saját egyéni rendje szerinti gyakorisággal, de mindig előre meghatározott

és szigorúan betartott rendszerességgel (tízpercenként, óránként, naponta stb.) állít elő. Előbb ugyan bocsáthat ki listát, mint az a rendszerből következik, de később nem. A kibocsátott lista emiatt is mindig tartalmazza a következő kibocsátás időpontját.

A szolgáltató akkor is generál egy új (tartalmilag az előzővel megegyező) listát, ha az nem tartalmaz az előző periódus óta visszavont tanúsítványt. Ez amiatt lényeges, hogy a felhasználó biztos lehessen abban, hogy aktuális listát használ. Elviekben lehetséges az is, hogy minden egyes kulcsvisszavonáskor (különösen ha ez nem túl gyakori) azonnal egy új visszavonási listát állítson elő a szolgáltató, de ez esetben a kibocsátás rendszertelensége miatt a felhasználó nem tudná megállapítani, hogy valóban a legújabb listával áll-e szemben. Például ha egy behatoló kitörli a nyilvános tanúsítványtár utolsó visszavonási listáját (a könyvtárszervernek nem kell szupervédettnek lennie, épp ez az előnye), ezt a felhasználó nem észlelhetné. Éppen ezért fontos a rendszeresség, amelyet nem érdemes nagyon gyakorira se venni, mert ez esetben túlságosan terheljük a felhasználók rendszerét, kommunikációs vonalait az állandó listaletöltési kényszerrel.

4.8.5 A visszavonási lista szétosztása

A visszavonási lista a tanúsítványokhoz hasonló módon, nyilvános tanúsítványtárban közzétéve és elektronikusan aláírva juttatható el az érdekeltekhez. Ez azért nagyszerű, mert a meglévő infrastruktúra erre a célra változtatás nélkül felhasználható, s mivel a lista szintén önvédelmező, itt sincs szükség kiegészítő védelmi megoldásokra.[54]

Bizonyos esetekben alkalmazzák a visszavonási listák direkt postázását is (vagy a két megoldás kombinációját), aminek az az előnye, hogy a kritikus visszavonásokról (például magánkulcs-kompromittálódás) azonmód értesülhetnek az érdekeltek. Hátránya viszont, hogy a postázáshoz biztonságos hálózati protokoll vagy e-mail megoldás szükséges (különben az e-mail eljutása a címzettjéhez megakadályozható), és nagyszámú felhasználó esetén kezelhetetlen forgalmat generálhat. Ezért ez a megoldás nem is terjedt el igazán. Léteznek viszont más alternatív vetélytársai az egyszerű visszavonási listának. Visszavonási listák ezek is, de másmilyenek. Másságukkal pedig egy másik problémára kívánnak megoldást adni, nem a sürgősségre, hanem a mennyiségre. Sok felhasználós közösségeknél ugyanis a visszavonási lista túl nagyra hízhat, olyan nagyra, hogy annak rendszeres letöltése már nem megoldható.[55]

4.8.6 A visszavonási lista ellenőrzése

A tanúsítvány-visszavonási lista ugyanis egyetlen bejegyzés a tanúsítványtárban, s így a benne történő kereséséhez a teljes listát le kell töltenie az érintett félnek.[56] A lista letöltésére sor kerülhet rendszeres időközönként, a kibocsátás-

hoz igazítva annak idejét, vagy csak szükség esetén. A listát letöltése után ellenőrizni kell sértetlensége, valamint a rajta szereplő aláírást a hitelesség és az érvényesség szempontjából (a lista aláírója a legtöbb esetben értelemszerűen megegyezik a tanúsítványok aláírójával). Ezt követően az érintett félnek a listában szereplő időpontokat (jelen és következő kibocsátás) össze kell hasonlítania a pontos idővel és az előző listában szereplő jóslattal, így meggyőződve arról, hogy a legutolsó listával van dolga. A szolgáltató előző listáját[57] ezek után felülírhatja a jelenlegivel[58]. Csak ezen lépések után kerülhet sor a listában való keresésre, mely egy adott tanúsítványra vonatkozik, s annak sorszáma alapján történik. Ha a tanúsítvány szerepel a listában, ellenőrizni kell a mellette szereplő attribútumokat is, a visszavonás okát és pontos idejét.

Az érintett félnek a felhasználói tanúsítványok esetében elviekben mindig az aláírás időpontjára vonatkozó érvényességet kell vizsgálnia. Ha a visszavonás ideje későbbi, mint az aláírás ideje, akkor a tanúsítvány még elfogadható. Mivel azonban az aláírás ideje hiteles formában nehezen állapítható meg (hacsak időbélyegző nem igazolja), a gyakorlatban mégis az ellenőrzés ideje lehet a mérce[59]. Az elfogadó fél persze lehet „rigolyás", és a visszavonás okától függően is hozhat különböző döntéseket az elfogadásról. A kulcskompromittálódás esetét például sokkal szigorúbban ítélheti meg, mint az adatváltozás esetét. Ilyen döntéseket viszont automatika csak nagyon nehezen hozhat, az csak a helyzetre és körülményekre hívhatja fel a figyelmünket. Az elfogadásról szóló döntést mindig az embernek kell meghoznia. Érintett félnek erre vonatkozó döntését különböző dokumentumok szabályozzák (lásd: 8. fejezet).

4.8.7 Visszavonási listák típusai

A méret csökkentésének első megoldásaként szétválasztották a felhasználók és a szolgáltató kulcsaira vonatkozó visszavonási listát[60]. Ez a megoldás nagyon sokat segít azokban az esetekben, mikor a tanúsítási lánc ellenőrzését végzik, hiszen ez utóbbi lista általában nagyon rövid (jó esetben teljesen üres), s így az ellenőrzése is gyorsan lezavarható. Nem oldja meg viszont a felhasználói tanúsítványok ellenőrzésének problémáját.

Ezt kezeli a visszavonási lista szétosztási pontok (CRL distribution points) rendszere, amely a felhasználók szegmentálásán alapszik. A csoportok kialakíthatók a tanúsítvány valamely jellemzője vagy a visszavonás oka alapján. Előbbi esetben a tanúsítványokat már a kibocsátáskor beosztják egy csoportba, és megbillogozzák. Ha egyenlő vagy közel azonos nagyságú partíciókat akarunk kialakítani, ez a célszerű (például a tanúsítvány sorszáma alapján ez csöppet sem bonyolult). Az utóbbi meg azon esetekben előnyösebb, amikor a visszavonás oka alapján eltérő listakezelést kívánunk bevezetni (mondjuk, a kulcskompromittálódás listáját a többi listánál jóval gyakrabban frissítjük). Ezek után az egyes partíciók saját visszavonási listával fognak rendelkezni. Hiába particionálunk azonban mérnöki pontossággal, ez nem jelenti azt, hogy a visszavoná-

sok száma partíciónként ugyanakkora lesz. Ezt garantálni nem tudjuk, legfeljebb a statisztikai eloszlás egyenletességében bízhatunk.

A billogozás azt jelenti, hogy a tanúsítványokban a legyártás során feltüntetésre kerül, hogy hol található az a visszavonási lista, és mi annak a becses egyedi neve, amely az ő csoportjához tartozik. Az ellenőrző így egyszerűen csak belekukkant a tanúsítványba, és az ott található címen ellenőrzi a listát s annak nevét[61]. Visszavonási ok szerinti szegmentálás esetében persze nem a tanúsítványhoz tartozik a csoport, s így ilyen billogozásra nincs szükség. Ennek a megoldásnak hátránya, hogy egy tanúsítvány érdekében az összes listát végig kell nézni (legfeljebb némelyeket ritkábban), ezért ez a módszer közvetlenül nem a méretproblémákat kezeli. A visszavonási lista szétosztási pontjára való hivatkozással elég gyakran találkozhat a felhasználó, igaz, ennek oka nem mindig az, hogy a szolgáltató valóban particionálja a tanúsítványokat, hanem az, hogy egyértelművé akarja tenni a tanúsítványban, hogy annak visszavonási listája hol érhető el.

Kevésbé gyakori a delta CRL és az indirekt CRL módszere. A delta CRL módszere abból indul ki, hogy minek a teljes visszavonási listát mindig közzétenni, e helyett inkább azt ajánlja, hogy egy előző listához képest mindig csak a változásokat publikáljuk. Vagyis az előző lista óta visszavont, felfüggesztett és újraérvényesített tanúsítványokat.[62] Bár az ötlet nagyszerű, a gyakorlatban számos hátulütője van. A legkevesebb az, hogy ilyen esetben az újraérvényesítésről és a korábban visszavont tanúsítvány érvényességi idejének a lejártáról is bejegyzés készül a listába. A súlyosabb gond az, hogy ez esetben a lista adminisztrációja a felhasználóra hárul, aminek komoly biztonsági vonzatai vannak.

Az indirekt CRL a „Világ listái, egyesüljetek!" jelszóból indul ki, s mint ilyen, érezhetően nem a méretcsökkentés az elsődleges célja. Ez esetben több külön lista egyesítéséről van szó (persze nem világméretekben), olyan listákéról, amit több szolgáltató vagy egyazon szolgáltató különböző hitelesítőegységei bocsátottak ki. Ennek előnye az lehet, hogy nagy és összetett közösségek esetén, melyek több szolgáltatóval és/vagy hitelesítőegységgel állnak kapcsolatban, a felhasználónak csak egyetlen listát kell bogarásznia. Mivel az ilyen listákat értelemszerűen nem ugyanaz bocsátja ki, mint aki a tanúsítványt, a tanúsítványban meg kell nevezni a visszavonási lista kibocsátóját, a lista elemeinek pedig tartalmaznia kell azt, hogy melyik bejegyzés melyik kibocsátótól való. Ez a módszer csak akkor működőképes, ha az így előálló listák nem túl nagyok, amelynek érdekében kombinálható a szétosztási pontok módszerével.[63] Például úgy, hogy csak a kulcskompromittálódás miatt visszavont tanúsítványok listáját egyesítik.

Nem hagyhatjuk ki természetesen, hogy felhívjuk a figyelmet az alkalmazások problémájára. A legtöbb alkalmazás még a „normál" visszavonási listát sem kezeli korrektül. Mivel a szétosztási pontok módszere nem kíván különösebb képességeket az alkalmazástól, így annak kezelésére van példa. A delta CRL és az indirekt CRL kezelése azonban meglehetősen ritka, bár a **Windows XP** a delta

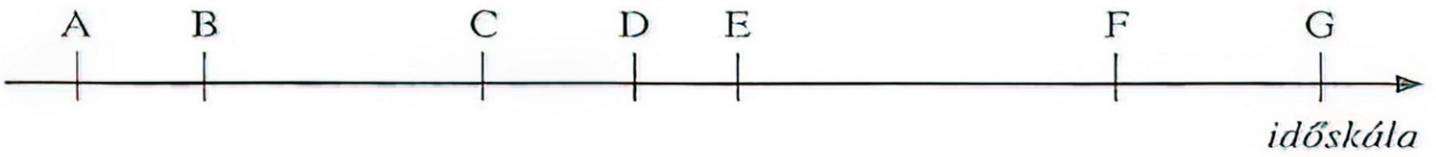
CRL kezelésére már képes. E dicséret mellett nem hagyhatjuk szó nélkül, hogy a **Windows** és az általam ismert valamennyi Microsoft-alkalmazás egy szót sem szól, ha a visszavonási listát nem képes elérni. Ez pedig gyakran bekövetkezhet, főleg vállalati környezetekben, ahol az üldözési mániás rendszergazdák letiltják az LDAP protokoll, illetve a neki megfelelő portok (389, 636, 1760, 3269[64]) használatát. A **Windows** pedig ilyenkor csak sunnyog, és úgy tesz, mintha minden rendben lenne. Ennek veszélyei hatalmasok, ezért minden felhasználónak ajánlom a lista manuális ellenőrzését is. A rendszergazdákat pedig ezennel kérem tisztelettel, hogy a biztonság érdekében a kifelé irányuló LDAP-kéréseket engedélyezzék a felhasználók számára.

4.8.8 Visszavonási időskála, felelősségi kérdések

A visszavonás során történt események időbeni egymásutániságának, pontos időpontjának és az ehhez kapcsolódó felelősségeknek adott esetben kritikus jelentősége lehet, ami miatt roppantul fontos, hogy ezeket a felhasználók is megismerjék. De lássuk először is, hogy mik ezek az események, és milyen sorrendben követik egymást:

A) A legutóbbi visszavonási lista kibocsátása.
B) Annak az eseménynek a bekövetkezte, ami később a visszavonáshoz vezet (például magánkulcs eltulajdonítása).
C) A felhasználó felismeri az eseményt és a kulcsvisszavonás szükségességét (például a kulcshordozó hiányának realizálása).
D) A felhasználó kérelmezi a visszavonást a szolgáltatónál.
E) A szolgáltató a tanúsítványt visszavonja vagy felfüggeszti (visszavonás ideje).
F) A következő visszavonási lista közzététele (már tartalmazza a tanúsítványt).
G) Az érintett fél letölti, és ellenőrzi a listát.

Nézzük meg mindezt egy időskálán is, amely a szemléltetés céljából több szempontból is leegyszerűsített, s nem arányos[65]:



Mindegyik időszak valamilyen szempontból érdekes, és különböző felelősségi kérdéseket vet fel. A legfontosabb tény az, hogy „B" esemény után a tanúsítvány már nem megbízható, amiről „C" ideig a tanúsítvány tulajdonosa sem tud, „D" ideig a szolgáltató sem, „G" ideig pedig a tanúsítvány ellenőrzője nem. A gond ott van, hogy lista ellenőrzésére természetesen „F" időpont előtt is sor kerülhet, amikor is az érintett fél még nem képes a tanúsítvány érvénytelenségének felismerésére. Ami nyilván nem az ő hibája.

A felelősség általánosságban úgy osztható meg, hogy „D" ideig a tanúsítvány tulajdonosát, „D" és „F" időpontok között a szolgáltatót, „F" időpont után pedig az érintett felet terheli felelősség a tanúsítvány jóhiszemű felhasználásából eredő károkért, de az érintett féltől elvárható az a gondosság, ami az „E" esemény utáni veszélyeket (azaz a szolgáltató felelősségét) csökkentik. Hogy mit értünk ez alatt? Nyilvánvalóan minden szolgáltató igyekszik csökkenteni a felelősségét, amely „D" és „F" időpontok között terhelik. Ha, mondjuk, a szolgáltató a visszavonási listát naponta publikálja, és egy tanúsítvány visszavonására a lista kibocsátását követő percekben kerül sor, a szolgáltató egy teljes napig felel az annak elfogadásából eredő károkért. Ezzel nagyon könnyen vissza lehetne élni. Kis hazánkban ez minden bizonnyal megélhetési forrást jelentene egyes-találékony körök számára, ha a szolgáltató nem tenne valamit ellene. A szolgáltató ezért például előírhatja, hogy az érintett fél minden egyes tanúsítvány elfogadása előtt várja meg a következő lista kibocsátását, hogy biztos lehessen abban, hogy a tanúsítvány az elektronikus aláírás megtételekor még érvényes volt. Ez sok esetben nem olyan szörnyen nagy dolog, mint amilyennek előre látszik, főleg ha a szolgáltató a kritikus esetekről gyakrabban bocsát ki visszavonási listát.

Összefoglalva: ez a szituáció a bankkártyák eseléhez hasonlít, azzal a korántsem elhanyagolható különbséggel, hogy az okozható kár jóval nagyobb is lehet, s az egyes tanúsítványok nem képviselnek olyan értéket, amely fedezetet jelentene erre. Éppen ezért is nem lenne életszerű a bankoknak a bankkártyák esetében alkalmazott „nagyvonalúságát", azaz a bejelentés időpontjától számító teljes felelősségvállalást elvárni a hitelesítésszolgáltatóktól.

És még két aprócska megjegyzés, biztos, ami biztos alapon, nehogy aztán engem hibáztassanak:

Tanúsítvány visszavonása mindig csak jelen időponttal történhet.[66] Visszamenőlegesen nem (ez alatt azt értem, hogy egy már kibocsátott visszavonási listába utólag nem lehet írni). Akkor sem, ha meg tudnám mondani, hogy múlt kedden tűnhetett el a magánkulcs, mikor felhoztam a lakásomra azt a kis cédát. Ezt a múltbeli időpontot ugyan lehet jelezni a visszavonási bejegyzésben, de ez „csak" „F" időpont után véd meg minket és az érintett feleket. A „csak" természetesen idézőjeles, hiszen „F" időpont után ez az információ nélkülözhetetlen. Ilyen esetben a kulcskompromittálódás visszavonást megelőző ideje átveszi a visszavonási idő szerepét (az ellenőrzőknek – amennyiben még módjuk van rá – ezen időpontot kell a megbízhatatlanság kezdeteként figyelembe venniük).

Ebből következően, ha a visszavonásra a felhasználó magánkulcsának kompromittálódása miatt kerül sor, s annak észlelése csak nagy késéssel történik, a felhasználónak nem árt egyéni hadjárat keretében csapot-papot értesítenie a sajnálatos eseményről. Azért szükséges ez, mert a kompromittálódás s annak észlelése között sok mindenki elfogadhatta emberünk aláírását, amiben neki ígéri lánya kezét és fele királyságát, s ők már utólag, még egyszer, nem fogják ellenőrizni a tanúsítvány érvényességét (hiszen ezt már „F" időpont előtt megtették egyszer). Ők már joggal isznak a medve bőrére.

4.8.9 Azonnali érvényesség-ellenőrzés

Vannak esetek, mikor a kulcsvisszavonási lista következő kibocsátásának megvárására nincs idő, mivel a lista periodikus kibocsátásából eredő időveszteség nem tolerálható az elfogadó fél által (például azonnali pénzátutalási megbízások). Ebből a célból fejlesztették ki az azonnali érvényesség-ellenőrzés (On-line Certification Status Protocol – OCSP[67]) megoldást, amely on-line képes a tanúsítványok érvényességéről tájékoztatást adni. Ez az azonnaliság természetesen szintén csak a visszavonás ideje után értelmezhető, de a következő lista kibocsátását nem feltétlenül kell megvárni.

A protokoll egy kérdés-felelet mechanizmusra épül, amelynek során a kliensalkalmazás a szolgáltató OCSP szerverének egy kérdést küld a tanúsítvány sorszámával. A szerver válaszul egy elektronikusan aláírt üzenetben közli a tanúsítvány érvényességi állapotát: „jó", „visszavont" vagy „ismeretlen". A „jó" státus nem jelenti azt, hogy a tanúsítvány valaha is ki volt bocsátva, vagy hogy a lekérdezés pillanata beleesik annak érvényességi idejébe, csak annyit jelent, hogy a tanúsítvány a válaszadó tudomása szerint nem visszavont vagy felfüggesztett. Amit a „visszavont" válasz jelez. Az „ismeretlen" válasz azt jelenti, hogy a válaszadónak nincs tudomása ilyen kiadott tanúsítványról. Az OCSP mechanizmus képes arra is, hogy a visszavonási lista információit meghaladóan tájékoztasson a tanúsítványok állapotáról, viszont nem képes arra, hogy a tanúsítvány egy múltbeli állapotáról adjon információt (a protokoll 2. verziója erre is képes lesz[68]).

A módszer hátránya – és ez válasz arra a kérdésre, miért nem így működik ez mindenhol –, hogy mivel minden egyes állapotválaszt alá kell írni, rettenetes erőforrásigényeket támaszt a szolgáltató rendszerével szemben (adott esetben percenként több ezer aláírás-generálásról is szó lehet), s a rendelkezésre állás, valamint a megbízhatóság tekintetében is rendkívüliek az elvárások.[69] A módszer természetéből következik az is, hogy az OCSP kiszolgáló és az ellenőrző között on-line kapcsolatnak kell lenni.

A koncepció elragadó, de a gyakorlatból is tudom, hogy a legtöbb esetben az érvényességi adatokat ilyen módon biztosító rendszer is a visszavonási listából szokott dolgozni, vagyis időben nem feltétlen nyer a felhasználó. Ha a visszavonásilista-kibocsátást azonnalira állítják, akkor a szolgáltatás valóban a mindenkor érvényes adatokat közli, de így a tanúsítványtár csak egy átmeneti adattárként (vagy háttértárként) funkcionál.

Akkor is lehet azonban értelme az OCSP-nek, ha a CRL-hez hasonlóan késleltetett adatokat közvetít:

- A felhasználó rendszerét az érvényesség-ellenőrzés e módja sokkal kevésbé terheli, felelőssége jóval kisebb, mint a hagyományos listás esetben.
- Az utólagos ellenőrzéshez az OCSP-válasz egyszerűen az aláírás mellé csatolható (nem szükséges a visszavonási listák archiválása).

- Az OCSP igen nagy közösségeket is ki tud szolgálni anélkül, hogy a CRL szétosztási problémái jelentkeznének.
- Az OCSP kérések több protokollon keresztül is működhetnek (például HTTP, SMTP, LDAP), így a tűzfalak sem állítanak neki akadályt.[70]
- A megoldás nem állítja pellengérre a visszavont tanúsítványok tulajdonosait (nincs „szégyenlista"-köröztetés, hanem rá kell kérdezni konkrétan az adott tanúsítványra).[71]

Látni kell, hogy az OCSP és a CRL megoldások különböző célokra, nem egymás kiváltására készültek, így valószínűleg még nagyon sokáig egymás mellett, egymással is együttműködve lesznek jelen digitális életünkben. Annál is inkább, mert az alkalmazások legtöbbje az OCSP protokollt még nem is ismeri.

4.9 Az X.509-es szabvány

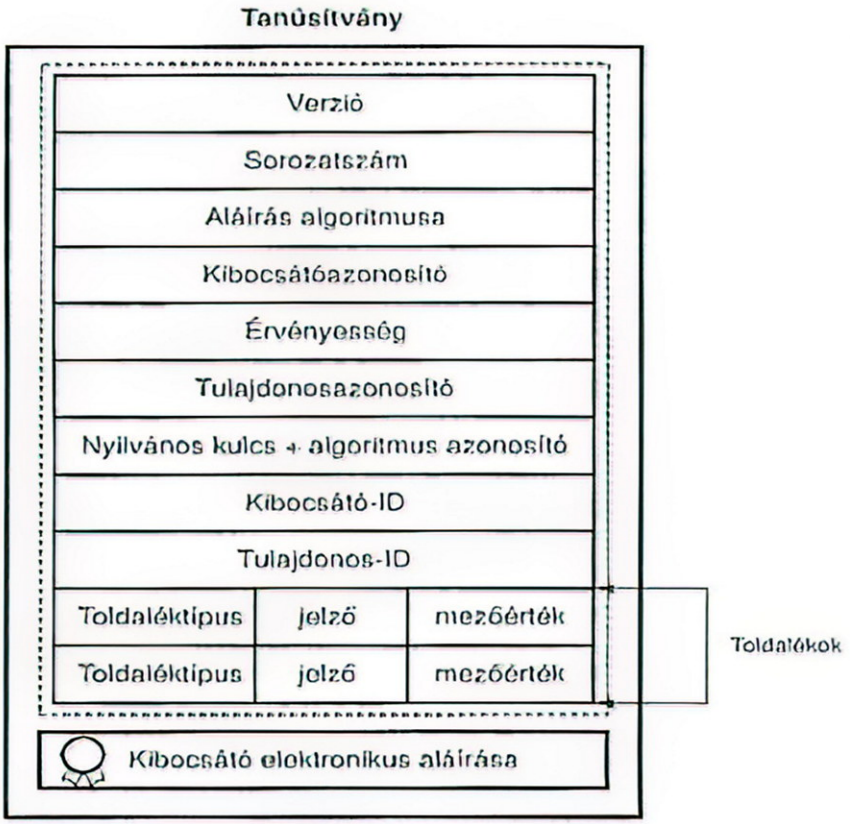
Mindvégig, hogy a tanúsítványok varázslatos és egyben elborzasztó világában kalauzoltam olvasóimat, kimondatlanul is legtöbbször az X.509-es szabvány járt a fejemben. Hiába is próbáltam általános logikai megközelítést alkalmazni, mikor az X.509 annyira egyeduralkodó ezen a területen, hogy gyakorlati értéke messze túlmutat az elvi megközelítésen.[72]

4.9.1 A szabvány

Az X.509 az ITU azon szabványa, mely a tanúsítvány- és tanúsítvány-visszavonási lista szerkezetére, felépítésére, tartalmára, kezelésére és még sok más, ezzel összefüggő dologra ad előírásokat. Mivel vetélytársa, amely akár csak távolról is megközelítené elfogadottságát, nem létezik, így a szabvány a tanúsítvánnyal foglalkozók egyfajta bibliája lett. A ma elérhető, elektronikus aláírást és tanúsítványt alkalmazó rendszerek szinte kivétel nélkül e szabványnak (többé-kevésbé) megfelelve működnek. Pontosabban az e szabványnak megfelelő tanúsítványokat képesek hasznosítani. Bármilyen sok dolgot is meghatároz a szabvány, még több dolog van azonban, amit nem. Így sok más szabvány is létezik, mely az X.509-re épül. Megnyugtatásul közlöm, hogy ezeket – de még az X.509-et sem – nem fogom részletesen bemutatni. Csak épp egy kicsikét, amennyit feltétlen tudni érdemes.

4.9.2 A tanúsítvány felépítése

Az X.509-es szabvány 3-as (legfrissebb) verziója szerint a tanúsítvány a következőképpen néz ki:



49. ábra
X.509 V3 tanúsítvány felépítése

A mezők jelentése a következő:

Verzió	A tanúsítvány a szabvány mely verziója alapján készült (v1, v2, v3)
Sorozatszám	A tanúsítvány egyedi sorszáma (hitelesítőegységen belül)
Aláírás algoritmusa	A kibocsátó által a tanúsítvány aláírására használt algoritmus azonosítója
Kibocsátóazonosító	A tanúsítványt kibocsátó hitelesítőegység egyedi (X.500) neve
Érvényesség	A tanúsítvány érvényességének kezdő és végdátuma
Tulajdonosazonosító	A tanúsítvány tulajdonosának egyedi (X.500) neve
Nyilvános kulcs	A tanúsítvány által hitelesített nyilvános kulcs és annak algoritmusazonosítója
Kibocsátó-ID	A kibocsátó egyedi azonosítója
Tulajdonos-ID	A tanúsítvány tulajdonosának egyedi azonosítója
Toldalék típusa	A toldalék típusának egyedi objektumazonosítója
Toldalékjelző	Kritikus / Nem kritikus
Toldalék értéke	A toldalék értéke a típusnak megfelelően

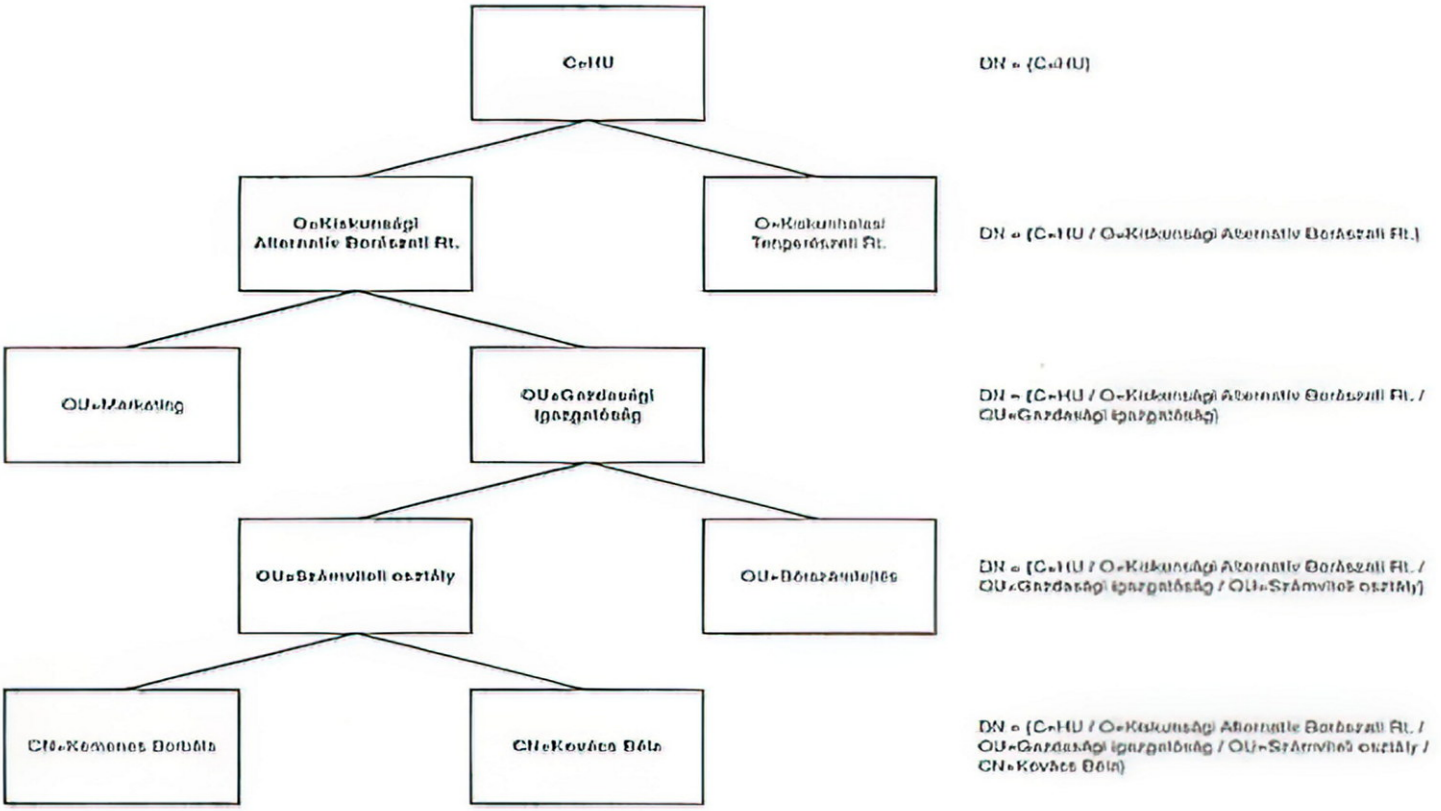
A Verziótól a Nyilvános kulcsig terjedő mezők már az első verzióban jelen voltak, és kötelezően kitöltendők. Ezek a mezők különösebb magyarázatra már nem szorulnak. A Kibocsátó-ID és Tulajdonos-ID mezők a második verzióban lettek bevezetve opcionális felhasználásra. Ezek a mezők azt a célt szolgálják, hogy a kötelező részbe foglalt azonosítókat egyértelművé tegyék abban az esetben, ha ugyanaz az X.500-as név az idő és a sors folyományaként újra kiosztásra kerülne, továbbá azt, hogy az X.500-as névformátumtól eltérő névkonvenciónak megfelelő nevet is fel lehessen tüntetni azonosítóként. A toldalék (kiterjesztés) mezők, melyekből több is követheti egymást, az alkotók óvatosságának és bölcsességének jele. Ahelyett, hogy negyedévente egészítenék ki a szabványt, a toldalékokkal lehetőséget biztosítanak arra, hogy bármely kibocsátó olyan adatot foglaljon a tanúsítványba, ami neki tetszik.

4.9.3 Az X.500 egyedinév-formátum

Azonosítóként az X.500 egyedi név (DN, azaz distinguished name) formátumát alkalmazzák, például valami ilyesmit: C=hu / O=Kiskunsági Alternatív Borászati Rt. / OU=Gazdasági igazgatóság / OU=Számviteli osztály / CN=Kovács Béla,[73] ami azt jelenti, hogy a magyarországi Kiskunsági Alternatív Borászati Rt. gazdasági igazgatóságának számviteli osztályán dolgozó Kovács Béla. Az X.500 névformátum használata, mely az 1. és 2. verzióban még kizárólagos volt, az X.500-as címtárak tanúsítványtárként való alkalmazására vezethetők vissza. Ennek egyedinév-formátuma hierarchiába (fastruktúrába) szervezett objektumokat azonosít egyértelműen. A hierarchiának szintjei vannak, melyek közül a leggyakrabban használatosak a **Country** (ország),[74] az **Organization** (szervezet), az **Organization Unit** (szervezeti egység) és a **Common Name** (általános név). Ezenkívül gyakran előfordulnak még a **Locality** (város), a **State** (állam), az **E-mail** (internet, X400 vagy más formátumban) mezők is.[75]

A hierarchia legfelső szintjét, ahol csak egyetlen bejegyzés található, gyökérnek szokták nevezni (ez legtöbbször egy országkód). A név elemeinek sorrendje a szintek szerveződésére utal, ami az ismétlődő bejegyezéstípusoknál hasznos igazán (például dupla OU vagy CN szint). Mivel a mezőket, azok szűkössége miatt, nem mindig az elnevezésüknek megfelelően töltik ki (például az O vagy CN mezőbe a tanúsítvány osztályának elnevezését írják, S-be a megyét), így a szolgáltató szabályzataiban tájékozódni kell a mezők jelentéséről.

A címtárban a bejegyzéseknek, melyet az egyedi név azonosít, különböző attribútumai lehetnek. Az attribútumok között előfordulhatnak a már bemutatott mezők (amely esetben azok nem keverendők össze a bejegyzés egyedi nevével[76]), valamint egyéb mezők is, például postacím, telefonszám. Ilyen attribútuma a bejegyzéseknek a tanúsítvány is.



50. ábra X.500 névhierarchia

4.9.4 Toldalékok

A toldalékok fogalma a szabvány 3-as verziójában lett bevezetve, felismerve az előző verzió hiányosságait s azt a tényt, hogy egy verzióváltás során a tanúsítványba foglalt új, kötött mezők nagyon hamar újra elégtelenek lesznek. A toldalékok egy szabadon, bárki által bővíthető kiterjesztése a tanúsítványba és visszavonási listába foglalható adatoknak. A toldalék típusának regisztrációja után az adott típusból, jelzőből és a hozzá tartozó értékből álló toldalékrekord a tanúsítványba foglalható. Az adat értékének típusát (egyben hosszát és értelmezését) a toldalék típusához kötődő objektum adja meg. A leggyakrabban használt toldalékok szabványosítva lettek[77], hogy széles körben azonos módon legyenek értelmezve. Maga az X.509-es szabvány is definiál ilyen toldalékokat, amelyek legfontosabbjait nemsokára be is mutatom[78]. Ugyanakkor ezekkel a toldalékokkal vigyázni is kell, mert ha nem szabványosak, az alkalmazások legtöbbje nem fogja megérteni őket (sokszor még a szabványos toldalékokkal is gondjaik akadnak).

A kritikus jelző pont erre való, értéke azt jelzi, hogy az adott toldalékrekord értékét meg kell-e érteni az alkalmazásnak. Ha valamely alkalmazás nincs tisztában a toldalék jelentésével, akkor nem feltétlen biztonságos a tanúsítvány vagy a visszavonási lista használata (mert adott esetben, például a toldalék azokat a körülményeket írja le, melyek esetén a tanúsítvány érvényes). Ezért ha a toldalék kritikus, és azt az alkalmazás nem érti, akkor vissza kell utasítania a tanúsítvány elfogadását.[79] Nem kritikus toldalékra ilyen esetben ügyet sem kell vetnie.

4.9.5 Objektumregisztráció

Az algoritmusok és a toldalékok típusának egyedi azonosítói olyan objektumok, melyeket objektumregisztrációs szervezeteken[80] keresztül regisztrálni kell. Aki rendelkezik saját objektumazonosítóval (OID), az a sajátja alá maga is fel tud venni új objektumazonosítókat. A regisztráció során az objektum egy egyedi, több tagból álló sorszámot kap, melynek részei szintén objektumazonosítók, s amelyek az objektumnak egy hierarchikus fastruktúrában lévő pozícióját adják meg. Például az „RSA aláírás MD5 hash eljárással" algoritmus egyedi objektumazonosítója a következő: 1.2.840.113549.1.1.4, ami annyit tesz, hogy: „ISO. MemberBody. USA. RSA Inc. PKCS. PKCS #1. MD5WithRSAEncryption", amely mezőknek a jelentése: „Szabványszervezet. Specifikáló szervezet típus. Országkód. Cégnév. Szabványkészlet. Szabvány. Algoritmus".

Ilyen objektumkódokkal számtalan helyen lehet találkozni az elektronikus aláírás környékén. A kód feladata elsősorban az egyedi azonosítás, másodsorban a névadás. A második célt korlátozottan teljesíti, ha a kód mellé nincs odafirva a jelentése, mert ez esetben jó néhányszor nem kis nyomozást igényel a rejtvény megfejtése.

4.9.6 A tanúsítvány szabványos toldalékai

Az X.509-es tanúsítványnak számos szabványos toldaléka létezik, amelyek nagyjából a következő csoportokba oszthatók:

– a tulajdonosra és a kibocsátóra vonatkozó toldalékok,
– a kulcsra és annak felhasználására vonatkozó toldalékok,
– a tanúsítási láncra vonatkozó toldalékok.

Ilyen toldalékok explicit már szerepeltek könyvemben, csak éppen azt nem említettem, hogy toldalékról van szó. A legfontosabbakat azért implicit is megemlítem, hiszen ezekkel olvasóm is biztosan fog találkozni. Ezek mellett szerepeltetni fogom az eredeti angol elnevezést is azok számára, akik nem magyar nyelvű alkalmazással dolgoznak.

A tulajdonosra és a kibocsátóra vonatkozó toldalékok (Subject alternative name, Issuer alternative name, Subject directory attributes) a legkevésbé izgalmasak. Ezek a tulajdonos és a kibocsátó nevének más, az X.500 elnevezési módjától eltérő formában történő leírását teszik lehetővé (például domainnév, e-mail-cím, IP-cím, Uniform Resource Identifier, és bármilyen regisztrált névformátum). Egyúttal módot adnak egyéb attribútumok tanúsítványban történő feltüntetésére is (például telefonszám, fénykép, biometrikus azonosító adatok), ami elsősorban zárt közösségek esetében lehet hasznos.

A kulcsra és annak felhasználására vonatkozó toldalékok közül a Subject key identifier és az Authority key identifier a tulajdonos és a kibocsátó kulcsának elnevezésére adnak lehetőséget, ami akkor válhat hasznossá, mikor a kulcs

az idő folyamán a lejárat miatt cserélődik. A Key usage és Extended key usage toldalékok a kulcs felhasználási lehetőségeit írják le. Ha a toldalék kritikus (s ez a valószínűbb), akkor a benne szereplő értékek szigorú kizárólagosságot jelentenek, ellenkező esetben csak ajánlást a kibocsátó részéről.

A Key usage kiterjesztés fontosabb értékei a következők:

a) keyCertSign: Tanúsítvány aláírására
b) CRLSign: Visszavonási lista aláírására
c) nonRepudiation: Letagadhatatlanság biztosítására (kivéve a és b)
d) digitalSignature: Elektronikus aláírásra (kivéve a, b, c)
e) keyEncipherment: Kulcsok és egyéb biztonsági információk rejtjelezésére
f) dataEncipherment: Adatok rejtjelezésére (kivéve e)
g) keyAgreement: Diffie-Hellman kulcsegyeztetés céljára
h) encipherOnly: keyAgreement esetén a felhasználó számára küldött adat rejtjelezésére
i) decipherOnly: keyAgreement esetén a felhasználótól kapott adat visszafejtésére

A felhasználási cél magyarázatánál a magánkulcs felhasználását tüntettük fel, de az természetesen a nyilvános kulcs felhasználását is meghatározza a magánkulcs inverzeként. Például a szolgáltató számára tanúsítvány aláírására szolgáló magánkulcs (keyCertSign) nyilvános párja a felhasználó számára a tanúsítványon lévő szolgáltatói aláírás ellenőrzésére szolgál. Az Extended key usage kiterjesztésben olyan kulcsfelhasználási célokat szoktak feltüntetni, melyet a Key usage nem definiál (például levelezés, webszerver és webböngésző, időbélyegzés, kódaláírás, EFS stb.)[81].

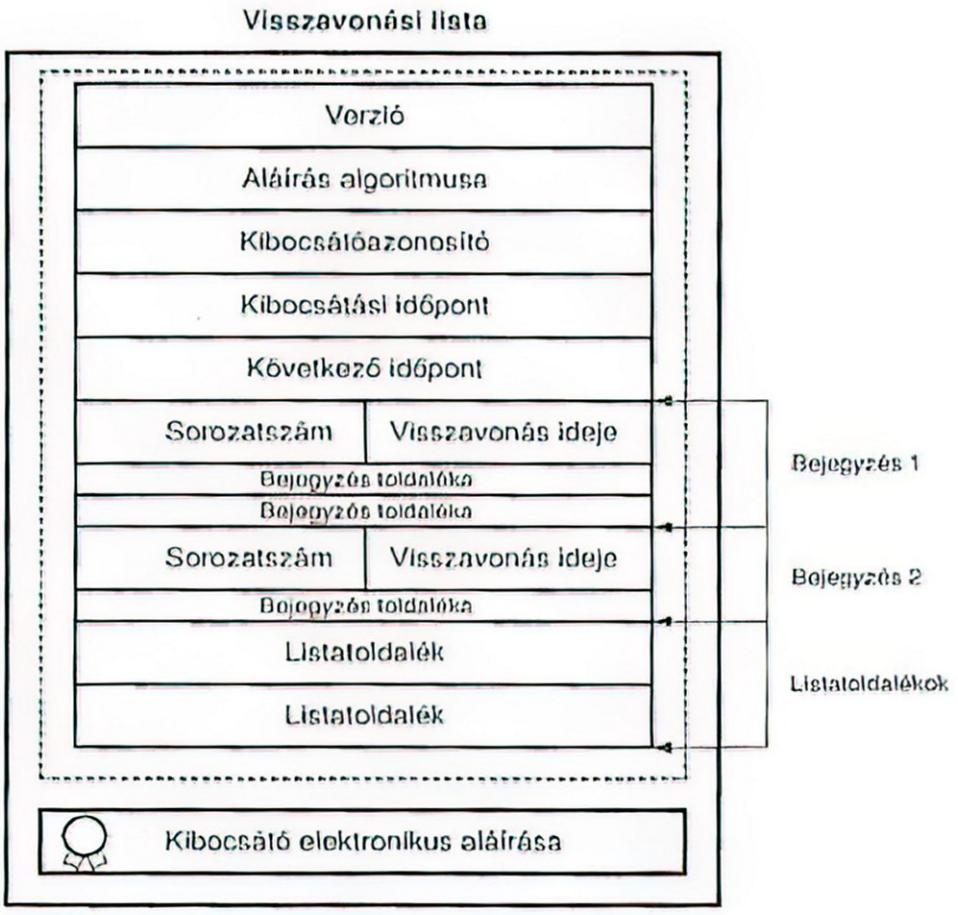
A Private key usage period toldalék a magánkulcs érvényességi idejének már említett korlátozására szolgál, a Certificate policies kiterjesztés pedig lehetőséget ad a szolgáltatónak, hogy a tanúsítványba foglaljon valamilyen hivatkozást (például OID, webcím, e-mail-cím) szöveges formátumú szabályzataira, amelyek a tanúsítvány és kulcs felhasználását részletesen szabályozzák. Erre azért van szükség, mert e dokumentumok terjedelme nem teszi lehetővé, hogy belefoglalják a tanúsítványba (lásd később). Ez persze a dokumentum változási lehetőségei miatt nem is lenne célszerű.

A tanúsítási láncra vonatkozó toldalékok közül a Basic Constraints a legfontosabb, mely azt határozza meg, hogy a tanúsítvány tulajdonosa aláírhat-e maga is tanúsítványokat, azaz viselkedhet-e hitelesítésszolgáltatóként. Mint ilyen, a legtöbbször kritikus. Ugyanígy kritikus a ritkán használt Name constraints toldalék, amely csak a szolgáltatói tanúsítványban szerepelhet. Értéke azt határozza meg, hogy az adott szolgáltatói tanúsítvánnyal hitelesített felhasználói tanúsítványok azonosítói milyen névtérbe eshetnek. Vonatkozhat mind a tulajdonos azonosítójára és alternatív neveire (például ha értéke DNS[82] formátumban

index.hu, akkor a felhasználói tanúsítvány DNS-neve akár indexmail.index.hu, akár forum.index.hu is lehet; ugyanígy, ha értéke mail address formátumban freemail.hu, akkor a felhasználói tanúsítványok azonosítóiban bármilyen freemail-es e-mail-cím szerepelhet, de másmilyen nem). Szintén csak a szolgáltatói, azon belül is csak kereszthitelesítő tanúsítványokban szerepelhet a Policy mappings toldalék, amely arra szolgál, hogy a két szolgáltató eltérő szabályzatait megfeleltesse egymásnak. Ezzel a kiterjesztéssel a szolgáltató biztosíthatja a felhasználókat arról, hogy a kereszthitelesített szolgáltató szabályzatai megfelelnek az övéinek.

4.9.7 Az X.509-es visszavonási lista

Az X.509-es szabvány nemcsak a tanúsítvány, hanem a visszavonási lista szerkezetét is leírja.



51. ábra
Az X.509 V2 visszavonási lista felépítése

A visszavonási lista esetében nemcsak a lista egészének lehetnek toldalékai, de az egyes bejegyzéseknek külön-külön is[83] (bár ugyanazon lista esetében az egyes bejegyzések toldalékai általában ugyanazok).

A mezők jelentése a következő:

Verzió	A lista a szabvány mely verziója alapján készült (v1, v2)
Aláírás algoritmusa	A kibocsátó által a lista aláírására használt algoritmus azonosítója
Kibocsátóazonosító	A visszavonási listát kibocsátó hitelesítőegység egyedi (X.500) neve
Kibocsátási időpont	A lista kibocsátásának időpontja
Következő időpont	A következő lista kibocsátásának időpontja
Sorozatszám	A visszavont tanúsítvány egyedi azonosítója
Visszavonás ideje	A tanúsítvány visszavonásának/felfüggesztésének időpontja
Bejegyzés toldaléka	A lista visszavonási bejegyzésének toldalékrekordjai
Lista toldaléka	A lista egészének toldalékrekordjai

4.9.8 A visszavonási lista szabványos toldalékai

A visszavonási lista és bejegyzéseinek generális toldalékait már bizonyára sejtik olvasóim, hiszen azokról már esett szó. Biztosan nem árt azonban, ha megállunk egy kicsit, és a tanúsítvány toldalékaihoz hasonlóan még egyszer áttekintjük őket. A listának egyetlen szabványos toldaléka érdemes említésre, mégpedig a CRL Number, azaz a lista sorszáma, amelynek értéke egy listakibocsátásonként szekvenciálisan növekvő szám. A listasorszám arra jó, hogy a felhasználó egyértelműen képes legyen megállapítani, nem mulasztott-e el egy kibocsátási listát (az időpontokból ez nem feltétlen állapítható meg), amely mindig hasznos lehet, de a delta CRL esetében egyenesen elengedhetetlen.

A legfontosabb két bejegyzéstoldalék a visszavonás oka (Reason Code) és az érvénytelenség ideje (Invalidity Date). A visszavonás oka nem szorul különösebb magyarázatra, legfeljebb az okok felsorolására. Az érvénytelenség ideje pedig az az idő, amiről már a kulcskompromittálódás kapcsán esett szó: mivel a visszavonási idő, ahogy a neve is mutatja, a visszavonás idejét azonosítja, és nem azt az időt amikor a kulcs megbízhatatlanná vált (nem feltétlen kulcskompromittálódás miatt), így azt csak külön lehet feltüntetni. Míg a visszavonási ideje soha nem lehet korábbi, mint az előző lista kibocsátása, az érvénytelenség ideje annál jóval régebbi is lehet.

A szabványos visszavonási okok a következők:
– a felhasználói kulcs kompromittálódása,
– a szolgáltatói kulcs kompromittálódása,
– adatváltozás,
– elavulás,
– indok megszűnése,
– jogosultság visszavonása,
– felfüggesztés,
– listából kivezetve.

Az adatváltozás elsősorban a felhasználó, másodsorban a szolgáltató azonosítójának, harmadsorban a tanúsítvány más adatának változását jelenti. Gyakran változó azonosítókat, melyek nem feltétlen szükségesek a felhasználó azonosításához (például telefonszám), emiatt nem érdemes felvenni a tanúsítványba. Az elavulási okot azokban az esetekben érdemes használni, mikor a tanúsítvány visszavonására – annak frissítése miatt – a lejáratot megelőzően (pár nappal) kerül sor. Az indok megszűnése egyszerűen csak annyit jelent, hogy a felhasználónak már nem volt tovább szüksége a tanúsítványra s szépen visszaadta. A jogosultság visszavonása elsősorban attribútumtanúsítványoknál (lásd alább) értelmezett, s a tanúsítványban szereplő valamilyen jogosultság, cím, szerepkör stb. megszűnésére utal (például ha a tanúsítványban fel van tüntetve a tulajdonos rangfokozata, s őt érdemei elismerése mellett más, fontos beosztásba helyezik, akkor a tanúsítványt ezen ok feltüntetésével kell visszavonni). A felfüggesztésről már esett szó, de arról nem, hogy az így (mint egy visszavonási ok) jelölhető a visszavonási listában. Ehhez tartozik még egy szabványos bejegyzéskiterjesztés, méghozzá a Hold instruction, ami azt mondja meg, mit kell tenni akkor, amikor ezzel a felfüggesztett tanúsítvánnyal találkozik az ember. A listából kivezetve a delta CRL esetében értelmezett, és azt jelenti, hogy a bejegyzés újraérvényesítés vagy a tanúsítvány érvényességének lejárata miatt kikerült a visszavonási listából.

4.10 Attribútumtanúsítványok

A tanúsítvány elsődleges célja az, hogy egy adott személy (vagy szervezet, eszköz stb.) azonosságát igazolja egy elektronikus ügyletben (tanúsítja, hogy az adott nyilvános kulcs az övé). Gyakran felmerül azonban az igény arra is, hogy a tanúsítványba kiegészítő információként olyan adatokat foglaljanak, melyek a tanúsítvány tulajdonosának tanúsítványhasználathoz kapcsolódó jogait finomítják (korlátozzák). Így például megadhatják, hogy milyen összegig írhat alá a cég nevében és kikkel közösen, milyen típusú ügyletekben járhat el, milyen hozzáférési jogosultságokkal rendelkezik adott erőforrásokhoz stb.

Két körülmény azonban ellene szól annak, hogy az ilyen típusú tulajdonságadatokat a hagyományos identitástanúsítványokba foglaljuk:

- A tanúsítvány tulajdonosának ezen attribútumai (például hogy melyik osztályon, melyik projekten dolgozik, s ezért milyen jogai vannak) gyakrabban változnak, mint a tanúsítványba foglalt általános, elsősorban személyazonosságával kapcsolatos adatai.
- Az a hatóság, amelyik az általános tanúsítványt kibocsátja, nem feltétlenül rendelkezik a szükséges információkkal, vagy nem jogosult a felhasználó egyéb (pénzügyi, informatikai stb.) jogainak beállítására.

E problémák megoldására dolgozták ki az attribútumtanúsítvány koncepcióját, amit az X.509-es szabványba is belefoglaltak[84]. Az attribútumtanúsítvány feltűnően hasonlít mind felépítésében, mind kezelésében az identitástanúsítványokra, amelynek tulajdonképpen kiegészítője. Feladata, hogy a tanúsítványban megnevezett entitáshoz tulajdonságinformációkat kössön.

Az X.509-es szabvány szerint az attribútumtanúsítvány mezői a következők:

Verzió	A tanúsítvány a szabvány mely verziója alapján készült (v1)
Tulajdonosazonosító	A tanúsítvány tulajdonosának egyedi (X.500) neve
Kibocsátóazonosító	A tanúsítvány kibocsátójának egyedi (X.500) neve vagy hivatkozás a tanúsítvány tulajdonosának identitástanúsítványára
Aláírás algoritmusa	A kibocsátó által a tanúsítvány aláírására használt algoritmus azonosítója
Sorozatszám	A tanúsítvány egyedi sorszáma (hitelesítőegységen belül)
Érvényesség	A tanúsítvány érvényességének kezdő és végdátuma
Kibocsátó-ID	A kibocsátó egyedi azonosítója
Attribútumok	A tulajdonoshoz kapcsolódó attribútuminformációk
Toldaléktípusa	A toldaléktípusának egyedi azonosítója
Toldalékjelző	Kritikus / Nem kritikus
Toldaléktartalma	A toldaléktartalma a típusnak megfelelően

Mint látható, tényleg hasonlít a normál nyilvános kulcsú tanúsítványhoz. Alá van írva a kibocsátó által, vannak toldalékai, de van pár nagyon fontos különbség is. Legelőször is az, hogy ebben a tanúsítványban nincs nyilvános kulcs, vagyis elektronikus aláírásra, titkosításra nem alkalmas, sőt voltaképpen önmagában, egy nyilvános kulcsú tanúsítvány nélkül nem sok mindenre jó. De ez nem is cél, hiszen az attribútumtanúsítványok a hagyományos (személyazonosságot vagy egyéb, személyes adatot igazoló) tanúsítványok kiegészítéseként

működnek. Az attribútumtanúsítványok között lehetnek olyanok is, amelyek kizárólag nagyon rövid érvényű tulajdonságokat foglalnak magukban, s a tanúsítványt ennek megfelelő érvényességi idővel (akár csak pár nap) adják ki, így visszavonásukról sem kell külön gondoskodni. Az attribútumtanúsítványok ettől eltekintve a nyilvános kulcsú tanúsítványhoz hasonlóan kezelődnek (az attribútumokat például a kiterjesztéshez hasonlóan regisztrálni kell).

Az igazsághoz hozzátartozik, hogy – bármennyire is lenyűgöző a koncepció – az attribútumtanúsítványok használata még nem terjedt el a világban, aminek egyik okát megint csak az alkalmazásokban kell keresni, amelyek nem értik meg őket.

4.11 Találkozások a tanúsítvánnyal

Aki az eddigieken hősiesen átrágta magát, megérdemli, hogy újfent pár színes-szagos gyakorlati illusztrációval dobjuk fel meggyötört szürkeállományát. Gyorssegélyként így egy kis útmutató következik arról, mit kell tenni ahhoz, hogy tanúsítványokkal találkozhassunk. Szerencsére semmi rendkívüliről nincs szó, sőt óvatlan olvasóm szinte bármikor, akár a legváratlanabb helyeken is belebotolhat egy tanúsítványba.

4.11.1 Elektronikus levelezés

Az első, legkézenfekvőbb módszer az, ha az ember elmegy egy hitelesítésszolgáltatóhoz, és vesz magának. Hogyne, tudom, ez pénzbe kerül. Meg inkább először megnézné a szomszédot, hogyan boldogul vele, s ha neki bejön... Az ilyen óvatos olvasómnak azt javasolnám, hogy kérje meg valamelyik ismerősét, aki már rendelkezik tanúsítvánnyal, hogy írjon neki elektronikus aláírással ellátott levelet. Amennyiben olyan levelezőalkalmazással rendelkezik, amely kezeli az S/MIME protokollt, akkor azzal képes lesz a kapott levél elektronikusaláírás-ellenőrzési eljárásának részeként a tanúsítvány megtekintésére, ahogy azt a könyv elején is bemutattam. Ha ennek sikerén fellelkesülne, vegye használatba a DrótPostaGalambot, vagy igényeljen teszt tanúsítványt valamelyik szolgáltatótól. Mivel az így kapott tanúsítvány amolyan ingyenes termékmintaként funkcionál, s a felhasználó azonosításáról tulajdonképpen szó sincs, mindössze az e-mail-cím és a tanúsítvány összerendeléséről, annak felhasználási lehetőségei korlátozottak. Arra viszont biztosan alkalmas, hogy az olvasó a gyakorlatban is szembesüljön az itt olvasottakkal, és megbarátkozhasson az elektronikus aláírással. Sőt a tanúsítvány privát felhasználásra kiválóan megfelelhet a barátkozás utáni időszakban is.

Ha valakitől elektronikusan aláírt levelet kapunk, akkor levelezőalkalmazásunk az aláírás ellenőrzésére szolgáló, a levélhez csatolt tanúsítványban szereplő e-mail-címet hasonlítja össze a levél küldőjének tényleges e-mail-címével, és természetesen ellenőrzi a levél tartalmának sértetlenségét is.[85]

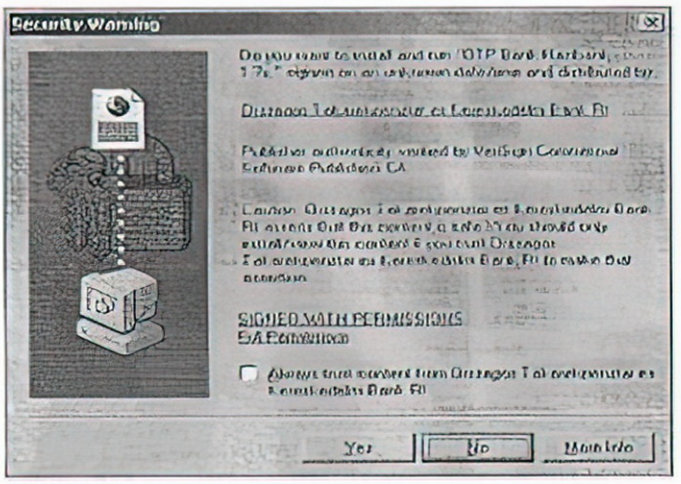
4.11.2 Biztonságos böngészés

Ahhoz, hogy egy webszerver-tanúsítvánnyal találkozhassunk, egy biztonságosnak nevezett weboldalt kell meglátogatnunk. Az, hogy sikerült egy ilyen oldalra lelnünk, az a könyv elején (lásd 2.4 fejezet) ismertetett jelek alapján észlelhető. A meglátogatott oldal ilyenkor biztonságosnak tekinthető, legalábbis abban az értelemben, hogy a megjelenő tartalom létrehozójában és az olvasott anyag eredetiségében, sértetlenségében biztosak lehetünk. Sok oldalhoz a hagyományos elérés mellett biztonságos módon is hozzáférhetünk. Hogy ilyen szolgáltatást nyújt-e az oldal (vagyis a mögötte lévő webkiszolgáló), azt a legkönnyebben úgy ellenőrizhetjük, ha az oldal címének az elején a protokollra utaló http betűcsoportot https-re cseréljük. Ezzel – tudományosan fogalmazva – a biztonságos kapcsolat felépítését magunk kezdeményezzük.

4.11.3 Aláírt programok

A leglátványosabb, de kevésbé gyakori találkozási lehetőség a szoftvertanúsítványok esete. Ha ilyet akarunk beszerkészni, akkor a legegyszerűbb, ha egy olyan magyar bankot vagy brókerházat keresünk fel, amely weben keresztüli banki és tőzsdei szolgáltatásokat nyújt. Az ezt biztosító alkalmazások[86] – egy magára valamit is adó pénzintézet esetében – elektronikus aláírással vannak ellátva.

A böngészőben ilyen alkalmakkor megjelenő **Security Warning** (Biztonsági figyelmeztetés) ablak nemcsak valamiféle veszélyre hívja fel figyelmünket, hanem arról is tanúskodik, hogy az éppen gépünkre lecsusszanni akaró, és ott mindenfajta ismeretlen műveletet végrehajtani szándékozó programhoz a gyártója a nevét adja. Teszi ezt méghozzá abból a nemes célból, hogy minket – akik rábízzuk komoly értéket képviselő erőforrásainkat és az azon tárolt adatainkat – megnyugtasson a program származása és sértetlensége felől. Az aláírás ugyan nem garantálja, hogy a program nem fogja leformázni a háttértárolónkat, nem utalja át összes pénzünket a program fejlesztőjének, vagy hogy a program helyesen működik, de valamivel több az esély arra, hogy ilyen kellemetlenségeket megússzunk, mint egyébként. Ha ezt mégis megtenné, akkor legalább tudhatjuk, kit okoljunk.



52. ábra
Aláírt program futásának engedélyezése

A képernyőn látható a letöltendő alkalmazás neve, a szervezet neve, mely ránk akarja tukmálni azt, valamint hogy milyen jogosultságokat kér az alkalmazás (**Full Permissions**). A szervezet nevére kattintva megjelenik az alkalmazás aláírására kibocsátott tanúsítvány. Ha nem adjuk meg az alkalmazás számára a kért jogosultságokat, akkor az nem indul el.

4.11.4 Mit nézzünk a tanúsítványon

Most már tudjuk, hogyan találkozhatunk tanúsítvánnyal, itt az ideje, hogy azt is megtudjuk, mit kell tennünk akkor, ha egy éles szituációban botlunk bele. A legalapvetőbb információkat ugyan az alkalmazások általában magukról is ellenőrzik (e-mail esetében összehasonlítják a levél küldőjének e-mail-címét a tanúsítványban feltüntetettel; weboldal esetében az oldal címét a tanúsítványban szereplővel; ellenőrzik, hogy a tanúsítvány érvényessége nem-e járt le; hogy a tanúsítvány kibocsátója a felhasználó által megbízhatónak minősített szolgáltatók közül való-e stb.), én mégis azt ajánlom mindenkinek, hogy vizsgálja meg alaposan saját szemével is a tanúsítványt, amivel összehozza a sors, mielőtt megbízhatónak minősíti.

Először is természetesen a tulajdonos és a kibocsátó kilétét, a tanúsítvány érvényességét és azt, hogy a tanúsítványt milyen célra bocsátották ki. Ezek az adatok a **Windows** esetében a tanúsítványt megjelenítő ablak főoldalán találhatók (lásd: 10.3.4 fejezet).

Különösen érdemes odafigyelni a tanúsítvány osztályának jelzésére és a szabályzatra való utalásra (a szabályzat tartalma külön tekinthető meg). Ezek az információk a tanúsítvány „erősségét" (biztonsági szintjét és a mögötte álló garanciákat) határozzák meg. Az egyébként teljesen hasonló módon megjelenő tanúsítványok csak ezen apró attribútumukban különböztethetők meg, de ez az apróság akár nagyságrendi különbséget is jelenthet. Ezzel összefüggésben is érdemes megvizsgálni a tanúsítási láncot, mivel a legfelső szinten megjelenő szolgáltatói hitelesítőegység elnevezése is általában a hitelesítési osztályra utal. Az említett ellenőrzéseket érdemes a tanúsítási lánc valamennyi tanúsítványával kapcsolatban elvégezni.

Hasznos tudni ugyanakkor, hogy a tanúsítvány ellenőrzése nem egyezik meg az aláírás ellenőrzésével. Bár az aláírás alapszintű ellenőrzését (az aláírás-tanúsítványban szereplő nyilvános kulccsal való visszafejthetőségét és az információ sértetlenségének ellenőrzését) az alkalmazások automatikusan elvégzik, az aláírás is tartalmazhat olyan attribútumokat (például aláírásiszabályzat-azonosítót), amelyek ellenőrzése emberi közreműködést igényelhet.

JEGYZET

1 Mely módszerekkel persze a hangfelismerés és a telefon azonosításának biztonsági szintjére csökkentjük a tanúsítvány erősségét.

2 A PGP kriptorendszer ehhez hasonló hálós bizalmi modellel működik, aminek – az igazsághoz hozzátartozik – vannak előnyei is (pl. a kulcs hitelesítése nem kerül semmibe).

3 A tanúsítvány kérdésköre a hitelesítésszolgáltató témájától nehezen elválasztható, s bár azzal külön fejezet foglalkozik, néhol mégis kénytelen leszek annak elévágva, a hitelesítésszolgáltatókról is pár gondolatot megosztani olvasóimmal. Ahhoz azonban, hogy a teljes kép összeálljon valószínűleg a hitelesítésszolgáltatókról szóló fejezetet, sőt végső soron az egész könyvet el kell olvasni. Remélem, lesz türelmük hozzá.

4 Lásd a Fogalomtár meghatározásait is.

5 A kereskedelmi szolgáltatók pénzért árusítják a tanúsítványokat.

6 Lásd 4.8.1 fejezet.

7 A hitelesítésszolgáltató nélküli nyilvános kulcsú rendszereknek az az egyik legnagyobb hátrányuk, hogy ilyen nyilvántartással általában nem rendelkeznek.

8 Az érvényességi idő lejáratakor vagy azt követően nem sokkal a tanúsítványok a tanúsítványtárból törlésre, illetve archiválásra kerülhetnek. Ez bekövetkezhet akár a tanúsítvány visszavonását követően is. A hitelesítésszolgáltató természetesen dönthet úgy is, hogy az érvénytelen tanúsítványokat még egy darabig, akár évekig is, a tanúsítványtárban tárolja (bár a törvény ezt nem tiltja, adatvédelmi aggályokat felvethet).

9 A lejárt/érvénytelen visszafejtő magánkulcs lehet már nem bizalmas adat (lehet, épp kompromittálódás miatt lett visszavonva), így a nyilvános kulccsal rejtjelezett adatok visszafejthetők lehetnek más által is (titkosításra nem a saját, hanem partnerünk nyilvános kulcsát használjuk).

10 Ha nincs ezt cáfoló explicit jelölés, a magánkulcs (itt nyilván saját magánkulcsunkról beszélünk) visszafejtésre akár az örökkévalóságig felhasználható. Mindez persze az érvényesség ideje alatt titkosított dokumentumokra értelmezhető.

11 Itt saját magánkulcsunkról van szó.

12 Itt viszont partnerünk nyilvános kulcsáról.

13 Ez nem is olyan egyszerű, mint amilyennek látszódik. Egy állomány letörlése például még messze nem jelenti annak megsemmisülését. Ügyes emberek még a szemétre kidobott formattált floppyról és háttértárolóról is visszahalásszák az adatokat.

14 Mindez nem okoz gondot azoknak, akik múltbeli adatokra kíváncsiak, hiszen visszamenőlegesen visszavonni úgysem lehet.

15 Mindez persze okozhat problémát azoknak is, akik múltbeli adatokban kutakodnak, ha a visszavonási lista felülíródik, s így nem tartalmazza az érvénytelen állapotra vonatkozó korabeli információkat.

16 Tipikusan ilyen a hitelesítésszolgáltató saját (aláíró) tanúsítványának érvényességi ellenőrzése egy általa kibocsátott felhasználói tanúsítvány ellenőrzése kapcsán. Ekkor nem azt akarjuk megtudni, hogy a hitelesítőegység tanúsítványa a felhasználói tanúsítvány kibocsátásakor érvényes volt-e (nagy baj lenne azzal a szolgáltatóval, amelyiknél nincs így), hanem azt, hogy azóta nem történt-e olyan esemény, ami a szolgáltatói aláíró kulcsot kompromittálta volna.

17 Hogy az alkalmazások vajon hogyan viselkednek, mikor milyen érvényességet ellenőriznek, és milyen állapotinformációt kérdeznek le, arra lehet, jobb nem is gondolni. Erről az alkal-

mazások gyártóit kellene megkérdezni, de a dokumentációkban hiába is keresünk útmutatót ezekre a kérdéseinkre.

18 A gyakorlatban ez egy véletlenszerű adat aláírásával történik. Ha a szolgáltató ezt vissza tudja fejteni, az azt jelenti, hogy a mellékelt nyilvános kulcs párját birtokoljuk. A tanúsítvány legyártása után ellenőrizni kell, hogy valóban az általunk küldött nyilvános kulcsból lett tanúsítvány (valaki nem cserélte-e azt ki még védtelen formájában).

19 Azaz a felhasználó besétál aláíró eszközével a szolgáltatóhoz (annak regisztrációs szervezetéhez), vagy esetleg a szolgáltató regisztrációs üzletkötője keresi fel az ügyfelet.

20 Abban az értelemben, hogy amíg együtt van a két kulcs, addig „nincs" biztonság. Mihelyst elválasztottuk őket, az algoritmus adja, amit adnia kell.

21 Hardware Security Module, azaz hardveres biztonsági modul.

22 A **Windows** operációs rendszerek ebből a szempontból nem érdemelnek dicséretet, mivel nem támogatják a hajlékonylemezről történő kulcshasználatot.

23 Kivéve a kulcsegyeztetés esetét.

24 Azt aláíró magánkulcsról ne készítsünk biztonsági mentést, mert az pont a biztonság ellen van. A mentett példány csak egy újabb lehetőség a rossz embereknek, hogy valahonnan megszerezzék kulcsunkat. Ha egyik példányunk elveszett, vagy kételyek merülnének fel, úgyis vissza kell vonni a tanúsítványt. Akkor meg minek a mentés? Lehetnek persze ez alól kivételek. Egy tökéletesen biztos, páncélba zárt, rendszeresen ellenőrzött mentés esetleg jól jöhet, ha a háttértárolót gyenge pillanatunkban leformázzuk (ez esetben nem feltétlen lenne szükséges a visszavonás). Az ilyen szituációk azonban az esetek mindössze egy százalékát adhatják, a maradék 99 százalékban jobb a mérlegelés nélküli visszavonás.

25 A gyakorlatban ez nem annyira jellemző, a kulcsok legtöbbször ugyanolyan típusúak és méretűek, kivéve azokat az eseteket, amikor ezt maga az algoritmus akadályozza, mint például a DSA aláíró algoritmus esetében, ami titkosításra nem alkalmas.

26 A magyar törvénynek is van erre vonatkozó jogi korlátozása. Lásd: 9.5 fejezet.

27 Egyéb kulcstípusokat lásd: 4.9.6 fejezet.

28 Ha például a közösség egy vállalat (és ő fizet a tanúsítványokért), jogosan él ilyen előírással, arra az esetre gondolva, hogy a kulcsot titkosításra felhasználó munkatársa esetleg a fluktuáció áldozata lesz. A cég nyilván munkatársa távozása esetén is hozzá akar férni annak rejtjelezett dokumentumaihoz (melyeket munkakörében állított elő), s a munkatárs saját mentése a kulcsról erre semmiképp nem ideális megoldás. Vannak olyan országok is (még a demokratikusnak nevezett USA is sokáig „kacérkodott" ezzel), ahol a hatalom nyálkás kocsányon lógó kíváncsi szeme akar mindenhova beférkőzni, s ezért írják elő a letétbe helyezést.

29 Mint az látható lesz, (többek között) erre van kitalálva a hitelesítési szabályzat. Lásd: 8.5 fejezet.

30 Elnézést kérve a motorizációban járatlanabb olvasóimtól: szappantartó és luxuslimuzin (vagyis jó nagy különbség).

31 Az osztályokat és azok kezelését a szolgáltatási szabályzat szokta tárgyalni.

32 A minősítettség nem kifejezetten mint osztály van definiálva, de úgy értelmezhető a legkönnyebben.

33 A tanúsítási láncról és gyökér hitelesítőegységről bővebben lásd: 5.8.3 fejezet.

34 A Lotus Notes levelezőrendszer például így működik. Felhasználás előtt a levelezőrendszer a számára megadott adatainkból automatikusan készít tanúsítványt, illetve generál kulcsokat, s azok kezelését végig el is rejti a felhasználó elől.

35 Amennyiben elektronikus aláírással történik az igénylés, a kiadott tanúsítvány erősségi fokozata értelemszerűen nem lehet nagyobb, mint az igényléshez használt tanúsítványé.

36 Szerencsére ilyen azonosító nincs. Félreértés lenne azt hinni, hogy a könyv szerzője ilyen azonosító bevezetését támogatná. Az igazság az, hogy az ilyen törekvéseket határozottan opponálom, mert kifejezetten károsnak tartom – többek között – a könyvben tárgyalt elektronikus kommunikáció bizalmassága szempontjából is.

37 Ez esetben persze van egy olyan azonosító (maga a tanúsítványunk), amelynek segítségével az egyes államigazgatási szervek elviekben összefuttathatják adatbázisaikat.

38 Az azonosítónak egyébiránt nem lenne szükséges mindenáron egyedinek lenni, hiszen a tanúsítvány egyediségét más tényezők (pl. maga a nyilvános kulcs, illetve a tanúsítvány sorszáma) biztosítják.

39 Mint már említettem, vannak azonban nem egyszerű földi halandók is.

40 Annak, aki ilyen álneves tanúsítvány felhasználásában gondolkodik, nem árt, ha ezeknek a körülményeknek bővebben is utánanéz a szolgáltató szabályzataiban.

41 Erre a magyar törvények szerint is van joga a szolgáltatónak.

42 Ha a magánkulcs érvényessége nem rövidebb, mint a tanúsítványé, mert ezen ritka esetekben a tanúsítványt a magánkulcs érvényességének lejártát megelőzően kell frissíteni. Ilyen esetben a tanúsítványt nem szokták visszavonni a frissítést követően.

43 Kettő–öt évente, de az is lehet, hogy a szolgáltató nem támogatja a frissítést.

44 Olyan felhasználói tanúsítványt nem ad ki egy szolgáltató sem, amely meghaladná saját tanúsítványának érvényességét.

45 A nyilvántartás „hivatalossága" éppen ezért korlátozott: a benne szereplő információk csak a szolgáltató aláírásával érvényesek, s az aláírás ereje – ha ellentmondás vagy kétely merülne fel – mindig nagyobb, mint a nyilvántartásokban való szereplés vagy az onnan történő hiányzás ténye.

46 A jelenleg használatos módszerek az aláírással együtt ezért a tanúsítványt is elküldik, s a visszavonási lista elérhetőségét a tanúsítvány tartalmazza.

47 Újság esetében a tanúsítvány lenyomatát (a hash-függvénnyel képzettet) érdemes kinyomtatni az azonosítás végett.

48 Lightweight Directory Access Protocol – Az X.500 által definiált DAP protokoll diétás változata.

49 Az LDAP v1 utáni változatai már nem csak elérés módját határozzák meg.

50 Egy javaslat: www.ldapbrowser.com

51 Elnézést, bármilyen morbid is, de ha a gyászoló rokon besétál egy halotti bizonyítvánnyal, az is egy visszavonási ok.

52 A felhasználó és a szervezet személyes megjelenésére ilyenkor többnyire nincs szükség, egy visszavonási jelszó bemondásával (ami véletlenül sem ugyanaz, mint a magánkulcs aktiviváló adata) a visszavonás érvényesíthető.

53 Az angol megfelelő, a Certificate Revocation List rövidítése

54 Azt, hogy a visszavonási lista hol érhető el, a szolgáltatók dokumentálni szokták, illetve belefoglalják a tanúsítványba.

55 „Független" megfigyelések szerint a tanúsítványok nagyjából tíz százaléka szokott visszavonásra/felfüggesztésre kerülni. Ha a lista egy bejegyzése, mondjuk, húsz bájt méretű, akkor egy pontosan egymillió érvényes tanúsítvánnyal rendelkező szolgáltató esetében a visszavonási lista mintegy százezer bejegyzést fog tartalmazni, ami csingilingik nélkül két megabájt méretet jelent. Ha csak százezer érvényes tanúsítvánnyal számolunk, ez még mindig 200 kilobájt, aminek a rendszeres letöltése elképzelhető, milyen terhelést jelent a felhasználó rend-

szerének és a kommunikációs vonalaknak, nem is beszélve szerencsétlen könyvtárszerverről. A tíz százalék persze erősen függ a tanúsítvány érvényességi idejétől (minél hosszabb ideig érvényes a tanúsítvány, annál nagyobb a valószínűsége, hogy nem éri meg élettartama végét). Erre gondolva sem érdemes a tanúsítvány élettartamát túl hosszúra venni (de túl rövidre meg az adminisztrációs nehézségek miatt nem érdemes állítani).

56 Ellenben azzal, hogy a tanúsítványok külön bejegyzésekhez tartoznak, és ezért a közöttük történő kereséseket (a tanúsítvány egyedi neve alapján) végre lehet hajtatni a könyvtárszerverrel.

57 Minden szolgáltató saját visszavonási listákat (akár többet is) bocsát ki, így az érintett félnek adott esetben egy sereg visszavonási listát kell kezelnie, mindig a tanúsítványhoz tartozó megfelelő listát elővéve.

58 Amennyiben a lista adatai alapján jelentős döntést hozott, felülírás helyett érdemesebb lehet a régi listát az ellenőrzőnek is archiválni, annak ellenére, hogy az a szolgáltatónál később is hozzáférhető.

59 A szituáció, amiről beszélek, a következő: Kapunk egy aláírt üzenetet, hogy megrendeltek tőlünk három hajórakomány fűrészport. A megrendelés 16 órakor kelt (aláírás ideje), mi 22 órakor ellenőrizzük, s így látjuk, hogy a 21 órakor kibocsátott visszavonási listában szerepel az aláíráshoz tartozó tanúsítvány 19 órai visszavonással. Ha az aláírás 16 órai kelte teljesen biztos, akkor elvileg elfogadhatjuk a megrendelést, de én még ekkor sem ajánlanám, főleg abban az esetben nem, amikor a visszavonás oka kulcskompromittálódás.

60 ARL: Authority Revocation List

61 Az egyedi listanév feltüntetésére és ellenőrzésére azért van szükség, mert ha ilyen nem létezne, rosszindulatú embertársunk egy másik szétosztási ponton lévő listát másolhatna ide (akár egy üreset is), ami könnyen észrevétlen maradhatna, s alapos felfordulást okozna.

62 A lista nem mindig a legutolsó listához viszonyított változásokat tartalmazza. Lehet egy mesterlista, amit, mondjuk, naponta egyszer bocsátanak ki, és óránként a változásokat ehhez képest. A delta CRL-ben éppen ezért mindig jelölni kell, mi az a mesterlista, amihez képest a változásokat ez a delta lista hordozza.

63 Hozzá tartozik az igazsághoz, hogy a gyakorlatban ilyen megoldással még nem találkoztam.

64 A 389 a szimpla LDAP, a 636 az SSL-lel megspékelt, az 1760 egy webes megoldás, a 3269, pedig a Microsoft-féle.

65 Valójában „B" és „E" időpontok között annyi idő is eltelhet, hogy ezen időszak alatt akár több visszavonási lista publikálására is sor kerülhet. „D" és „E" pontok között általában igen kevés idő telik el, mert a szolgáltató, ha nem képes a kérelem gyors ellenőrzésére, a késlekedést megelőzve gyorsan fel szokta függeszteni a tanúsítványt. Jó esetben „C" és „D" időpontok között sem telik el sok idő, mert a felhasználónak elemi érdeke, hogy gyorsan cselekedjen, miután észrevette, hogy baj van.

66 A szolgáltatók általában az adott jövőbeni időpontban történő visszavonást se támogatják (ha, mondjuk, előre tudja valaki, hogy jövő héten bekötik a fejét, és felveszi a férje nevét, ami adatváltozást jelent, és így tanúsítvány-visszavonást von maga után).

67 Első verzióját az IETF szabványosította RFC 2560 néven.

68 Az OCSP V2-nek létezik egy kidolgozás alatt álló vetélytársa is SCVP (Simple Certificate Validation Protocol) néven.

69 Amit nem könnyű teljesíteni, hiszen az OCSP szerver különösen kellemetlenül érintheti egy DoS támadás.

70 Az igazsághoz hozzá tartozik, hogy a CRL lekérdezés sem csak LDAP protokollon keresztül lehetséges, a legtöbb könyvtárszerver például HTTP kéréseket is kiszolgál.

71 A hagyományos CRL sem olyan veszélyes ebből a szempontból, hiszen a visszavonási listában a tanúsítványok sorszáma szerepel, ami alapján a címtárban keresni nem lehet. A szolgáltatók némelyike mégis nyújt olyan szolgáltatást, amivel a visszavont tanúsítványok között név alapján lehet keresni (lásd 2.7 fejezet).

72 Egyeduralkodó, de nem egyedüli. A PGP tanúsítványok felépítése nem ezt a szabványt követi (bár a PGP rendszer már kezeli az X.509-es tanúsítványokat is).

73 A gyakorlatban általában ékezetek nélkül, mert az alkalmazások egy része még mindig nem kezeli helyesen az ékezeteket.

74 Az ISO 3166 szabvány szerinti országkódok megjelölésével

75 Van példa arra, hogy egyedi névbe is raknak sorszámot, ami megegyezhet a tanúsítvány sorszámával, de attól eltérő is lehet. Egyik esetben sem téveszthető össze a két mező.

76 Például a bejegyzés egyedi neve C=HU / O=Kőfaragó Rt., s a bejegyzés attribútumai között szerepel az E=info@kofargo.hu e-mail-cím. Ilyen esetben az e-mail-cím nem része az egyedi névnek!

77 Az ISO/IEC, az ITU, az ANSI X9 munkacsoportja és más szabványosítási szervezetek is foglalkoznak ilyen tevékenységgel.

78 Az eredeti szabványnak ezek nem voltak részei, de mint későbbi kiegészítések bele lettek dolgozva.

79 Ezért aztán ritka is a kritikus toldaléK. A bemutatott szabványos toldalékok, ahol ezt máshogy nem jelöltük, nem kritikusak.

80 Ennek semmi köze a hitelesítésszolgáltató regisztrációs szervezetéhez.

81 A felhasználási célok ezen utóbbi listája elviekben szabadon bővíthető kinek-kinek az igényei szerint. Az erre szolgáló objektum azonosítók regisztrációjának azonban az ITU-T X.660 és az ISO/IEC 9834-1 szabványának megfelelően kell történnie.

82 Itt Domain Name Service.

83 Ezért is nehéz megmondani egy bejegyzés pontos méretét.

84 Az ANSI X9 munkacsoportja dolgozta ki, s az ANSI X9.57 szabvány is tartalmazza.

85 Ahogy azt az S/MIME protokoll ismertetésekor említettem, a levél címének és egyéb attribútumainak sértetlenségét viszont nem vizsgálja.

86 Ezek olyan általában Javában írt (vagy ActiveX, esetleg más) programok, melyek a webszerverről töltődnek le.

5 A hitelesítésszolgáltató

Ajánlás:

Mindenkinek. Főleg azoknak,
akik szeretnek a dolgok mögé látni.

z ideális világban egyetlen megbízható harmadik fél, azaz esetünkben hitelesítésszolgáltató működne, természetesen ingyen és tökéletes biztonságot nyújtva. Ez a kívánság persze képtelenség, s az „ideális" is csak a tanúsítvány ellenőrzésének egyszerűségét illetően merülhet fel jelzőként. A való világ – ahogy ezt már örökbecsű dalok is megörökítették – azonban korántsem ilyen. Abban hitelesítésszolgáltatók hada versenyez egymással vagy él békésen egymás mellett a felhasználók más-más szegmensét kiszolgálva. E szolgáltatók eltérő módon épülnek fel, másfajta modellt követnek, különböző rendszereket használnak, szabályzataik, felelősségvállalásuk is eltérő, ami csöppet sem könnyíti meg a tanúsítványt ellenőrzők dolgát. Az ugyanis, hogy egy elektronikus aláírás és a mögötte lévő tanúsítvány egy adott szituációban elfogadható-e, számtalan dologtól függ. Ezek megértését nagyban segíti, ha tudjuk, milyen különböző modellek alapján, hogyan épül fel és működik egy hitelesítésszolgáltató.

5.1 A hitelesítésszolgáltató feladatai

A hitelesítésszolgáltató legalapvetőbb feladatai a felhasználó oldaláról nézve a következők:

- A felhasználók regisztrálása.
- Felhasználói kulcspár generálása (opcionálisan).
- Magánkulcs védelmét ellátó eszköz aktivizáló adatának generálása (opcionálisan).
- Tanúsítvány összeállítása és aláírása.
- Tanúsítvány közzététele a nyilvános tanúsítványtárban.
- Magánkulcs és tanúsítvány kulcshordozó eszközre helyezése (opcionálisan).
- Kulcshordozó átadása a felhasználónak.
- Aktivizáló adat átadása a felhasználónak (opcionálisan).
- Tanúsítványokkal kapcsolatos műveletek fogadása és azok végrehajtása.
- Visszavonási lista összeállítása.
- Visszavonási lista közzététele a nyilvános tanúsítványtárban.
- Lejárt tanúsítványok archiválása.
- Titkosító kulcsok letétbe helyezése (opcionálisan).
- Szabályzatok készítése és karbantartása.

- Nyilvános szabályzatok közzététele.
- Tanúsítványtár üzemeltetése és karbantartása.
- Azonnali érvényesség-ellenőrzési kérések kiszolgálása (opcionálisan).

5.2 Hitelesítésszolgáltató-típusok

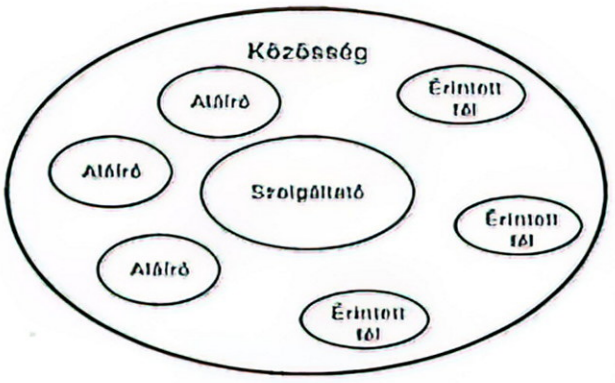
A hitelesítésszolgáltatók két alapvető típusát különböztethetjük meg: nyilvános és nem nyilvános hitelesítésszolgáltató. A nyilvános jelző azzal a közösséggel kapcsolatos, amelyet kiszolgálnak: ha a közösségnek bárki tagja lehet, akkor a szolgáltató nyilvános, ellenkező esetben nem nyilvános. Ez legalábbis az elv, ami a gyakorlatban szokás szerint nem ilyen egyszerű, és éppen ezért a két különböző szolgáltatótípust nem is lehet ennyire élesen elválasztani. Viszonylag könnyű beazonosítani az egyértelműen nem nyilvános hitelesítésszolgáltatókat: ezek valamilyen, eleve zárt, jól körülhatárolható közösséget szolgálnak ki. Lehet például egy vállalatnak, kamarának vagy bármely más szervezetnek saját hitelesítésszolgáltatása, amely saját tagjai számára bocsát ki tanúsítványokat. Ekkor a szolgáltatást valójában nem egy megbízható harmadik fél nyújtja, hanem „önkiszolgálás" alapon az adott szervezet önmagának.

Az úgynevezett nyilvános szolgáltatók esetében a közösség nem ennyire zárt, illetve nem ennyire korlátozott, de biztosan feltételekhez kötött a tanúsítvány kibocsátása. Ezek a feltételek adott esetben egy meglehetősen zárt felhasználói kört is létre tudnak hozni. A legalapvetőbb feltételek életkorhoz, a szolgáltatási díjak megfizetéséhez, esetleg állampolgársághoz és ehhez hasonló dolgokhoz kötődnek. Vannak azonban olyan „kvázi" nyilvános hitelesítésszolgáltatók is, akik közvetlen nem nyújtanak szolgáltatást bármely, utcáról beszédelgett felhasználónak, hanem csak különböző szervezeteken keresztül. E szervezetek viszont saját maguk szűkíthetik tovább a felhasználók körét: azok lehetnek kizárólagosan saját munkatársaik, tagjaik, ügyfeleik[1].

Éppen ezért a nyilvánosságot elsősorban nem is az alapján érdemes behatárolni, hogy ki lehet tanúsítványtulajdonos, hanem az alapján, hogy ki lehet érintett fél. Azaz ki lehet az aláírás elfogadója, és ki kérdezheti le a tanúsítványtárat. Ha a tanúsítványtár elérése bárki számára lehetséges, vagyis bárki lehet elfogadó fél, akkor a szolgáltató nyilvános. Ha a tanúsítványtár lekérdezése korlátozott, a szolgáltatás zárt.

5.3 Közösség

Az előbb elmondottak könnyebb megértése végett álljon itt ez a kis Móricka-ábra, amely azt a bizonyos közösséget szemlélteti, amiről már oly sokszor beszéltem:



53. ábra
Közösség és tagjai

A közösségnek három különböző típusú tagja létezik: a hitelesítésszolgáltató, az aláíró (felhasználó, tanúsítványtulajdonos stb.) és az érintett fél (elfogadó). A közösség számtalan aláíróból és érintett félből állhat, sőt egyes elfajult esetekben akár több hitelesítésszolgáltató is kiszolgálója lehet.[2] A szolgáltató az aláíróval (a tanúsítvány tulajdonosával) elsősorban a regisztrációs szervezeteken keresztül, az érintett féllel pedig a tanúsítványtáron keresztül tart kapcsolatot.

Nyilvános közösség esetében az érintett felek száma nem behatárolt, hacsak a föld népességét nem vesszük annak, és az aláírók száma is igen nagy lehet. A közösség határait és jellemzőit azok a szabályzatok definiálják, melyeket a hitelesítésszolgáltató alkalmaz. Ha több hitelesítésszolgáltató alkalmazza ugyanazt vagy valamilyen módon egymásnak megfeleltethető szabályzatokat, akkor szerepelhet a közösségben egynél több szolgáltató. Ez azonban igen ritka jelenség, az életben az egy szolgáltató – egy szabályzat párosítás a legjellemzőbb, és ennek megfelelően a közösségnek egyetlen szolgáltató szokott a tagja lenni.

Zárt közösség esetében a tanúsítvány, a visszavonási lista, a szabályzatok és egyéb, korábban nyilvánosnak titulált dolgok nyilvánossága valójában a közösségre korlátozott, a vonatkozó szabályoknak megfelelően.

5.4 A hitelesítésszolgáltató felépítése

A hitelesítésszolgáltató több különböző részre tagozódik, amelyeknek jól elkülöníthető szerepük van. A főbb részek a következők:

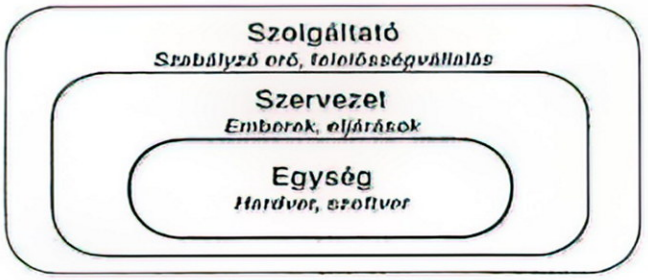
- szabályzó szervezet,
- hitelesítőszervezet,
- regisztrációs szervezet,
- tanúsítványtár.

Ezeket az alábbi opcionális részek egészíthetik ki:

- kulcsletétszervezet (vagy egység),
- valós idejű állapotinformációs egység.

Terminológiám szerint a szervezet egy összetettebb entitás, mint az egység. Míg az egység alatt legfőképpen egy informatikai rendszert értek, a szervezet alatt egy komplex, embereket, eljárásokat és sok más egyebet is mozgósító apparátust, amely mögött nyilván informatikai támogatás is áll.[3] Egy szervezet több egységet üzemeltethet, s a szolgáltató több szervezetből áll. A szolgáltató

e szervezetek együttműködését biztosítja a közös szabályzatok segítségével. A szervezetek felelősek saját tevékenységükért, a szolgáltató felelős mindegyik szervezetért.



54. ábra
Szolgáltató – szervezet – egység

A tanúsítványtár, a kulcsletét egység és a valós idejű állapotinformációs egység működhet a hitelesítőszervezet részeként is. Ez esetben ezen egységek üzemeltetéséért és karbantartásáért is a hitelesítőszervezet a felelős. Lehetnek azonban ezen egységek egy más szervezet kezelésében is, illetve megjelenhetnek önálló szervezetként is a szolgáltató hierarchiájában.

5.4.1 Hitelesítőszervezet

A hitelesítőszervezet a szolgáltató központi szervezete, amely a tanúsítvány összeállításáért és aláírásáért, a tanúsítványokkal kapcsolatos műveletek végrehajtásáért, a visszavonási lista összeállításáért és a lejárt (tanúsítványtárból törölt) tanúsítványok archiválásáért felelős. A hitelesítőszervezet legfőbb segítsége ebben a hitelesítőegység, amely a tanúsítvány aláírásához saját magánkulcsát veszi igénybe. A hitelesítőegység a nyilvános tanúsítványtártól szeparált saját belső adatbázissal is rendelkezik, amelyben a kibocsátott tanúsítványokat és a velük kapcsolatos változásokat tartja nyilván. Ez alapján készíti el meghatározott rendszerességgel a visszavonási listát, és továbbítja azt – akárcsak a tanúsítványokat – a nyilvános tanúsítványtárba közzététel céljából.

A hitelesítőszervezet önmagában nem képes nagyszámú előfizetői kör kiszolgálására, különösen akkor nem, ha ez a kör földrajzilag nem egy jól behatárolt területen belül helyezkedik el. Másfelől a hitelesítőegységet fizikailag, logikailag (például adminisztratív úton, személyi hozzáférés tekintetében) és informatikailag egyaránt a lehető legmagasabb fokú védelemben kell részesíteni, amely követelmény a személyes megjelenéssel járó ügyfélfogadással, de a hálózaton (web, e-mail) keresztüli eléréssel is szöges ellentétben áll. A hitelesítőszervezetet voltaképpen nevezhetjük tanúsítványgyárnak is, ahol a vevőknek semmi keresnivalója, legfeljebb gyárlátogatás alkalmával.[4]

5.4.2 Regisztrációs szervezet

Ezért fejlesztették ki a regisztrációs egységnek nevezett megoldást, mely egy technikailag különálló hardver-szoftver modul, ami a hitelesítőegységgel távol-

ról és biztonságos módon képes kapcsolatot tartani. A regisztrációs egységet regisztrációs szervezet működteti, egy szervezet akár több egységet is, fizikailag elkülönülő helyszíneken. Ezeket a helyszíneket szokás regisztrációs pontoknak, helyeknek vagy kirendeltségeknek nevezni.

A regisztrációs szervezet regisztrációs pontja a hitelesítésszolgáltató egy kihelyezett fiókja, helyi képviselete vagy mintaboltja, amelyet nem szükséges abban a fokú fizikai védelemben részesíteni, mint a hitelesítő-központot,[5] de a hitelesítőszervezethez hasonló eljárásrendi, személyi, szakmai és biztonsági követelményeknek kell megfeleljen. Ez azért van így, mert ugyan nem a regisztrációs egység magánkulcsával írják alá a tanúsítványt, de a regisztrációs egység magánkulcsával előállítható olyan tanúsítványkérelem, amit aztán a hitelesítőszervezet automatikusan teljesít. Hiszen – mint az, az elnevezésből és az elmondottakból már bizonyára kiderült – a felhasználók regisztrálását (az adatok felvételét és ellenőrzését) a regisztrációs szervezet végzi, s a regisztrációs szervezet által ellenőrzött tanúsítványkérelmeket a hitelesítőszervezet már nem ellenőrzi újra. Legfeljebb olyan rendkívüli esetekben nem szolgálja ki, mint egy egyszer már kiosztott felhasználói azonosító esetleges ismétlődése (az a bizonyos Kovács Béla). Bár a regisztrációs szervezet legfontosabb feladata a regisztráció, messze nem ez az egyetlen. A legtöbb esetben a felhasználói kulcspár, valamint a magánkulcs védelmét ellátó aktivizáló adat generálása is ott történik, szoftveresen a regisztrációs egységben vagy a felhasználó aláíró eszközében (melyet a regisztrációs szervezet is biztosíthat, vagy a felhasználó is beszétálhat sajátjával). Szoftveres generálás esetében a regisztrációs szervezet helyezi a kulcshordozóra a magánkulcsot, és gondoskodik a kulcshordozó és az aktivizáló adat felhasználóhoz való eljuttatásáról (az aktivizáló adatot az ügyfél is beállíthatja, amely esetben erre nincs szükség). A regisztrációs szervezet jó ügyfélszolgálathoz illően tájékoztatja a tanúsítványigénylőket, s nem veszi le a kezét a felhasználókról a tanúsítvány kibocsátása után sem. Ezt követően a tanúsítványokkal kapcsolatos műveletek fogadását (visszavonás, felfüggesztés, megújítás stb.) és azok hitelesítőszervezethez való továbbítását is ellátja. A regisztrációs szervezethez lehet fordulni egy már létező tanúsítvány adatainak megváltozása vagy egy archivált tanúsítvánnyal kapcsolatos információkérés esetén is, illetve minden ügyes-bajos dologgal őket kell felkeresni. Míg a felhasználók elsősorban a regisztrációs szervezetet boldogíthatják, az érintett felek esetében nem ilyen egyértelmű a helyzet, főleg azért nem, mert a tanúsítványból sokszor nem derül ki, hogy azt melyik regisztrációs szervezet melyik regisztrációs pontja regisztrálta. Az érintett felek ezért bármely regisztrációs szervezetet vagy a hitelesítésszolgáltatónak egy központi ügyfélszolgálatát zaklathatják abban az esetben, mikor önállóan nem boldogulnak.

Ha egy regisztrációs szervezet függetleníti magát a hitelesítésszolgáltatótól, és több hitelesítésszolgáltatóval lepaktálva, főállásban foglalkozik regisztrációval (és a többi említett feladattal), beszélhetünk regisztrációs szolgáltatóról. A regisztrációt végző szervezetnek azonban ilyen esetben is teljes mértékben be kell tarta-

nia a hitelesítésszolgáltató regisztrációra és egyéb eljárásokra vonatkozó szabályzatait. A regisztrációs szervezetért a hitelesítésszolgáltató felel, s a felhasználó jogi értelemben jobbára csak a hitelesítésszolgáltatóval áll kapcsolatban.

5.4.3 Tanúsítványtár

A tanúsítványtár feladata a tanúsítványok és visszavonási listák közzététele, ezek lekérdezhetőségének, a köztük való keresésnek a biztosítása az érintett felek számára. A tanúsítványtár ezenkívül felelős lehet a szolgáltató nyilvános szabályzatainak közzétételéért is. A tanúsítványtárt általában a hitelesítőszervezet működteti, de az lehet bármilyen másik szervezet tulajdonában és kezelésében is. A központi tanúsítványtár tartalmát gyakran replikálják másodlagos tanúsítványtárakba a lekérdezések gyorsítása végett, főleg olyan esetekben, mikor a szolgáltató nagy szervezeteket szolgál ki. Egy cégnek például, amely belső kommunikációjában használ szolgáltatói tanúsítványokat, érdemes lehet saját címtárába is replikálni a tanúsítványokat.

5.4.4 Valós idejű állapotinformációs egység

A valós idejű állapotinformációs egységet – a tanúsítványtárhoz hasonlóan – legtöbbször a hitelesítésszolgáltató működteti. Az egység feladata az azonnali érvényesség-ellenőrzési kérések kiszolgálása. Az egység lelke egy hardveres kriptográfiai modul, amely a szoftveres megoldásoknál nagyságrendekkel gyorsabban képes aláírások készítésére a saját magánkulcsával. Az egységnek ezenkívül szüksége van egy megbízható pontos időforrásra is, amely a válaszokba foglalandó időt biztosítja.

A valós idejű állapotinformációs egység egyes esetekben saját adatbázisban szokta nyilvántartani a tanúsítványok állapotára vonatkozó információkat, hogy a lekérdezésekkel ne terhelje az elsődleges tanúsítványtárat, illetve a hitelesítőegység saját adatbázisát.

5.4.5 Szabályzószervezet

Legvégére hagytam a szabályzószervezetet, melynek feladata a szolgáltató szabályzatainak elkészítése és folyamatos karbantartása, valamint a szabályzatok betartásának ellenőrzése. A szabályzószervezet ennek érdekében egy bizottságból áll, amelyben a szolgáltató vezetői, jogi, informatikai és biztonságtechnikai szakemberei kapnak helyet. Ha a szolgáltató ügyfelei között nagyobb szervezetek vannak, vagy ha a regisztrációban részt vevő partnerek erre igényt tartanak, akkor a bizottságban ők is helyet kaphatnak. Ez a bizottság a szolgáltató egyik legfőbb döntéshozó szerve, amely a gazdasági és üzleti-stratégiai kérdéseken kívül szinte mindenbe beleütheti az orrát, és mindenkinek a körmére koppinthat. A szabályzószervezet gondoskodik a nyilvános szabályzatok közzétételéről is,

amely – többek között – a tanúsítványtáron vagy a szolgáltató weboldalain keresztül történhet. A szabályzatok karbantartása a változási igények felismerését, megtételét és bevezetését foglalja magában, továbbá része a szabályzatok egyes verzióinak kezelése is. A szabályzószervezet gyakran saját ügyfélszolgálatot is működtet, amely a szabályzatokat érintő kérdésekkel kereshető meg.

5.5 Hitelesítésszolgáltatások

Ha az előbb elmondottakat kifordítjuk, és a szolgáltatások felől közelítjük meg, akkor azt mondhatjuk, hogy a hitelesítésszolgáltatás számos „alszolgáltatásból" tevődik össze. Ezek egy része a szolgáltatás jellegéből fakadóan kötelező (nem konkrét törvényi előírás, de értelemszerű törzseleme a technikának), mások a szolgáltatás megnyitásával válnak kötelezővé (itt sem feltétlen jogszabály által, hanem a felhasználók elvárásai miatt), míg a fennmaradók opcionálisak nyílt szolgáltatás esetén is.

Ebben a fejezetben a szolgáltatások felől megközelítve írom le ugyanazt, amit az előbb, illetve majdnem ugyanazt, mert jóval részletesebb leszek, bízva abban, hogy az esetleges ismétlések nem fognak ártani. Ezt a fejezetet mindazonáltal csak azoknak ajánlom, akiket a belső mechanizmusok részletei is érdekelnek (55. ábra).

E elrettentő hatású ábrán a hitelesítésszolgáltatásokat gyűjtöttem össze oly módon, hogy látszódjon azok egymáshoz, valamint a szolgáltatást igénybe vevőkhöz való viszonya. A különböző egységeknél bemutatom az általuk ellátott szolgáltatásokat (az elsődleges felelőshöz rendelve őket, bár más egységek is részt vehetnek benne).[6] Az egyes nyilak az információk áramlását jelzik az egységek egymás közötti és a felhasználókkal való viszonyában, az ellipszisekben a szolgáltatással valamilyen módon kapcsolatba kerülő ügyfelek találhatók.

5.5.1 Hitelesítésszolgáltatások felosztása

Alapszolgáltatások (azok a szolgáltatások, melyek zárt szolgáltatás esetén is kötelezőek):

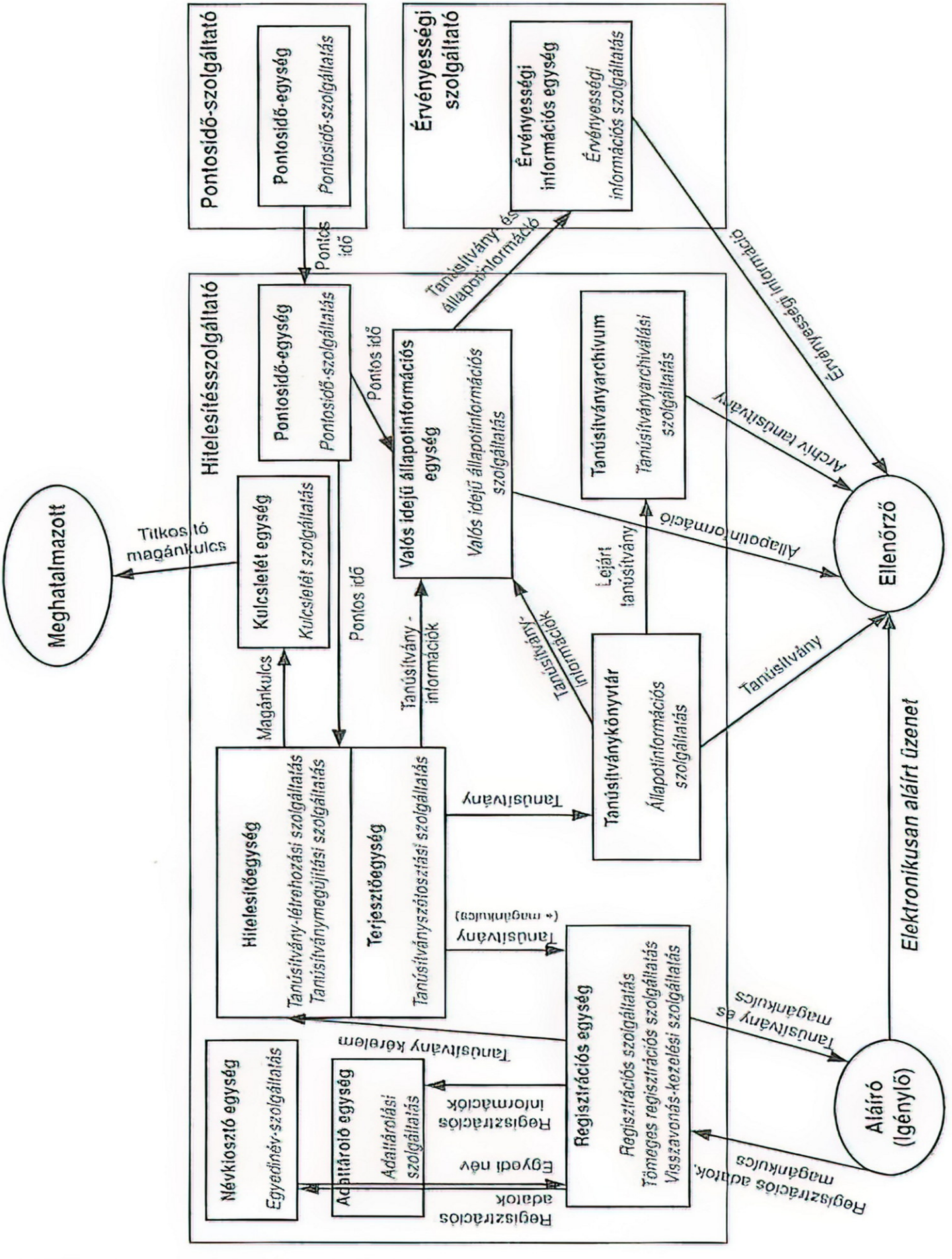
- tanúsítvány-létrehozási szolgáltatás,
- regisztrációs szolgáltatás,
- egyedinév-szolgáltatás,
- tanúsítványszétosztási szolgáltatás.

Jogszabály szerint minősített szolgáltatás esetén kötelező:

- visszavonás-kezelési szolgáltatás,
- tanúsítványarchiválási szolgáltatás.

Nyílt szolgáltatások (azok a szolgáltatások, melyek nyílt szolgáltatás esetén válnak kötelező erejűvé):

- állapotinformációs szolgáltatás,
- adattárolási szolgáltatás.



55. ábra Hitelesítésszolgáltatások és azok kapcsolatai

Opcionális szolgáltatások (azok a szolgáltatások, melyek nem kötelezőek nyílt szolgáltatás esetén sem):

- tanúsítványmegújítási szolgáltatás,
- kulcsletét szolgáltatás,
- tömeges regisztrációs szolgáltatás,
- valós idejű állapotinformációs szolgáltatás,
- érvényességi információs szolgáltatás,
- aláírás-létrehozó eszközzel kapcsolatos szolgáltatások.

5.5.2 Tanúsítvány-létrehozási szolgáltatás

A tanúsítvány-létrehozási szolgáltatás a hitelesítésszolgáltatás legbensőbb, leglényegibb része, melyet a hitelesítőegység végez teljesen automatizált módon. A tanúsítvány létrehozása a regisztrációs egységtől kapott felhasználóadatok és az aláírás-ellenőrző adat (nyilvános kulcs), valamint a hitelesítésszolgáltatóra vonatkozó és szabályzatok által előírt egyéb konstans adatok együttes aláírását jelenti. A szolgáltatásnak része lehet a kulcspárgenerálás is, ha azt valamilyen különös ok folyományaként nem a regisztrációs szolgáltatás látja el.

A szolgáltatást biztosító hardverek egy védett helyen lévő szerverszobában kapnak helyet, ahova szigorúan csak a berendezések kezelőszemélyzete léphet be. A hitelesítőegység az aláíró magánkulcsának védelméről még ezenfelül is gondoskodnak egy hardveres, babrálásbiztos kulcstároló egységgel. A folyamatos működés és rendelkezésre állás érdekében a szervereket duplikálni szokták, az elektromos betáplálást megkettőzik, tartós (dízelgenerátoros) szünetmentes tápegységeket telepítenek, katasztrófavédelmi és üzletfolytonossági eljárásokat dolgoznak ki.

5.5.3 Regisztrációs szolgáltatás

A regisztrációs szolgáltatás feladata, hogy tanúsítványigényléskor felvegye az igénylő személyes, szervezeti és egyéb adatait, ellenőrizze azokat a személyazonossággal együtt a szolgáltató szabályzatainak megfelelően. Ezen adatok egy része a tanúsítványba lesz foglalva, mások a tanúsítványtárban vagy más nyilvános adatbázisban jelenhetnek meg, míg megint másokat a szolgáltató saját belső nyilvántartásában őriz meg (lásd: adattárolási szolgáltatás). A nyilvános és magánkulcs generálása történhet e tevékenység részeként, vagy az aláírónak a saját maga által előállított nyilvános kulcsot kell átadnia a regisztrációs adatokkal együtt. A felvett és ellenőrzött adatokat ezek után a tanúsítvány-létrehozási szolgáltatás dolgozza fel. A regisztrációs szolgáltatásnak része lehet a legyártott tanúsítvány és magánkulcs, valamint az aktivizáló adat és a kulcshordozó visszajuttatása az igénylőhöz.

A regisztráció háromféleképpen történhet: személyes, távoli és tömeges módon. A személyes mód azt jelenti, hogy az igénylőnek személyesen kell befáradni egy regisztrációs kirendeltségbe s ott bemutatni személyazonosságát iga-

zoló és egyéb iratait. Nyilvános szolgáltatás esetében ez tipikusan egy elosztott szolgáltatás (hogy az ügyfeleknek ne kelljen messzire utazniuk), míg zárt közösség esetén egy magányos irodát is jelenthet. A távoli regisztráció esetében az ügyfeleknek nem kell személyesen megjelenniük a szolgáltató előtt, csak valamilyen kommunikációs módszerrel beküldeniük adataikat. Ez a módszer lehet posta, fax, e-mail stb., de bármi is az, biztosan nem garantálja a biztonságnak a személyes megjelenéssel járó szintjét. Az adatokat azonban ilyen esetben is a regisztrációs szervezetnek kell beküldeni, nem a hitelesítőszervezetnek.

A tanúsítvány igénylése történhet PKCS #10 és RFC 2511 formátumban vagy az elsősorban hardveregységek által alkalmazott SCEP (Simple Certificate Enrollment Protocol) protokollal. A PKCS #10 tanúsítványigénylés négy mezőből áll: verziószám, az igénylő azonosítója, nyilvános kulcsa és a tanúsítvány attribútumai. Az igénylés a regisztrációs egység által aláírásra kerül. Az RFC 2511 formátum lehetővé teszi toldalékok belefoglalását is az igénylésbe. A SCEP protokollt a Cisco és a Verisign közösen fejlesztette ki. Az igénylő (ez esetben egy hálózati eszköz) a protokollnak megfelelően HTTP kéréssel elkéri a hitelesítőegység tanúsítványát, majd a regisztrációs adatokat egy PKCS #7 üzenetbe csomagolva, hitelesített formában elküldi a szolgáltatónak. Ezek után addig pollozza (figyeli) a hitelesítőegységet, amíg választ nem kap a tanúsítványkérésre.

5.5.4 Egyedinév-szolgáltatás

Az egyedinév-szolgáltatás feladata, hogy a tanúsítvány igénylőjének regisztrációs adatai alapján, a szolgáltató által alkalmazott névkiosztási szabályoknak megfelelően, egyedi azonosítót adjon a tanúsítványnak. A kiosztott névnek meg kell felelnie a szolgáltató által meghatározott formátum követelményeinek, azaz általában az X.500 egyedinév-formátum előírásainak, illetve az e mellett esetleg kiegészítő azonosítóként használt egyéb névformátumoknak.

A szolgáltatást legtöbbször a regisztrációs szervezetek munkatársai látják el a tanúsítványtár adatai alapján. Előfordul az is, hogy a névkiosztás automatizált és központosított, a regisztrációs adatok alapján egy erre létrehozott névkiosztó egység látja el. Akár több hitelesítésszolgáltató is működtethet közösen egy ilyen névkiosztó egységet, ezzel biztosítva, hogy a kiosztott nevek az általuk lefedett közös névtartományban is egyediek legyenek.

5.5.5 Tömeges regisztrációs szolgáltatás

A tömeges (más néven automatikus) regisztrációs szolgáltatás a regisztrációs szolgáltatás egy speciális változata. Míg a hagyományos regisztrációs szolgáltatás esetében az ügyféladatok egyedi ellenőrzéséről és felvételéről van szó az ügyfél kérelme alapján, a tömeges regisztrációs szolgáltatás esetében a regisztrációs adatok egy autentikus adatbázisból származnak. Feldolgozásuk történhet teljesen önműködően, mert az adatok tényleg megbízhatóak, és így ellenőrzésükre nincs

szükség, vagy mert ellenőrzésük is történhet elektronikus úton, automatizálva. Ezt a szolgáltatást olyan szervezetek szokták igénybe venni, amelyek tagjaiknak, ügyfeleiknek igényelnek tanúsítványt, és rendelkeznek a regisztrációhoz szükséges, egyszer már ellenőrzött adatokkal – természetesen elektronikus formában. A tömeges regisztrációs szolgáltatás leggyakrabban egy erre szakosodott regisztrációs ponton működik, egyes esetekben a hitelesítőszervezet közvetlen kontrollja alatt.

5.5.6 Adattárolási szolgáltatás

Az adattárolási szolgáltatás a regisztráció során felvett nem nyilvános felhasználói adatok megőrzését jelenti. Az adattárolás történhet elektronikus formában vagy papíron, illetve a kettő kombinációjával (a felhasználók aláírt igénylését, szerződését, nyilatkozatát az adatok helyességéről a digitalizálás mellett is megőrzik eredeti papír formájában). Az adattárolási szolgáltatás tipikusan egy központosított adattároló egységben és irattárban kap helyet, amely gondoskodik az adatok biztonságos megőrzéséről. A szolgáltatás a regisztrációs egységtől kapja a tárolásra szánt információkat. A szolgáltatásnak része az adatok visszanyerése is, amely esetén a bizalmas információkhoz való hozzáférésre vonatkozó jogosultságok ellenőrzésére is sor kerül.

5.5.7 Tanúsítványszétosztási szolgáltatás

A tanúsítványszétosztási szolgáltatás feladata, hogy a tanúsítvány-létrehozási szolgáltatás által legyártott tanúsítványokat az igénylő és az ellenőrzők részére átadja, elérhetővé tegye. Amennyiben a tanúsítvány-létrehozási szolgáltatás magánkulcsokat is generál, akkor a tanúsítványszétosztási szolgáltatás annak igénylő részére történő átadásáról is gondoskodik. Az átadás az igénylők részére rendszerint a regisztrációs egységen, az ellenőrzők részére a tanúsítványtáron keresztül történik. A tanúsítványszétosztási szolgáltatás feladata ezen túl a tanúsítványi állapotinformációk eljuttatása a tanúsítványtáron és a valós idejű állapotinformációs egységen keresztül az ellenőrzők részére.

A tanúsítvány-ellenőrzőkhöz történő eljuttatása érdekében a terjesztőegység[7] a tanúsítványtárban elhelyezi a tanúsítványokat, ahonnan bárki (aki eléréssel és jogosultsággal rendelkezik a címtárhoz) letöltheti azokat. Az állapotinformációk terjesztése végett a tanúsítvány-visszavonási listát szintén a tanúsítványtárba helyezi. Az igénylő részére a tanúsítványt külön útvonalon is eljuttathatja: közvetlenül elektronikus levélben elküldve, vagy a magánkulccsal együtt kulcshordozóra írva hagyományos levélben, illetve futárral kézbesítve, vagy a regisztrációs egységnek visszaküldve, ahol az ügyintéző személyesen is át tudja adni azt. A magánkulcs központi előállítása esetén szükséges lehet a magánkulcsot védő aktivizáló adat eljuttatása is az igénylő részére a magánkulcs célba juttatásától eltérő útvonalon vagy időben.

5.5.8 Visszavonás-kezelési szolgáltatás

A visszavonás-kezelési szolgáltatás célja, hogy biztosítsa a lehetőséget a kiadott tanúsítványok érvényességének végleges megszüntetésére és opcionálisan ideiglenes felfüggesztésére. Ennek érdekében módot ad érvényes tanúsítványok visszavonására és felfüggesztésére, valamint felfüggesztett tanúsítványok újraérvényesítésére. Ezeket a tanúsítvány érvényességét befolyásoló műveleteket a regisztrációs szervezetnél kell kezdeményezni a szolgáltató szabályzatainak megfelelően személyes megjelenéssel, telefonon, faxon, e-mailben, weben vagy más módon. A regisztrációs szervezet munkatársai a szolgáltató szabályzatának megfelelően elvégzik a szükséges ellenőrzéseket, és a kérést a regisztrációs egységbe táplálva továbbítják a hitelesítőegység felé, mely a műveletet ténylegesen végrehajtja. Ennek eredményeként a hitelesítőegység a visszavonási listába felveszi a visszavont vagy felfüggesztett tanúsítványt, s a tanúsítványszétosztási szolgáltatás segítségével a tanúsítványtárban publikálja.

A szolgáltató a visszavonás kezelését központosíthatja egy erre a célra létrehozott speciális regisztrációs irodánál (ügyfélszolgálatnál) is, de delegálhatja mindegyik regisztrációs ponthoz is, akár az ügyfél visszavonási lehetőségének egyetlen regisztrációs pontra való korlátozásával is (arra, ahol a tanúsítvány igénylése történt).

5.5.9 Tanúsítványarchiválási szolgáltatás

A tanúsítványok lejáratkor (vagy azt követően) kikerülhetnek a nyilvános tanúsítványtárból. Ennek oka a tanúsítványtár méretének csökkentése és a lekérdezések gyorsítása. Erre lehetőséget ad az, hogy az elektronikus aláírások legtöbbjét azok elkészítése után nem sokkal ellenőrizni szokták, és a későbbi ellenőrzés biztosítható saját tanúsítványpéldány vagy a tanúsítvány aláírótól történő beszerzésével. Vannak azonban olyan esetek, amikor az aláírás ellenőrzésére jóval az aláírás megtétele után kerül sor, s ehhez a tanúsítvány már nem elérhető sem saját nyilvántartásban, sem az aláírónál. Ilyen esetekben segít a tanúsítványarchívum, amelyből a rég lejárt tanúsítvány is beszerezhető, ha nem is olyan automatikusan, mint a tanúsítványtárból. A tanúsítványarchiválási szolgáltatás ugyanis a tanúsítványokat a tanúsítványtárból való kikerülésével egyidejűleg kisgömböcként felfalja, és még hosszú évekig csücsül rajtuk.

5.5.10 Állapotinformációs szolgáltatás

Az állapotinformációs szolgáltatás keretében a szolgáltató a korábban kiadott és a tanúsítványszétosztási szolgáltatás keretében nyilvánosságra hozott tanúsítványok állapotában bekövetkezett változásokról tájékoztatja az ellenőrzőket és az aláírókat. A tanúsítvány állapota érvényes, visszavont és felfüggesztett lehet. Az első esetben a szolgáltatásnak nincs tennivalója, a másik két esetben a

visszavonási listába foglalva közölnie kell a tanúsítvány sorszámát és állapotát. A tanúsítvány-visszavonási listát rendszeres időközönként frissítenie kell a szolgáltatónak. Az állapotinformációs szolgáltatásra zárt szolgáltatás esetén nem feltétlen van szükség, különösen azokban az esetekben nem, mikor az érintett felek más módszerekkel (például egy belső adatbázis segítségével) is meggyőződhetnek a tanúsítvány érvényességéről.

5.5.11 Valós idejű állapotinformációs szolgáltatás

A valós idejű állapotinformációs szolgáltatás az állapotinformációs szolgáltatás egy speciális formája, amit nagy értékű és gyors elbírálású tranzakciós rendszerek esetében alkalmaznak. Míg a hagyományos állapotinformációs szolgáltatás megadott időközönként (például egy nap) bocsát ki visszavonási listákat, a valós idejű állapotinformációs szolgáltatás a tanúsítvány aktuális állapotáról ad információt. Jelentős különbség a két szolgáltatás között, hogy míg az állapotinformációs szolgáltatás egy nyilvántartás ellenőrző általi letöltését jelenti, addig a valós idejű állapotinformációs szolgáltatás esetében egy kérdés-felelet mechanizmusról van szó. A valós idejű állapotinformációs egység közvetlen a terjesztő egységtől vagy a tanúsítványtárból szerzi be a tanúsítvány állapotára vonatkozó információkat.

5.5.12 Tanúsítványmegújítási szolgáltatás

A szolgáltató a minimálisan szükséges tanúsítványkezelő szolgáltatásokon (előállítás, visszavonás stb.) túl nyújthat egyéb tanúsítványmenedzsment-szolgáltatásokat is. Ilyen például a tanúsítványmegújítási szolgáltatás, amely a tanúsítvány lejárat előtti újbóli legyártását jelenti az előző (megújított) tanúsítványban szereplő adatokkal, de új érvényességi idővel. A tanúsítvány megújítása csak akkor lehetséges, ha a tanúsítványban szereplő adatok még érvényesek. Ebben az esetben mód van a tanúsítvány kulcscsere nélküli és a kulcs cseréjével történő megújítására egyaránt. A tanúsítványmegújítási szolgáltatással kapcsolatos műveletekhez érvényes tanúsítvánnyal kell az ügyfélnek rendelkeznie, így nem szükséges személyesen megjelennie a hitelesítésszolgáltató előtt. Ilyen műveleteket a szolgáltató végezhet automatikusan a tanúsítványtulajdonos megkérdezése nélkül, vagy a regisztrációs szervezethez benyújtott kérelem alapján. Automatikus megújítás esetén a regisztrációs szervezet a meg nem újításra vonatkozóan kell elfogadjon kéréseket.

5.5.13 Kulcsletét szolgáltatás

A kulcsletét szolgáltatás feladata a felhasználó titkosító vagy kulcsegyeztetésre szolgáló magánkulcsának biztonságos őrzése (nyilvános kulcsokat és aláíró magánkulcsot a szolgáltatás nem tárol). A szolgáltatás célja az, hogy ha a felhasználónál tárolt titkosító magánkulcs megsemmisülne, elveszne vagy elérhetetlenné válna, akkor az általa tárolt példánnyal lehetővé tegye az ügyfél titko-

sított dokumentumainak visszafejtését. A letétbe helyezett kulcshoz a felhasználó és más arra jogosultak férhetnek hozzá a szolgáltató előírásainak megfelelően. Ilyen jogosult lehet például a felhasználó munkáltatója (ha a kulcsot a felhasználó alkalmazotti minőségében használta) vagy bíróság is, peres eljárás esetén. A letétbe helyezés teljesen automatikus, a visszanyerés során viszont szükség lehet emberi közreműködésre a kérelem jogosultságának elbírálásához, az ezzel kapcsolatos adminisztrációhoz és a kulcs felhasználóhoz juttatásához.

5.5.14 Aláírás-létrehozó eszközzel kapcsolatos szolgáltatások

Az „aláírás-létrehozó eszköz ellátó" szolgáltatás olyan szolgáltatás, mely a felhasználók számára beszerzi, előkészíti, fizikailag megszemélyesíti (nyomtatással, dombornyomással, hologrammal látja el) és eljuttatja az aláírás-létrehozó eszközt. Az eszköz logikai megszemélyesítése (magánkulcs telepítése) hivatalosan az „aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése" nevet viseli.

5.5.15 Elérhetőség, rendelkezésre állás

Az egyes szolgáltatásoknak nem ugyanolyan mértékben kell elérhetőnek lennie és rendelkezésre állnia a felhasználók, az érintett felek és egymás számára. A tanúsítvány kiadásával kapcsolatos szolgáltatások (így a tanúsítvány-létrehozási szolgáltatás, a regisztrációs szolgáltatás, a tanúsítványszétosztási szolgáltatás, a tanúsítványmegújítási szolgáltatás, a kulcsletét szolgáltatás és az aláírás-létrehozó eszközzel kapcsolatos szolgáltatások) a legtöbbször elegendő, ha munkanapokon és munkaidőben elérhetők. A tanúsítványok érvényességének kezelésével kapcsolatos szolgáltatásoknak (visszavonás-kezelési szolgáltatás, állapotinformációs szolgáltatás és valós idejű állapotinformációs szolgáltatás) viszont az év összes napján, a nap mind a huszonnégy órájában folyamatosan elérhető módon kell üzemelnie a lehető legnagyobb rendelkezésre állással, a szolgáltatásokat működtető berendezések karbantartáshoz szükséges idők minimálisra szorításával. Az adattárolási szolgáltatásnak és a tanúsítványarchiválási szolgáltatásnak folyamatosan működnie kell, de az elérhetőségük és rendelkezésre állásuk erősen korlátozott lehet (ez azt jelenti, hogy a tanúsítványokat folyamatosan tárolni, menteni, archiválni kell, de a lekérdezésük elegendő, ha csak egy-két rendszer-adminisztrátor számára elérhető, speciális esetekben, nem feltétlen azonnali válaszadással).

5.6 Egyéb bizalmi szolgáltatások

Eddig egyetlen bizalmi szolgáltatásról, a (tanúsítvány) hitelesítésszolgáltatásról beszéltünk. Ezenkívül léteznek más bizalmi szolgáltatások is, amelyek valamilyen módon mind a nyilvános kulcsú kriptográfiát használják fel. Vannak közöt-

tük egyszerűbbek, amelyek csak a biztonság valamely szegmensét célozzák meg, de léteznek összetettebbek is, melyek komplex rendszert alkotva igyekeznek megoldást adni és körülbástyázni egyébként nem biztonságos eljárásokat.

5.6.1 Érvényességi információs szolgáltatás

Az érvényességi információs szolgáltatás az állapotinformációs szolgáltatásoknál jóval több információt ad a tanúsítvány érvényességéről. Míg az állapotinformációs szolgáltatások kizárólag a tanúsítvány státusát ellenőrzik (érvényes, visszavont, felfüggesztett), addig az érvényességi információs szolgáltatás számos más érvényességi tulajdonságot is megvizsgál. Így például megvizsgálhatja a tanúsítvány érvényességi idejét, a teljes tanúsítási lánc érvényességi idejét, a hitelesítési és aláírási szabályzat előírásainak történő megfelelést és egyebeket. Az érvényességi információs szolgáltatás helyet kaphat a hitelesítésszolgáltató repertoárjában is, de önálló szolgáltatásként is megjelenhet. A szolgáltatás koncepciója a tanúsítvány ellenőrzésével járó feladatok terhének és felelősségének levétele az ellenőrző gyönge válláról. Érvényességi szolgáltató jelenléte esetén elsősorban nem a hitelesítésszolgáltatóban, hanem az érvényességi szolgáltatóban kell megbízniа az ellenőrzőnek.

5.6.2 Időbélyegzés szolgáltatás

Az időbélyegzés szolgáltatás (más néven időpecsételés vagy digitális közjegyzői szolgáltatás) alatt olyan szolgáltatást értünk, mely bizonyos adatok adott időben való létezését igazolják, az adat- és pontosidő-információk szolgáltató által történő aláírásával. Ez szükséges lehet egy feltaláló számára a találmányhoz fűződő elsőségének igazolására, irodalmi és zenei művek, szoftverek stb. szerzői jogainak érvényesítésére, és nagyon hasznos lehet mindenfajta üzleti tranzakció során, különösen, mondjuk, értékpapírok adásvételekor, ahol a megbízás megtételi és teljesítési idejének igazolására szolgálhat.

Az időbélyegzés-szolgáltató és ügyfele kapcsolatában az ügyfélnek minden egyes aláírandó adathalmaz lenyomatát el kell küldenie a szolgáltatónak, amely az általa lekérdezett pontos idő adathoz csatolása után az információt aláírja, és az így előállt időbélyegzőt visszaküldi az ügyfélnek. A szolgáltató a pontos időt úgynevezett pontosidő-szolgáltatóktól[8] szerzi be műholdon, interneten vagy rádiókapcsolaton keresztül, de saját, rendkívüli pontosságú időforrással is rendelkezik. Mivel az ügyfél csak az adat lenyomatát küldi el, nem kell tartania az esetlegesen érzékeny vagy bizalmas információ felfedésétől, illetéktelen tudomására jutásától. Utólag azonban, ha szükséges, az időbélyegzőben szereplő aláírt lenyomat és az eredeti dokumentumból képzett lenyomat egymás mellé állításával képes igazolni azt, hogy a dokumentum már akkor is létezett, mikor a szolgáltató aláírta annak lenyomatát. Ez voltaképpen majdnem olyan, mint egy „időben visszafelé néző gép", amivel utólag megbizonyosodhatunk múltban történt eseményekről, amennyiben anno megfelelő felvételeket készítettünk.

Az időbélyegzés szolgáltatás egy időbélyegző egységen alapul, ami teljesen automatizáltan látja el az időbélyegzés feladatát. A szolgáltatás lehet zártkörű vagy teljesen nyílt (az interneten keresztül több ilyen elérhető), működhet egy hitelesítésszolgáltató kebelén belül vagy attól teljesen függetlenül is. A szolgáltatás megbízhatóságát a viszonylag evidenciának tekinthető kriptográfiai biztonságon túl elsősorban a szolgáltató hitelessége és semlegessége adja. Ez különösen azért igaz, mert a szolgáltató elvileg képes lehet utólag előállítani időbélyegzőket bárminek egy adott időpontban való létezésének az igazolására. Bár ennek esélyét szubmikroszkopikusra lehet csökkenteni a szolgáltató informatikai rendszerének körültekintő felépítésével és független fél által történő átvizsgálásával, ismeretlen nevű, hálózaton keresztül elérhető, ingyenes szolgáltatásoktól én óvakodnék.

Sokat segít az esetleges visszaélések megakadályozásában, ha a szolgáltató minden egyes időbélyegzőknek egyedi sorszámot is ad, és azokat maga is naplózza. Még többet az, ha az egyes időbélyegzők (napló adatai) egy láncot alkotva mindig függnek az előzőleg kiadott bélyegtől.[9] Így elkerülhető az, hogy a szolgáltató egy utólag előállított időbélyegzőt beszúrjon a naplóállományba is. Az időbélyegzés-szolgáltató időbélyegző előállítására használt magánkulcsának biztonsága hasonló módon kulcskérdés, mint a hitelesítésszolgáltató esetében. Annak nyilvánosságra kerülése azonban a már említett láncmódszer és a szolgáltató naplózása esetén önmagában nem feltétlenül kérdőjelezi meg a korábban kiadott időbélyegzők hitelességét (de sokak megtévesztésére alkalmas).

Bár az időbélyegzés szolgáltatás elérése (a bélyegző igénylése, annak fogadása és dokumentumhoz csatolása) posonegyszerű s létező szabványok szabályozzák, mégis igen kevés alkalmazásnak része. Ezért a szolgáltatók egyelőre saját kliensprogramot szoktak biztosítani szolgáltatásuk eléréséhez.

5.6.3 Tranzakcióhitelesítő szolgáltatás

A tanúsítványhitelesítés szolgáltatás esetében a szolgáltató az egyes kommunikációs tranzakciók szintjén nem érintett (kivéve az állapotinformációk nyújtását), és az időbélyegzés szolgáltatás esetében sem vesz részt közvetlenül az ügyfelek közti kommunikációban. A tranzakcióhitelesítő szolgáltatás esetében viszont a szolgáltató egyfajta közvetítő szerepet tölt be az ügyfelek közötti adatcserében. Az ügyfél a hitelesnek szánt információt (vagy annak lenyomatát) nem közvetlenül a partnerének küldi, hanem a szolgáltatónak, amely a szükséges ellenőrzések után saját aláírásával ellátva juttatja el azt a címzettnek. Ez alkalmat kínál számára az egyes tranzakciókkal kapcsolatos mentésekre is, időbélyegzés használatára és egyéb kiegészítő biztonsági eljárásokra. A szolgáltatás lehetővé teheti azt is, hogy a feladó visszajelzést kapjon arról, hogy a címzett megkapta és elolvasta a dokumentumát, mindezt a címzett által letagadhatatlan módon.

A szolgáltatás esetében a felek bizalmi szempontból nem egymással, hanem a szolgáltatóval állnak kapcsolatban. A módszer óriási előnye, hogy a feladó elektronikus aláírásának ellenőrzésére a címzettnek nincs szüksége, ő mindig

csak a szolgáltató aláírásával találkozik. Így nemcsak a nyilvános tanúsítványtár spórolható meg, de a címzett elfogadási eljárása is végtelenül leegyszerűsödik, hiszen a szolgáltató aláírása esetében mindössze algoritmikus ellenőrzésére van szükség, a mögötte álló tanúsítvány érvényességében biztos lehet.

Bár így leírva gyönyörűen hangzik, s Magyarországon is történt kísérlet ilyen szolgáltatás beindítására, az sem hazánkban nem sikerült, sem a világban máshol nem honosodott meg igazán. A felhasználók kényelmének itt túl nagy ára van: mivel a szolgáltató minden tranzakcióba beleüti az orrát, az egy bizonyos felhasználószám és intenzív használat felett nehezen teljesíthető számítási és tárolási kapacitásokat igényel a szolgáltató rendszerétől. A szolgáltatás ettől függetlenül is igen összetett és bonyolult, így csak zárt, elsősorban katonai és nemzetbiztonsági területen van példa a használatára.

5.7 Szolgáltatók megbízhatósága

A szolgáltatás biztonsága és a szolgáltató megbízhatósága számos szempontból értelmezhető. Így kriptográfiai, informatikai, fizikai, adminisztratív, szabályzati, személyi, jogi, üzleti aspektusokból, és még talán ezeken kívül is vannak tényezők, melyek együttesen adnak egy „mutatót". Hiába erős a szolgáltató kiemelkedő mértékben akár több területen is, ha másokat elhanyagol. A szolgáltatás mindig csak annyira lesz biztonságos, amennyire a legkevésbé erős szegmense az. A rendszernek körkörös védelemre kell berendezkednie, és egyenszilárdságúnak kell lennie. Marketingértéke lehet, de gyakorlati értelme nem sok van, ha a szolgáltató például 4096 bites saját kulcsokat használ, ezer méterrel a föld felszíne alá telepíti le a rendszerét, de munkatársainak nem eléggé megbízható és képzett személyeket választ. Ez még akkor is így van, ha az alkalmazott hardver- és szoftverrendszerek „tökéletesen" védettek, és a belső visszaéléseket műszakilag kizárják. A biztonság ugyanis nagyon sokrétű: nemcsak a szolgáltató magánkulcsához való hozzáférést, és így hamis tanúsítványok és visszavonási listák fabrikálásának a lehetőségét kell kizárni. Arra is ügyelni kell, hogy a regisztráció során ne lehessen becsapni az ügyintézőt hamis személyi okmányokkal, álbajusszal, Fantomas álarccal, ne adj' isten ne lehessen lefizetni, megzsarolni egy, a kívánságoknak megfelelő tanúsítványért cserébe. Ezek mellett a legnyilvánvalóbb haszonszerzésre törekvő visszaélések mellett a szolgáltatónak egyaránt fel kell készülnie a külvilág felől jövő és a belső támadásokra, a hétköznapi barbarizmusra, sőt a gazdaságban betöltött szerepének a növekedésével az államhatalom túlzott kíváncsiságára és az azzal ellenséges erők romboló szándékú attakjaira. Ezek nem feltétlen aláírások hamisítására, gazdasági visszaélések megalapozására irányulnak, hanem csak őszintén és egyszerűen a pusztításra. Így például a nyilvános tanúsítványtár támadásával megakadályozható a tanúsítványok érvényességének lekérdezése, a regisztrációs egységek ostromával pedig az esetleges kompromittálódások bejelentése. Mindkét

esetben a szolgáltatás biztonsága sérül, s a szolgáltató hírnevén eshet folt, ha nem tett meg minden tőle telhetőt annak kivédésre.

Az alábbiakban bemutatok pár példát arra, hogy minek kell megfelelnie egy hitelesítésszolgáltatónak,[10] továbbá megmutatok ezzel kapcsolatos veszélyeket, követelményeket és megoldásokat is, vegyesen. Ez nemcsak empatikus készségfejlesztés a szolgáltató nehéz életét illetően és illusztrációja annak, mi mindent kell megfizetni a szolgáltatás árában, de hasznos információk arra nézve is, hogy mi mindenre kell odafigyelni szolgáltatóválasztás esetén. Azoknak, akik szeretik a kémregényeket, még érdekes is lehet mindez, ha olyasfélképpen olvassák, hogy mi mindent kell leküzdeni, mondjuk, James Bondnak, mikor meg akarja szerezni az ellenséges szolgáltató magánkulcsát.

5.7.1 Üzleti-jogi biztonság

A hitelesítésszolgáltatónak üzleti és jogi értelemben számos feltételnek meg kell felelnie. Ezek némelyike teljesen nyilvánvaló: a szolgáltató cég legyen bejegyezve mint gazdasági társaság; tulajdonosi háttere legyen megbízható; megfelelő alaptőkéje és vagyona legyen; meglegyenek a szükséges hatósági engedélyei; rendelkezzen irodákkal a szolgáltatás, az adminisztráció és az ügyfélszolgálat számára és így tovább. Mások nem ennyire magától értetődők: a szolgáltatónak visszavonhatatlan bankgaranciával és teljes körű felelősségbiztosítással kell rendelkeznie; szerződéses rendszerének rögzítenie kell a szereplők kötelezettségeit és felelősségeit; partnereit, beszállítóit, alvállalkozóit (különös tekintettel azokra, akik tevékenyen részt vesznek a szolgáltatás nyújtásában) úgy kell megválogatnia, hogy azok képességei, lehetőségei arányban legyenek a szolgáltatás által megkívántakkal, s az elvárásoknak való megfelelést folyamatosan monitoroznia kell.

Vizsgálatot érdemel, hogy egyéb tevékenységeivel mennyire összeegyeztethető a hitelesítésszolgáltatói tevékenység, például egy adósságbehajtással, üzleti információszerzéssel vagy rendezvényszervezéssel foglalkozó cég mennyire vehető komolyan mint hiteles hitelesítésszolgáltató.

Megjutalmazva azokat, akik eddig eljutottak, itt adnék egy témába vágó tippet a szolgáltatóválasztásra: A szolgáltató alaptőkéjének és vagyonának nagysága önmagában „legfeljebb" arra adhat mutatót, hogy a szolgáltatás fennmaradása és fejlesztése mennyire biztosított, arra semmiképp, hogy baj esetén a szolgáltató milyen anyagi felelősségvállalást és kártérítést vállal. Azt mindegyik szolgáltató korlátozza, általában a felelősségbiztosítás összegének megfelelően. A gyakorlatban előfordul az is, hogy kisebb tőkeerejű cég nagyobb garanciákat párosít tevékenysége mellé, mint tőkeerős társa. Ezért melegen ajánlott a szolgáltató szerződéses feltételeiben a felelősségvállalás mértékének tüzetesen utánanézni.

5.7.2 Személyi biztonság

A személyi biztonság követelményeinek megfelelve a szolgáltatónak megfelelő számú és tudású alkalmazottat kell foglalkoztatnia. A szolgáltatónak pontosan és részletesen kidolgozott, folyamatosan karbantartott személyzeti politikával és munkaköri leírásokkal kell rendelkeznie. A személyzeti politikának megfelelően dokumentálnia kell a munkatársak kiválasztási és megfelelőség-ellenőrzési rendszerét, az állandó és ideiglenes szerepköröket és felelősségeket, valamint a felmérhető kockázati besorolásokat. A munkaköri leírásoknak tartalmazniuk kell a szükséges szakismereti és tapasztalati követelményeket, a munkakörrel és a munkatárs feladataival összefüggő tevékenységek leírását, a felelősségek körét és mértékét, a kapcsolódó munkakörök megnevezését.

A bizalmi munkakört (biztonsági tisztviselő, rendszer-adminisztrátor, rendszer-üzemeltető, rendszervizsgáló[11]) betöltő személynek munkaviszonyban kell állnia a szolgáltatóval, és a munkakörük betöltéséhez szükséges szakértelmet szakmai gyakorlattal, végzettséggel vagy szakképesítéssel igazolniuk kell. Az informatikai rendszerért általánosan felelős munkakört csak olyan személy tölthet be, aki szakirányú végzettséggel és az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik. Egy személy többféle bizalmi munkakört nem tölthet be, s mindenkinek személyes felelősséggel kell rendelkeznie. A szolgáltató munkatársainak és vezetőinek büntetlen előéletűnek kell lennie, és függetlennek az összes olyan érdektől, ami hátrányosan érintheti a szolgáltató semlegességét. A munkatársak nem kerülhetnek bizalmi funkciókba mindaddig, amíg a személyükkel kapcsolatos ellenőrzések és a szükséges nyilatkozatok megtétele meg nem történt.

A személyzeti előírások egy részét a beszállítók, az alvállalkozók és a partnerek munkatársaira is ki kell terjeszteni, különösen ha azok hozzáféréssel rendelkeznek a szolgáltató erőforrásaihoz, informatikai és adminisztratív rendszeréhez, vagy belépési jogosultsággal rendelkeznek a cég kiemelt biztonságú övezeteibe. A regisztráció területén dolgozó munkatársaknak ismerniük kell a forgalomban lévő hatósági dokumentumokat, azok fajtáit, ismertetőjegyeit, hamisítási módszereit, képeseknek kell lenniük az átadott iratok valódiságának, érvényességének megállapítására.

5.7.3 Fizikai biztonság

A fizikai biztonság elsősorban a szolgáltató erőforrásaihoz való jogosulatlan fizikai hozzáférést hivatott megakadályozni. A hitelesítésszolgáltatónak gondoskodni kell a rendszereihez és eszközeihez való fizikai hozzáférés felügyeletéről és a fizikai-környezeti biztonsági kockázatok megfelelő minimalizálásáról. A tanúsítvány előállításával (beleértve a regisztrációt is), az aláíró eszköz biztosításával és a visszavonás-kezelési szolgáltatásokkal foglalkozó munkahelyekhez való fizikai hozzáférést csak az arra feljogosított személyek számára szabad

megengedni. A szentélyt, vagyis azokat a helyiségeket, melyek a szolgáltató központi rendszereinek, archív nyilvántartásának ad helyet, a jogosulatlan hozzáféréstől fizikailag is védeni kell, az illetéktelen személyek bejutását kizárva, a belépésre jogosultak tartózkodását és mozgását naplózva. Ez gyakorlatilag egy zsilipkapuval védett, eszköz alapú vagy biometrikus azonosítással ellátott rendszert jelent. Ezekbe a helyiségekbe az idegen személyek belépését (például újságírók, VIP-ügyfelek) minimalizálni kell, s semmi esetre sem szabad megosztani idegen szervezetekkel (bérlőtárs az Aladdin lámpása Bt., s a Harcikutya-tartók Dél-alföldi Szövetségének a szervere is ott kap helyet).

Ahogy a fegyverraktárakban szokás, rendszeres ellenőrzésekkel, leltározással itt is biztosítani kell a személyi azonosítóeszközök, archív adathordozók, regisztrációs nyilvántartások, egyéb eszközök és információk meglétét, hogy azok esetleges elvesztését, sérülését, kompromittálódását a lehető leghamarabb felfedezzék.

A fizikai biztonság témakörébe tartozik a természeti katasztrófa (tűz, víz, földrengés stb.), a lopás, betörés, lehallgatás és erőszakos károkozás elleni védelem s a működéshez szükséges feltételek (például áramellátás, telekommunikáció, légkondicionálás) biztosítása is. Az előbbiek ellen a szolgáltató leghatékonyabban a rendszere földrajzilag távol lévő helyszíneken történő duplikálásával védekezhet, az utóbbiak tekintetében szintén a duplázás segít: két különböző szolgáltatótól csorgó áram és redundáns hálózati kapcsolat. A kritikus adathordozókat (biztonsági és archív mentések, magánkulcs titokszeletjei stb.) tűzbiztos szekrényben, több helyszínen párhuzamosan kell tárolni.

A szolgáltatónak üzletfolytonossági és katasztrófaelhárítási tervvel is rendelkeznie kell, melyek útmutatót adnak katasztrófa jellegű esetek kezelésére, a fellépő károk minimalizálására, a szolgáltatás biztonságának megőrzésére és minél előbbi újraindítására.

5.7.4 Informatikai biztonság

Az informatikai biztonság célja a szolgáltató erőforrásaihoz való jogosulatlan logikai hozzáférés megakadályozása, a folyamatos működés (rendelkezésre állás), hitelesség, adatbiztonság, megbízhatóság, nyomon követhetőség, ellenőrizhetőség és számonkérhetőség kritériumainak biztosítása, a rendszerek és információk sértetlenségének védelme. Jogosulatlan logikai hozzáférés alatt egyaránt értünk hálózati betöréseket, belső támadásokat, vírusok, egyéb rosszindulatú és engedély nélküli szoftverek indítását. Ennek érdekében az informatikai rendszer minden kezelőjének személy szerint azonosítottnak kell lennie (természetesen biztonságos PKI-módszerekkel). A hozzáférési jogosultságok megadását, módosítását és visszavonását legalább két, bizalmi munkakört betöltő személy együttesen végezheti csak.

Itt említem meg a szolgáltatói magánkulcs biztonságának követelményét is[12]. A magánkulcs létrehozását, mentését és helyreállítását előre szabályozott szeánszok keretében, fizikailag védett környezetben, legalább két bizalmi sze-

mély együttes részvételével, más személyek jelenlétét kizárva kell végezni. A magánkulcsot olyan babrálásbiztos hardvermodulban kell tárolni, amely illetéktelen erőszakos hozzáférés esetén a kulcs fizikai megsemmisítésére is kész. A magánkulcsot menteni csak több darabban lehet, oly módon, hogy annak helyreállításához több bizalmi személy együttes jelenléte legyen szükséges.[13]

A hitelesítésszolgáltatónak gondoskodnia kell arról is, hogy a tanúsítványok kibocsátásának, felfüggesztésének és visszavonásának időpontja pontosan meghatározható legyen. Ebből a célból az alkalmazott rendszerek idejét – az időbélyegzés szolgáltatáshoz hasonlóan – hiteles időforráshoz kell szinkronizálni oly módon, hogy az elfogadott referenciaidőtől egy másodpercnél nagyobb mértékben ne térjen el. Időbélyegzés-szolgáltatók esetében az eltérés legfeljebb 0,1 másodperc lehet.

A szolgáltatónak minden, a szolgáltatás nyújtásával és az informatikai rendszerével kapcsolatos eseményt naplóznia kell, annak időpontjával és végrehajtójával együtt oly módon, hogy abból minden fontosabb eseményt rekonstruálni lehessen. A napló bejegyzéseit védeni kell a módosításoktól, és biztosítani kell, hogy a napló tartalmához csak az arra jogosultak férhessenek hozzá. A naplót úgy kell kezelni, hogy annak megsemmisítése, a bejegyzések sorrendjének megváltoztatása vagy törlése észrevétlenül ne legyen lehetséges.[14]

Az érzékeny adatokat tartalmazó adathordozó eszközöket s a szolgáltatói magánkulcsot, amennyiben azokra nincs többet szükség, olyan biztonságos módon kell megsemmisíteni, hogy azok további használata lehetetlenné váljon.

5.7.5 Adminisztratív, szervezeti, szabályzati biztonság

Az adminisztratív biztonság alatt azt értjük, hogy a szolgáltató eljárásainak megfelelően dokumentáltnak, s az adminisztráció gyakorlatának a dokumentált eljárásokkal koherensnek kell lennie. Ennek érdekében a szolgáltatónak ISO 9000 minőségbiztosítási rendszert kell bevezetnie, és azt külső, akkreditált tanúsítócéggel auditáltatnia kell. A szervezeti biztonság követelményeinek megfelelően a szolgáltató felépítésének, működési módjának, döntési mechanizmusainak, felelősségi köreinek világosan dokumentáltnak és egyértelműnek kell lenni.

A szabályzati biztonság keretében a szolgáltatónak szabályoznia kell összes tevékenységét, ami a tanúsítványok menedzsmentjével és a szolgáltatás biztonságával kapcsolatos. Ezeknek egy részét – mely a szolgáltatás színvonalának és biztonságának megítéléséhez szükséges – nyilvánosságra kell hoznia addig a mértékig, amíg ezen információk felfedése nem fenyegeti a biztonságot (bővebb információ a 8. fejezetben).

5.7.6 Audit és minősítés

Mivel a szolgáltatónak nyilvánosságra kell hoznia azokat az eljárásait, amelyekkel az előbbiekben említett biztonsági kérdéseket kezeli, a felhasználónak

megvan a lehetősége arra, hogy azokat áttanulmányozva eldöntse, a szolgáltatás mennyiben felel meg az ő biztonsági elvárásainak. Ha a felhasználó egy nagy cég, mely rendelkezik szakértő munkatárssal, akkor ezt ideális esetben el is tudja végezni. Ha viszont a felhasználó egy laikus, akinek kisebb gondja is nagyobb annál, mintsem hogy ezt a sok süketlenséget megértse, akkor hiábavaló ez a nagy exhibicionizmus. Majdnem hiába, ugyanis erre is van megoldás. A felhasználók joggal bízhatnak abban, hogy akad segítségük a szolgáltató- és szolgáltatásválasztás (ugyanazon szolgáltatónak eltérő színvonalú szolgáltatásai) emberpróbáló feladatában. Ott vannak egyrészt a független szakértők és újságírók vagy a kevésbé függetlenek, akiket a versenytárs alkalmaz, hogy kiszúrják a konkurencia gyenge pontjait. Az ő lehetőségeik azonban korlátozottak, hiszen csak a szolgáltató nyilvános dokumentumaihoz férnek hozzá. Ebben segít a kötelező és önkéntes minősítések és auditok rendszere. A minősítés alatt elsősorban hatósági minősítést értünk, a minősített szolgáltatónak való megfelelőség ellenőrzését. Ennek során a szolgáltató felügyeleti szerve mindazt és még sokkal többet is ellenőriz, mint amit én fentebb példaértékkel kiragadtam. A szolgáltató emellett is minősítheti magát más minőségi rendszereknek megfelelően. Erre szolgál az audit, ami a minősítéshez hasonló tevékenység, de nem hatóság vagy szabványügyi testület végzi, hanem egy független auditorcég. Az audit szintén valamilyen követelményrendszernek való megfelelésre vonatkozik, s kiterjedhet a hagyományos pénzügyi vizsgálat mellett a biztonság valamennyi szegmensére. Ekkor e független cég pecsétje igazolja azt, hogy a szolgáltató és annak szolgáltatása megfelel egy bizonyos, vélhetően széles körben elismert kritériumrendszer feltételeinek.[15] A minősítések és auditok eredményeként a szolgáltató meghatározott ideig minősített lesz, amelynek lejártáig a vizsgálatokat meg kell ismételtetnie.

A felhasználónak így a biztonság megítélése végett elegendő ezt a hatósági vagy független cég általi pecsétet keresnie s azt megvizsgálnia, hogy a vizsgálat milyen rendszernek megfelelően és ki által készült, s annak megállapításai érvényesek-e még.

5.7.7 Szolgáltatók típusai, Nagy Testvér komplexus

A felhasználók különböző típusú szolgáltatókkal állhatnak kapcsolatban, egyszerre akár többel is. Említettem már a bankkártyákhoz hasonlítva a dolgot, hogy a felhasználók több tanúsítvánnyal is fognak rendelkezni. Talán még jobb hasonlat az e-mail-címek esete. Elvetemültebb internetfelhasználók – mint magam is – akár négy-öt e-mail-címmel is rendelkezhetnek egyidejűleg. Például egy hivatalos cégessel, eggyel a privát levelezésre, eggyel a családi vállalkozáshoz, egy titkossal a marihuánafogyasztók és -termelők levelezési listájához, és eggyel a drogellenes ligában betöltött vezetői pozícióhoz. Mivel egy tanúsítvány egy e-mail-címet képes értelmes módon igazolni,[16] így minden e-mail-címhez külön tanúsítványra lesz szükség. A bankunk lehet, egy hatodik beszer-

zésére fog kényszeríteni minket, mert az általa alkalmazott biztonsági elvárásoknak jelenlegi tanúsítványaink nem felelnek meg, az állam meg egy hetedikkel lep meg minket, amiben szerepelnek azok az adatok, amik az adóbevalláshoz szükségesek. A hivatalos céges tanúsítványunkat munkáltatónktól kapjuk, aki saját hitelesítésszolgáltatást működtet, a bankit a bankunk résztulajdonában álló hitelesítésszolgáltatótól, az államit az egyik minisztérium által működtetett hatósági szolgáltatótól, a privát levelezéshez és a levelezési listához egy ingyenes teszttanúsítványt tartunk fenn egy külföldi szolgáltatónak köszönhetően, de a családi bétés és ligás címhez egy magyar szolgáltatótól veszünk különböző osztályú tanúsítványokat.

Lehet, nem tudatos választás folytán teszünk így, csak haladunk az árral vagy meghajlunk a kényszer alatt, esetleg jól bevált önvédelmi ösztöneink működnek. Akárhogy is, van egy nagy előnye ennek a sokszínűségnek: az, hogy sokkal nehezebb nyomon követni tevékenységünket a Nagy Testvér mániában szenvedő hatalmi szerveknek. Az előbbiekben máris megkülönböztettünk legalább három szolgáltatói típust: céges, hatósági és független, valamint ezek különböző szolgáltatásait. Nemcsak üldözési mániában szenvedő olvasóim figyelmébe ajánlom, hogy körültekintő módon válasszanak szolgáltatót adatvédelmi szempontból is. Mivel a céges (munkáltató kebelén működő) szolgáltató függetlensége erősen megkérdőjelezhető, s az általa garantált biztonság mértéke is kívánnivalókat hagyhat maga után, én a céges tanúsítványt nem használnám másra, mint hivatalos célra. Bizonyára a fiatalkori élmények és kamaszkori olvasmányok teszik, de az állammal is hasonló fenntartásaim vannak: privát célra és dörti biznisz bonyolítására senkinek nem ajánlanék állami tanúsítványt. Én a független szolgáltatókat tartom a legmegfelelőbbnek, amennyiben valóban függetlenek. Kérdéses például, hogy egy, a munkáltatóval vagy az állammal folytatott vita kapcsán, melyben az elektronikus aláírás megtétele vagy bizalmas információhoz való hozzáférés a vita tárgya, mennyire tekinthető az állam, illetve a munkáltató mint hitelesítésszolgáltató független félnek. A kétely mindig ott bujkálhat az emberben, hogy minden minősítés és pecsét dacára nem rendelkeznek-e a magánkulcsom másolatával, amivel nevemben bármi aljasságot elkövethetnek. Összeesküvés-elméletek hívőit még talán a saját kártyán teliholdkor végzett kulcsgenerálás sem nyugtatja meg. Ezek a szolgáltatók ráadásul felfedhetik bizalmas adataimat hatósági megkeresés esetén, így az amúgy lesajnált teszttanúsítványoknak is lehet egy nagyon nagy előnye: azokhoz nem kell valódi adatokat megadni. Nem árt emlékezni arra, hogy a partnereink számára lehetővé téve hiteles azonosításunkat egyúttal mindenki más számára is lehetővé tesszük ugyanezt. Persze a titkosítás felhasználásával összességében sokkal nagyobb biztonságban érezhetjük magunkat, azért célszerű a körültekintés.

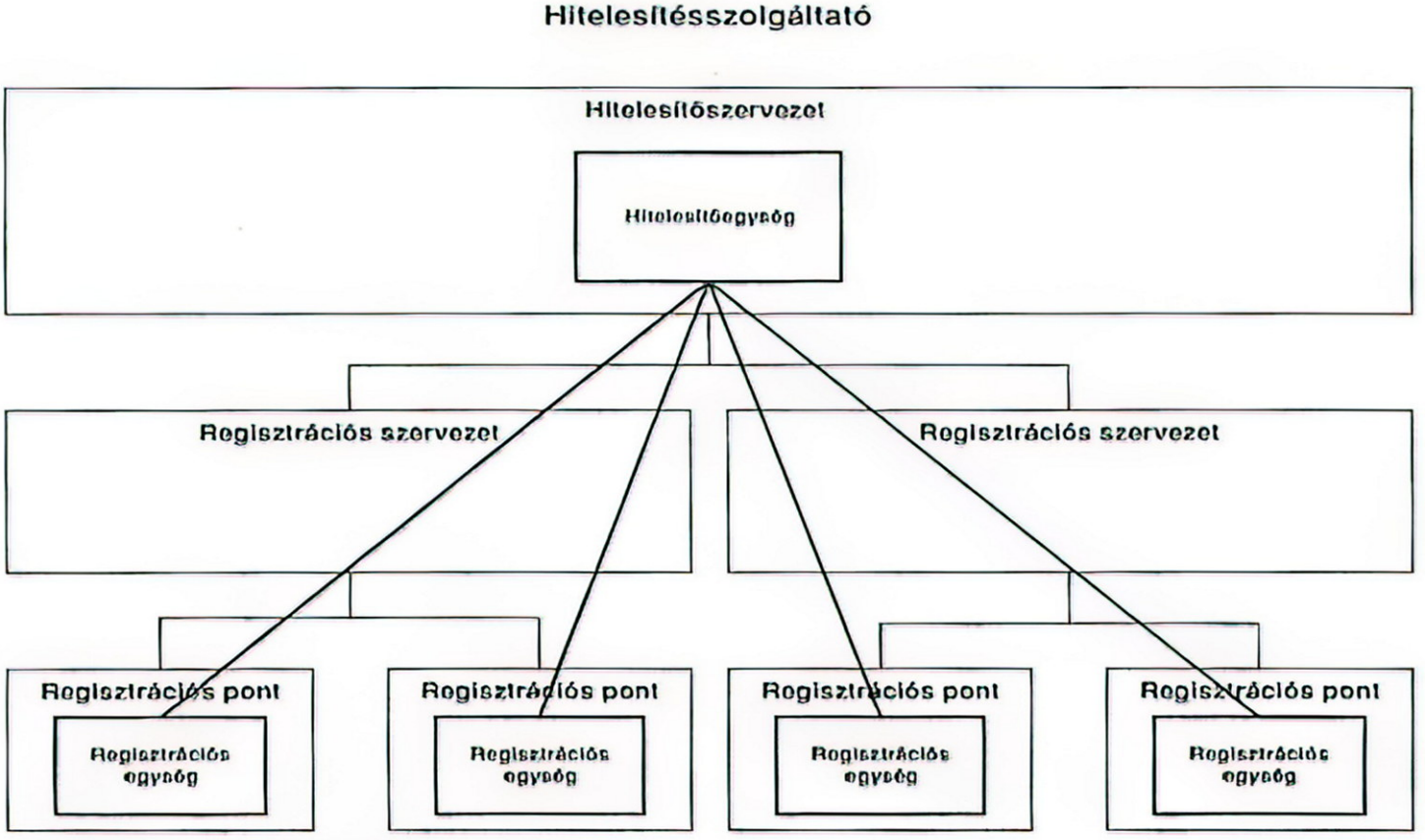
Az állami szolgáltatóknak egyébként nagy előnye az ellenőrző fél szempontjából, hogy mivel a hatóságok működtetik a közhiteles nyilvántartásokat, azokból a legmegbízhatóbb tanúsítványok kiadására képesek. Minthogy ők hivatalból értesülnek az adatainkban történő változásokról és egyéb visszavonás-

hoz vezető körülményekről (cég megszűnése, személyazonosító okmány elvesztése, név- és címváltozás stb.), azokra reagálva a tanúsítvány érvényességének kezelése is megbízhatóbb lehet, mint egy független szolgáltató esetén. Hiszen egy független szolgáltató csak a tanúsítvány tulajdonosától vagy egy harmadik féltől értesülhet ezekről. Az állami szolgáltató a feledékeny és rosszhiszemű aláírók ellen ezért többletvédelmet jelent az aláírás ellenőrzőjének.

5.8 Struktúrák

5.8.1 Regisztrációs struktúrák

Említettem már, hogy egy hitelesítésszolgáltató több regisztrációs szervezettel állhat kapcsolatban, s egy regisztrációs szervezet több regisztrációs pontból állhat. Ez egy háromszintű logikai fastruktúrát alkot, tetején a hitelesítési szervezettel, alatta a regisztrációs szervezettel, legalul a regisztrációs ponttal. A struktúra alsó és felső pontján található hitelesítő- és regisztrációs egységek együttműködése szükséges a tanúsítványok menedzsmentjéhez. A regisztrációs szervezet egy logikai entitás, mely az egyes regisztrációs pontokat üzleti, jogi, szervezeti, földrajzi vagy más értelemben összefogja. E logikai értelemben a regisztrációs szervezetek akár több szinten is egymásra épülhetnek, alszervezeteket, csoportokat, sejteket és brigádokat alkotva, ez az informatikai megoldás kétrétegű struktúráját



56. ábra Regisztrációs struktúra

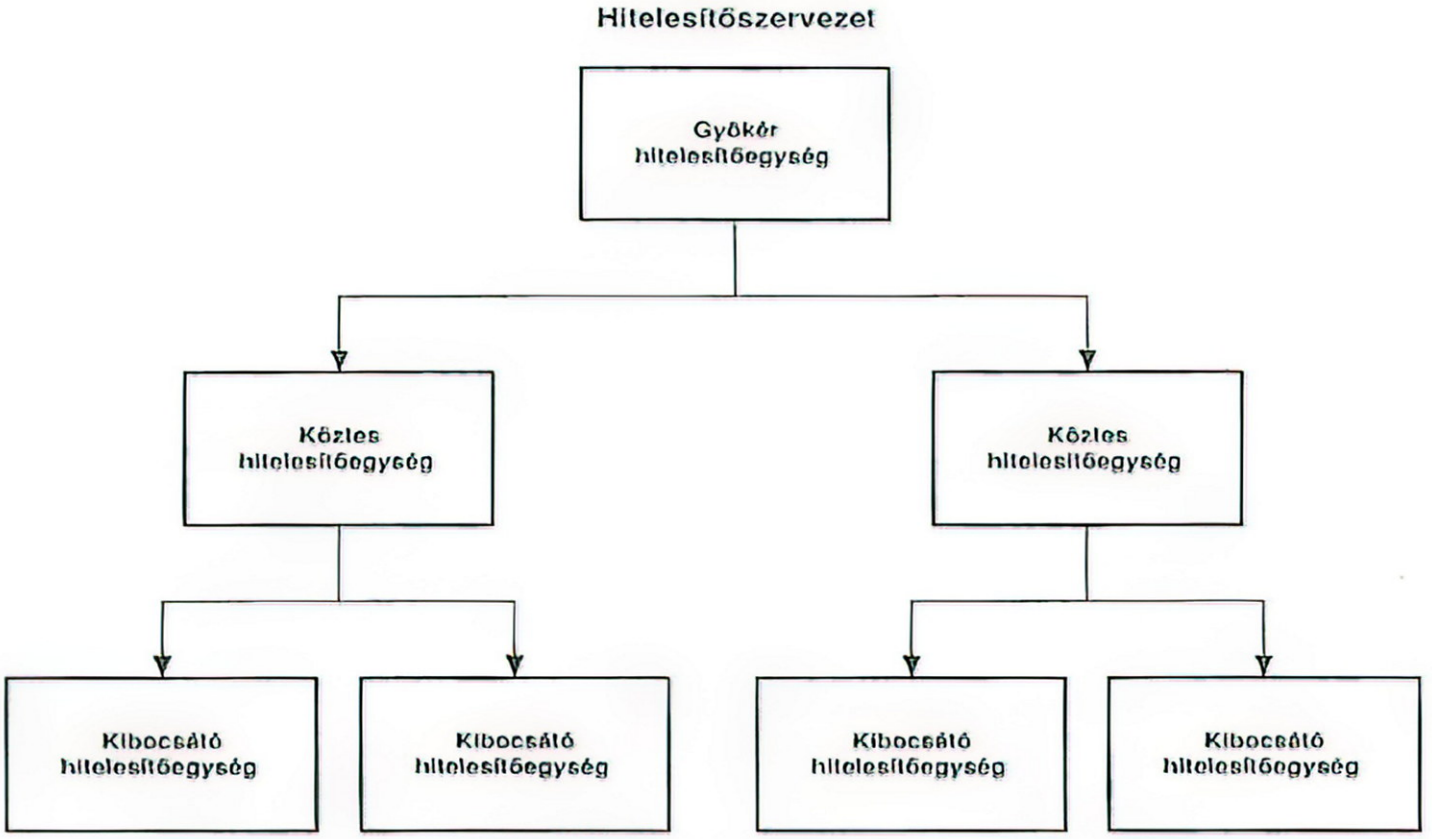
azonban nem érinti.[17] Példa lehet erre egy, több országban szolgáltatást nyújtó hitelesítőcég, amely országonként külön regisztrációs szervezettel köt szerződést, mely regisztrációs szervezetek különböző alvállalkozókkal állnak kapcsolatban, mely alvállalkozók több regisztrációs pontot is működtetnek.

Az ugyanazon regisztrációs szervezetben működő regisztrációs pontok között feladat-, illetve felelősségmegosztásra is mód van. Az egyik pont által rögzített regisztrációs adatokat például a másik pont ellenőrizheti a nagyobb biztonság végett, vagy a tanúsítványigénylés és -kiadás feladatát szétoszthatják egymás között.

5.8.2 Hitelesítési struktúrák

A hitelesítőegységek önmagukban is struktúrába szerveződhetnek egy hitelesítőszervezeten belül. Ennek több oka is lehet. A leggyakoribb a szolgáltató merészen optimista jövőképe, mely tanúsítványok százezreinek, millióinak és tízmillióinak a kibocsátásával számol üzleti tervében. Olyan mennyiséggel, amelyet egyetlen hitelesítőegység nem tud kezelni, ezért több egység együttes munkájára lesz szükség. A szolgáltató gondolhatja úgy is, hogy a különböző tanúsítványosztályok és -típusok kibocsátását különböző egységekkel oldja meg, technikai kényszerűségből vagy józan megfontolásból. Ami nem lehet ok, az a geográfiailag széles ügyfélkör, hiszen a hitelesítőegység fizikai előfordulása nem lényeges a közösségen belül (egy száz mérföldre lakó ügyfelet ugyanúgy ki tud szolgálni, mint a sarki fűszerest). A szolgáltató ezért hitelesítőegységeit egymás fölé, mellé, alá rakja, és egymással hitelesíti őket. Vagyis az egyik hitelesítőegység tanúsítványát aláírja a másik, így ismerve el, hogy egy családból származnak. A hitelesítőegységek többféle módon is struktúrába szerveződhetnek, de e szerveződések közül én csak a legelterjedtebb változatot, a hierarchikus, egyirányú struktúrát mutatom be. Ebben a struktúrában a hierarchia legtetején egy gyökér hitelesítőegység trónol, ami sokszor tényleg szinte csak uralkodik, mert más dolga nincsen, mint a hierarchiában közvetlen alatta lévő hitelesítőegységek hitelesítése. A hierarchia akár többszintű is lehet, s ebben az esetben az alsóbb szinteken lévő hitelesítőegységeket mindig a felsőbb szinteken lévő hitelesítőegység hitelesíti. A gyökér hitelesítőegység a felhasználók számára biztonsági okokból nem szokott tanúsítványokat kiadni, azt gyakorlatilag unplugged üzemmódba rakják, vagyis lezárják, miután elvégezte a kibocsátó hitelesítőegység „megtermékenyítését". Újbóli életre keltésére csak akkor van szükség, mikor a kibocsátó vagy a köztes hitelesítőegység tanúsítványát meg kell újítani vagy vissza kell vonni.

Egymás hitelesítésével a hitelesítőegységek azt igazolják, hogy a másikban ugyanolyan módon meg lehet bízni, mint bennük. Ahogy különböző tanúsítványosztályokat nem ildomos ugyanazon hitelesítőegységgel kiadni (hiszen az osztályok közti különbség pont a bizalmi szintben van), ugyanígy nem illik egy struktúrában keverni a különböző osztályokat. Vagyis minden osztály saját hierarchiát kíván. Egy struktúra ugyanakkor akár több hitelesítőszervezetet, szolgáltatót is átfoghat, ha ugyanazt a tanúsítványosztályt adják ki, ugyanazon sza-



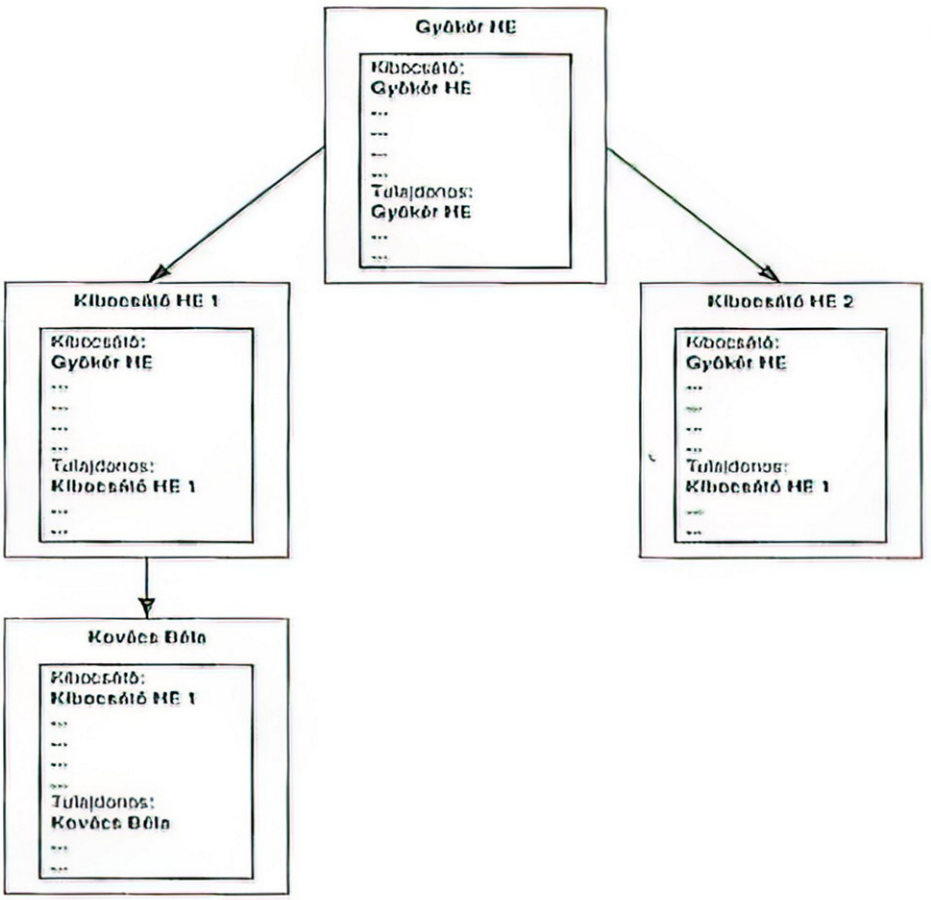
57. ábra Egyirányú, hierarchikus hitelesítőstruktúra

bályrendszernek megfelelve. A gyakorlatban ez kereszthitelesítéssel szokott megvalósulni, ami két struktúra utólagos összekötését jelenti valamely szinten.

Ebben a struktúrában ugyanakkor nincs mód a felülre építkezésre (a kereszthitelesítés nem erre lett kitalálva), így a hitelesítésszolgáltatók általában tanúsítványosztályonként egy gyökér és egy kibocsátó hitelesítőegységgel indulnak, és struktúrájukat az igényeknek megfelelően fejlesztik tovább lefele vagy oldalirányban.

5.8.3 Tanúsítási láncok

A hitelesítőegységek felülről lefelé építkező aláírásait, melyek a gyökér hitelesítőegységgel kezdődnek és a felhasználó tanúsítványáig tartanak, tanúsítási láncnak[18] nevezzük. A felhasználó tanúsítványát akkor tekinthetjük érvényesnek, ha a tanúsítási láncban felette álló összes tanúsítvány érvényes. Ennek ellenőrzéséhez a felhasználónak a lánc összes tanúsítványával rendelkeznie kell, és első lépésként mindig a lánc létezéséről és épségéről kell megbizonyosodnia: a tanúsítványokon felfelé lépkedve ellenőriznie kell az azt kibocsátó szervezet aláírását (hitelesség és sértetlenség szempontjából) mindaddig, míg a gyökér hitelesítőegység tanúsítványáig el nem jut. A gyökér hitelesítőegység tanúsítványa saját farkába harap, ugyanis ezt úgynevezett önhitelesítéssel maga a gyökér hitelesítőegység hitelesíti. Ezen aláírás ellenőrzésére a felhasználónak más, megbízható forrásból kell a gyökér tanúsítvánnyal rendelkeznie (ennek módszereit már ismertettem). A lánc e legfelső elemét szokták bizalmi pontnak nevezni, mivel az iránta való bizalom a lánc többi eleme tekintetében is bizalmat jelent.

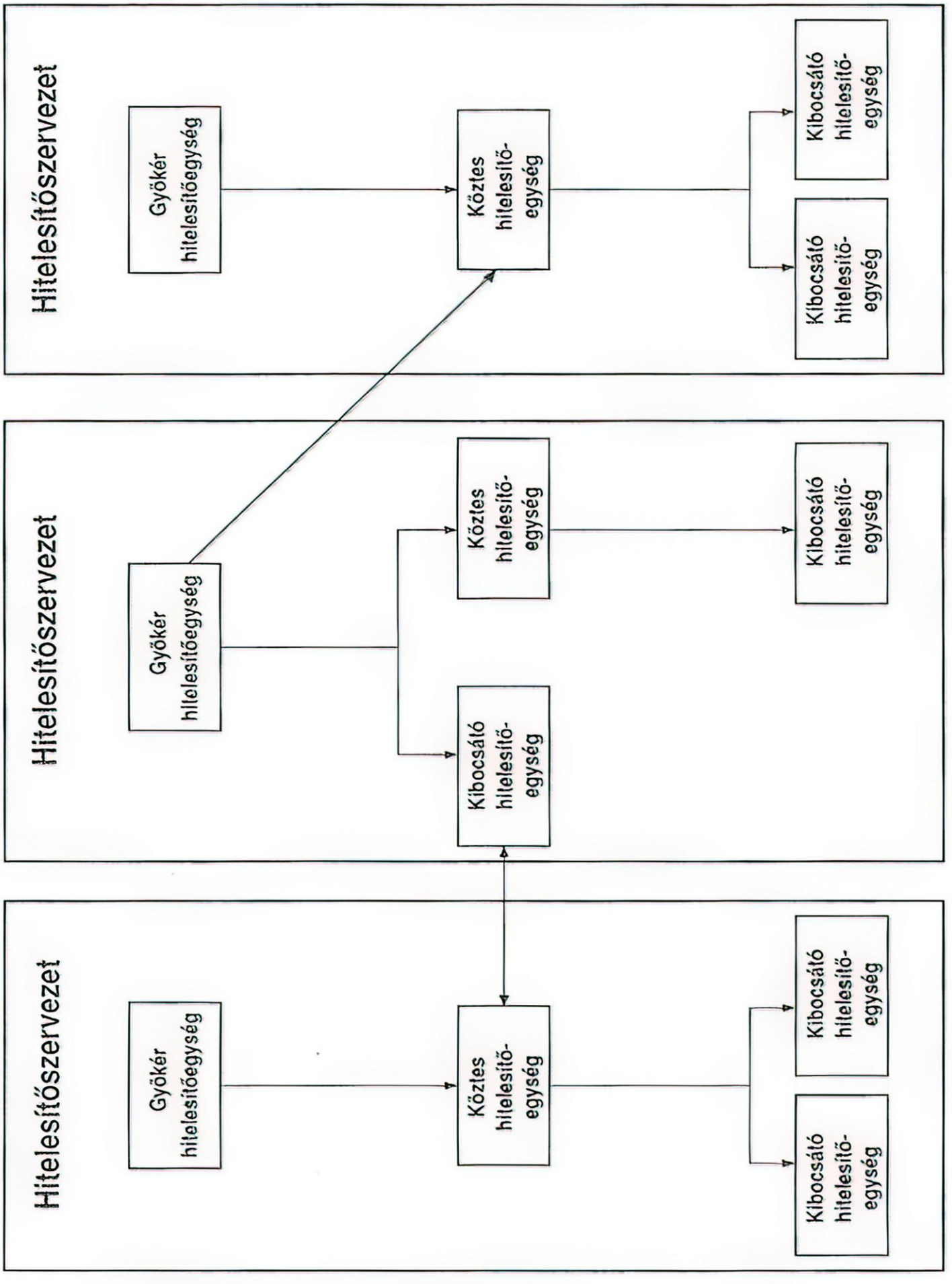


58. ábra
Tanúsítási lánc

5.8.4 Kereszthitelesítés

Kereszthitelesítés esetén a hitelesíteni kívánt hitelesítőegység számára történik egy plusztanúsítvány kibocsátása (a másik struktúrában már létező tanúsítványa mellé) azon hitelesítőegység által, mely a másik struktúrát el kívánja ismerni. A kereszthitelesítés lehet kétoldalú, azaz a kereszthitelesítésben részt vevő mindkét hitelesítőegység kibocsát a másik számára egy ilyen „ráadás" tanúsítványt, vagy egyoldalú, amikor a kereszthitelesítés viszonzatlan marad. A kereszthitelesítő tanúsítvány ugyanazt a nyilvános kulcsot hitelesíti, mellyel a kereszthitelesített hitelesítőegység a láncban alatta állókat (felhasználókat vagy hitelesítőegységeket) hitelesíti. A kereszthitelesítő tanúsítvány a kereszthitelesítendő hitelesítőegység saját tanúsítványának (amit a hitelesítőegység fölött álló egység vagy saját maga bocsátott ki) egyéb attribútumait is át szokta venni, így tulajdonképpen két megegyező tanúsítvány jön létre, mely csak az azt hitelesítőszervezet tekintetében különbözik. A hitelesítőegység ilyenkor gyakorlatilag ugyanazt a tanúsítványtestet írja alá saját magánkulcsával, amely már korábban is létezett. A kereszthitelesítés később e kereszthitelesítő tanúsítvány visszavonásával egyszerűen megszüntethető.

Amennyiben a kereszthitelesítés a gyökér hitelesítőegységek szintjén történik, akkor a két struktúra teljes mértékben elismeri a másikat, ha a kibocsátó egységek szintjén, akkor csak részlegesen, a kibocsátó egységek szintjétől „lefele". A kereszthitelesítés ugyanakkor történhet különböző szintek között is: az egyik oldalon lévő gyökér hitelesítőegység hitelesíti a másik oldalon lévő kibocsátó hitelesítőegységet.



59. ábra Különböző kereszthitelesítések

5.8.5 Láncbejárás

Az alábbi ábrán egy kereszthitelesítéssel megtűzdelt láncot mutatok be, mely a jobb megértés végett csak egyoldalú. Csak az egyik oldal ismeri el magáénak a másik hitelesítési láncot, azt sem teljesen, mert a kereszthitelesítés nem a gyökér hitelesítőegységek szintjén történik, hanem a kibocsátó egységek szintjén. Megspórolva a további felesleges okfejtést, ennek példáján keresztül mutatom be teleregény stílusban, hogyan működik a kliens oldalon a tanúsítási lánc felépítése és bejárása.

A felvázolt hitelesítési struktúrában Béla Kibocsátó HE 1-ben és Gyökér HE 1-ben bízik meg, Zsolt Kibocsátó HE 2-ben és Gyökér HE 1-ben, László Kibocsátó HE 3-ben és Gyökér HE 2-ben, Edit pedig Kibocsátó HE 4-ben és Gyökér HE 2-ben, vagyis azokban, akik felettük állnak a hierarchiában.

Eset1: Kovács Béla kap egy elektronikusan aláírt levelet Fehér Lászlótól.

Kovács Béla a Fehér László tanúsítványán szereplő Kibocsátó HE 3 hitelesítőegységet nem ismerve utánanéz az azt hitelesítőegységnek. Annak tanúsítványaihoz eljutva kissé meglepődik, hogy kettőt is talál (mert Kibocsátó HE 2 és Gyökér HE 2 egyaránt kibocsátott Kibocsátó HE 3 számára tanúsítványt), de sebaj, mindkettőt megvizsgálja. Egyik se mond neki semmit, így mindkét irányban továbbindul. Először csacska módon Gyökér HE 2 felé, de az zsákutcának bizonyul. Sebaj, feledve a kudarcot, újult erővel elindul a másik útvonalon, ahol Kibocsátó HE 2 tanúsítványán felfedezi Gyökér HE 1 aláírását. Halleluja, őt ismeri és elismeri. Itt a vége, fuss el vele, Kovács Béla elfogadja Fehér László aláírását.

Eset2: Szabó Zsolt kap egy elektronikusan aláírt levelet Fehér Lászlótól.

A helyzet hasonló, mint az előző esetben, de a bejárás hamarabb véget ér, mivel Szabó Zsolt Kibocsátó HE 2 aláírását is elismeri, s azzal már Kibocsátó HE 3 egyik tanúsítványán is találkozik.

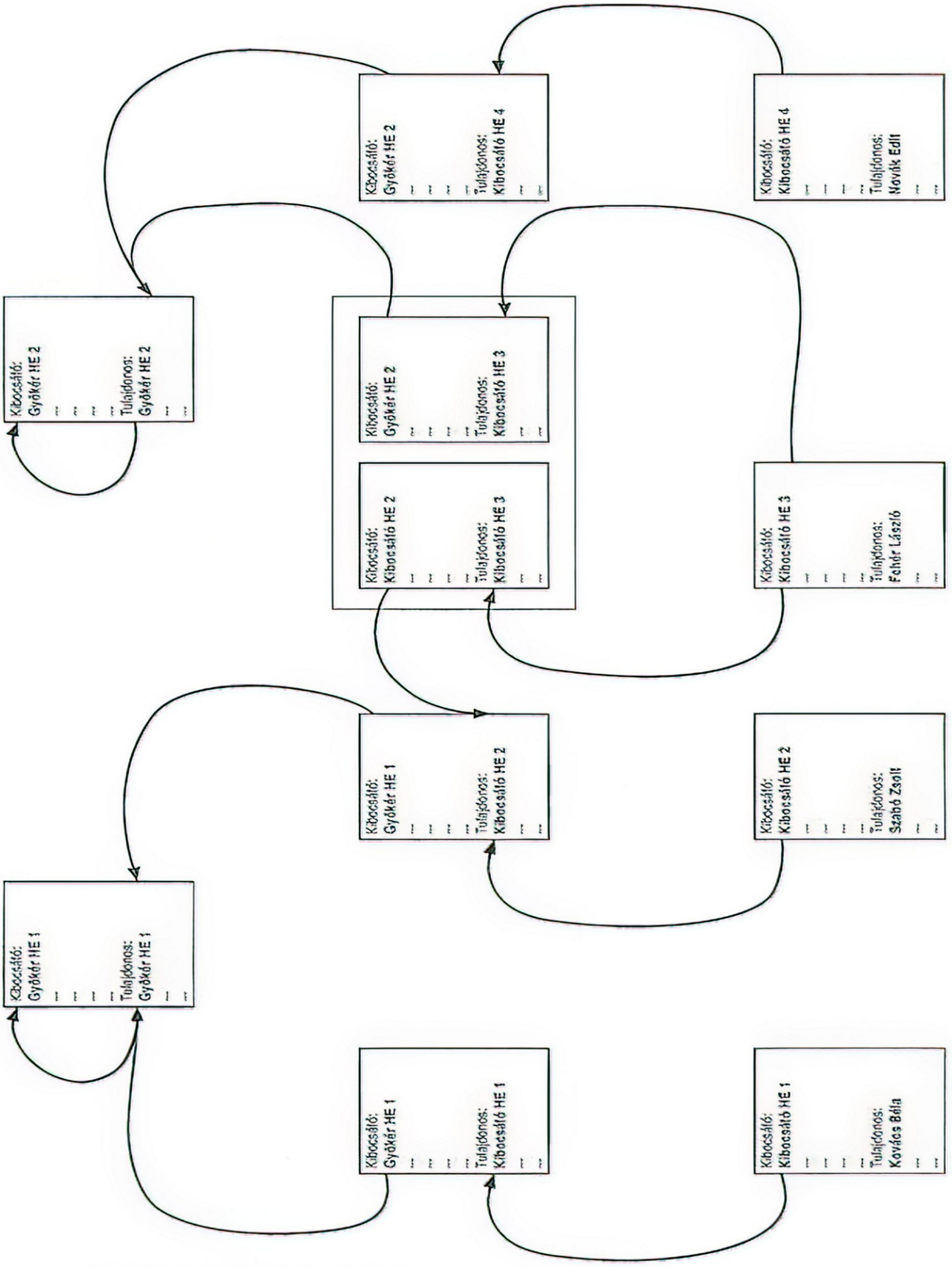
Eset3: Kovács Béla kap egy elektronikusan aláírt levelet Novák Edittől.

Béla Novák Edit tanúsítványán Kibocsátó HE 4 aláírásával találkozik, amely tanúsítványát ellenőrizve Gyökér HE 2-be botlik, ahonnan nincs tovább út. Ezzel vége is, mert Béla Gyökér HE 2-t sem ismeri el. Edit aláírását Béla nem tudja elfogadni. (Szabó Zsolt persze ugyanígy járna).

Eset4: Fehér László egy elektronikusan aláírt levelet kap Szabó Zsolttól.

László Zsolt tanúsítványán Kibocsátó HE 2 aláírásával találkozik, amely tanúsítványát ellenőrizve Gyökér HE 1-be botlik, ahonnan nincs tovább út. Mivel a kereszthitelesítés csak egyirányú volt, László nem jut el olyan hitelesítőegységhez, amelynek tanúsítványát elfogadná, Zsolt aláírását vissza kell utasítania. (László ugyanígy járna Béla aláírásával is, és Edit se lenne jobb helyzetben, mint László).

A példa kedvéért ismertetett módszer a vak bejárás, aminél van intelligensebb is, ha nagyon szükséges (két-három szintű egyszerű hierarchiáknál ilyen intelligencia felesleges). Az se biztos, hogy ellenőrzőnek minden tanúsítvány rendelkezésre áll az összes út bejárásához, jobb esetben csak azokkal rendelkezik, amire szüksége van, rosszabb esetben pont azokkal nem. A lánc tanúsítványait az aláíró leveléhez csatolva is elküldheti a címzett részére, aki ennek hiányában egyéni nyilvántartásából vagy a tanúsítványtárból is összevadászhatja azokat.



60. ábra Hitelesítési lánc bejárása[19]

5.8.6 Hitelesítőegység-tanúsítványok

A kereszthitelesítésben részt vevő tanúsítványok ugyanolyan tanúsítványok, mint amiket a hierarchiában máshol alkalmaznak a hitelesítőegységek tanúsítványaként. Valójában minden hitelesítőegység-tanúsítványt, amit egy másik hitelesítőegység ír alá, kereszthitelesítő tanúsítványnak nevezik. A kereszthitelesítés logikai volta (fölérendeltség, mellérendeltség) ebből a szempontból lényegtelen, az valójában csak egy olyan ábrázolási mód, melyre az emberi értelemnek van szüksége. A tanúsítási lánc ellenőrzése során ez a hierarchia amúgy sem bontakozik ki. Akkor az erre szolgáló mechanizmus vaksin kutakodik és járja be az egyes hitelesítési útvonalakat, amíg nem talál egy általa elismert hitelesítőegységet. A kereszthitelesítő tanúsítványon kívül még két különböző típusú hitelesítőegység-tanúsítvány létezik, amelyek mindegyikét ugyanazon hitelesítőegység írja alá, amely tulajdonosként abban meg van nevezve. Ilyen a gyökér tanúsítványok esetében alkalmazott „önaláírt" tanúsítvány, amely esetben a tanúsítvány aláírása a benne foglalt nyilvános kulccsal ellenőrizhető (mert annak magánkulcs párjával lett aláírva); valamint az „önkibocsátott" tanúsítvány, mely egy másik kulcspárt azonosít, és így a hitelesítőegység egy másik tanúsítványával ellenőrizhető. Ez utóbbi megoldás például a hitelesítőegység kulcscseréjekor alkalmazható.[20]

5.8.7 Házi hitelesítő-központ

Sokan a tanúsítványkibocsátást maguk kívánják megoldani házon belül cégük, szervezetük számára egy mini hitelesítő-központ felállításával. E törekvésnek komoly katalizátora a **Microsoft Certificate Server** hitelesítőegység-szoftver, mely a **Windows 2000** részeként, kvázi ingyenessége folytán (az operációs rendszerért természetesen fizetni kell) egyre több helyen elérhető.[21] Ezzel boldog-boldogtalan hitelesítés-szolgáltatást indít, aminek körülbelül annyi értelme van, mint a házi szénfek. Jobb, mint a semmi, de meg sem közelíti azt a biztonságot, mint ha a pénzt bankba tennénk.

Ennek az oka nem a szoftverek minőségében keresendő, hanem abban a biztonsági rendszerben, amit az önjelölt vagy „kényszerszolgáltató" vélhetően nem tud olyan színvonalon kiépíteni, ahogy azt egy professzionális kereskedelmi szolgáltató tenné. A sokszor kétes értékű szabályzatok és biztonsági rendszerek által nyújtott látszatbiztonság pedig még veszélyesebb lehet, mint ha nem élnénk ezekkel a biztonsági szolgáltatásokkal.[22]

Mivel e zártkörű szolgáltatások kiépítésére egyedi szabályzatok és eljárásrendek alapján kerül sor, e házi hitelesítőszervezetek által kiszolgált közösségek mindmind elkülönülő szigetet alkotnak. A szűk megcélzott közösségen kívül így senki nem fogadja el az általa kiadott tanúsítványokat, e szigetecskék utólagos összekötése pedig értelmes módon nem lesz egykönnyen kivitelezhető, a későbbiekben sem. Vagyis ezek a rendszerek örök magányra és lassú elmúlásra vannak ítélve.

Bár úgy tűnik, ezzel nem akarok senkit lebeszélni arról, hogy e termékeket használja, hiszen a másik oldalról megközelítve a dolgot: a befőttesüvegnél a szél tud jobb lenni. De nem is beszélhetek le senkit, mert ezek a termékek nagymértékben integráltak az operációs rendszerrel, ami felhasználásukat leegyszerűsíti, sőt az operációs rendszer bizonyos PKI-funkciói csak ezen a módon elérhetőek. Ezt a felhasználást azonban nagyon körültekintően kell tenni, a biztonság valamennyi szegmensére odafigyelve, szabványos megoldásokat felhasználva, különösen a szabályzatok megvalósításakor. Az így elért biztonsági szintet reálisan kell felmérni, s ennek megfelelően szabad csak az így kibocsátott tanúsítványokat felhasználni.

JEGYZET

1 Ilyen módon működik a GIRO és a Matáv szolgáltatása is, s a NetLock is nyújt nyilvános szolgáltatása mellett szervezeteken keresztüli hitelesítést. Lásd: 10.4 fejezet.

2 Az ábrán feltüntetett megnevezések nem egyéneket, hanem szerepeket takarnak (ugyanaz a személy lehet aláíró és elfogadó fél is, illetve a szolgáltató maga is fel szokott lépni ilyen szerepekben).

3 Angol eredetiben félrevezető módon sokszor mindkettő „authority", vagyis hatóság, amely kifejezést jogi megfontolások miatt nem javaslok átvenni, s a könyvben is jobbnak láttam mellőzni.

4 Ez a fizikai védelem néhány esetben odáig fajul, hogy régi háborús bunkerekbe, akár száz méterrel is a földfelszín alá telepítik a hitelesítőegységet. Gyárlátogatáshoz hasonló eseménynyeket pedig tényleg szoktak szervezni, de a hitelesítőegységet körülvevő biztonsági zónába még az illusztris látogatókat sem szokták beengedni.

5 Az a helyszín, ahol a hitelesítőegységet működteti a hitelesítőszervezet.

6 Az ábra egy lehetséges logikai megoldást mutat be, amitől a gyakorlatban számtalan módon el lehet térni. Az egyes egységek egyetlen szolgáltatónál vagy különböző szolgáltatóknál is helyet kaphatnak, nem feltétlen kell jelen lenniük, és nem feltétlen a bemutatott módon. Az egyes szolgáltatások leírásánál igyekszem áttekinteni a kivételeket is.

7 A terjesztőegységet, ami lehet fizikailag is független modul, korábban nem különböztettük meg a hitelesítőegységtől. Az egység feladatainak legnagyobb részét teljesen automatikusan végzi, emberi közreműködésre csak a kulcs hordozóra történő írása és a borítéknyomtatás esetében lehet szükség.

8 A pontosidő-szolgáltatók az ún. koordinált egységes időt alkalmazzák (Co-ordinated Universal Time – UTC), ami időzónától független.

9 A CBC blokktitkosítási módszerhez hasonlóan.

10 Nem mindegyik bemutatott követelmény értelmezhető zárt szolgáltatás esetén vagy a nem minősített szolgáltatás esetében, de az egyszerűség végett megkülönböztetéseket nem teszek. Ezek nem (mind) törvényi előírások, s bár sokuk szerepel a minősítés követelményei között, nem hivatalos követelményjegyzékről van szó.

11 Biztonsági tisztviselő: általánosságban felelős a szabályzatok végrehajtásáért, ő hagyja jóvá a tanúsítványok generálását, visszavonását, felfüggesztését. Rendszer-adminisztrátor: telepíti, konfigurálja és fenntartja a szolgáltató rendszereit. Rendszer-operátor: a szolgáltató rendszereit üzemelteteti, elvégzi a rendszermentés és – ha kell – a helyreállítás feladatait. Rendszerauditor: a szolgáltató archívumait és auditnaplóit kezeli.

12 A legtöbb veszély komplex védelmet kíván mind fizikai, mind informatikai, mind személyi és egyéb szempontokból. Így azok besorolása az egyes fejezetekbe csak esetleges tud lenni.

13 Erre szolgál az a bizonyos titokmegosztó protokoll.

14 Az időbélyegzőnél említett bejegyzéslláncolási módszerhez hasonló módon.

15 Ez olyasmi, mint a mindenki által ismert és elvárt TÜV pecsét a barkácsgépeken.

16 Elviekben különböző kiterjesztésekbe több e-mail-cím is befoglalható, de ezt egy alkalmazás se fogja megérteni, s a cél lehet pont az, hogy ezen e-mail-címek ne jelenjenek meg együtt sehol sem.

17 Vannak olyan regisztrációs szoftvermegoldások, amelyek a közös LAN-on működő regisztrációs pontokat összefogják, és egy regisztrációs rendszerben működtetik, de ennek különösebb elméleti jelentősége nincsen.

18 Más elnevezéssel: hitelesítési lánc, hitelesítési út stb.

19 Az ábrán szereplő nyilak a bejárási útvonalakat jelzik, amik a tanúsítás irányával pont szembemutatnak.

20 A tanúsítvány érvényessége ez esetben jóval meghaladhatja a magánkulcs érvényességét.

21 A Novell hálózati kiszolgálója már a **Windows**-t megelőzve is tartalmaz(ott) hitelesítőszoftvert.

22 Érdemes a 8.8 fejezetben bemutatott tartalomjegyzékre egy pillantást vetni, hogy vajon az ott bemutatott szabályzati és biztonsági komponensek mind kezelve vannak-e egy ilyen esetben (s a lista csak a nyilvánosságra tartozó dolgokat említi).

6 Az aláíró eszköz

Ajánlás:

Azoknak, akik magas fokú biztonságra törekszenek.

6.1 Kulcstároló és aláíró eszközök

Az aláíró eszközök véletlenül sem tévesztendők vagy mosandók össze a kulcstároló eszközökkel. Míg az utóbbiak csak tárolják a kulcsot, s így beletartozik körükbe a floppy disk, a háttértár és a memória is, az előbbiek kulcstároló szerepükön túl magának az aláírásnak a műveletét is elvégzik. Teszik méghozzá ezt ideális esetben úgy, hogy közben a magánkulcs soha nem hagyja el az aláíró eszköz biztonságos környezetét. „Ha a hegy nem megy Mohamedhez, Mohamed megy a hegyhez" alapon az aláírandó adat (a lenyomat) vándorol az aláíró eszközhöz, és ott lesz belőle aláírás. Az aláíró eszköz ugyanis egy saját memóriával és mikroprocesszorral rendelkező miniatűr számítógép, amely bár többcélú tároló- és feldolgozó egység, bizonyos feladatokra, így például elektronikus aláírás céljára optimalizálva van. Az eszköz képes maga generálni a kulcsokat, így a magánkulcs a külvilággal tényleg soha nem érintkezik.[1] Ennek kizárására az eszköz egyes tárolóegységei védettek a külső olvasások ellen, aminek köszönhetően a magánkulcs az eszközön kívülről nem hozzáférhető. Az eszköz, melyet én csak aláíróként nevezek, a többcélúságnak köszönhetően persze titkosításra is alkalmas lehet.

6.2 Aláíró eszköz és aláíró környezet

Az aláíró eszköz ugyanígy nem mosandó össze az aláíró és aláírás-ellenőrző környezettel. Az utóbbiakba beleértjük azt a teljes környezetet, mely az aláírás létrejöttében és ellenőrzésében szerepet játszik. Azt a számítógépet és háttértárat, melyben az aláírandó dokumentum megszületik és tárolódik; azt a képernyőt, amin az aláíró számára megjelenik; a billentyűzetet, mellyel kiadja a parancsot az aláírásra, és befrja a kulcs aktivizáló adatát; a processzort, mely előállítja a dokumentum lenyomatát, valamint ezen eszközök kapcsolatát és együttműködését biztosító egyéb elemeket, azokat is, melyek az aláíró eszközzel való kapcsolattartást biztosítják. Egyszerűbben és gyakorlatiasabban fogalmazva lehetett volna azt is mondani, hogy az aláíró környezet a személyi számítógép maga, amely korántsem képes azt a biztonságot biztosítani, mint az aláíró eszköz. Ez a környezet számos ponton támadható: például a lenyomatkészítő algoritmus vagy az egyes elemek kommunikációja, mely végeredményét tekintve ugyanúgy az aláírás hamisí-

tásához vezethet, mint, mondjuk, az algoritmus feltörése. Ha például egy trójai faló az aláírandó adat lenyomatát egy másikkal helyettesíti az aláírási folyamatban, mielőtt az az aláíró eszközre jutna, akkor az aláíró nem azt az adatot írja alá, mint amit szándékozott (ami a képernyőn korábban megjelent).

Az ilyen típusú visszaélések ellen jelenleg az aláíró eszközt kezelő meghajtóprogramok és alkalmazások aláírásával (szoftveraláírás), valamint a meghajtóprogram és az eszköz között kommunikáció hitelesítésével és titkosításával védekeznek. Ezáltal az eszköz nyújtotta biztonság részben kiterjeszthető az aláíró környezetre is: megnehezíthető az aktivizáló adat ellopása és a lenyomatba való belepiszkálás is.

E visszaélések kivédésére törekedve továbbá igyekeznek az aláíró eszközt felszerelni minél több olyan funkcióval, amit az aláíró környezet lát el (ezáltal minél kevesebb támadható felületet adni), valamint a hagyományos aláíró környezet biztonságát fokozni. A feladat nehézségét az adja, hogy az aláíró környezet gyengéje az operációs rendszer, de erre az operációs rendszerre szükség van az aláírandó dokumentumok kezeléséhez. Hiába szereljük fel saját képernyővel az aláíró eszközt, az csak a hagyományos operációs rendszer és felhasználói alkalmazások funkcionalitása által lesz képes megjeleníteni a dokumentumot. Ez amolyan róka fogta csuka: ahhoz, hogy biztos lehessek abban, mit írok alá, a biztonságos eszköznek képesnek kéne megjeleníteni azt. Ahhoz viszont, hogy erre képes legyen, rendelkeznie kéne a normál számítógépek és operációs rendszerek számos tulajdonságával, ami pont a biztonságot veszélyezteti. Ráadásul ennek a törekvésnek igen komoly költségvonatkozásai is vannak. Némely aláíró eszköz az aláírandó dokumentum lenyomatát képes ugyan megjeleníteni, de ez a biztonságot nem növeli jelentős mértékben.

A jövő nagy valószínűséggel a PDA-szerű eszközöké, melyek valamilyen szabványos leírónyelven (például XML) leírt aláírandó adatokat fognak megjeleníteni. Bár az aláírandó dokumentum nem feltétlen biztonságos környezetben jön létre, de már biztonságos környezetben folyik az aláírás teljes menete a dokumentum megjelenítésével, az aláírásra vonatkozó megbízás kiadásával, a lenyomat előállításával, az aktivizáló adat megadásával és a lenyomat kódolásával. Hasonló biztonságos módon kell működni az aláírás ellenőrzésének is.

6.3 Az aláíró eszközök fajtái

Az aláíró eszközöknek több fajtája létezik. Hardveres biztonsági modulnak azokat az összetett eszközöket nevezzük, melyek általában egy önálló dobozként vagy egy szerverbe helyezhető (például PCI sloton keresztül) nagyobb méretű kártya formájában öltenek testet. Ezek a kártyák mind a biztonság, mind a számítási sebesség tekintetében a hétköznapi elvárásokat jóval meghaladó feltételeknek felelnek meg. Babrálásbiztosak (behatolás érzékelése esetén megsemmisítik a védett adatokat), és percenként több száz vagy akár több ezer aláírásra is

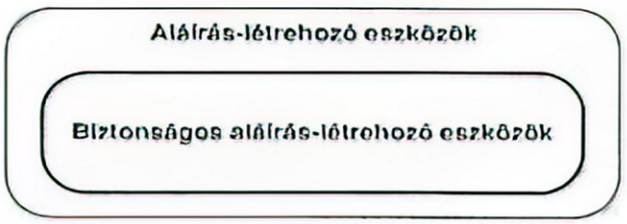
képesek. Webszerverekben, tűzfalakban, útválasztókban és olyan egyéb helyeken használják őket, ahol nagy mennyiségű aláírás generálására van szükség megadott időtartam alatt, s a biztonság is kritikus. Ilyen hely természetesen a hitelesítésszolgáltató hitelesítőegysége is.

Egy második csoportot alkotnak a tokenek[2], amelyek egyéni felhasználásra lettek szánva. Körükbe tartoznak az intelligens kártyák, az USB tokenek (amelyek úgy néznek ki, mint egy kulcstartó) és egyéb kisméretű eszközök, például PCMCIA-kártyák.

Az utolsó csoportba azokat az eszközöket sorolom, melyek multifunkciósak, és az elektronikus aláírás csak egy sokadrangú funkció az eszköz rengeteg szolgáltatása közül. Ilyen eszköz lehet szinte bármi, de elsősorban a PDA és a mobiltelefon lebeg a szemem előtt, mikor erre gondolok.

6.4 ALE és BALE

Jogi értelemben az aláíró eszközök két típusra oszthatóak: az aláírás-létrehozó eszközökre és az ennek alhalmazaként definiálható biztonságos aláírás-létrehozó eszközökre (lásd még a 9. fejezetet).



61. ábra
ALE és BALE

Az aláírás-létrehozó eszköz (ALE) olyan hardver-, illetve szoftvereszköz, melynek segítségével az aláíró az aláírás-létrehozó adatok felhasználásával az elektronikus aláírást létrehozza. A biztonságos aláírás-létrehozó eszköz (BALE) ennek egy erősebb változata. A BALE-nak megfelelő technikai és eljárási eszközökkel biztosítania kell, hogy az aláírás készítéséhez használt aláírás-létrehozó adat aláírásként biztosan mindig különbözik[3], s titkossága kellően biztosított. Továbbá garantálnia kell, hogy az aktuálisan elérhető technológiával az aláírás készítéséhez használt aláírás-létrehozó adat nem rekonstruálható, megvalósítható annak a jogosulatlan felhasználókkal szembeni védelme, illetve az aláírás nem hamisítható. A biztonságos aláírás-létrehozó, illetve -ellenőrző eszközöknek nem szabad az aláírandó elektronikus dokumentumot módosítaniuk, illetőleg az aláírás folyamatában lehetővé kell tenniük e dokumentum megjelenítését az aláíró számára.[4] Ezek szerint egyszerű aláírás-létrehozó eszköznek tekinthetjük a sarokban porosodó PC-nket is, biztonságos aláírás-létrehozó eszköznek viszont semmiképp sem, hiszen a PC-ben tárolt magánkulcsok nincsenek megfelelő biztonságban, s az aláírás folyamata sem kellően védett. Ilyen eszköznek manapság egyes tokenek és a hardveres biztonsági modulok számítanak.

6.5 Intelligens kártyák

Az általános értelemben vett tokenek legelterjedtebb megjelenési formája az intelligens kártya, ami egy bankkártya méretű műanyag lapocska egy ráültetett mikrochippel. Jelenleg több mint kétmilliárd intelligens kártya van forgalomban a világon[5], melynek jóval több mint fele SIM-kártya, a maradék nagy része banki felhasználású kártya, s mindössze kicsiny töredékük a számunkra igazán érdekes multiapplikációs kártya. Bár a mobilkommunikáció céljára kifejlesztett SIM- és a banki célú kártyák is rendelkeznek kriptográfiai képességekkel, aláíró eszközként való felhasználásukat jelentősen gátolja, hogy ezen intelligens kártyák meghatározó hányada gyártóspecifikus operációs rendszerrel rendelkezik.

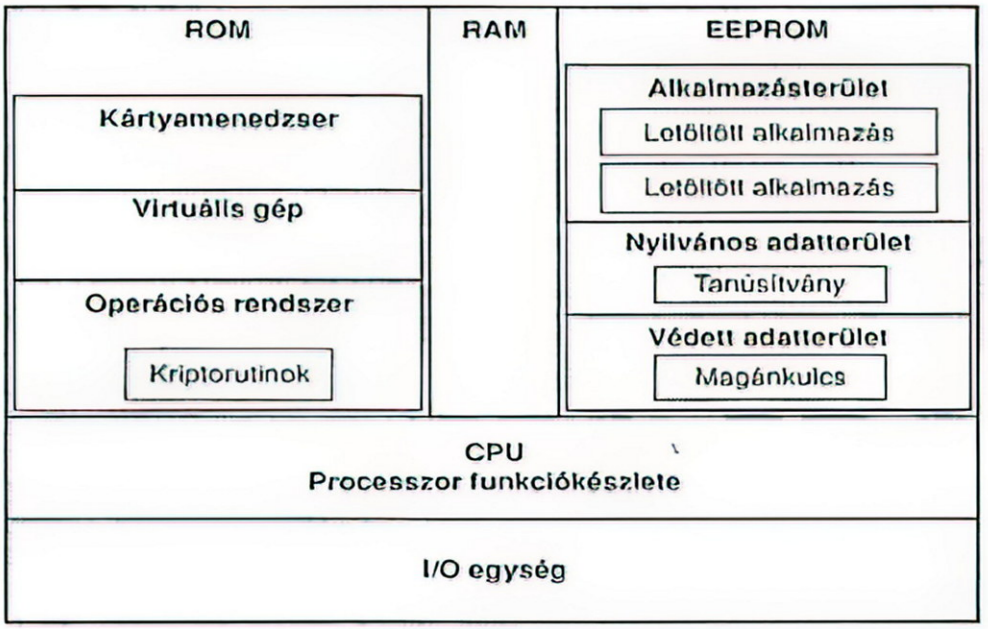
A kártyák számítástechnikai felhasználásához gyártófüggetlen, nyílt platformú megoldások szükségesek, melyek egyedileg telepítendő meghajtóprogramok és bonyolult hókuszpókuszok nélkül működőképesek bármely gépen. A jövő nagy valószínűséggel az elektronikus aláírás területén is a multiapplikációs operációs rendszerrel működő kártyáké.

6.5.1 Multiapplikációs kártyák

A multiapplikációs kártya egy ujjbegynyi méretű számítógép saját processzorral, az olvasóval kapcsolatot biztosító I/O egységgel és memóriával (RAM-mal, ROM-mal és EEPROM-mal). A kártya ROM-ja tartalmazza előre beégetve a kártya operációs rendszerét és különböző, a gyártó által definiált adatokat, a RAM a működés során keletkező temporális adatok átmeneti tárolására szolgál, az EEPROM pedig a kártyára utólag letöltött programok és azok felhasználása közben keletkezett adatok tárolására való.[6] Az EEPROM ugyan lassú, és a beírások száma korlátozott, tartalma viszont a RAM-mal ellentétben a kártyaolvasóból való eltávolításával sem vész el (a kártya számára a tápfeszültséget az olvasó biztosítja).[7]

A multiapplikációs kártyák az operációs rendszer mellett beégetett virtuális gépet és kártyamenedzser-alkalmazást tartalmaznak. Az operációs rendszer ad hozzáférést a kártya fizikai erőforrásaihoz, és tartalmaz olyan alaprutinokat is, mint a kriptográfiai algoritmusok. A virtuális gép az utólag telepített alkalmazások futtatását végzi, számukra biztosít egy binárisan kompatibilis felületet, a különböző operációs rendszerek közti eltéréseket elfedve. A kártyamenedzser feladata az alkalmazások kártyára telepítése, onnan való törlése s a külvilággal való kommunikáció biztonságának általános érvényű biztosítása.

A multiapplikációs kártya legnagyobb előnye, hogy azon több alkalmazás is működhet, egymástól függetlenül, és ezeket az alkalmazásokat utólag is fel lehet tölteni a kártyára ugyanúgy, mint egy személyi számítógép esetében. Ilyen alkalmazás lehet például a SIM modul, egy elektronikus pénztárca vagy hűségkártya-alkalmazás, esetleg egy elektronikus aláírás és rejtjelező algoritmus, amennyiben ezek nincsenek az operációs rendszer szintjén implementálva.



62. ábra
Az intelligens kártya felépítése, aláíró eszközként alkalmazása

6.5.2 Kártyaplatformok

A multiapplikációs intelligenskártya-platformok területén három megoldás verseng egymással: a MasterCard által támogatott MULTOS, a SUN JavaCardja, amit a VISA is szupportál, valamint a Windows for Smart Cards.[8]

A JavaCard voltaképpen a virtuális géppel kezdődik, és ott is ér véget. A virtuális gép alatt bármilyen gyártó bármilyen operációs rendszerrel implementált kártyája dolgozhat, kártyamenedzsert pedig a specifikáció nem definiál. Ezt pótolja többek között a Visa Open Platformja,[9] amely az alkalmazások biztonságos installálásán és törlésén kívül az alkalmazások számára közös PIN-kódra vonatkozóan is szabályokat ad. Az Open Platform kártyafüggetlen specifikáció, melyet a többi platform is követhet.

Így például a Windows for Smart Cards, melyből egyelőre szintén hiányzik a kártyamenedzsment. Lehet ennek oka a nagy spórolás, amivel a Microsoft az alvégekről akar betörni a kártyapiacra. Az olcsóságra törekvés miatt van az is, hogy a WfSC operációs rendszere modulszinten telepíthető a kártya kibocsátója/gyártója által. Ha akarja, ráteszi a SIM funkcionalitást, az elektronikus aláírást, a hitelkártya-funkciókat stb., amire viszont nincs szüksége, azzal nem terheli a kártya szűkös kapacitásait.[10]

Az eredetileg elektronikus pénztárca céljára kifejlesztett MULTOS platform – az előbbiekkel szemben – magában foglalja az operációs rendszert, a virtuális gépet és a kártyamenedzsert is. Az összes platform közül ez tekinthető a legkiérleltebb megoldásnak, ez biztosítja a legmagasabb szintű biztonságot és átjárhatóságot. A MULTOS-kártyák minden implementációjának el kell nyernie az ITSEC E6-os minősítést. Hátránya ugyanakkor, hogy mindhárom megoldás között ez a legdrágább.

A kártyákra tipikusan Javában (cardleteknek hívott), C-ben vagy Visual Basicben kifejlesztett, bájtkódra fordított, és elektronikusan hitelesített alkalmazások telepíthetők (bizonyára kitalálják, melyikre melyik).[11]

Az egységes platform hiánya sajnos egyelőre a kártyák elterjedésének az egyik legnagyobb gátja: egyértelmű győztes hiányában a gyártók haboznak a kártyakezelés hardveres és szoftveres követelményeit termékeikbe beépíteni. Azok csak utólagos olvasóillesztéssel és installálással teremthetők meg, ami a mobilitást erősen korlátozza.[12]

6.5.3 Kártyamenedzsment, biztonság

Azon közösségeknek, amelyek tömeges méretekben alkalmaznak kártyákat vagy más tokeneket, a kulcsok kezeléséhez hasonlóan kártyamenedzsment-rendszerrel is kell rendelkezniük. Ez egyrészt előírásokból és eljárásokból áll, másrészt különböző hardver- és szoftvereszközökből. A rendszernek felügyelnie kell a kártya teljes életciklusát: a megszemélyesítéstől és a kibocsátástól kezdve, az alkalmazások és adatok telepítésén át, a visszavonásig és a megsemmisítésig. A megszemélyesítésnek része a fizikai (nyomtatás, dombornyomás, gravírozás, fényképelhelyezése, hologram stb.) és logikai megszemélyesítés (alkalmazások és adatok kártyára telepítése). A kibocsátásnak része, illetve része lehet a PIN-kód aktivizálása, PIN-boríték nyomtatása és kézbesítése, a kártyatulajdonos és a kártya adatainak regisztrációja. A menedzsment ezen adatok további kezelését is jelenti.

Bár a kártyán történő magánkulcstárolás az egyik legbiztonságosabb módszer, mégsem tökéletesen biztonságos.[13] Léteznek módszerek memóriájának kiolvasására, áramkörének visszafejtésére, amelyek azonban igen komoly műszaki felkészültséget igényelnek. Jóval egyszerűbb lehet a PIN-kód megszerzése egy trójai faló programmal (amennyiben a kód megadása a számítógépen keresztül történik) vagy valamilyen más hagyományos módszerrel. Ezek után már csak a kártya eltulajdonítását kell megoldani, és máris minden adott a visszaéléshez.

6.5.4 Kártyaolvasók

Az intelligens kártyák felosztható a külvilággal való kapcsolattartás módja szerint is. E felosztás szerint léteznek az érintkezős kártyák, amelyek a kártyaolvasónak nevezett interfészen keresztül kommunikálnak, valamint a kontaktus nélküli kártyák, amelyek rádiófrekvenciás jelekkel tartják a kapcsolatot a külvilággal (ezekben a leolvasó készülék által kibocsátott rádiófrekvenciás jel gerjeszt feszültséget). A már említett felhasználási területek mind az előbbiekre jellemzők, az utóbbiak a felhasználóazonosítás és a fizikai beléptetés területén jeleskednek.

A kártyaolvasó lehet önálló egység, amit a soros-, párhuzamos-, billentyűzet-, USB- vagy infravörös porton, PCMCIA sloton keresztül lehet a számítógéphez csatolni, de be lehet építve valamilyen eszközbe is, például a billentyűzetbe, egérbe vagy mobiltelefonba. Kártyaolvasó van beépítve azokba a terminálóknak nevezett feldolgozó egységekbe is, amelyek komplex szolgáltatást nyújtanak a kártya alapú azonosításra építve, a kártyán tárolt adatokat felhasználva. Ilyenek a pénzkiadó automaták, a kártyás fizetést lehetővé tévő POS terminálok és a köztéri webterminálok legújabb nemzedéke.

6.5.5 Kártyaszabványok

Az érintkezős kártyák alapszabványa az ISO/IEC 7816. Ez a tíz részből álló szabvány a kártyák és érintkezőinek fizikai méretétől és paramétereitől kezdve a kommunikációs protokollokon át, egészen a kártyák alapvető I/O parancskészletéig szinte minden alapszintű tényezőt szabályoz. A kontaktus nélküli kártyák alapszabványa az ISO/IEC 14443 (kis távolságon belül használható kártyák) és az ISO/IEC 15693 (nagyobb távolságon belül is használható kártyák). Ezek a fizikai paramétereken és kommunikációs protokollokon túl a használható frekvenciákat és a több kártya együttes kezelésékor fellépő kommunikációs ütközések kezelését is tárgyalják. Kidolgozás alatt vannak a kártyaalkalmazásokat érintő szabványok is.

Míg az említett szabványok alkalmazásfüggetlenek, a kártyák különböző célú felhasználási területei mind kidolgozták a saját szabványaikat. Így a mobil kommunikáció az ETSI GSM 11.11 és GSM 11.14 szabványokban írja le a SIM-kártya adatainak és alkalmazásainak kezelését. A pénzügyi szektor az EMV (Europay-MasterCard-Visa) szabványban tárgyalja az intelligens kártyák bankkártyaként történő felhasználását. A számítógépekkel való felhasználásra ugyanígy léteznek szabványok: az egymással versenyző PC/SC és OCF (Open-Card Framework)[14] szabványok a számítógépen futó alkalmazások számára írja le, hogyan érhetik el a kártyán implementált funkciókat és adatokat.[15] Az előbbi Microsoft-támogatású, és így csak **Windows** környezetben használható (de bármely fejlesztőkörnyezettel), az utóbbi a SUN bábáskodásával született, és így bármely operációs rendszeren működhet (de csak Java alkalmazásokkal).

Az elektronikus aláírás – mint egy speciális felhasználási terület – szempontjából feltétlen megemlítendőek az RSA mindenféle tokenen értelmezett szabványai, a PKCS #11 (Cryptographic Token Interface Standard) és PKCS #15 (Cryptographic Token Information Format Standard), amelyek a tokenen futó kriptoalkalmazások elérését[16] és az ott tárolt kriptoadatok formátumát (magánkulcsok, tanúsítványok) írják le.

A kártyák és általában véve a kriptográfiai modulok (melybe a HSM-ek és különböző tokenek is beletartoznak) biztonsági követelményeit a NIST FIPS PUB 140-1 szabványa írja le, mely négy biztonsági kategóriát definiál. Az 1-es szint a leggyengébb, a 4-es, amelyet csak kevés nem katonai készülék teljesít, a legerősebb.

6.6 Gyártók, árak

Az intelligens kártyák legnagyobb gyártói szinte mind franciák. Ők a kártyagyártás úttörői is: a Gemplus, a Schlumberger (ők ketten a világpiac mintegy kétharmadát uralják) és az Oberthur.[17] Az ismertebb chipgyártók közé tartozik az Atmel, a Hitachi, a Siemens által tulajdonolt Infineon, a Phillips, az ST Mi

croelectronics és még sokan mások.[18] Az USB tokenek egyik legismertebb szállítója az izraeli Aladdin, valamint a kártyákat és olvasókat is gyártó amerikai Spyrus. A HSM modulok gyártói közül kiemelendő a Chrysalis és az nCipher. A gyártók tekintetében is megfigyelhető azonban a szakosodás: vannak kártyagyártók, olvasógyártók, chipgyártók, alkalmazásfejlesztők, beültetők, fizikai megszemélyesítők és így tovább.

A multiapplikációs intelligens kártyák ára ma még több nagyságrenddel meghaladja a mágnescsíkos kártyák árát, de legalább egy nagyságrendnyi különbség a legprimitívebb (például telefonkártyaként funkcionáló) chipkártyákkal szemben is fennáll. Ez a platformtól, a biztonsági szinttől, a memória (elsősorban az EEPROM) méretétől és a biztosított szolgáltatásoktól függően mindenképp több ezer forintot jelent. Egy 32 kbájt memóriával rendelkező multiapplikációs kártya akár tízezer forintot is kóstálhat a felhasználó számára. Nem is olyan nagy ez az összeg ugyanakkor, ha azt nézzük, hogy cserébe egy teljes értékű, többfunkciós miniatűr számítógépet kapunk. Bár terjednek a gyárilag kártyaolvasóval ellátott noteszgépek, billentyűzetek (sőt egérpadok) is, ma még az asztalainkon zümmögő számítógépek többsége nem rendelkezik ilyen olvasóval, ami miatt a kártya árával nagyságrendileg megegyező összegért (nyolctízezer forintért), külön kell ilyen berendezést beszereznünk. Az USB tokenek a kártyákkal összemérhető költségűek, nagy előnyük viszont, hogy nem szükséges hozzájuk külön olvasó, csak a ma már minden új gépen megtalálható USB port (viszont bankkártyaként, SIM-kártyaként stb. nem hasznosíthatók). Az árskála másik végén szokták emlegetni az egy-két dolláros kártyákat, amelyek alatt általában a nem multiapplikációs kártyákat értik. Ilyen kártyák is rendelkezhetnek azonban kriptográfiai szolgáltatásokkal.[19]

Bár a HSM modulok felhasználására csak ipari körülmények között szokott sor kerülni, érdekességképpen megemlítendő, hogy ezek költsége a biztonsági szinttől és az aláírási teljesítménytől függően tipikusan sok millió forintot kóstál.

JEGYZET

1 Nem árt körültekintőnek lenni, mert egyes (ma már elavultnak számító) eszközök nem képesek belső kulcsgenerálásra.

2 A token fogalmát hol általános érvénnyel használják, az intelligens kártyát is beleértve; máskor csak az USB tokenekre gondolva alatta. Az OTP-s tokenkalkulátorok jelen esetben nem értendők a körbe.

3 Mondja ezt a törvény, de ezt a BALE értelemszerűen nem biztosíthatja egyedül. Egy szolgáltató saját rendszerén belül erre figyelhet.

4 A követelmények az eat.-ból valók. A törvénybe belecsúszott egy aprócska, de nagy jelentőségű hiba, melytől az érthetőség kedvéért nagyvonalúan eltekintünk. Az aláíró eszközök ugyanis – ahogy azt már említettem – szinte soha nem képesek az aláírandó dokumentum megjelenítésére, ez az aláíró környezetnek a feladata.

5 Az érmét helyettesítő hagyományos telefonkártyákat nem ide számítva.

6 A ma használatos kártyák esetében a memóriák tipikus mérete a következő: ROM: 16–32 kilobájt, RAM: 1-2 kilobájt, EEPROM:4–64 kilobájt.

7 Vannak olyan kártyák is, amelyek az EEPROM mellett hagyományos mágnescsíkkal vagy lézerrel olvasható memóriacsíkkal is rendelkeznek. Ezek nem védett, de nagyobb kapacitású tárolóterületet biztosítanak, melyet a kártya processzora nem kezel.

8 A megoldások mögött komoly konzorciumok és szervezetek állnak, amelyeknek neves cégek a tagjaik. Itt csak a legfőbb „márkaneveket" említettem meg. További információ: www.multos.com, java.sun.com/products/javacard, www.microsoft.com/smartcard

9 Pontosabban: a GlobalPlatform konzorcium Open Platform elnevezésű specifikációja, amelyet eredetileg a VISA International dolgozott ki VISA Open Platform név alatt.

10 Ez a szabadosság persze azzal jár, hogy a WfSC-kártyák néha önmagukkal sem kompatibilisek.

11 De ha mégsem: JavaCard–Java, Windows for Smart Cards–Visual Basic, MULTOS–C és Java.

12 Hiába rendelkezem saját olvasóval és kártyával, azt egy internetkávézóban képtelen leszek használni, mert az ottani gépre nem dughatom rá, meghajtó programjaimat arra nem telepíthetem fel.

13 A kártya angol terminológiával élve legfeljebb tamper-resistant, azaz babrálásálló tud lenni, de nem tamperproof, azaz babrálásbiztos.

14 További információ: www.pcscworkgroup.com és www.opencard.org

15 Ezek a szabványok (EMV, GSM stb.) is mind az ISO 7816-ra épülnek.

16 Ebből a célból definiálja a Cryptoki nevű fejlesztői felületet.

17 Angol és német zsánerük ellenére ejtsd franciásan, befogott orral: zsemplű, óbertűr és slumberzsé.

18 A kategorizálás a kibocsátott kártyák mennyisége alapján történt, nem multiapplikációs kártyákra specifikusan.

19 Ilyen kártyával jelent meg nemrég a magyar piacon az IBM és az Állami Nyomda.

7 Szabványok

Ajánlás:

Azoknak, akiknek fontos, hogy szabványos megoldást használjanak.
Különösen tanácsadóknak.

Bár a felhasználóktól nem lehet elvárni, hogy ismerjék a téma akárcsak fontosabb szabványait is, számukra is különösen fontos, hogy az általuk használt termékek, melyre sok pénzt adnak ki, szabványosak legyenek. Főleg abban az értelemben, hogy együttműködjenek más megoldásokkal. Valójában szabványos termék csak annyira létezik, mint a minden foltot eltávolító mosópor, vagyis sosem szabad vakon bedőlni a gyártók ilyen irányú állításainak. Minden egyes esetben meg kell vizsgálni, hogy az állítás mire vonatkozik, melyik szabvány(ok)ra a kismillió közül, és az mit jelent adott körülmények között a számunkra. Az, hogy egy elektronikus aláírási termék az X.509-es szabványt támogatja – mely kétségkívül a legfontosabb a téma szabványai között – még messze nem jelenti azt, hogy a termék szabványos, és bármilyen másik, hasonlóan „szabványos" termékkel képes lesz együttműködni.

Jelen fejezetben nem az elektronikus aláírás szabványait gyűjtöttem össze, nem konkrét szabványokat mutatok be, sőt még csak nem is hivatkozom ilyenekre, hanem azokat az ismereteket kívánom megosztani olvasóimmal, amelyek a szabványok rengetegében való önálló boldogulást segítik.

7.1 Mit jelent a szabvány

A szabvány „hivatalosan megállapított és előírt méret, minőség, norma".[1] Eme meghatározásnak megfelelően én sokáig hittem azt, hogy a szabvány valamiféle egyediséget jelent, de ez korántsincs így. Ott vannak például a mindenki által ismert mértékegységszabványok: a méter, a liter, a kilogramm és cimboráik, ami annyira természetes volt számomra, mint a tízes számrendszer vagy az arab számok (melyek bizonyos értelemben szintén szabványnak tekinthetők). Aztán rá kellett jönnöm, hogy egyes civilizálatlan népek még mindig lábban és mérföldben mérik a távolságot, gallonban az űrmértéket, fontban a tömeget, mi több, némelyikük az út bal oldalán közlekedik. Mivel ugyanezen népek tettek a legtöbbet a kriptográfia és az elektronikus aláírás területén is, sokkal jobb helyzet itt sem várható.

7.2 Szabványok tengere

Sőt a helyzet még talán rosszabb is. Annak, aki szabványos elektronikus aláírási, kriptográfiai megoldásba vágja a fejszéjét, fel kell készülnie arra, hogy jó néhány csapásra lesz szüksége, míg megbirkózik a feladattal. Ha más nem is, annyi bizonyára látszódik a könyvből, hogy a nyilvános kulcsú infrastruktúra igen összetett. Ha ennek az összetett infrastruktúrának és az ezt működtető mechanizmusoknak valamely tagja nem ért szót a másik taggal, akkor az az egész rendszer működőképességét lehetetleníti el. Olyan szabvány viszont nem létezik, amely a teljes szisztémát szabályozná. Léteznek ehelyett szabványok, kvázi szabványok, ajánlások százszámra, amelyek között az eligazodás igazán emberpróbáló feladvány. Különösen, hogy sokszor nem matematikai, informatikai vagy más szakmai ismérvei miatt kerül előtérbe egy-egy szabvány.

A dolog mögött valószínűleg az a lexikonbeli meghatározásból is kitetsző félreértés áll, hogy a szabványosítás egy hivatalos tevékenység. Bár ez bizonyos körülmények között igaz is lehet, a valóság azonban mégiscsak az, hogy ez a tevékenység ugyanolyan üzlet, mint minden más, és itt is mindent a pénz, a hatalom és az érdek mozgat. Szabványosítási szervezetet tulajdonképpen bárki létrehozhat, legyen az egy kormány, egy nemzetközi szervezet, szakmai testület, bármilyen cégcsoportosulás vagy akár egy ipari vállalkozás is. Ha bármi is predesztinálja arra, hogy komolyan vegyék, vagy az elismerést ügyesen kiharcolja, akkor tényked ése igen zsíros biznisz tud lenni: pénzt kér a szabvány kidolgozásáért vagy elbírálásáért, ügyintézésért, a megfelelőség ellenőrzéséért, meg amiért még nem szégyell, sőt pénzt kér a szabvány minden egyes elektronikus és papír alapú változatáért azoktól, akik azt fel akarják használni, vagy csak egyszerűen meg akarják ismerni.

Így aztán vannak szabványosítási szervezetek, amelyeket komolyabban lehet venni, és vannak, amelyeket kevésbé. Vannak függetlenek és kevésbé függetlenek, és az általuk létrehozott szabványok ugyanúgy versenyeznek egymással a piacon, mint minden más termék. A versenyben pedig sokszor nem a műszaki ismérvek döntenek, hanem a szabvány mögött felsorakozó gazdasági erő és egyéb érdekek. Egy szabvánnyal kapcsolatban a legfontosabb ismérvek ezért a tartalmán túlmenően, azt meg is előzve, hogy: ki dolgozza ki, ki nyújtja be szabványosításra (mert a benyújtó sokszor nem ugyanaz a szervezet, mint amely kidolgozza), hogy melyik szervezet szabványosítja, és ez kire nézve kötelező, kire ajánlás, és kire az sem, illetve hogy melyik szervezetek és országok veszik át automatikusan, és melyek egyedi eljárás keretében.

7.3 Szabványosítási szervezetek

Hogy eligazodjunk az így létrejövő dzsungelben, először is meg kell ismernünk a legfontosabb szabványosítási szervezeteket. A legismertebb szabványosítási szervezetek az elektronikus aláírás területén is a nemzetközi szabványügyi testü-

letek, melyek vagy szakterületektől független mamutszervezetek, vagy egy-egy internacionalista szakmai társulás, kamara által létrehozott, az adott szakma kérdéseire koncentráló szervezetek. E szervezetek által létrehozott szabványokat a szabványosítási szervezethez csatlakozó nemzetek vagy nemzeti szervezetek általában automatikusan átveszik, és „otthoni" használatát kötelezővé teszik jogszabályi vagy szabályzati szinteken saját állampolgáraik, tagjaik számára. A nemzetközi szervezeteknek létezhetnek az egyes országokban saját szabványosítási szervezeteik is, illetve tőlük független társulások is csatlakozhatnak hozzájuk.

7.3.1 Nemzetközi és amerikai szervezetek

A legfontosabb ilyen nemzetközi szervezet az ISO (International Organisation for Standardisation), melynek Magyarország a Magyar Szabványügyi Testületen keresztül tagja. Az internacionalista szakmai szervezetre jelen esetünkben az első számú példa a Nemzetközi Telekommunikációs Egyesület, az ITU (korábbi nevén CCITT), mely ugyanúgy az ENSZ égisze alatt működik, mint a nála sokkal nagyobb ismertségnek örvendő IMF, WTO vagy UNICEF (mely szervezetek az elektronikus aláírás szempontjából irrelevánsak). Második számú példa az IEC (International Electrotechnical Commission), amely az ISO-t „helyettesíti" az elektrotechnológiai szabványosítás területén (szintén az MSZT képviseli Magyarországon).

Mivel a bizalmas és hiteles kommunikáció a kereskedelem egyik alappillére, a Nemzetközi Kereskedelmi Kamara (ICC) szintén szerepet tölt be az elektronikus aláírás szabványosításának területén. Még komolyabb szabványosítási tevékenységgel bírnak a W3C (World Wide Web Consortium), az IETF (Internet Engineering Taskforce) és az IEEE (Institute of Electrical and Electronics Engineers) független szervezetek (az előbbinek cégek a tagjai, az utóbbiaknak magánszemélyek).

Amerikában a legmérvadóbb szabványosítási szervezetnek az ANSI (American National Standards Institute), az ISO amerikai tagszervezete és a NIST (National Institute of Standards and Technology) számít.[2]

Az egyes szervezeteken belül külön csoportok és alcsoportok foglalkoznak az elektronikus aláírással kapcsolatos kérdések szabványosításával. Így például az ANSI-n belül az X9 munkacsoport, az IETF-en belül pedig a PKIX munkacsoport.

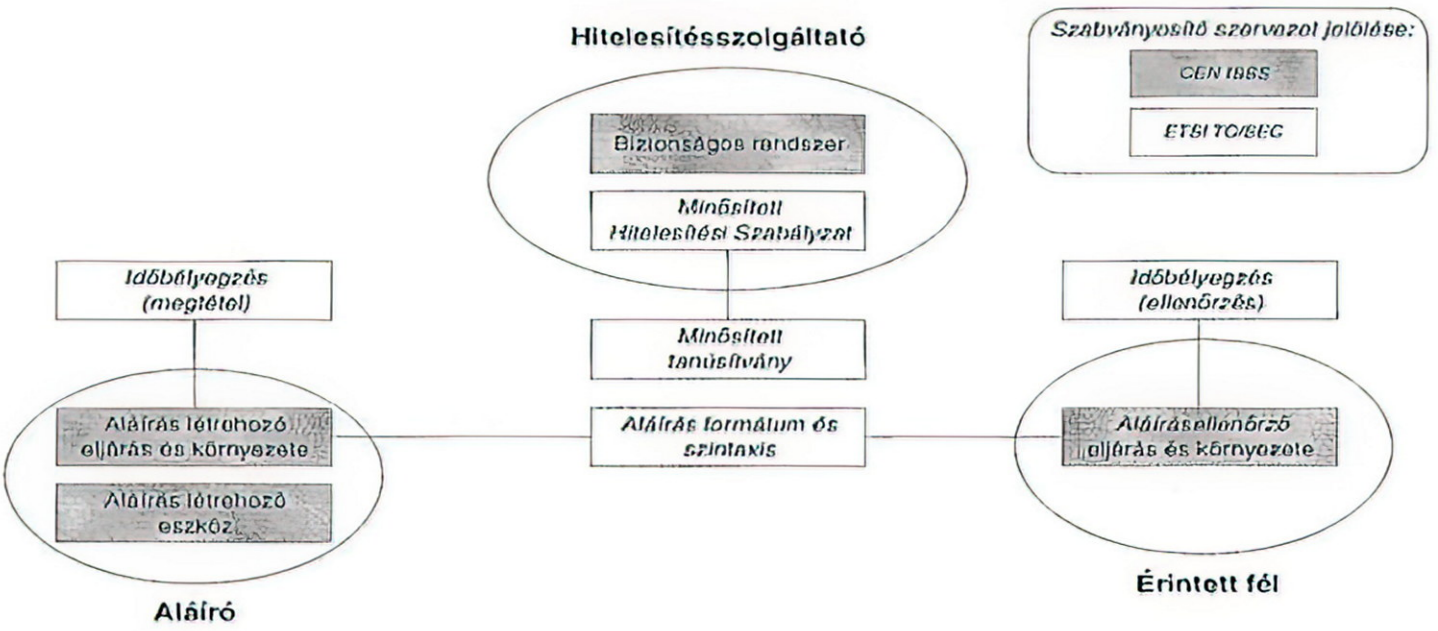
7.3.2 Európa – EESSI

Európában az elektronikus aláírás területén az Európa Tanács határozatának megfelelően az ICTSB (European Information and Communications Technology Standards Board) által létrehozott EESSI (European Electronic Signature Standardization Initiative) kezdeményezés a legaktívabb, melybe több európai és nemzetközi szabványügyi testület is bedolgozik, így az ETSI (European Telecommunications Standards Institute), a CEN (Comité Européen de Normalisa-

tion), az IETF és az EA (European cooperation for Accreditation) is[3]. Az EESSI feladata, hogy kidolgozza azokat a szabványokat és ajánlásokat, amelyek az EU elektronikus aláírásról szóló irányelvében megfogalmazott általános elvek és követelmények alsóbb, szakmai szintű kifejtéseinek tekinthetők. Ezek vagy konkrét műszaki megoldások, vagy olyan követelmények, melyeket követni kell a „szabványos" címre törekvő termékeknek.

Az EESSI szabványosítási tevékenysége az egyes tagszervezetekhez vannak delegálva. Szabványosítási céljai közül a legfontosabbak a minősített tanúsítványok kibocsátását végző hitelesítésszolgáltatók megbízható rendszereire vonatkozó biztonsági követelmények definiálása; az általuk alkalmazott biztonsági menedzsmenttel és hitelesítési szabályzattal kapcsolatos elvárások lefektetése; az X.509 tanúsítványok minősített tanúsítványként való felhasználására vonatkozó szabványok; a biztonságos aláírás-létrehozó eszközökre vonatkozó biztonsági és garanciális követelmények meghatározása; általában az aláíró és ellenőrző eszközökre vonatkozóan specifikációk és ajánlások készítése; az elektronikus aláírás szintaxisára és kódolásra vonatkozó formátumok megalkotása és az időbélyegzés szolgáltatással való együttműködést szabályozó protokollok kidolgozása.

Ezenkívül számtalan más kezdeményezés is igyekszik újabb szabványokat alkotni vagy más módon biztosítani a termékek, szabályzatok és jogi keretek kompatibilitását. Ilyen például az EEMA (European Forum for Electronic Business) szervezésében létrejött projektek, a pki Challenge, az ESPRIT és a TELEMATICS projekt keretein belül futó ICE-CAR (az ICE-TEL utóda).



63. ábra Európai szabványosítási törekvések

7.3.3 Vállalati szabványok

Az egyes szabványügyi szervezeteken kívül sokszor maguk a technológiában élen járó vállalatok vagy más szervezetek is kidolgoznak szabványokat. Ezek

sokszor nem is szabványnak készülnek, hanem megoldásnak, de annyira elterjednek, hogy kvázi (de facto) szabványnak tekinthetők. Máskor a vállalat be is nyújtja egy szabványosítási szervezetnek a megoldását, ami azt de jure is szabványosítja. Ezek a vállalati szabványok rendszerint sokkal gyakorlatiasabbak, mint az elméletből kiindulva aprólékosan kidolgozott, sok egyeztetést átélt, „igazi" szabványok. Magyarul megmondva: nemegyszer kevésbé fejlett megoldást képviselnek. Sokszor mégis képesek legyőzni a hivatalos szabványokat, hiszen egyszerűbben implementálhatóak, és működő termékekben hamar képesek testet ölteni. Márpedig a gyorsaság ezen a területen is felér egy fél győzelemmel.[4] Ennek ellenére, még az is lehet szerencsés eset, ha egy ilyen fejlettebb megoldás elbukik, és romjain csökevényesebb társa virágzik. Mert van még egy ennél is rosszabb variáció: mikor egy bizonyos probléma megoldásaként két vagy több szabvány verseng egymással, s így megosztva a piacot valójában egyik sem válik igazán „szabványossá" (lásd: intelligens kártyák esete). Egy ilyen helyzet egy egész iparág fejlődését visszavetheti.

Az elektronikus aláírás és titkosítás területének legismertebb szabványosító cégei a Baltimore, az Entrust, az RSA, a Microsoft, a Netscape és a Verisign, vagyis a piac meghatározó szereplői. Közülük is feltétlen ki kell emelni a már többször is említett RSA-t, mely az RSA algoritmuson túl is számtalan hőstettel vívott ki magának elismerést. Az általa úttörő jelleggel kidolgozott és széles körben implementált PKCS szabványcsalád, melyet időközben „igazi" szabványok is átvettek, felhasználtak vagy beépítettek önmagukba, immár tizenöt tagot számlál.[5]

7.4 Szabványok, specifikációk, ajánlások

7.4.1 A szabványosítás területei

A szabványok követése nemcsak azért nehéz feladat, mert sok van belőlük, és állandóan újak keletkeznek, hanem mert ezek bonyolult viszonyban is állnak egymással. Egyes szabványok egymásra épülnek, mások tovább finomítják társaikat vagy az általuk kihagyott lyukakat foltozzák, megint mások egyszerűen felüldefiniálják elődeiket. Az egyes szabványok így nemcsak megszűnnek, de mindegyiknek – akárcsak a programoknak – több verziója is van, amiket folyamatosan követni kell. Az összes, témába vágó szabvány ismertetése így nemcsak terjedelmi okokból volna lehetetlen, de gyors idejét múlása miatt is értelmetlen volna.

A szabványosítási törekvések olyan széles körűek, hogy csak a területek felsorolása is komoly vállalkozásnak tekinthető. Azért vágjunk bele:

- Tanúsítványok, visszavonási listák, aláírások, időbélyegzők formátuma.
- Aláírási, rejtjelezési, lenyomat és véletlenszám-generálási algoritmusok.
- Tanúsítványtárra vonatkozó szabványok.
- Fejlesztői interfészek definiálása.

- Biztonságos böngészésre, levelezésre és egyéb, kommunikációra vonatkozó protokollok (mint az elektronikus aláírás és titkosítás felhasználási lehetőségei).
- Aláíró és aláírás-ellenőrző eszközökre vonatkozó specifikációk meghatározása.
- Szabályzatokra vonatkozó elvárások és ajánlások.
- Hitelesítésszolgáltatók rendszereire és gyakorlatára vonatkozó követelmények.
- Kulcsmenedzsmentre vonatkozó előírások.
- Minősített tanúsítványra vonatkozó szabványok.
- Elektronikus aláírás megtételének és ellenőrzésének szabályai.
- És minden más, amiről már e könyvben volt szó.

Bár sorolhatnék mindegyikre példákat, ezt most nem teszem meg. Az egyes témák tárgyalásánál a legfontosabb odavágó szabványokat viszont megemlítettem.

7.4.2 A szabványosítás szabványtalansága

A szabványosítás területén minden szervezet a saját feje után megy, így ez a tevékenység, bármenyire hatásvadásznak tűnik is a kifejezés, teljesen „szabványtalan". Sorvezetőnek szánva nézzük meg a legfontosabb szervezetek által követett gyakorlatot, illetve ennek a szabványok kibocsátására vonatkozó részét:

Az ITU X.*xxx* elnevezéssel dobja piacra szabványait (például X. 509, X. 500, X.660). Az IETF az „RFC *xxxx*" megnevezést használja (például RFC 2459, RFC 2630, RFC 2634), mely neve ellenére („request for comment") igazi szabványt jelent. Még nem végleges szabványterveinél a PKIX elnevezést használja, ami a szabványokért felelős munkacsoport nevére utal. Az IETF mindenképp kiemelendő a sorból, mert szabványai szabadon hozzáférhetőek, s a szabványosítási tevékenységbe magunk is bekapcsolódhatunk. Az ANSI az ANSI X9.*xx* elnevezést követi elektronikus aláírással kapcsolatos szabványai tekintetében (például ANSI X9.17, ANSI X9.31, ANSI X9.62). A CEN a CWA *xxxxx* névformátumot használja (például CWA 14167, CWA 14172), ami a „CEN Workshop Agreements" kifejezés akronimja, az ETSI pedig a TS *xxx xxx* elnevezést (például TS 101 456, TS 101 733), ahol a TS a „Technical Specifications" megfelelője. Az RSA a PKCS sorozatát PKCS #1 és PKCS #15 között bocsátotta eddig ki, de a család még szaporodhat. A NIST a FIPS PUB *xxx* elnevezést követi (például FIPS PUB 180, FIPS PUB 186), amely a „Federal Information Processing Standards Publication" kifejezésre utal, az IEC pedig, mivel az ISO-val karöltve adja ki szabványait, az ISO/IEC *xxxxx* (például ISO/IEC 8824, ISO/IEC 10181) elnevezést követi.[6]

Az egyes szervezetek weboldalain a szabványok ennek megfelelően hozzáférhetőek, de a legtöbb helyen fizetni kell értük. Sajnos olyan oldalt nem tudok ajánlani, ahol az elektronikus aláírásra vonatkozó szabványok szervezeteken átívelve, naprakészen, csoportosítva és az egymáshoz való függőségi viszonyokat feltárva össze lennének gyűjtve. Ennek kidolgozása valószínűleg egy külön tanulmány tárgya lehetne[7].

JEGYZET

1 Az Officina egyetemes lexikon meghatározása.

2 A szervezetek webcímei: www.iso.ch, www.mszt.hu, www.itu.int, www.iec.ch, www.ietf.org, www.w3.org, www.ieee.org, www.iccwbo.org, www.ansi.org, www.nist.gov

3 A szervezetek webcímei: www.ict.etsi.fr/cessi/EESSI-homepage.htm, www.etsi.org, www.cenorm.be/isss/Workshop/e-sign

4 Ez történt korábban az X.500 címtár és X.400 levelezési szabványokkal és az OSI hálózati protokollal, amiket az LDAP, a MIME és a TCP/IP győzött le. A kriptográfia területéről ilyen például a S-HTTP-t két vállra fektető SSL protokoll.

5 Igaz, néhány ezek közül már érvénytelen. Információ: http://www.rsasecurity.com/rsalabs/pkcs

6 Ettől eltérő elnevezések is előfordulnak az egyes szervezetek egyes munkacsoportjain belül, főleg a munkaváltozatok esetében. A CEN ISSS munkacsoportja például a WS/E-Sign) N xxx elnevezést követi a Workshop on Electronic Signatures kifejezésre utalva.

7 A legjobb, ami ehhez a vágyálomhoz hasonlít: http://www.pki-page.org/

8 Szabályzatok

Ajánlás:

Mindenkinek (bár száraznak tűnhet).

A szabályzat, definíciója szerint, „valamely szakterület valamennyi érvényes előírásainak összessége; például szolgálati, munkahelyi, sportszabályzat".[1] Az elektronikus aláírásnak, mint szakterületnek, ugyanígy megvannak a maga szabályzatai. Ezen szabályzatok nagy része a hitelesítésszolgáltatásra, kisebb része pedig az elektronikus aláírás megtételére és ellenőrzésére vonatkozik.

A szabályzatok a biztosítási szerződések helyi megfelelői, sőt bármennyire hihetetlen, mind terjedelemre, mind emészthetetlenségre messze felülszárnyalják azokat. A sokszor több száz oldalnyi műszaki, jogi és eljárásrendi fejtegetés között azonban igen fontos információk bújnak meg. Például hogy milyen anyagi felelősséget vállal a tanúsítvány kibocsátója abban az esetben, ha, mondjuk, a kibocsátott tanúsítvány mégsem annak lett volna kiadva, aki fel van benne tüntetve tulajdonosként. Vagy milyen kötelezettségei vannak a közösség szereplőinek, és hogyan kell értelmezni a tanúsítványban feltüntetett adatokat. Ezen információk nélkül az elektronikus aláírás megtétele és ellenőrzése voltaképpen a közlekedési szabályok ismerete nélküli vezetéshez hasonlítható.[2]

8.1 A szabályzatok forrásai

A szabályzatok azonban mégis inkább a biztosítási szerződéshez hasonlíthatók, mint a KRESZ-hez, mert nem törvényi szabályozásra vagy más, általánosan elismert előírásokra gondolok alattuk. Itt is minden egyes közösségnek saját szabályzata van. A szabályzatok legfontosabb forrása a hitelesítésszolgáltató, de nem biztos, hogy ő az egyetlen, akinek a szabályzatait követnie kell a felhasználóknak. Így minden egyes országban lehetnek hatóságilag létrehozott szabályzatok, melyek például a minősített aláírás kezelését szabályozzák vagy az állami szervekkel való elektronikus kapcsolattartást. A közösség követhet egy szabványügyi szervezet által létrehozott szabályzatot is, vagy maga is dolgozhat ki ilyen szabályzatokat. Ezenkívül a felhasználó munkáltatója (az a szervezet, mely számára a tanúsítványt biztosítja) is előírhat különböző szabályokat.

A felhasználóra érvényes szabályokról a hitelesítésszolgáltatónak kötelessége tájékoztatást adni. Az aláíró számára a tanúsítvány igénylésekor szóban és írásban, az aláírás elfogadóinak pedig a tanúsítványba foglalt utalás segítségével. Ez az utalás egy szöveges figyelmeztetés mellett tartalmazza a szabályzatok elérhetőségi helyét (webcímét, illetve e-mail- vagy postacímet, ahonnan be-

szerezhetők). Az aláírás ellenőrzője az elfogadást megelőzően itt tájékozódhat a tanúsítvány által szavatolt garanciák mértékéről.

8.2 A szabályzatok megjelenési formája

A szabályzatok számos formában megjelenhetnek előttünk attól függően is, hogy ki alkotta meg őket: ölthetnek jogszabályi külsőt, szabvány előírást, szerződéses alakot, szabályzat, tájékoztató, üzleti és technikai dokumentáció, eljárásrend, utasítás formáját.

A szabályzatok nyilvános, belső és titkos minősítést kaphatnak. A nyilvános dokumentumokat meg kell ismertetni, illetve lehetővé kell tenni a megismerését a közösség minden tagja számára. A belső dokumentumok a hitelesítésszolgáltató vagy a szervezet adott területen dolgozó munkatársai, alvállalkozói, beszállítói, partnerei számára elérhetők, míg a titkos dokumentumokat csak meghatározott személyek ismerhetik és kezelhetik (egyéb szabályzatokban szabályozott elvek szerint).[3]

A szabályzatok sokféleségének és nagy terjedelmének legfontosabb oka nem a technológia összetettsége, hanem a szereplők sokasága s az ő eltérő érdekeik, amelyeket mindegyik védeni akar, megfelelően körülbástyázva magát az őt fenyegető veszélyek ellen.

8.3 A szabályzatok szerepe

A nyilvános és belső (beleértve a titkos minősítésűeket is) szabályzatoknak – gondolva itt elsősorban a hitelesítésszolgáltató szabályzataira – eltérő szerepük van. Mindkettőre igaz ugyanakkor, hogy egy írott és alkalmazott szabálygyűjteményről beszélünk, amely a nyilvános kulcsú infrastruktúra elveinek és eljárásainak használatát rögzíti, párosítva a veszélyek (és az általuk okozható kár) mértékét az elhárításuk érdekében kifejteni szükséges kontrollal. Vagyis mindkettő tartalmaz tájékoztató jellegű információkat, szabályok leírását, szerepek meghatározását, bizonyos cél érdekében követendő cselekmények (azaz eljárások) leírását. A belső dokumentumok azonban kizárólag a szolgáltató szervezeteire (hitelesítési, regisztrációs stb.) és munkatársaira vonatkoznak, az ő feladataikat, kötelezettségüket és felelősségüket szabályozzák, míg a nyilvános dokumentumok emellett az aláírók és az ellenőrzők részéről is tárgyalja ugyanezeket.

A nyilvános dokumentumoknak azonban van egy másik szerepük is azon túl, hogy a felhasználók számára használati utasításként funkcionálnak. Ez pedig a bizalom megalapozása (ez, ami igazán felszaporítja az oldalak számát). Egy hitelesítésszolgáltatás esetében, különösen ha az kereskedelmi szolgáltatásként (megbízható harmadik fél alapon) valósul meg, alapkérdés a bizalom. A bizalmat a szolgáltató azon a képen keresztül tudja megteremteni, amit magá-

ról és szolgáltatásairól a külvilág felé közvetít. Ennek a képközvetítésnek az egyik eszköze (a marketinghalandzsa mellett) a szolgáltató által követett gyakorlat nyilvánosságra hozatala. Ha a szolgáltató leírja, milyen, biztonságot garantáló eszközöket és módszereket használ, milyen személyzettel dolgozik, milyen adminisztrációs és informatikai rendszere van és így tovább, mindent, ami a szolgáltatás komolyságát hangsúlyozhatja, a felhasználók bizalma akkor is ugrásszerűen megnő, ha nem értik teljesen pontosan, mi mit jelent.

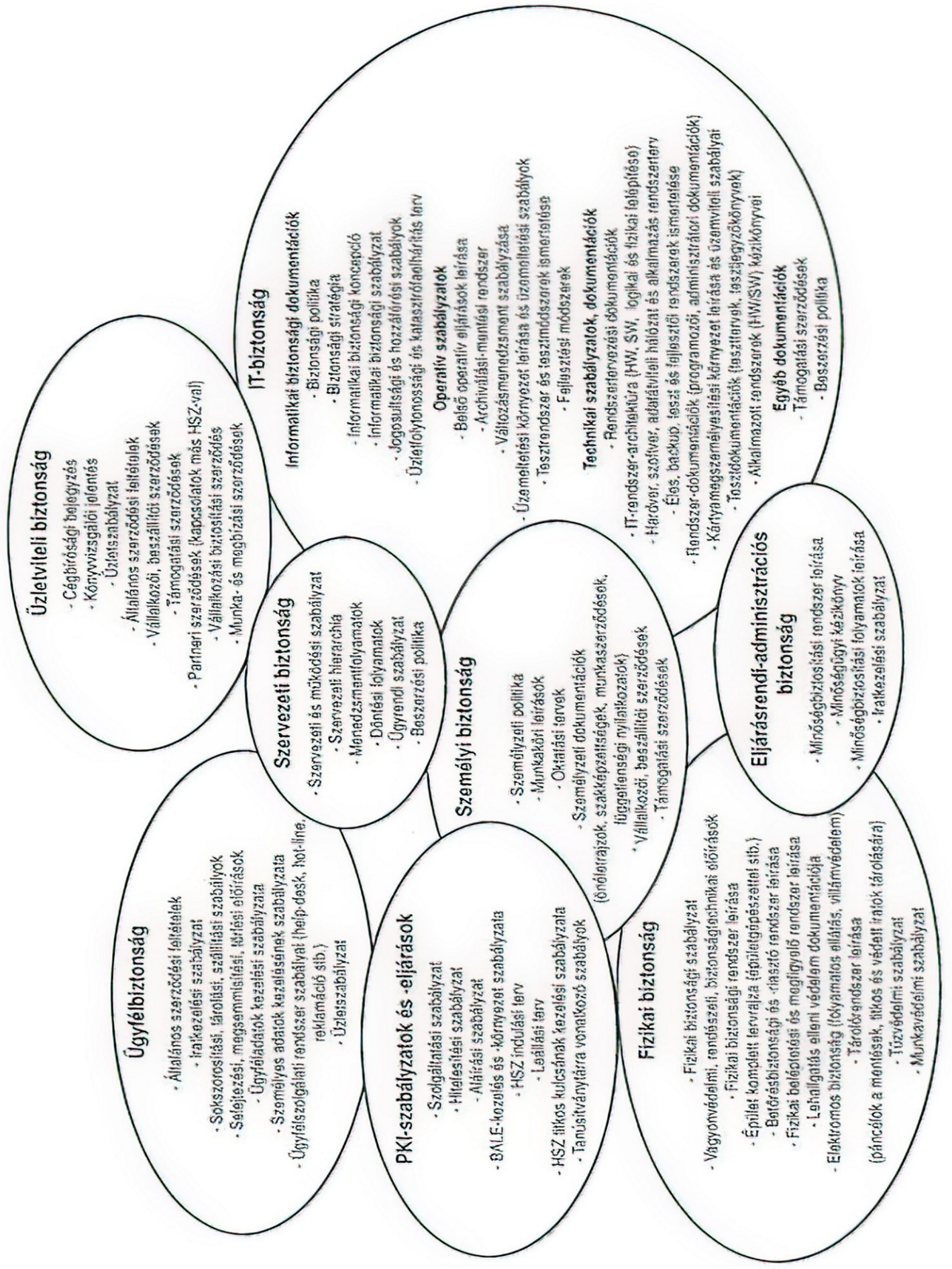
A hatósági és auditvizsgálatok szempontjából a nyilvános dokumentumok szerepe nem igazán jelentős, hiszen ők a belső dokumentumokhoz is hozzáférnek. A külső szakértők, újságírók és bármely hozzáértő szakember számára viszont ezek a dokumentumok is sokat mondanak, hiszen ők a benne leírtakat értik, és képesek összehasonlítani azt más szolgáltatók és különböző ajánlások ide vonatkozó leírásaival, követelményeivel. Ez alapján a rendszer biztonságának a mértékét elég pontosan meg tudják állapítani, s ezeket az információkat amolyan civil kontrollként meg tudják osztani a nagyközönséggel.

Hogy a nyilvános dokumentumokban leírtak igazak, azt hatósági ellenőrzések és független auditok garantálhatják. Ezen vizsgálatok során a szakértők, akik a megvalósítást minősítik, ezeket a dokumentumokat hasonlítják aztán össze a szolgáltató gyakorlatával s várják el a neki való megfelelést.

8.4 Szabályzatok egymás hegyén-hátán

A szabályzatok architekturális és működési terveket generálnak; adminisztrációs és dokumentációs követelményeket állítanak fel; meghatározzák a nyilvános kulcsú infrastruktúra elemeit és azok külső-belső együttműködését, a közösség egyes tagjainak kötelezettségeit, felelősségét és jogosultságait; leírják, milyen osztályú és típusú tanúsítványok léteznek, ezeknek mi a tartalma; kulcsmenedzsment-kérdéseket szabályoznak; szervezeti, menedzsment- és működtetési szabályokat alkotnak és így tovább, folytatni lehetne a sort még sokáig. A helyzet összetettség tekintetében a szabványokéhoz hasonló: a különböző kérdéseket különböző dokumentumok szabályozzák, melyekkel itt is tengert lehetne rekeszteni. Az egyes dokumentumok egyrészt logikailag különülnek el egymástól, másrészt az azokat hasznosító személyek és az ezzel összefüggésben lévő bizalmassági szabályok szerint (nyilván nem lehet egy dokumentumba rakni olyan témákat, amelyek különböző részeihez különböző emberek férhetnek hozzá).

Az alábbi ábra e dokumentumokról ad egy elrémisztő képet, a biztonság különböző szegmenseibe csoportosítva őket (némely, több témával is összefüggésben lévő dokumentum több halmazban is megjelenik).



64. ábra Szabályzatok rendszerezése

8.5 Fontosabb szabályzatok

Mielőtt rituális öngyilkossági hullámot indítanék el, gyorsan megnyugtatom olvasóimat, hogy e dokumentumok mindegyikét nem ismertetem, annál is kevésbé, mert legtöbbjük nem nyilvános, és így kevés az esélyük arra, hogy ezekkel találkozzanak. Mindössze négy fontosabb szabályzat ismertetését tervezem: a hitelesítésszolgáltatáshoz kötődő szolgáltatási szabályzat, a hitelesítési szabályzat és az általános szerződési feltételek mellett az aláírási szabályzatét,[4] mely a szolgáltatástól független szokott lenni.

A szolgáltatóknak kötelezően rendelkezniük kell szolgáltatási szabályzattal és általános szerződési feltételekkel, melyekről kötelességük tájékoztatni a szolgáltatást igénylőt, s azokat minden felhasználó (beleértve az érintett feleket is) számára szünet nélkül elérhető és biztonságos módon[5] elektronikusan publikálniuk kell. A szabályzatokban történt változásokról a szolgáltatónak kötelessége tájékoztatni a közösséget a változás életbe lépését megelőzően. A szabályzatokat egyedi objektumazonosító azonosíthatja.

8.5.1 Szolgáltatási szabályzat

Az elektronikus aláírás törvény szerint a „szolgáltatási szabályzat a szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat", míg egy másik definíció úgy fogalmaz, hogy a „szolgáltatási szabályzat azoknak a gyakorlatoknak a nyilatkozatként megfogalmazott dokumentuma, melyeket a hitelesítésszolgáltató a tanúsítványok kibocsátása és kezelése folyamán alkalmaz".[6]

Mindkét meghatározás jó, de legjobb, ha a szolgáltatási szabályzat céljából indulunk ki: a szolgáltatási szabályzat célja, hogy összefogja azokat a szabályzatokat és információkat, melyeket a hitelesítésszolgáltatóval valamilyen módon kapcsolatba kerülő feleknek (elsősorban az aláíróknak és az aláírás-ellenőrzőknek) tudni érdemes. Mint ilyen, a szolgáltató működésének átláthatóságát biztosítja, s lehetővé teszi a felhasználók számára, hogy megállapítsák, annak gyakorlata, illetve adott tanúsítványosztálya és -típusa mennyiben felel meg az elvárásaiknak. A szolgáltatási szabályzat ellenőrzésével a tanúsítvány elfogadóinak egyértelműen meg kell tudni állapítani a tanúsítvány kezelésének módját, az általa garantált biztonság mértékét és az erre vonatkozó technikai, üzleti és pénzügyi garanciákat, jogi felelősségvállalásokat.

A szolgáltatási szabályzat éppen ezért egy rettentő édes-savanyú-keserű-csípős vegyes saláta, mely részben a szolgáltató önálló deklarációja, részben törvényi szabályozások és kötelezően előírt vagy önkéntesen alkalmazott szabványügyi előírások együttese, és részben magánjogi szerződés formáját ölti a szolgáltatóra és felhasználókra vonatkozó előírások felsorolásával (a jogi rész magyar viszonylatban kevésbé hangsúlyos az általános szerződési feltételek mellett). Így különlegesen pikáns keveréke biztonsági, kriptográfiai, informatikai, jogi, üzleti és egyéb kinyilatkoztatásoknak.

A szolgáltatási szabályzat tartalma meghatározza, hogyan épülnek fel, és miképp működnek az egyes (közös struktúrába szerveződő) hitelesítő- és regisztrációs egységek, bemutatja logikai és fizikai kapcsolatukat, az egyes modulok feladatait, kommunikációját, az azonosítást és egyéb biztonsági funkciókat. Szabályozza a kulcsmenedzsmenttel és a tanúsítványok kezelésével kapcsolatos kérdéseket, meghatározza a szolgáltató üzleti és jogi viszonyát ügyfeleivel és az érintett felekkel kapcsolatban. Leírja a szolgáltató és a tanúsítványt felhasználó felek kötelezettségeit és felelősségi körét, a felelősség mértékét, megosztásának, korlátozásának módját, ismerteti a szolgáltató pénzügyi felelősségvállalását és a kártérítési kötelezettség körülményeit. Felsorolja azokat a hitelesítési szabályzatokat és a bennük definiált tanúsítványosztályokat és -típusokat, melyek kezelését tárgyalja.

8.5.2 Hitelesítési szabályzat

A hitelesítési szabályzat (használatban van a tanúsítványtípus megnevezés is) szerepe nem annyira letisztult, mint a szolgáltatási szabályzaté. Több felfogás is él egymás mellett, melyek mind a szolgáltatási szabályzattal kapcsolatban igyekeznek valamilyen módon hírbe hozni a hitelesítési szabályzatot. Az egyik definíció szerint a hitelesítési szabályzat „szabálygyűjtemény, mely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára".[7] Egy másik definíció azt mondja, hogy „a hitelesítési szabályzat egy adott közösségen belül definiálja a szereplőket, egymáshoz való viszonyukat és kötelezettségeiket, valamint az elfogadható felhasználási módszereket".[8]

Az egyik felfogás szerint a hitelesítési szabályzat követelményeket állít fel a szolgáltató (például ellenőrzések, naplózások, értesítések), az aláírók és az aláírást ellenőrzők irányában, a közösség minden résztvevője számára definiálja jogaikat, feladataikat és kötelességeiket. A másik felfogás szerint pedig a hitelesítési szabályzat az egyes tanúsítványtípusok jellemzőit írja le (ezért használt a tanúsítványtípus elnevezés is). A két felfogásnak lehet közös metszete, hiszen a követelményrendszer ki lehet dolgozva tanúsítványtípusonként is. A hitelesítési szabályzat alapja lehet több szolgáltató együttműködésének, amennyiben mindannyian annak egy szabványosított, illetve közösen elfogadott példányát alkalmazzák, vagyis abból levezetve, az ott meghatározott követelményeknek megfelelve dolgozzák ki gyakorlatukat (és az azt leíró szolgáltatási szabályzatukat). Ilyen esetben a különböző szolgáltatók által kibocsátott, de ugyanazon hitelesítési szabályzatnak megfelelő tanúsítványok automatikusan megfeleltethetőek egymásnak kereszt-, illetve felülhitelesítés alkalmával. Ez azért fontos, mert így az elektronikus aláírást kezelő alkalmazások automatikusan elfogadhatják a másik szolgáltató egyenértékűnek elismert tanúsítványát (amennyiben a két szolgáltató között valamilyen hiteles viszony áll fenn). A hitelesítési szabályzat ebből következően lehet a szolgáltatótól független szervezet által kiadott és kezelt is.

8.5.3 Aláírási szabályzat

Az aláírási szabályzat „szabálygyűjtemény, mely adott szerződéses és/vagy jogi keretek között érvényesnek tekinthető elektronikus aláírás készítését és ellenőrzését határozza meg”[9], szól első definíciónk. De van egy másik is azok összezavarására, akik ezt esetleg megértenék: az aláírási szabályzat „olyan technikai és eljárásrendi követelményjegyzék az aláírás elkészítésére és ellenőrzésre vonatkozóan, mely alapján az aláírás érvényessége megállapítható”[10]. Saját magam pedig azt mondanám, hogy az aláírási szabályzat célja, hogy az aláírást készítő és az azt ellenőrző egyének számára egységesen kezelhető, közös szabálygyűjteményként meghatározza azokat a feltételeket, amelyek alapján egy aláírás érvényesnek tekinthető.

Az aláírási szabályzat az elektronikus aláírás felhasználásának feltételeit definiálja egy adott kontextusban. Ez a kontextus lehet egy tranzakciós környezet, egy törvényi szabályozás, az aláíró fél által felvett szerepkör stb. Az aláírási szabályzat feladata, hogy támogassa dokumentumok elektronikus aláírását. Ennek érdekében információkat kell adnia a következő témákban:

- egy bizonyos technológia használata,
- engedélyezési szintek,
- engedélyezési lánc egy szervezeti hierarchián belül,
- ellenőrzési lánc egy szervezeti hierarchián belül,
- jogi és szervezeti követelmények az üzleti környezetnek megfelelően,
- az üzleti, illetve tranzakciós kontextus definíciója.

Előírhatja speciális aláíró és kulcstároló eszközök használatát, megadhatja a használt algoritmusok fajtáját, a kulcsok hosszát, időbélyegző használatának szükségességét, az archiválások mikéntjét, a tanúsítvány visszavonásához és ennek közzétételéhez kívánatos feltételeket stb. Tranzakciótípusonként szabályozhatja a bevonni szükséges szolgáltatókat és a bizalom mértékét, meghatározhatja a tanúsítási láncokat és ezen láncok tanúsítványai által alkalmazott hitelesítési szabályzatokat.

Az aláírás-ellenőrzési szabályzat, amit az aláírási szabályzat részeként is ki szoktak emelni, az aláírók és aláírás-ellenőrzők számára az elektronikus aláírás feldolgozására vonatkozó technikai szabályokat specifikálja. Szabad formátumú szövegként vagy gépileg feldolgozható nyelvként is leírható.

A következő információkat kell tartalmaznia:

- szabályok a tanúsítási lánc ellenőrzésére és felépítésére,
- szabályok a visszavonási állapotinformációk kezelésére (például CRL, OCSP),
- szabályok az időinformációk, időmegjelölések, időbélyegzők kezelésére,
- aláírás-ellenőrzési adatok, amelyeket az aláíró biztosít,
- aláírás-ellenőrzési adatok, amelyeket az aláírás-ellenőrzőnek kell beszerezni,
- az aláírások megtétele számára engedélyezett időtartam[11],

- az elfogadott kötelezettségvállalási típusok listája,
- az aláíró szerepekre vonatkozó szabályok,
- az aláíró algoritmusra és kulcshosszokra vonatkozó megkötések.

8.5.4 Általános szerződési feltételek

A nyilvános hitelesítésszolgáltató a szolgáltatás igénybevételére vonatkozóan szerződést kell hogy kössön a tanúsítvány kibocsátását kérő személlyel, szervezettel. Szerződéses feltételeit az egyéb szabályzatokhoz hasonlóan nyilvánosságra kell hoznia. Ennek formája a törvény által definiált általános szerződési feltételek. A dokumentum tartalmát a törvény nem határozza meg, így csak saját kútfőmből mondom, hogy az tulajdonképpen a szolgáltatási szabályzat jogi vonatkozású részeinek transzformációjaként is értelmezhető, kiegészítve egyéb általános szerződéses pontokkal. A gyakorlatban a szolgáltató és a tanúsítvány tulajdonosa között egy, az általános szerződési feltételekre épülő ügyfélszerződés/előfizetői szerződés megkötésére szokott sor kerülni, mely esetleg háromoldalú is lehet a regisztrációs szervezet, felhasználó munkáltatója vagy egyéb érintett felek bevonásával. Előfordulhat, hogy az előfizetői szerződés megkötésére nem közvetlenül a hitelesítésszolgáltatóval, hanem a regisztrációs szolgáltatóval kerül sor, s ez a szerződés tartalmaz utalást az általános szerződési feltételekre. Akármi is a szerződéses struktúra, az igazán fontos nem a formája, hanem a tartalma, melyben esetleg ott csücsül eldugva a sok kisördög.

8.6 Dokumentumok viszonya

Senki ne essen kétségbe, ha az elmondottak alapján vannak még homályos foltok a szabályzatokat illetően. Néha nekem is az volt az érzésem, hogy ez az egész azért annyira bonyolult, hogy még véletlenül se lehessen megérteni. Majd aztán magam is elkezdtem szabályzatokat írni, s rá kellett jönnöm, hogy ez a terület azért tűnik ki bonyolultságával, mert igyekszik teljes körű és hű leképzése lenni az életnek, az elképzelhető összes lehetőségre igyekszik szabályt adni, s az összes veszélyforrást kizárni. A legegészségesebb úgy tekinteni rájuk, mint referenciadokumentációkra: minden részletükkel nem kell tisztába lennünk, sőt nélkülük is elboldogulhatunk, ha pedig nincs más lehetőség, akár fel is lehet lapozni őket. A körültekintőbbeknek mindenesetre ajánlatos megismerkedni velük előre is, s ennek megkönnyítése érdekében még egy próbálkozást teszek az egyes dokumentumok viszonyának leírásával.

8.6.1 A hitelesítési szabályzat és a szolgáltatási szabályzat

A hitelesítési szabályzat és a szolgáltatási szabályzat viszonya úgy jellemezhető, hogy egy szolgáltatási szabályzat több hitelesítési szabályzatnak is megfe-

lelhet. Sajátoknak és mások által kidolgozottaknak, különböző alkalmazás követelményeket kielégítve és/vagy különböző közösségek igényeit kiszolgálva. Ugyanakkor, ebből következően, ugyanazon hitelesítési szabályzatot alkalmazhatja több szolgáltató is, melyek szolgáltatási szabályzatai eltérőek.

A hitelesítési szabályzat egy követelményrendszert állít fel, azt mondja meg, „minek kell megfelelni", a szolgáltatási szabályzat pedig azt írja le, „hogyan felel meg" a szolgáltató ezeknek a követelményeknek.[12] A gyakorlatban ennek megfelelően általában a hitelesítési szabályzat alapján készítik el a szolgáltatási szabályzatot. De akad példa arra is, hogy egy szolgáltatási szabályzat egyben hitelesítési szabályzat is, sőt még arra is, hogy egy szolgáltatási szabályzathoz utólag készülnek hitelesítési szabályzatok. A hitelesítési szabályzat és a szolgáltatási szabályzat szabadon hivatkozhat egymásra, átruházhatja a másikra a szabályozás feladatát, illetve átvehet egyes részeket a másik anyagából. Ugyanazon hitelesítési szabályzat keretében kibocsátott tanúsítványok értéke, biztonsági szintje, az eltérő szolgáltatási szabályzatot alkalmazó szolgáltatók esetében is meg kell hogy egyezzen. Ezt a szolgáltatóknak vagy a szabályzat kibocsátójának kell garantálni. A szolgáltató felelős azért is, hogy a tanúsítványban jelölt szabályzatoknak eljárásrendje és gyakorlata teljes mértékben megfeleljen. A szolgáltatási szabályzatnak tételesen választ kell adni a hitelesítési szabályzatban megfogalmazott összes követelményre. Így tartalmi elemei közé tartozik a hitelesítési szabályzatban felsorolt pontok gyakorlatát tárgyaló valamennyi rész.

Amennyiben a hitelesítési szabályzatot a tanúsítványtípusok leírásaként alkalmazzák, akkor az felfogható a szolgáltatási szabályzat kiegészítésének, specializálásának is, mely csak az egyes tanúsítványtípusok egyedi sajátosságait tárgyalja. Ez esetben készülhet egy-egy külön hitelesítési szabályzat minden tanúsítványtípushoz vagy egy közös, mely az összes tanúsítványtípus leírását magában foglalja.

8.6.2 A hitelesítési szabályzat és az aláírási szabályzat

A hitelesítési szabályzat döntően a tanúsítvány kibocsátójára, kisebb mértékben az aláíró kötelezettségeire és az érintett fél aláírás-ellenőrző tevékenységében a tanúsítvány felhasználásával kapcsolatosban tartalmaz előírásokat. Az aláírási szabályzat viszont úgy tekinthető, mint egy dokumentálási módszer egy szervezet aláírási és aláírás-ellenőrzési tevékenységének megközelítését illetően. Ebben az értelemben a hitelesítési szabályzat felfogható úgy is, mint az aláírási szabályzat részhalmaza.

A gyakorlatban aláírási szabályzatot általában szervezetek, illetve zárt közösségek szoktak kibocsátani saját tagjaik számára, különösen egyes alkalmazásokkal összefüggésben. Így az a szolgáltató által kibocsátott általános érvényű hitelesítési szabályzatnál sokkal konkrétabb előírásokat tartalmaz, egyfajta felhasználói dokumentációként is felfogható.

8.6.3 Szabályzatok közti ellentétek kezelése

Mint látható, az egyes dokumentumok tartalmában van némi átfedés. A kibocsátóknak kötelességük minden, módjukban álló eszközzel megelőzni az ennek következtében esetlegesen fellépő ellentétek kialakulását. A konfliktusok elkerülésére a legkézenfekvőbb módszer, ha az egyes szabályzatok csak azon pontokat tartalmazzák, melyeket az egyéb szabályzatok nem tárgyalnak, a többire pedig hivatkozást adnak. Vannak azonban esetek, amikor ez a módszer nem járható. Egy elektronikus aláírás például tartalmazhat referenciát egy aláírási szabályzatra, a tanúsítványon keresztül pedig egy hitelesítési szabályzatra, melyek eltérő szabályokat kínálnak bizonyos esetekre. Ilyen esetekben felmerülhet az a kérdés, hogy melyik dokumentum szabályozása a döntő erejű. Erre válaszul a szabályzatok valamelyike tartalmazhat egy záradékot, mely kinyilvánítja annak döntő mivoltát más szabályzatokkal szemben, illetve azok felett.

8.7 Az RFC 2527 szabvány

A hitelesítési és szolgáltatási szabályzatok tartalmára és felépítésére az IETF RFC 2527 szabványa (Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework) ad útmutatót, melyet a szolgáltatók nagy része több-kevesebb hűséggel követni szokott.[13] A szabvány által definiált szerkezet következetes használata megkönnyíti a szabályzatírók dolgát (mert sorvezetőként segíti őket), valamint leegyszerűsíti két, eltérő hitelesítési szabályzat egymásnak történő megfeleltetését kereszttanúsítás esetén. Ugyanígy megkönnyíti egy szolgáltatási szabályzat ellenőrzését a hitelesítési szabályzatnak való megfelelőség szempontjából vagy két szolgáltatási szabályzat összevetését.

8.8 Szabályzati tartalomjegyzék

Az alábbiakban közlöm egy példaértékű hitelesítési és szolgáltatási szabályzat leegyszerűsített tartalomjegyzékét, mely az RFC 2527 szabványon alapszik, de a magyar törvényi előírásoknak is megfelelve azt némileg ki is bővíti. Terjedelmi okok miatt sajnos magyarázattal nem tudok szolgálni az egyes pontokhoz, de bármely szolgáltató szabályzatát fellapozva azok magukért beszélnek.

1 Bevezetés
1.1 Áttekintés
1.2 Azonosítás
1.3 Közösség és alkalmazhatóság
1.3.1 Hitelesítőszervezet
1.3.2 Regisztrációs szervezetek
1.3.3 Szabályozószervezet
1.3.4 Végfelhasználók
1.3.5 Alkalmazhatóság

1.4 Tanúsítványok osztályai és típusai
1.5 Szolgáltató adatai
2 Általános rendelkezések
2.1 Kötelezettségek
2.1.1 Szolgáltató kötelezettségei
2.1.2 Regisztrációs szervezet kötelezettségei
2.1.3 Igénylő és Előfizető kötelezettségei
2.1.4 Érintett fél kötelezettségei
2.1.5 Címtár kötelezettségei
2.2 A közösség tagjainak felelőssége
2.2.1 Hitelesítőszervezet felelőssége
2.2.2 Regisztrációs szervezet felelőssége
2.2.3 Előfizető felelőssége
2.2.4 Érintett fél felelőssége
2.3 Pénzügyi felelősség
2.3.1 Kártérítés
2.3.2 Megbízotti kapcsolatok
2.3.3 Adminisztratív eljárások
2.4 Értelmezés és alkalmazás
2.4.1 Irányadó törvény
2.4.2 Érvénytelenség, hatályosság, megszűnés, értesítések
2.4.3 Vitás kérdések kezelése
2.5 Díjak
2.6 Nyilvánosságra hozatal és tárolás
2.6.1 Szolgáltatói információk közzététele
2.6.2 Közzététel gyakorisága
2.6.3 Elérési szabályok
2.6.4 Tanúsítványtár
2.7 A megfelelőség tanúsítása (audit)
2.7.1 A megfelelőség ellenőrzésének gyakorisága
2.7.2 A tanúsító szervezet megnevezése és jellemzői
2.7.3 A tanúsító szervezet és az ellenőrzött fél kapcsolata
2.7.4 Az ellenőrzés által érintett területek
2.7.5 Hiányosságok esetén végrehajtandó tevékenységek
2.7.6 Az eredményekről való tájékoztatás
2.8 Bizalmasság – Adatkezelési szabályzat
2.8.1 Bizalmas információk
2.8.2 Nem bizalmas információk
2.8.3 Tanúsítvány-visszavonási és -felfüggesztési információk felfedése
2.8.4 Feltárás törvényi meghatalmazással rendelkezők részére
2.8.5 Feltárás polgári eljárás keretében
2.8.6 Feltárás tulajdonos kérésére
2.8.7 Feltárás más esetekben
2.9 Szellemi tulajdonhoz fűződő jogok

3 Azonosítás és hitelesítés
3.1 Kezdeti regisztráció
3.1.1 Nevek típusa
3.1.2 Névszemantika
3.1.3 Különböző névformátumok értelmezése
3.1.4 Nevek egyedisége
3.1.5 Névigénylési viták feloldása
3.1.6 Védjegyek elismerésének és hitelesítésének módszere
3.1.7 Magánkulcsbirtoklás ellenőrzésének módszere
3.1.8 Szervezeti identitás hitelesítése
3.1.9 Személyes identitás hitelesítése
3.2 Tanúsítványmegújítás
3.3 Tanúsítvány megújítása visszavonás után
3.4 Visszavonási kérés
4 Működésre vonatkozó követelmények
4.1 Tanúsítványkérelem
4.2 Tanúsítványkibocsátás
4.3 Tanúsítványelfogadás
4.4 Tanúsítvány-visszavonás és -felfüggesztés
4.4.1 Visszavonáshoz vezető körülmények
4.4.2 Visszavonás kérelmezése
4.4.3 Visszavonási eljárás
4.4.4 Visszavonás időbelisége
4.4.5 Felfüggesztéshez vezető körülmények
4.4.6 Felfüggesztés kérelmezése
4.4.7 Felfüggesztési eljárás
4.4.8 Felfüggesztett állapotra vonatkozó korlátozások
4.4.9 CRL-kibocsátás gyakorisága
4.4.10 CRL-ellenőrzési követelmények
4.4.11 On-line visszavonási állapot szolgáltatás
4.4.12 On-line visszavonás-ellenőrzési követelmények
4.4.13 Visszavonási állapot közlés más formái
4.4.14 Visszavonási állapot közlés más formáinak ellenőrzési követelményei
4.4.15 Magánkulcs-kompromittálódás speciális követelményei
4.4.16 Tanúsítványmegújítás
4.5 Biztonsági naplózás folyamatai
4.5.1 Naplózott eseménytípusok
4.5.2 Naplóadatok feldolgozásának gyakorisága
4.5.3 Naplóadatok tárolási ideje
4.5.4 Naplóadatok védelme
4.5.5 Naplóadatok mentési eljárásai
4.5.6 Naplóadatok gyűjtési rendszere
4.5.7 Rendkívüli eseményekről történő értesítés
4.5.8 Sebezhetőség kiértékelése

4.6 Adatarchiválás
4.7 Szolgáltatói kulcscsere
4.8 Katasztrófaelhárítás
4.8.1 Hardver-, szoftver- vagy adatsérülés esete
4.8.2 Szolgáltatói nyilvánoskulcs-visszavonás esete
4.8.3 Szolgáltatói magánkulcs-kompromittálódás esete
4.8.4 Természeti katasztrófa esete
4.8.5 Üzletfolytonossági és katasztrófaelhárítási terv
4.9 Hitelesítésszolgáltató tevékenység megszüntetése
5 Fizikai, eljárásrendi és személyzeti biztonsági szabályozások
5.1 Fizikai biztonsági szabályozások
5.1.1 Elhelyezés és szerkezeti felépítés
5.1.2 Fizikai hozzáférés
5.1.3 Áramellátás, légkondicionálás
5.1.4 Beázás és elárasztódás veszélyeztetettsége
5.1.5 Tűzmegelőzés és tűzvédelem
5.1.6 Médiumok tárolása
5.1.7 Selejt kezelése és megsemmisítése
5.1.8 Mentési példányok fizikai elkülönítése
5.2 Eljárásrendi szabályozások
5.2.1 Megbízható munkakörök
5.2.2 Az egyes feladatokhoz szükséges személyzet létszáma
5.2.3 Az egyes szerepkörökben elvárt azonosítás és hitelesítés
5.3 Személyzeti szabályozások
5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények
5.3.2 Háttér-ellenőrzési eljárások
5.3.3 Képzési követelmények
5.3.4 Továbbképzési gyakoriságok és követelmények
5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje
5.3.6 A felhatalmazás nélküli tevékenységek következményei
5.3.7 Szerződő személyzetre vonatkozó követelmények
5.3.8 A személyzet számára biztosított dokumentációk
6 Technikai szabályozások
6.1 Kulcspárgenerálás és -installálás
6.1.1 Kulcspárgenerálás
6.1.2 Magánkulcs felhasználóhoz történő eljuttatása
6.1.3 Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz
6.1.4 Hitelesítőszervezet nyilvános kulcsának eljuttatása a felhasználókhoz
6.1.5 Kulcsméretek
6.1.6 Nyilvánoskulcs-paraméterek előállítása
6.1.7 Nyilvánoskulcs-paraméterek ellenőrzése
6.1.8 Szoftveres/hardveres kulcsgenerálás
6.1.9 Kulcsfelhasználási célok

6.2 Magánkulcs védelme
6.2.1 Kriptográfiai modulra vonatkozó szabványok
6.2.2 Magánkulcs többszemélyes kontrollja
6.2.3 Magánkulcs letétbe helyezése
6.2.4 Magánkulcs mentése
6.2.5 Magánkulcs archiválása
6.2.6 Magánkulcs kriptográfiai modulba helyezése
6.2.7 Magánkulcs aktiválása
6.2.8 Magánkulcs deaktiválása
6.2.9 Magánkulcs megsemmisítése
6.3 Kulcspárkezelés egyéb aspektusai
6.3.1 Nyilvános kulcs archiválása
6.3.2 Nyilvános és magánkulcs felhasználási ideje
6.4 Aktivizáló adatok
6.4.1 Aktivizáló adatok generálása és installációja
6.4.2 Aktivizáló adatok védelme
6.4.3 Aktivizáló adatok egyéb aspektusai
6.5 Számítógép-biztonsági szabályok
6.5.1 Számítógép-biztonság technikai követelményei
6.5.2 Számítógép-biztonsági értékelések
6.6 Életciklus technikai szabályok
6.6.1 Rendszerfejlesztési szabályok
6.6.2 Biztonságkezelési szabályok
6.6.3 Életciklus-biztonsági értékelések
6.7 Hálózati biztonsági szabályok
6.8 Kriptográfiai modul műszaki szabályok
7 Tanúsítvány- és kulcsvisszavonási profil
7.1 Tanúsítványprofil
7.1.1 Verziószám
7.1.2 Tanúsítvány-toldalékok
7.1.3 Algoritmus azonosítók
7.1.4 Névformák
7.1.5 Névmegkötések
7.1.6 Szabályzatobjektum-azonosító
7.1.7 Szabályzatmegkötési mezők használata
7.1.8 Szabályzatminősítő szintaxis és szemantika
7.1.9 Kritikus szabályzat kiterjesztés feldolgozása
7.2 Visszavonásilista-profil
7.2.1 Verziószám
7.2.2 Visszavonási lista és visszavonás bejegyzési kiterjesztések
8 Szabályzat adminisztrációja
8.1 Változáskezelési eljárások
8.2 Közzétételi és tájékoztatási szabályok
8.3 Elfogadási eljárások

JEGYZET

1 Az Officina egyetemes lexikon meghatározása.

2 Amerikai illetékességű nyelvtanárom évekig vezetett és biciklizett Budapesten a jobbkéz-szabály ismerete nélkül, abban a hitben, hogy tábla nélkül neki van elsőbbsége. Bár élve megúszta, senkinek sem ajánlanám a követését.

3 Ez a felosztás meglehetősen leegyszerűsített, a belső szabályzatok legtöbbje bizonyos értelemben titkos, s az ahhoz hozzáférő személyek köre valamilyen módon korlátozott.

4 Eredeti angol elnevezésekkel, ÁSZF nélkül: Certificate Practice Statement (CPS), Certificate Policy, Signature Policy.

5 Véleményem szerint a tanúsítványokhoz és visszavonási listákhoz hasonlóan, saját elektronikus aláírásával ellátva (bár ez nem törvényi előírás).

6 Az ABA Guidelines és az IETF RFC 2527 meghatározása.

7 Az ITU X.509, az ETSI TS 101-456, és az IETF RFC 2527 szabványok által alkalmazott meghatározás.

8 A CARAT Guidelines meghatározása.

9 EESSI–Signature Policies

10 CEN/ISSS WS/E-Sign N 140, ETSI ES 101-733

11 Az az időpont, ami előtt és (opcionálisan) után a szabályzatra hivatkozva tilos aláírni.

12 ETSI TS 101 456

13 A szabványnak 2002 januárjában elkészült egy új változata is, mely a könyv írásakor még nem végleges állapotú.

9 Az elektronikus aláírás jogszabályi háttere

Ajánlás:

Jogászoknak és azoknak,
akik jogi bizonyító erőt kívánnak
az aláírás felhasználásához fűzni.

Az elektronikus aláírás jogszabályi hátterének bemutatása nem pofonegyszerű, mert noha még korántsem zárult le a szabályozási folyamat, máris számtalan irányelv, törvény, rendelet igyekszik regulázni az ezzel kapcsolatos tevékenységeket. Ahol csak lehet, igyekszem majd pontosan idézni a szabályokat. A kivonatos ismertető, amit megengedhetek magamnak, azonban nem adhat tökéletes képet minden esetre és feltételre vonatkozóan, csak a szabályozás legfőbb elveit hivatott ismertetni, melyek egyes pontjai alól számtalan kivétel akad, s melyekhez számos feltételes mód tapad. Ezek megismerése nem lehetséges másképp, mint a jogszabályok eredetijének gondos áttanulmányozásával.[1]

9.1 A szabályozás szintjei

Az 1075/2000. és 1014/2001. kormányhatározatokat követően, melyek a szabályozási alapelvekről és a szükséges intézkedésekről rendelkeztek, az elektronikus aláírás jogszabályi hátterét az elektronikus aláírásról szóló 2001. évi XXXV. törvény (Eat.) teremtette meg Magyarországon. A jogszabály – igazodva az európai uniós elvárásokhoz – az Európai Parlament és az Európa Tanács az elektronikus aláírások közösségi keretszabályairól szóló 1999/93/EK irányelvével összeegyeztethető szabályozást tartalmaz. A törvény módosítja a polgári törvénykönyv, a polgári perrendtartás, a büntetőeljárásról, az államigazgatási eljárásról szóló törvény és egyéb jogszabályok egyes rendelkezéseit is annak érdekében, hogy megteremtse az általuk szabályozott területeken az elektronikus dokumentumok felhasználásának lehetőségét. A törvény felhatalmazásokat ad végrehajtási rendeletek (kormány-, miniszteri és önkormányzati rendeletek) megalkotására, amelyek közül néhány már a törvény 2001. szeptember 1-jei hatálybalépésével egyidejűleg, illetve ezt nem sokkal követően lépett hatályba:

- A 15/2001. MeHVM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról.
- A 16/2001. MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről.
- A 151/2001. kormányrendelet a Hírközlési Főfelügyeletnek[2] az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól.

– A 20/2001. MeHVM rendelet a Hírközlési Főfelügyeletnek az elektronikus aláírással összefüggő minősítéssel és nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról.

A kézirat lezárása előtt pár nappal jelent meg a közlönyben még két fontos jogszabály:

– A 2/2002. MeHVM irányelv a minősített elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó biztonsági követelményekről.
– A 7/2002. MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről.

Előbbi jogszabály (melynek megalkotásában szerény személyem is komoly részt vállalt) funkcionális és biztonsági ajánlásokat fogalmaz meg a minősített hitelesítésszolgáltatók irányába, s így a minősítési tevékenységnek lesz az alapja. Utóbbi pedig azon szakértők kijelölését tárgyalja, akik ennek megfelelően a hitelesítésszolgáltatóval szemben támasztott egyes követelményeknek való megfelelőséget igazolják (vagyis a minősítés szakmai részét ténylegesen lefolytatják).

A jogi szabályozás e rendeleti szintjén, a törvény útmutatásainak megfelelően még további jogszabályok megszületése várható a kormány, az egyes minisztériumok és a helyi önkormányzatok részéről:

– a központi közigazgatási szervek és a helyi önkormányzati szervek által készített elektronikus dokumentumokkal kapcsolatos sajátos követelményekkel kapcsolatban;
– azoknak a jogviszonyoknak a körét illetően, melyekkel kapcsolatos államigazgatási eljárásokban mód van kizárólag elektronikus iratok használatára;
– valamint az elektronikus dokumentumok és elektronikus aláírás alkalmazásával történő ügyintézés sajátos szabályait illetően[3].

A hatósági szabályozások közé sorolható továbbá a Hírközlési Felügyelet (HÍF) jogalkalmazási gyakorlata is.

Érdemes még megemlíteni, hogy – szintén a kéziratzárás előtt nem sokkal – a kormány megbízta az informatikai kormánybiztost és a belügyminisztert a kormányzati elektronikus aláírási rendszer (KEAR) felállításáról. A közigazgatás központi elektronikus aláírási infrastruktúrája részeként a Belügyminisztériumban hitelesítésszolgáltatás lesz kiépítve, mely 2002. szeptember 30-tól fokozott biztonságú, 2003. március 31-től, pedig minősített elektronikus tanúsítványokat ad majd ki. Az erről szóló alsóbb szintű jogszabályok a Magyar Közlöny 39. számában jelentek meg:

– 1026/2002. kormányhatározat a kormányzati elektronikus aláírási rendszer kiépítésével összefüggő egyes feladatokról és a kormányzati hitelesítésszolgáltató felállításáról,
– 47/2002. kormányrendelet a kormányzati elektronikus aláírási rendszer kiépítésével összefüggő egyes kormányrendeletek módosításáról.

9.2 Az EU-irányelv

Az Európai Unió 1999/93/EK irányelvének célja „az elektronikus aláírás használatának lehetővé tétele és jogi elismerésének elősegítése". Ennek érdekében „az elektronikus aláírásokhoz és bizonyos hitelesítésszolgáltatásokhoz kialakít egy keretszabályozást", vagyis az elektronikus aláírás témakörében csak az alapelveket definiálja, a konkrét törvényi szabályozást a tagországok hatáskörébe utalva.

Az irányelv kötelezi a tagállamokat, hogy legkésőbb 2001. július 19-ig az irányelv rendelkezéseire figyelemmel szabályozzák az elektronikus aláírások használatát, vagy ha korábban már létezett tagállami szabályozás, akkor teremtsék meg az irányelv rendelkezései és a saját szabályozásuk közötti összhangot.[4] Az irányelv rendelkezései két csoportra oszthatók: az első csoportba azok a rendelkezések tartoznak, amelyek az áruk és szolgáltatások, konkrétan az elektronikus aláírási termékek és a hitelesítésszolgáltatók által nyújtott szolgáltatások EU-n belüli szabad mozgását, illetőleg a fogyasztók érdekeinek védelmét hivatottak biztosítani; a másik csoportba, pedig azok a rendelkezések, amelyek az elektronikus kereskedelemben rejlő lehetőségek kiaknázhatósága érdekében az elektronikus aláírások jogi elismerésére kötelezik a tagállamokat.

A tagállami szabályozás alapelvei között kiköti:

- a tagállamok nem köthetik a hitelesítésszolgáltatás nyújtását előzetes hatósági engedély megszerzéséhez,
- a tagállamok kötelesek felügyelni azon hitelesítésszolgáltatók tevékenységét, amelyek minősített tanúsítványokat bocsátanak ki,
- az önkéntes akkreditáció elvét a minősített szolgáltatók számára (bár a tagállamok a hitelesítésszolgáltatók akkreditálásának saját rendszerét alakíthatják ki, de az akkreditálást nem tehetik a szolgáltatók számára kötelezővé),
- tagállami hitelesítésszolgáltatók által kibocsátott tanúsítványok elismerésére vonatkozó kötelezettséget,
- biztosítani kell az elektronikus adathitelesítés technológiasemlegességének[5] és az elektronikus aláírási termékek együttműködésének támogatását.

Az irányelv az elektronikus aláírások jogi elismerése szempontjából három aláírástípust különböztet meg:

- Elektronikus aláírás – Ezek vonatkozásában az irányelv arra kötelezi a tagállamokat, hogy bírósági és hatósági eljárásokban biztosítsák azt, hogy az elektronikus aláírással aláírt iratok és az elektronikus aláírások bizonyítási eszközként való felhasználását ne tagadják meg pusztán azok elektronikus formája miatt.
- Fokozott biztonságú elektronikus aláírás (biztonságos aláíró eszközzel készült és minősített tanúsítványon alapuló elektronikus aláírás) – Ezen aláírásoknak olyan joghatást kell biztosítani, amilyen jogi hatást a saját kezű aláírásoknak biztosít az adott tagállam jogrendszere (ha teljesülnek a kézi aláírásokra meghatározott követelmények).

– Elektronikus aláírások közszférán belüli használata – A tagállamok további követelményekhez köthetik. Ezeknek a követelményeknek azonban objektíveknek, arányosnak és előre megismerhetőnek kell lenniük, továbbá nem vezethetnek a piaci szereplők hátrányos megkülönböztetéséhez.

Az irányelv a függelékeiben követelményeket definiál a minősített tanúsítványokat kibocsátó hitelesítésszolgáltatókra, azok szolgáltatásaira, a minősített tanúsítványokra magukra, a biztonságos aláíró eszközökre, továbbá a biztonságos aláírás-ellenőrzésre vonatkozóan.

9.3 A magyar elektronikus aláírási törvény

Ahogy az a magyar elektronikus aláírási törvény bevezetőjében olvasható, a törvény célja, hogy „megteremtse a hiteles elektronikus nyilatkozattétel, illetőleg adattovábbítás jogszabályi feltételeit az üzleti életben, a közigazgatásban és az információs társadalom által érintett más életviszonyokban". Vagyis annak biztosítása, hogy az elektronikus iratok ugyanazzal a bizonyító erővel rendelkezzenek, ugyanolyan joghatást váltsanak ki, mint a papír alapú társaik.

A törvény legfontosabb funkciója az egyes elektronikus aláírástípusokhoz tartozó jogkövetkezmények, azok bizonyító erejének valamint felhasználási lehetőségeiknek és korlátjaiknak meghatározása.

9.3.1 A törvény személyi és tárgyi hatálya

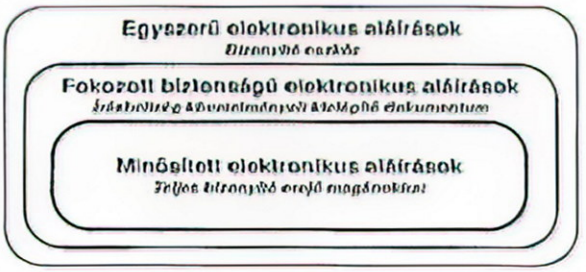
A törvény személyi hatálya az elektronikus aláírással kapcsolatos szolgáltatást végzőre (hitelesítésszolgáltató), valamint az elektronikus aláírással kapcsolatos szolgáltatást igénybe vevőre (aláíró), illetőleg az elektronikus aláírást felhasználóra (ellenőrző) terjed ki. Az aláíró kizárólag természetes személy lehet, ami a törvény egy igen nagy gyengesége. Azokra az eszközökre, amelyek aláírást végeznek egy szervezet vagy személy megbízásából, a saját nevük alatt (pl. egy cég webszervere), nem lehet alkalmazni. A szolgáltató és a felhasználó egyaránt lehet természetes, illetve jogi személy vagy jogi személyiség nélküli szervezet. A törvény tárgyi hatálya az elektronikus aláírással kapcsolatos szolgáltatásokra és az elektronikus aláírás felhasználásának kérdéseire vonatkozik.

Az egymással szerződéses viszonyban álló felek az elektronikus dokumentumok elfogadásának feltételeit – bizonyos kötöttségekkel – a törvény szabályaitól eltérően is megállapíthatják.

9.3.2 Az elektronikus aláírás fajtái

A törvény – az EU-irányelvre emlékeztető, de attól eltérő módon – többfajta elektronikus aláírást is megkülönböztet, azok megbízhatósági szintje szerint. Az erősebb szintű elektronikus aláírások megfelelnek a gyengébb szintűek ismérveinek is, így ezek egy egyre szűkülő halmazként is felfoghatók.

- Az egyszerű (vagy jelző nélküli) elektronikus aláírásba beletartozik minden olyan elektronikus aláírás is, amely nem alkalmas arra, hogy biztonságosan azonosítsák az aláíró személyét, és bizonyíthatóvá tegyék, hogy az aláírt szöveg nem változott az aláírás óta. Ez alatt érthetjük azt is, ha egy Word-dokumentum végére egyszerűen odapötyögjük a nevünket.
- A fokozott biztonságú elektronikus aláírás olyan elektronikus aláírás, amely alkalmas az aláíró azonosítására, egyedülállóan hozzá köthető, olyan eszközökkel hozták létre, melyek kizárólag az aláíró befolyása alatt állnak, és a dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az aláírás elhelyezését követően az iraton, illetve dokumentumon tett – módosítás érzékelhető. Ez a gyakorlatban a nyilvános kulcsú technológia felhasználásával készülő aláírás.
- A minősített elektronikus aláírás olyan fokozott biztonságú elektronikus aláírás, amely biztonságos aláírás-létrehozó eszközzel készült, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.



65. ábra
Elektronikus aláírások osztályozása

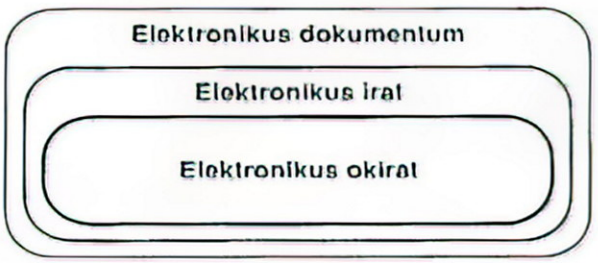
Az aláíró aláírásával felelősséget vállal az aláírt elektronikus dokumentum tartalmáért. A felelősségvállalás jogi érvényesíthetősége és a hitelesség (személyi és tartalmi hitelesség) bizonyítási lehetőségei összefüggenek az elektronikus aláírás biztonsági fokával.

9.3.3 Az elektronikus dokumentumok fajtái

Az elektronikus aláírás egyes szintjeihez hasonlóan – de nem ahhoz köthető módon – a törvény az elektronikus dokumentumokat is szintekre osztja:

- A jelző nélküli elektronikus dokumentum olyan, bármely elektronikus eszközzel érzékelhető adat, melyet elektronikus aláírással láttak el. Azaz lehet aláírt program, zene vagy film is.
- Az elektronikus irat olyan elektronikus dokumentum, melynek funkciója az, hogy szöveget közöljön. Más adat legfeljebb ennek illusztrálására, hatósági azonosítására (például fejléc) szerepel benne, illetve egyes digitális jeleket a szöveggel összefüggő informatikai funkciók megvalósítása érdekében, az olvasó számára nem érzékelhetően tartalmaz.
- Az elektronikus okirat olyan elektronikus irat, mely nyilatkozattételt, illetőleg nyilatkozat elfogadását vagy nyilatkozat kötelezőnek elismerését foglalja magában.

A törvény értelmében az elektronikus aláírással szignált dokumentumok bíróság előtt bizonyítási eszközként felhasználhatók, a minősített elektronikus aláírással ellátott elektronikus okiratok pedig teljes bizonyító erejű magánokiratnak számítanak.



66. ábra
Elektronikus dokumentumok osztályozása

9.3.4 Alapelvek

A törvény legalapvetőbb kijelentése az, hogy elektronikus aláírás, illetve elektronikus irat vagy dokumentum elfogadását – beleértve a bizonyítási eszközként történő alkalmazást – megtagadni, jognyilatkozat tételére, illetve joghatás kiváltására való alkalmasságát kétségbe vonni nem lehet kizárólag amiatt, hogy az aláírás, illetve az irat vagy dokumentum elektronikus formában létezik.

Családjogi, illetve öröklési jogi ügyekben ugyanakkor nem lehet az elektronikus formán kívüli dokumentumokat mellőzve, csak elektronikus aláírást felhasználni, illetve elektronikus iratot vagy dokumentumot készíteni[6]. Ennek oka e jogviszonyok hosszú időhorizontja, statikus jellege és különös jelentősége, amely esetben a kizárólag elektronikusan hitelesített forma nem nyújtana elegendő biztonságot (emlékezzünk csak az algoritmusok feltörési mutatóira). Vagyis egy darabig még nem fogjuk az anyakönyvezető előtt elektronikus aláírással bekötni kedvesünk fejét.

Két másik fontos alapelv az, hogy jogszabály – az adókötelezettség teljesítését megállapító törvény kivételével[7] – nem teheti elektronikus aláírás felhasználását ügyfél részére kötelezővé, valamint hogy minősített tanúsítványt bármely bírósági vagy államigazgatási eljárásban el kell fogadni.

9.3.5 Jogkövetkezmények

A törvény a jövendőbeli felhasználások és a jogkövetkezmények különbözősége alapján teremti meg és határolja el az elektronikus dokumentum fogalmát és fajtáit:

Ha a jogszabály írásba foglalást ír elő, e követelménynek eleget tesz az elektronikus iratba foglalás is, ha az elektronikus iratot fokozott biztonságú elektronikus aláírással írják alá. Ha az elektronikus dokumentumon minősített elektronikus aláírás szerepel, és az aláírás ellenőrzésének eredményéből más nem következik, vélelmezni kell, hogy a dokumentum tartalma az aláírás óta nem változott.[8] Fokozott biztonságú elektronikus aláírással ellátott dokumentum esetében a törvény szerint, ha a fokozott biztonságú elektronikus aláírás el-

lenőrzésének eredményéből más nem következik, a dokumentum adatait meg nem hamisítottnak kell tekinteni.[9] Amennyiben az időbélyegzést olyan szolgáltató végezte, amely az időbélyegzéskor szerepelt a minősített szolgáltatók nyilvántartásában, és az időbélyegző ellenőrzésének eredményéből más nem következik, az ellenkező bizonyításáig vélelmezni kell, hogy a dokumentumban foglalt adatok az időbélyegző elhelyezése óta nem változtak. A minősített elektronikus aláírással ellátott elektronikus okirat – annak teljes bizonyító ereje következtében – bizonyítékul szolgál arra, hogy kiállítója az abban foglalt nyilatkozatot megtette, illetőleg elfogadta vagy magára kötelezőnek ismerte el, továbbá, hogy a dokumentum nem hamis.

Ahogy az a fentiekből kitűnik, minősített elektronikus aláírás esetén annak esetlegesen hamis voltát annak kell bizonyítani, aki azt kétségbe vonja. Fokozott biztonságú elektronikus aláírás esetében az érvényesség és valódiság bizonyítási kényszere az aláírót és a hitelesítésszolgáltatót terheli.

Érdemes még megemlíteni, hogy ügyvédi ellenjegyzésre minősített elektronikus aláírással is sor kerülhet. Az ellenjegyzés ebben az esetben azt bizonyítja, hogy a minősített elektronikus aláírással ellátott elektronikus okirat tartalma az ügyvéd által készített elektronikus okiratéval megegyezik.

9.3.6 Elektronikus aláírás szolgáltatások

A törvény által szabályozott elektronikus aláírással kapcsolatos szolgáltatások a következők:

- elektronikusaláírás-hitelesítés szolgáltatás,
- időbélyegzés,
- aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése.

A hitelesítésszolgáltatás keretében a hitelesítésszolgáltató azonosítja az igénylő személyét, tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait, továbbá nyilvánosságra hozza a tanúsítványhoz tartozó szabályzatokat, az aláírás-ellenőrző adatokat és a tanúsítvány aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat. Időbélyegzés során a szolgáltató az elektronikus dokumentumhoz időbélyegzőt kapcsol. Az időbélyegzőre a tanúsítvány, a minősített időbélyegzőre, pedig a minősített tanúsítvány erre vonatkozó rendelkezéseit kell a törvénynek megfelelő módon alkalmazni. Az aláírás-létrehozó adat elhelyezése az aláírás-létrehozó eszközön a gyakorlatban a magánkulcs intelligens kártyára helyezését, illetve azon történő generálását jelenti.

Ezek a szolgáltatások együttesen vagy külön-külön is nyújthatók. A minősített hitelesítésszolgáltatók kötelesek biztonságos tanúsítvány- és adattárolási szolgáltatást[10], valamint biztonságos és azonnali tanúsítványfelfüggesztési, illetve -visszavonási szolgáltatást is biztosítani a hitelesítésszolgáltatás részeként.

9.3.7 A szolgáltatások nyújtásának feltételei

A fokozott biztonságú szolgáltatás végzését a szolgáltató a megkezdéssel egyidejűleg köteles bejelenteni a felügyeletnek. Bejelentkezni annak a szolgáltatónak kell, amely szolgáltatását üzleti tevékenységként (ellenértékért) nyújtja, amibe a nem közvetlen ellentételezés is beletartozik.[11]

Ha a szolgáltató minősített szolgáltatást kíván nyújtani, az ehhez szükséges személyi, technikai és egyéb feltételek meglétét tanúsító minősítést kell beszereznie a felügyelettől a tevékenység megkezdése előtt. Minősített tanúsítvány kibocsátását, illetve minősített időbélyegzést az a szolgáltató végezhet, amely további műszaki, pénzügyi, személyi és egyéb követelményeknek megfelel.

9.3.8 A hitelesítésszolgáltatási tevékenység

A szolgáltató a szerződéskötést megelőzően köteles tájékoztatni a szolgáltatás igénylőjét a szolgáltatás felhasználásának módjáról, biztonsági fokáról, szolgáltatási szabályzatáról és a szerződés feltételeiről. A hitelesítésszolgáltató a minősített tanúsítványban meghatározhatja a tanúsítvány felhasználásának tárgybeli, földrajzi vagy egyéb korlátait, illetve az egy alkalommal vállalható kötelezettség legmagasabb értékét.

A szolgáltató a szolgáltatás keretein belül azonosítja az igénylő személyét, majd a saját elektronikus aláírásával aláírt tanúsítvánnyal hitelesíti az igénylő elektronikus aláírását. Fogadja és feldolgozza a tanúsítványokkal kapcsolatos változások adatait, nyilvántartást vezet a tanúsítványok aktuális helyzetéről, esetleges felfüggesztéséről, visszavonásáról. Ezeket és a tanúsítványkibocsátásra vonatkozó saját szabályzatait, az aláírás-ellenőrző adatokat, továbbá a visszavont tanúsítványok nyilvántartását bárki számára hozzáférhető és folyamatosan elérhető módon közzéteszi.

A szolgáltatás befejezését a törvény szigorúan szabályozza: a szolgáltatónak ez irányú szándékát előre jeleznie kell ügyfelei és a felügyelet felé, és az általa kibocsátott összes tanúsítványt vissza kell vonnia.[12] Köteles intézkedni arról is, hogy nyilvántartásait egy vele azonos besorolású szolgáltató átvegye,[13] ellátva ezek megőrzését, s gondoskodva arról, hogy a tanúsítványok tartalma az előírt ideig megállapítható legyen.

9.3.9 Adatvédelem

Mivel a szolgáltató széles körben kezel személyes adatokat, a törvény adatvédelmi rendelkezései különböző korlátozásokat állapítanak meg vele szemben. Adatszolgáltatási kötelezettséget írnak elő a hatóságok felé, valamint a tanúsítvány érvényességét érintő polgári peres és nem peres eljárásokban.

A törvény az elektronikus aláírással kapcsolatos szolgáltatások megfelelősége és hitelessége érdekében egyértelműen meghatározza azokat a jogokat, ame-

lyek segítségével a szolgáltató képes az igénylő személyazonosságát, illetve képviseleti jogosultságát megállapítani. A személyazonosításra alkalmas okmányokba ezért betekintést enged, s az így megismert adatok ellenőrzése céljából pedig adategyeztetési kötelezettséget ír elő számára.

9.3.10 A szolgáltató felelőssége

A hitelesítésszolgáltató felelőssége akkor áll fenn, ha saját tevékenységében hibázik.[14] A tanúsítványban (illetve az ahhoz kapcsolódó szabályzatokban) meghatározott korlátokat meghaladó ügyletekben kibocsátott és aláírt elektronikus dokumentumból származó követelésekért, illetve az így okozott kárért azonban ekkor sem felel. A szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a polgári törvénykönyv 339. §-a szerint, az aláíróval szemben pedig a szerződésszegésért való felelősség szabályai szerint felelős a minősített elektronikus aláírással vagy időbélyegzővel, illetve az ezzel ellátott elektronikus dokumentummal okozott kárért, ha a jogszabályi előírásokat megszegte. A szabályok megtartását kétség esetén a szolgáltatónak kell bizonyítania.

9.3.11 Az aláíró jogai és kötelezettségei

Azonkívül, hogy az aláíró jogosult az aláírás-létrehozó adatot birtokolni s a képviselt személyhez és szervezethez hasonlóan kérheti a tanúsítvány felfüggesztését, visszavonását, a törvény túl sok jogot nem definiál számára. Annál több kötelezettséget, melyek közül a legfontosabb, hogy az aláíró az aláírás-létrehozó adatot kizárólag az aláírás létrehozására használhatja (lásd: 9.5 fejezet), betartva a tanúsítványban jelzett esetleges egyéb korlátozásokat is. Ezenkívül az aláírónak különböző tájékoztatási kötelezettségei vannak, amelyek elmulasztása esetén az abból eredő kárért felelős. Így köteles haladéktalanul tájékoztatni a hitelesítésszolgáltatót:

- az azonosításához szükséges adatokról és ezek változásáról,
- az aláírás-létrehozó adat kompromittálódásáról,
- az általa észlelt, törvényben meghatározott rendellenességekről és
- elektronikus dokumentummal kapcsolatos jogvita megindulásáról.

9.3.12 A felügyelet feladatai

A szolgáltatás felügyeleti szerveként eljáró Hírközlési Felügyelet nyilvántartásba veszi a hitelesítésszolgáltatókat és az elektronikus aláírási termékeket tanúsító szervezeteket, és ezeket a nyilvántartásokat bárki számára hozzáférhető és folyamatosan elérhető módon közzéteszi. Ez az az autentikus forrás, amiből a halandó tájékozódhat arról, hogy melyik szolgáltató működik legálisan, mikortól, milyen minősítéssel, milyen szabályzatok alapján.

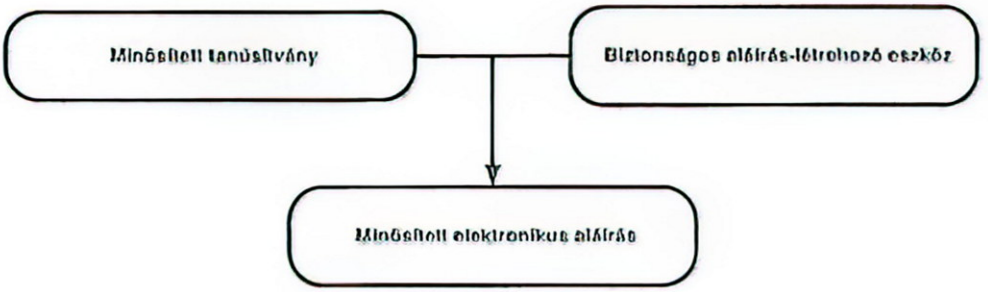
A felügyelet folytatja le a szolgáltatók minősítési eljárását s felügyeli működésüket (megfelelnek-e a törvény, a felhatalmazása alapján kiadott jogszabályok, a szolgáltatási szabályzat, illetve az általános szerződési feltételek előírá-

sainak). A felügyelet a követelmények nem teljesítése esetén intézkedéseket és szankciókat alkalmazhat.

9.4 Mitől lesz egy aláírás minősített?

A törvény definíciója szerint a minősített elektronikus aláírás olyan – fokozott biztonságú – elektronikus aláírás, amely biztonságos aláírás-létrehozó eszközzel készült, és amelynek hitelesítése céljából minősített tanúsítványt bocsátottak ki.

Mivel a fokozott biztonságú elektronikus aláírás és biztonságos aláírás-létrehozó eszköz[15] fogalma már szerepelt, az állítás érthetősége érdekében már csak a minősített tanúsítvány fogalmával kell megbarátkozni.



67. ábra
Miből lesz a minősített aláírás

9.4.1 A minősített tanúsítvány

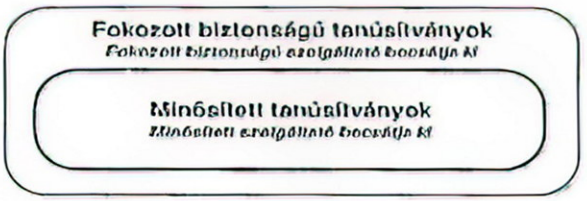
Minősített tanúsítványoknak azokat a tanúsítványokat nevezzük, melyek szigorúbb biztonsági követelményeket elégítenek ki. Elsősorban azáltal, hogy ellenőrzött biztonsági és operatív eljárásoknak, szabályzatoknak felelnek meg, amelyek szerint magasabb fokú technikai, felelősségvállalási, jogi eljárásokat alkalmaznak. A törvény szerint minősített tanúsítvány olyan, különböző (a törvény mellékletébe foglalt) követelményeknek megfelelő tanúsítvány, amelyet minősített szolgáltató bocsátott ki. A gyakorlatban ez azt jelenteni, hogy a minősített tanúsítvány teljesen ugyanolyan felépítésű tanúsítvány lesz, mint a nem minősített (fokozott biztonságú) tanúsítvány, de fel lesz benne tüntetve a minősítettségre utaló jelzés.[16]

A törvény szerint minősített tanúsítványt a szolgáltatónak biztonságos aláírás-létrehozó eszközzel kell aláírnia, nem határozza meg azonban a magánkulcs tárolási módját, ami így lehet egyszerű aláíró eszköz is. Azok a minősített tanúsítványok viszont, melyeknek magánkulcs párja nem BALE-n lett kibocsátva, nem alkalmasak minősített aláírás létrehozására.

9.4.2 A fokozott biztonságú tanúsítvány és szolgáltató

Mivel minősített aláírást minősített szolgáltató által kibocsátott minősített tanúsítvánnyal lehet létrehozni, felmerülhet a gondolat, hogy fokozott biztonságú aláírást fokozott biztonságú szolgáltató által kibocsátott fokozott biztonságú tanúsítvánnyal lehet előállítani. A törvény eredeti változata e két utóbbi fogalmat azonban nem

használja, még kevésbé definiálja. A 2. számú melléklet módosítása nyomán viszont csak megjelent a törvényben a fokozott biztonságú tanúsítvány fogalma (mint olyan jellemző, amit jelölni kell a tanúsítványban), a 16/2001. MeHVM rendelet pedig bevezeti a fokozott biztonságú szolgáltató ideáját is. Meghatározás nélkül is boldogulhatunk azonban egy kis józan ész segítségével, s mondhatjuk azt: az a fokozott biztonságú szolgáltató, aki nem minősített (de a HÍF nyilvántartásba vette), s ugyanígy az a fokozott biztonságú tanúsítvány, amely nem minősített (de fokozott biztonságú szolgáltató bocsátotta ki). Bár a gondolatmenet hatására a fogalmakat tisztáztuk, a következtetés azonban mégsem teljes, mert fokozott biztonságú aláírást minősített tanúsítvánnyal is létre lehet hozni, ha nem biztonságos aláírás-létrehozó eszközt használunk az aláírás megtételéhez.



68. ábra
Tanúsítványok osztályozása

Érdemes megemlíteni azt is, hogy minősített szolgáltató kibocsáthat fokozott biztonságú tanúsítványt is. Ezért is fontos, hogy a tanúsítványban feltüntetésre kerüljön annak biztonsági szintje.

9.5 A titkosítás szabályozása

Az EU-irányelv és az Eat. a titkosítás szabályozását nem vállalta fel. Bár műszakilag a titkosítás az egyszerűbb, jogilag ő jelent sokkal erősebb diót a szabályozás számára. Ennek legfőbb oka az államhatalom túlzott kíváncsisága, melylyel a magánszemélyek privát kommunikációja iránt viselkedik. Ez a nemzetbiztonságra való hivatkozásban szokott megnyilvánulni, ami nyilvánvaló félrevezetés, hiszen a rejtjelezés technikája csak az állam számára teljesen veszélytelen kisstílű, képzetlen bűnözők számára jelent bonyolult feladatot.

A jogalkotók ezért a titkosítás kérdését mindenhol akkurátusan leválasztották az elektronikus aláírás témaköréről, áldozatul vetve azt a magasabb cél érdekében.[17] Nem is tiltják, de nem is engedélyezik azt, a szabályozatlansággal azonban mégis ingoványos területre vezetik a rejtjelezés felhasználóit, de még az elektronikus aláírás infrastruktúráját is.

9.5.1 Titkosítás Eat. módra

Az Eat. annyiban utal a titkosításra, hogy „az aláíró az aláírás-létrehozó adatot kizárólag az aláírás létrehozására használhatja…". A törvényhez fűzött általános indokolás el is oszlat bármiféle oktalan jóhiszeműséget sejtő feltételezést: „A bekezdés nemzetbiztonsági érdekből nem teszi lehetővé az aláírás-létrehozó adatnak titkosítás céljából történő felhasználását." Bár a szándék kendőzetlenül dicstelen,

megszövegezése annyira sutára, sőt szerencsétlenre sikerült, hogy olvasóimat titkosításra bátorítva – úgy hiszem – nem követem el a felbujtás főbenjáró bűntettét.

Ha a könyv első felében tárgyalt algoritmikus ismeretek nem hullottak terméketlen talajra, még emlékezhetnek rá, hogy titkosítani nem az aláírás-létrehozó adattal (vagyis a magánkulccsal), hanem a címzett(ek) nyilvános kulcsával szoktak, sőt azzal is csak a titkosítást ténylegesen végző, az üzenetváltás idejére létrejövő kapcsolati kulcsot, ami nincs se a küldő, se a címzettek tulajdonában, mert szimmetrikus algoritmus muzsikál mögötte. A titkosításra pedig külön titkosító kulcspárt szoktak kibocsátani, hiszen a két kulcspárnak (az aláíró és a titkosító kulcspárnak) egészen mások az adminisztrációs igényei.

Bár a sete-suta fogalmazás elbizonytalaníthat bárkit, másképp nem is értelmezhetjük a jogszabályt, minthogy az aláírás és a titkosítás céljára külön kulcspárt kell kibocsátani.[18] Ha titkosításra szolgáló kulcspárok egyáltalán nem lennének kiadhatók, akkor nemcsak az elektronikus kereskedelem számára nélkülözhetetlen bizalmasságot lőnék hasba, de magát az egész nyilvános kulcsú infrastruktúrát is. Hiszen az aláíró kulcspárokat és tanúsítványokat kibocsátó szolgáltatók is e módszereket használják a szervezet különálló egységei (például a hitelesítőegység és a regisztrációs egység) közötti kommunikáció titkosítására. Ez pedig a regisztráció során felvett személyes adataink diszkréciójának megőrzése miatt elengedhetetlen.

A titkosítás területén egyéb jogszabályi előírásokra is tekintettel kell lenni, s feltétlen külön kell választani az állami és civil szférát. Az állami területre – különösen az állam- és szolgálati titok védelmének területére – természetesen eltérő jogszabályok vonatkoznak, melyek végrehajtásáért külön hatóság felelős.

9.5.2 Adatvédelmi ajánlás

Titkosítás tekintetében – kimondottan a nyilvános kulcsú kriptográfia használatával összefüggésben – a korábbi adatvédelmi biztos, Majtényi László adott ki ajánlást, melyet én követendő zsinórmértéknek érzek minden civil számára. Ennek szövegrészletét a legkisebb változtatás nélkül közlöm: „A hálózat közegében fokozottan sérülékeny a magánszféra: az üzenetekben továbbított személyes adatok biztonsága csak megfelelő titkosító eszközök használatával érhető el. Az ilyen szoftverek használatával végzett polgári célú titkosítás jelenleg Magyarországon nem tiltott. Nemzetközi példák nyomán várható, hogy a rendvédelmi szervek részéről felmerül az az igény, hogy a polgári célú titkosítás alkalmazását az állam szabályozza, s a szabályozás bizonyos jogi feltételek fennállta mellett biztosítja e szervek számára a kulcsokhoz történő hozzáférést. A nemzetközi példák nyomán arra az álláspontra jutottam, hogy a polgári célú kriptográfia jogszerű használatának korlátozása káros, a bűnüldözés hatékonysága szempontjából előnyei kétségesek, viszont a személyes adatok védelme szempontjából hátrányai kétségtelenek."

Úgy érzem, ehhez túl sok kommentár nem kívánkozik, aki az ajánlás teljes szövegére kíváncsi, ezen a címen megtalálja: http://www.ombudsman.hu/adatved/magyar/interaj.htm

JEGYZET

1 A jogszabályok szövege elérhető a HÍF weboldalán: www.hif.hu (Tájékoztatás – Elektronikus aláírás).

2 Azóta a Hírközlési Felügyelet nevet vette fel.

3 Bírósági és államigazgatási eljárásokban csak akkor lehet kizárólag elektronikus formában eljárási lépéseket foganatosítani (például kérelmet benyújtani, hiánypótlást teljesíteni), ha azt jogszabály kifejezetten lehetővé teszi.

4 A szabályozásban élen járó Németországnak ezért például teljesen át kellett szabni korábbi, túl poroszosra sikerült törvényét.

5 Bár a tudomány mai állása szerint csak a nyilvános kulcsú kriptográfia képes az elektronikus aláírás biztonságos műszaki hátteréként szolgálni, az irányelv nem a konkrét technológia jogi hátteréként akart megjelenni, hanem képes kívánt lenni a jövőben esetlegesen megjelenő más technikák befogadására is. Ezért is van az, hogy a magánkulcs helyett az általánosabb érvényű „aláírás-létrehozó adat" kifejezést, intelligens kártya helyett „aláírás-létrehozó eszköz" kifejezést (és így tovább) használ.

6 A hagyományos formák használata mellett ugyanakkor nem is tiltja meg az elektronikus formát.

7 A 2001. évi LXXIV. törvény módosította ily módon az eredeti teljes kizárást, a kiemelt adózók elektronikus csatornára terelése érdekében.

8 Vagyis a szándékos módosításoktól és a kezelés során bekövetkező technikai hibáktól mentesnek kell tekinteni a dokumentumot. Ugyanezt a hatást a törvény az elektronikus okiratokra vonatkozóan a polgári perrendtartás 197. §-ának 2. bekezdésének módosításával éri el.

9 Az elektronikus dokumentumok kinyomtatott változatához természetesen nem fűződnek ugyanezen joghatások.

10 A hitelesítésszolgáltató a regisztráció során felvett adatokat a tanúsítvány érvényességének lejártától számított legalább tíz évig vagy a tanúsítvánnyal összefüggésben esetlegesen felmerült jogvita jogerős lezárásáig köteles megőrizni.

11 Így például ha egy internetszolgáltatáshoz kapcsolódóan – annak költségeitől nem elkülönítve – nyújt tanúsítványokat az internet- és egyben hitelesítésszolgáltató ügyfeleinek, akkor az bejelentkezési kötelezettséggel jár. Ha viszont egy vállalat saját dolgozóinak bocsát ki tanúsítványokat minden áttételes és rejtett költségek nélkül, annak nem kötelező bejelentkezni a felügyelethez.

12 A bejelentést követően természetesen új tanúsítványt sem bocsáthat ki. A visszavonásnak szerintem eleget tehet az egyetlen szolgáltatói kulcs visszavonásával is.

13 Ha ezt nem teszi meg, a HÍF jelöl ki ilyen szervezetet.

14 Ezzel nem csak arra gondolok, hogy az aláíró és az érintett fél hibáiért nem felel, de arra is, hogy az algoritmus esetleges feltöréséért sem felelős.

15 A biztonságos aláírás-létrehozó eszközökre vonatkozó követelményeket a törvény 1. számú melléklete határozza meg.

16 Erre vonatkozóan adnak útmutatót az ETSI 101-862 és RFC 3039 szabványok.

17 A magyar jogalkotási folyamat elején is volt egy pillanat, mikor a tudós emberek kerekasztal-megbeszélését megtisztelte érdeklődő és irányt mutató jelenlétével a titkosszolgálatok képviselője.

18 Némely esetben ez is gondot jelent, mert sok alkalmazás nem képes két külön kulcspár korrekt kezelésére.

10 Az elektronikus aláírás (és társai) lélektana

Ajánlás:

Mindenkinek.
Különösen rendszergazdáknak
és vállalati megoldások tervezőinek.

Ez a fejezet amolyan „tippek és trükkök" jegyzéke, kevésbé érdekfeszítően fogalmazva: mindazok összegyűjtve, amik az eddig elmondottakból kimaradtak (méghozzá általában azért, mert nem tartoztak szorosan az elméleti ismeretekhez). A lelki vonalat némiképp cáfolva nagyon is gyakorlati tudnivalók jönnek megint. Lélektan mégis abban az értelemben, hogy ezek a funkciók irányítják azt a matematikai-algoritmikus réteget, amelyre épülnek, s ezek vizsgálata mutatja meg számunkra, hogy hogyan működik valójában a rendszer.

10.1 A magánkulcs védelme

Mint azt már többször is említettem, a magánkulcs védelme kiemelt jelentőségű a nyilvános kulcsú rendszerek biztonsága szempontjából. Kétkomponensű volta kétfajta védelmet is jelent: egy fizikait a kulcs hordozójának és egy logikait az aktivizáló adat számára.

10.1.1 Fizikai védelem

Az aláíró eszköz és más mobil kulcshordozók fizikai védelme evidens: lehetőleg legyen mindig nálunk, soha ne veszítsük szem elől, vagy tartsuk biztos, védett helyen. Kezeljük minimum olyan gondossággal, amilyennel a bankkártyánkat. Ha a számítógép merevlemezén kell tárolni a magánkulcsunkat, akkor a géphez való hozzáférést mind a lokális, mind a hálózati felhasználók számára nehezítsük meg, amennyire csak tudjuk. Védjük a számítógépet fizikailag is (ne kapcsolhassa be bárki); tartsuk kikapcsolva, amikor nem használjuk; a hálózati kapcsolatot szakítsuk meg fizikailag is, amikor nincs rá szükségünk; használjunk személyes tűzfalat stb. Ilyen esetben a magánkulcsot tároljuk biztonságos fájlrendszeren (például NTFS), a jogosultságok korlátozásával, rejtjelezett formában. Az operációs rendszerbe való belépést jelszavakkal korlátozzuk (a **Windows 95, 98, ME** rendszerek esetében ez nem sokat ér). Különösen fontos mindez mobil számítógépek esetében, illetve helyi hálózatba kötött gépeknél.

Ha kulcshordozónk (intelligens kártyánk, számítógépünk stb.) eltűnését észlelnénk, azonnal függesszük fel tanúsítványunk érvényességét, majd vonjuk vissza, ha kiderül, nemcsak vaklármáról volt szó. Tegyünk ugyanígy, ha megalapozottan vélelmezhető a magánkulcsunkhoz való jogtalan hozzáférés. Soha-

se bízzunk meg teljesen az előbbiekben felsorolt védelmi megoldásokban (bármilyen körültekintően valósítottuk is meg őket) és az aktivizáló adat által nyújtott védelemben.

Ha ideiglenesen vagy véglegesen nem használjuk magánkulcsunkat, akkor a tanúsítvány felfüggesztése, illetve visszavonása mellett a magánkulcsot is tegyük hozzáférhetetlenné: zárjuk biztos helyre vagy semmisítsük meg. Soha ne hagyjuk a számítógép háttértárolóján a magánkulcsunkat, ha eladjuk vagy kölcsönadjuk a gépet. Ne letöröljük az állományt, hanem írjuk felül tartalmát véletlen bitsorozattal.

10.1.2 Az aktivizáló adat

Az aktivizáló adat, amelyet az aláírási eljárás során és visszafejtéskor meg kell adni, nem az eljárások paramétere, hanem a magánkulcs inicializálásához szükséges. Csak az az aláírási rendszer tekinthető biztonságosnak, amelyik a magánkulcsot aktivizáló adattal védi, s azt nem tárolja, hanem minden alkalommal elkéri a felhasználótól (ellenkező esetben a védelem nem kétkomponensű, hiszen a tudás fázisa kiiktatódik).

Az aktivizáló adat a hardveres kulcstároló és aláíró eszközök esetében egy PIN-kódot szokott jelenti, állományban tárolt kulcs esetében pedig jelszót. Veszélyt jelenthet rá a billentyűzetről való leolvasás vagy egy trójai falóként beépülő billentyűzetfigyelő programmal való ellopás. Ez ellen védelmet nyújthat, ha az aláíró eszköznek (illetve a kártyaolvasónak) saját számkódos billentyűzete van, vagy ha a billentyűzet és az aláíró eszköz között közvetlen a kapcsolat (s így az aktivizáló adat a billentyűzetről begépelve el sem jut a számítógépbe).[1] Ugyanígy veszélyt jelenthet a nyers erős (sokszoros) próbálkozás is. Mivel az eszközök bizonyos számú próbálkozás után letiltják a magánkulcs elérését, a PIN-kódnak nem kell különösebben szofisztikáltnak lenni. Az állományban tárolt magánkulcsok esetében azonban nincs ilyen korlát, így elővigyázatosabb módon kell jelszót választanunk magánkulcsunk védelmére.

10.1.3 A jelszó

De milyen a jó jelszó? Véletlenül sem ismert adatok kombinációja: házastárs, szerető, gyerek, háziállat neve, még „találékony" formában sem (például fordítva írva). Sőt még csak nem is az élő nyelvben (bármely nyelvben) használt szavak vagy azok összetétele (ezeket a szótár módszerrel pillanatok alatt fel lehet törni).[2]

A jó jelszónak nincs semmi értelme, kisbetűt, nagybetűt, számot és egyéb speciális karaktereket egyaránt tartalmaz, minimum nyolc karakter hosszú. Nem baj, ha van benne valami logika az egyszerűbb megjegyezhetőség végett, de az ne legyen nyilvánvaló, közismert tudásra építő. Semmiképp se legyen azonban annyira bonyolult, hogy fel kelljen írnunk valahova. Nem árt (igaz, nem is használ túl sokat), ha időnként megváltoztatjuk jelszavunkat. Ha viszont

ilyet teszünk, tegyük alaposan, ne csak az utolsó karakterként megadott számot növeljük egyesével nagyobbra. Az aktivizáló adat semmiképp ne egyezzen meg egyéb, bárhol máshol használt jelszavunkkal vagy mobilunk PIN-kódjával, bőröndünk számkódjával. Sokat tehetnek a biztonság érdekében az alkalmazásfejlesztők is a jelszómegadás számszerű vagy időbeli korlátozásával.

Hiába azonban minden ilyesfajta ügyeskedés, ha magánkulcsunkhoz tartósan hozzáférnek, netán arról másolatot képesek készíteni. A nyolckarakteres jelszavak tízbilliárd körüli kombinációs száma[3] ma már nem feltörhetetlen dió egy erősebb személyi számítógép számára sem.

10.2 Fizikai tanúsítványformátumok

Az X.509-es szabvány nem szabályozza a tanúsítvány fizikai (bájt szintű) tárolását. A tanúsítvány felépítésére, mezőinek, toldalékainak definiálására az absztrakt objektumok (például üzenetek és tanúsítványok) specifikálására kifejlesztett ASN.1 (Abstract Syntax Notation One) jelölőnyelvet[4] használja. Az egyes mezők kódolására a DER (Distinguished Encoding Rules) kódolást írja elő, amely a BER (Basic Encoding Rules) és CER (Canonical Encoding Rules) kódolás továbbfejlesztett változata.[5] A legtöbb alkalmazás ezért a tanúsítvány egészének kódolására is a DER kódolást használja. Emellett azonban széles körben elterjedtek más kódolási módszerek is. Ilyen például a Base64, melyet a MIME és S/MIME szabványok kapcsán fejlesztettek ki bináris csatolt állományok kódolására[6], s így implementációja minden internetes applikációban megtalálható. Elterjedt az RSA Laboratories által kifejlesztett két kódolás, a PKCS #7 (Cryptographic Message Syntax Standard) és a PKCS #12 (Personal Information Exchange) használata is. Az előbbi lehetővé teszi egy állományban több tanúsítvány összefogását is (egymástól független tanúsítványokat vagy egy tanúsítási lánc tagjait), és a tanúsítványok mellett különböző attribútumok tárolását is meg tudja oldani. Az utóbbi képes a tanúsítvány mellett a magánkulcs tárolására is, valamint szintén magába tudja foglalni egy tanúsítási lánc minden tanúsítványát. E két tárolási forma így tulajdonképpen nem is, illetve nem csak tanúsítványkódolási forma, de tanúsítványtár-formátum is.

Tanúsítványtárak a **Windows** által kezelt CTL (Certificate Trust List) és a Microsoft Serialized Certificate Store formátumok is. Az előbbi – tanúsítványbizalmi listaként fordítható – tár a hitelesítésszolgáltatók önhitelesített gyökér tanúsítványának listája. Ezt tipikusan egy szervezet ezért felelős adminisztrátora állítja össze a helyi szabályzatoknak megfelelően, korlátozva – ha szükséges – a benne szereplő tanúsítványok felhasználhatóságát, és aláírva a listát. Az utóbbi a Microsoft saját formátuma, amely a PKCS #7 és PKCS #12 formátumok tulajdonságait egyesítve több tanúsítványt is képes tárolni, azok magánkulcsaival együtt.

A különböző tanúsítványformátumok eltérő kiterjesztésű állományok formájában öltenek testet: a DER és Base64 kódolású tanúsítványok DER, CER

vagy CRT kiterjesztést kapnak, a PKCS #7 kódolásúak P7B, P7C[7] vagy SPC, a PKCS #12 kódolásúak P12 vagy PFX, a Certificate Trust List STL, a Microsoft Serialized Certificate Store SST kiterjesztést. Ezek a formátumokat mind ismeri és kezeli a **Windows**, exportálhatóak és importálhatóak a belső tanúsítványtárba, illetve onnan.

A visszavonási listák szintén helyt kaphatnak PKCS #7 formátumú tárakban és CRL kiterjesztésű állományokban.

10.3 A Windows és az Office

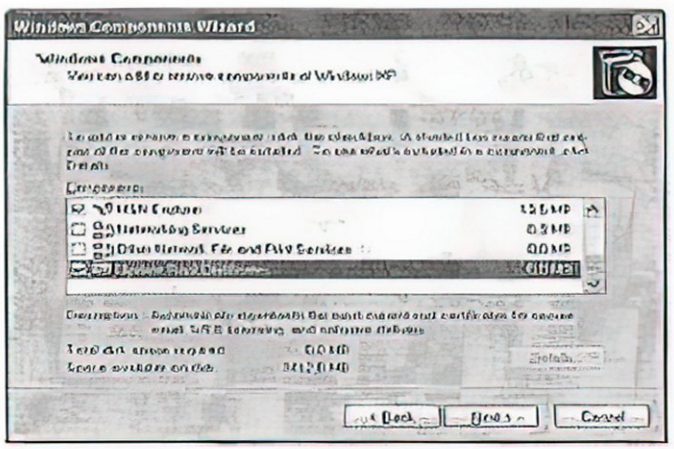
Nem egy még mindig létező hiányossága ellenére a **Windows** egyre fejlettebb módon valósítja meg a kriptográfia által biztosított lehetőségeket. Fájlrendszere titkosított formában képes az állományok tárolására, saját belső tanúsítványtárral rendelkezik, képes aláírások, tanúsítványok, hitelesítési láncok és visszavonási listák megjelenítésére és kezelésére, aláírt programok felhasználására, mindezen tevékenységek kapcsán természetesen aláírás-ellenőrzésre, valamint intelligens kártyák kezelésére. Kiszolgáló szolgáltatásai közül kiemelendő az Active Directory címtárszolgáltatás, ami alkalmas tanúsítványtárként funkcionálni tartományi felhasználók részére, valamint a beépített hitelesítőegység, amellyel tanúsítványokat lehet kiadni. Az **Internet Explorer** és **Outlook** programok elektronikusan aláírt és rejtjelezett kommunikációra képesek, s – amint azt láttuk – a többi **Office**-program is rendelkezik aláírási és titkosítási funkciókkal. E funkciók egy része már a **Windows/Office 2000**-ben megjelent, majd később a **Windows/Office XP**-ben teljesedett ki. Mindezen műveleteket szabványos módszerekkel támogatja, a leggyakrabban használt algoritmusokat (RSA, DES, SHA-1 stb.) megvalósítva, az X.509 tanúsítvány és visszavonásilista-formátumoknak, a PKCS szabványkészletnek és egyéb PKI-szabványoknak megfelelve. Az alábbiakban bemutatom ezeket a lehetőségeket mélyebben is, jelölve – ahol nem felejtem –, melyik funkció mely verziótól elérhető.

Ez a rész felfogható a könyv elején helyet kapott gyakorlati fejezet folytatásaként is. Azok az ott „bölcsen" elhallgatott apróságok és finomságok kaptak itt helyet, amelyek a két fejezet között tárgyalt elméleti ismeretek nélkül nem feltétlen lettek volna érthetőek, vagy kellő bevezetés nélkül túlságosan elrettentőek lettek volna.

10.3.1 Windows tanúsítványtár

A **Windows** egy saját tanúsítvány-nyilvántartással (Certificate Store) rendelkezik, melyben saját tanúsítványaink, partnereink tanúsítványai, a hitelesítésszolgáltatók (gyökér és kibocsátó) tanúsítványai, a megbízhatatlannak minősített tanúsítványok, a szoftverhitelesítők tanúsítványai, visszavonási listák és tanúsítványbizalmi listák kapnak helyet. A tanúsítványok mellett itt tárolódnak a tanú-

sítványhoz felvehető tulajdonságértékek is (lásd: 78. ábra). Ez a nyilvántartás szűz (frissen telepített) operációs rendszer esetében is tartalmaz tanúsítványokat, méghozzá a Microsoft által megbízhatónak tartott szolgáltatók tanúsítványait. Némi óvatosság elkél ennek kezelésekor, mert a Microsoft korábban nem volt véresen szigorú az ide történő bekerüléssel kapcsolatban (az idei évtől a bekerüléshez viszont már megkövetel független auditori vizsgálati jelentést[8]). Nagy gyengesége a listának, hogy vegyesen, minden megkülönböztetés nélkül tartalmaz teljesen eltérő erősségű szolgáltatásokhoz kapcsolódó szolgáltatói tanúsítványokat.[9] Mindenkinek azt javaslom, hogy nézze át a listát, és nyirbálja meg, csak azokat a szolgáltatókat meghagyva, amelyeket valóban ismer, nekik is csak azokat a szolgáltatásukat (tanúsítványosztályukat), melyek garantálják az általa megkövetelt biztonságot. A nyilvántartásban eleve szerepel két megbízhatatlan tanúsítvány is, amely az ominózus Verisign által tévedésből kiadott, a Microsoft nevére szóló tanúsítványokat takarja. A lista automatikus frissítése a **Windows Component Wizards**-ban (**Control Panel – Add or Remove Programs – Add/Remove Windows Components**) az **Update Root Certificates** kontrollkocka segítségével állítható be.[10]



69. ábra
Gyökér szolgáltatók listájának frissítése

A nyilvántartás később saját, partnereink és az általunk megbízhatónak minősített hitelesítésszolgáltatók tanúsítványaival szaporodik, amelyeket vagy interneten keresztül töltünk le, vagy explicit beimportáljuk őket.

A tanúsítványtár a következő logikai egységekre tagozódik:[11]

- Personal: Ez a saját tanúsítványok könyvtára, ahol olyan tanúsítványok tárolódnak, melyek magánkulcsával is rendelkezünk. Tipikusan saját részre vagy a felügyeletünk alatt álló számítógépek és alkalmazások részére kibocsátott tanúsítványok. Az itt tárolt tanúsítványok mellett a hozzájuk tartozó magánkulcsra és kriptográfiai szolgáltatóra is van utalás.
- Third-Party Root Certification Authorities: Megbízhatónak minősített külső hitelesítésszolgáltatók gyökér tanúsítványai.
- Trusted Root Certification Authorities: Az előbbi tár kiegészítve a Microsoft, valamint saját szervezetünk hitelesítésszolgáltatásának gyökér tanúsítványaival.
- Enterprise Trust: A szervezet tanúsítványbizalmi listáinak (CTL-ek) könyvtára.
- Intermediate Certification Authorities: Kibocsátó hitelesítőegységek tanúsítványainak könyvtára.

- Trusted People: Olyan, nem szolgáltatói tanúsítványok listája, melyek tipikusan önaláírtak, s ezért explicit bizalmat kellett szavaznunk számukra (például ide kerülnek az EFS tanúsítványok).
- Other People: Olyan, nem szolgáltatói tanúsítványok listája, melyek hitelesítésszolgáltató által aláírtak, s ezért implicit megbízhatóak (például ide kerülhetnek levelezőpartnereink tanúsítványai).
- Trusted Publishers: Az általunk megbízhatónak minősített szoftverhitelesítők tanúsítványai.
- Untrusted Certificates: Megbízhatatlannak minősített tanúsítványok (általunk vagy a Microsoft által).
- Certificate Enrollment Requests: Még el nem bírált vagy visszautasított tanúsítványkérések.
- Active Directory User Object: A felhasználó Active Directoryban publikált tanúsítványainak logikai képe.

A tanúsítványtár különböző szegmensekre is tagozódik. A gépen felhasználói azonosítóval rendelkező valamennyi felhasználónak, szerviznek (rendszerszolgáltatásként futó program) és magának a gépnek is van egy szegmense, amin belül az előbb felsorolt logikai egységekkel találkozhatunk (nagyjából).[12] A logikai egységek jelentése és tartalma alapesetben megegyezik minden szegmens esetében. A Personal könyvtár természetesen mindenhol az adott felhasználóra, gépre, szervizre vonatkozik, és tartalma csak addig ugyanolyan mindenhol, ameddig üres. Amennyiben felveszek vagy kitörlök egy tanúsítványt az egyik szegmens egyik logikai egységéből, az általában nincs hatással egy másik szegmens (például egy másik felhasználó vagy egy másik szerviz) ugyanazon logikai egységére. Azért csak általában, mert van egy kivétel, mégpedig a gép szegmense, azon belül is a szolgáltatói tanúsítványok logikai egységei (különböző Certification Authorities és Enterprise Trust egységek). E logikai egységek beállításait a felhasználói szegmens ugyanezen logikai egységei is átveszik. Ez azt jelenti, némi példával szemléltetve, hogy ha a személyes szegmensünk gyökér tanúsítványai közül töröljük az egyik hitelesítésszolgáltató tanúsítványát, attól még egy másik felhasználó vagy egy szerviz, valamint maga a gép is még meg fog bízni ebben a szolgáltatóban; ha viszont a gép gyökér tanúsítványai közül töröljük az egyik hitelesítésszolgáltató tanúsítványát, akkor a többi felhasználó sem fog megbízni ebben a szolgáltatóban.[13]

A megbízhatónak minősített szolgáltatói tanúsítványok listájának sértetlensége – bár azt a legtöbbször nem említik – biztonsági szempontból ugyanannyira kritikus, mint magánkulcsunk védelme. Ha rajtunk kívül bárki képes tanúsítvány elhelyezésére a listában, akkor azzal olyan aláírások elfogadására vesz rá minket, amit magunktól nem tennénk. Méghozzá úgy, hogy ez számunkra észrevétlen marad mindaddig, míg nem nézzük át tüzetesen a listát, vagy addig, amíg nem kerülünk bajba e visszaélés miatt. A **Windows** esetében az ilyen típusú visszaélések mindazok számára lehetségesek, akik nevünkben vagy adminisztrátorként képesek bejelentkezni gépünkre.

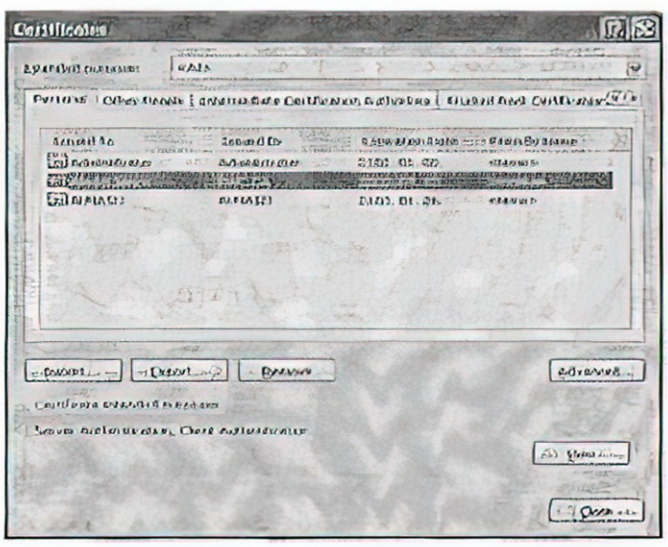
A belső tanúsítványtár fizikailag három különböző helyen tárol tanúsítványokat: a Registryben, állományban a winchesteren és csoportszabályzatban.[14] A fizikai tárolás megjelenítésével láthatóvá válik, hogy melyik tanúsítvány hol tárolódik e fizikai tárolóhelyek közül.[15] A Registryn belül leginkább a HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates alatt találhatunk tanúsítványokat (alapos böngésző még további helyeken is), a fájlrendszeren belül pedig system fájlformátumban, a \Documents and Settings*felhasználó*\Application Data\Microsoft\SystemCertificates könyvtárban.

A magánkulcsokat a **Windows** egy úgynevezett védett tárban (protected store) tárolja. A védelem itt egy rejtjeles tárolási formát jelent, amiről a CryptoAPI gondoskodik. A kulcsok ténylegesen a \Documents and Settings*felhasználó*\Application Data\Microsoft\Crypto\RSA könyvtárban találhatók.[16]

A magánkulcsok és a tanúsítványok részei a felhasználói profilnak, s mikor először jelentkezünk be egy hálózati gépre, átmásolódnak oda a profilgazda gépről. Ugyanígy a menet közben szerzett kulcsok és tanúsítványok a profil részként kijelentkezéskor a profilgazda gépre másolódnak. Ez a kényelem a másik oldalon gyengeség, hiszen izgő-mozgó felhasználóként magánkulcsunkat számos gépen otthagyjuk, ami jelentősen megkönnyíti annak rosszhiszemű megszerzését.

10.3.2 Tanúsítványok menedzsmentje – Certificates ablak

A belső tanúsítványtár felhasználói szegmenséhez hozzáférést biztosító **Certificates** ablak (az **Internet Explorer** része) a **Control Panel – Internet Options – Content – Certificates** útvonalon keresztül érhető el vagy **Internet Explorer**-ből, a **Tools – Internet Options...** menüpontokon keresztül.[17] Ebben az ablakban mindig a bejelentkezett felhasználóra vonatkozó tanúsítványokat látjuk, a gép vagy egyes szervizek tanúsítványainak megjelenítésére itt nincs mód (más felhasználó szegmensének megtekintéséhez be kell jelentkezni az ő nevében).



70. ábra
Tanúsítványok menedzsmentje a Certificates programmal

A képernyőn lehetőségünk van tanúsítványok fájlból történő importálására (megfelelő jogosultság esetén) vagy oda történő exportálására, valamint tanúsítványok törlésére a tárból. Exportálni drag and drop módszerrel is lehet a kívánt tanúsítványt az **Intéző** ablakába mozgatva. Az ekkor használatos állo-

mányformátumot az **Advanced** opcióknál adhatjuk meg. A tanúsítványt megnézhetjük kettőt klikkelve rá vagy a **View** parancsal. A megjelenített tanúsítványokat felhasználási cél szerint szűrni tudjuk (**Intended purpose**). Visszavonási listák importálására is módunk van itt, de az exportálás nem lehetséges, minthogy a visszavonási listák ebben az ablakban nem jelennek meg.

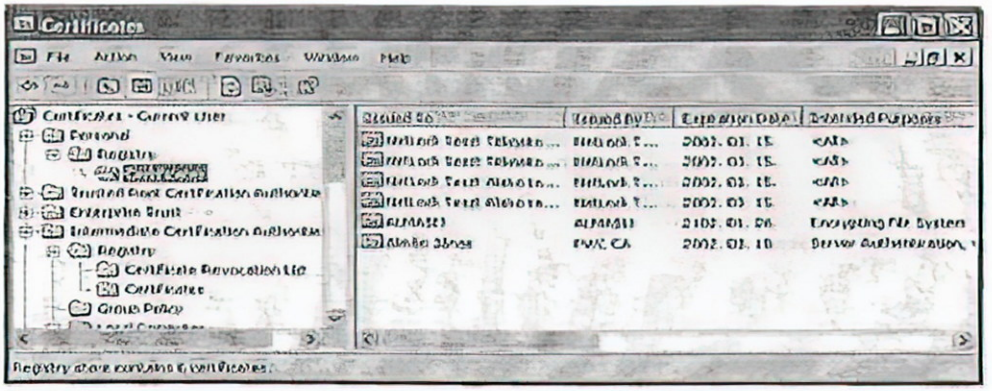
10.3.3 Tanúsítványok menedzsmentje – MMC

A tanúsítvány-nyilvántartás elérhető a **Microsoft Management Console** felületén keresztül is.[18] Ehhez a **Certificates** modult kell a konzol felületére varázsolnunk, amit a \WINDOWS\system32\certmgr.msc sablonfájl betöltésével vagy az **Add/Remove snap-in** parancsal (**Standalone** fül alatt **Add...** gomb) érhetünk el. Ez utóbbi esetben meg kell határoznunk, hogy a személyes tanúsítványainkhoz vagy egy szerviz, illetve egy gép saját tanúsítványaihoz akarunk hozzáférni (a sablon fájl betöltésével csakúgy, mint a **Certificates** ablakon keresztül, csak személyes tanúsítványainkhoz férünk hozzá). Gépet választva megadhatjuk, melyik gép, szervizt választva pedig hogy melyik gép melyik szervizének tanúsítványai iránt érdeklődünk (lásd: 72. ábra, itt lokális gép és egy szerviz is látható). Másik felhasználó tanúsítványaihoz ilyen módon nem férünk hozzá, ahhoz az ő nevében kell bejelentkeznünk.

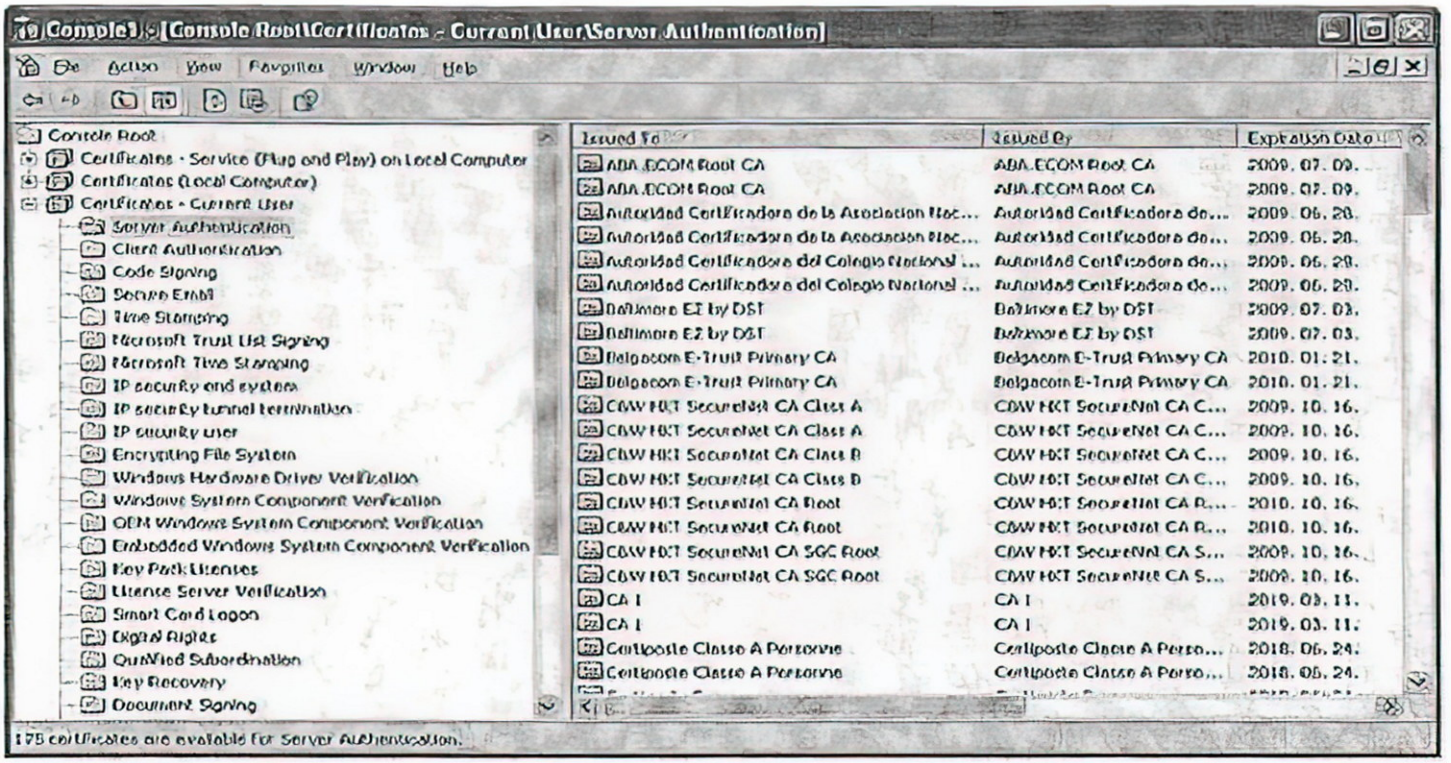
Az **MMC** összetettebb megtekintési és kezelési módszert biztosít a tanúsítványok számára, mint a **Certificates** ablak. A **View** menü **Options** ablakán (amely az **MMC** bal oldali fastruktúrájának valamely felsőbb szintű elemén állva érhető csak el) beállítható, hogy a tanúsítványok fizikai tárolóhelye is megjelenjen, továbbá mód van az archív (már lejárt érvényességű) tanúsítványok megjelenítésére is.[19] A jobb egérgomb hatására megjelenő menü **Find Certificates** menüpontján keresztül keresni lehet a tanúsítványok között. Ugyanezen menü **All Tasks** almenüjén keresztül mód van tanúsítványok exportálására és importálására, valamint a fizikai tárolóegység szintjén állva a tárolóegység adott szintjének Microsoft Serialized Certificate Store formátumban történő exportálására (az **Export List** parancs csak a képernyő jobb oldali paneljának adatait írja ki szöveges formátumban, a tanúsítványok tartalmát nem).

Az **Options** ablakban beállítható az is, hogy a tanúsítványok ne az alapértelmezés szerinti logikai tárak szerint jelenjenek meg, hanem a felhasználás célja szerint rendezve.

Az egyes tanúsítványok a tárolók között a szokásos vágólapparancsok (CTRL-C, CTRL-V, stb.) és drag and drop műveletek segítségével másolhatók, mozgathatók, ennek gyakorlását azonban csak annak ajánlom, aki biztos annak következményeiben, amit tesz.



71. ábra Tanúsítványok menedzsmentje MMC-vel



72. ábra Tanúsítványok megjelenítése a felhasználás célja szerint rendezve

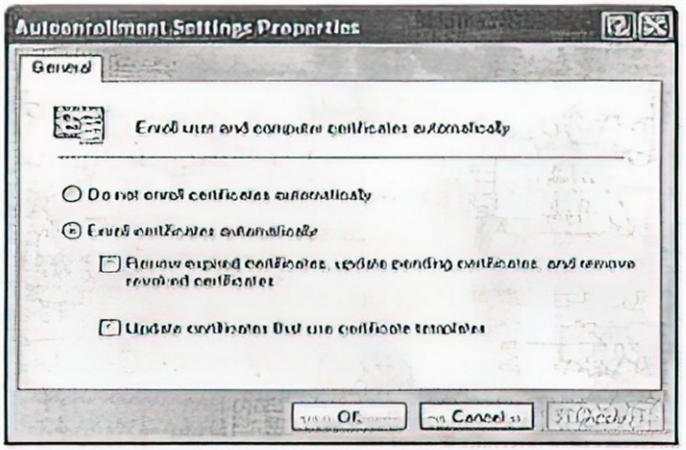
10.3.4 Microsoft Certificate Server

A **Windows 2000 Server** (csak a Server kiépítés) rendelkezik egy beépített hitelesítőegységgel, a **Microsoft Certificate Server**-rel. Ennek belső működését nem kívánom ismertetni, mert ezzel csak néhány vállalati rendszergazda érdeklődését keltheteném fel. A hitelesítőegység szolgáltatásai azonban mindazon vállalati felhasználók számára érdekesek lehetnek, ahol a cég ilyen biztonsági rendszert üzemeltet.

A hitelesítőegységet két üzemmódban lehet beüzemelni: Stand-alone és Enterprise módban.[20] Az előbbi nem feltétlen integrált az Active Directoryval, utóbbi igen, és így összetettebb szolgáltatások nyújtására képes. Utóbbi esetben a kibocsátott tanúsítványok és visszavonási listák, de az egység(ek) helye és a velük kapcsolatos szabályzatok is, mind a címtárban kerülnek közzétételre. Az előbbi esetben kevésbé szofisztikált módszerekre kell hagyatkoznunk: például egy közös könyvtárban való CRL közzétételre.

Stand-alone mód esetében csak weboldalon keresztüli tanúsítványmenedzsment-műveletek működnek. Ekkor a tanúsítvány igénylését, megújítását, visszavonását mind egy céges belső weboldalon kell intézni, amely oldalt a cég rendszergazdái készítenek el. Ez nyilván minden cég esetében máshogy néz ki, de lényegét tekintve a könyv elején bemutatott eljárásról van szó (lásd: 2.1 fejezet). Enterprise mód esetén szintén használhatjuk a weben keresztüli menedzsmentet (s ez esetben vélhetően kevesebb adat megadására lesz szükségünk, mert a címtárból hozzákeresheto, ami kell), valamint módunk van az **MMC** felületéről történő tanúsítványkezelésre is.[21] Ekkor a tanúsítványkérelem egy tanúsítványvarázsló segítségével történhet, amihez a **Certificates** modult kell az **MMC** konzoljára tennünk, s a Personal könyvtáron állva a jobb egérgombbal előhívható **All Tasks** menü **Request New Certificate** menüpontját kell választanunk. Ily módon tanúsítványt tudunk kérni saját magunk vagy a gép számára (de egy szerviznek nem). Hasonló módon, egy már létező tanúsítványon állva, a tanúsítvány megújítható vagy új tanúsítvány igényelhető ugyanazon kulccsal vagy új kulccsal.

Microsoft Certificate Server használata esetén a **Control Panel – Administrative Tools – Local Security Policy** képernyő **Public Key Policies** beállításainál találhatunk lehetőséget a tanúsítványok megújításának automatizálására (**Windows XP** esetén).



73. ábra
Automatikus tanúsítványmegújítás beállítása

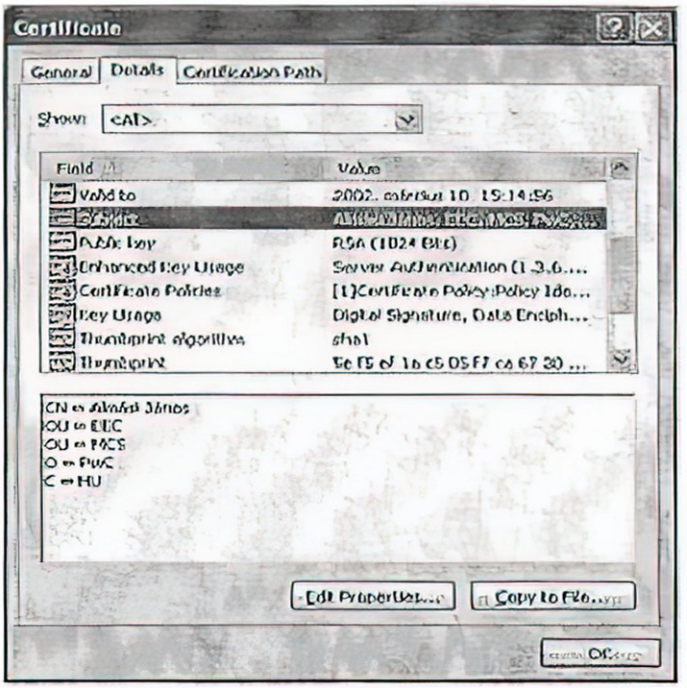
10.3.5 A Certificate ablak

A tanúsítványok tartalmának megjelenítését a **Windows** egy három–öt füllel rendelkező ablakban végzi. Az első fül alatt (főoldalon) a legfontosabb információk kivonata található. A tanúsítvány felhasználási célja (a kulcshasználat, kiterjesztett kulcshasználat és Netscape tanúsítványtípus szabványos toldalékok alapján),[22] a hitelesítési szabályzat OID-ja (ha az a tanúsítványban szerepel), a tanúsítvány tulajdonosának és kibocsátójának neve (az azonosítók Common Name mezője alapján), a tanúsítvány érvényessége és az, hogy a rendszer ismeri a tanúsítvány magánkulcs párját (saját tanúsítványok esetén nyilván igen, egyébként nem).

A bal felső sarokban található tanúsítvány szimbólum kinézete fontos jelentést hordoz. Alap formában (ami alant látható) azt jelzi, hogy a tanúsítvánnyal

nincs probléma. Egy piros körben megjelenő fehér kereszt feltűnése arra utal, hogy a tanúsítvány nem érvényes (mert például lejárt), vagy a kibocsátó szervezet nincs benne a megbízható hitelesítőszervezetek listájában.[23] A kis sárga háromszögben feltűnő felkiáltójel azt jelenti, hogy a **Windows** nem képes a tanúsítvány ellenőrzésére (mert például nem rendelkezik a hitelesítőszervezet tanúsítványával). Ezen állapotokra vonatkozóan szöveges információ is megjelenik a szimbólum alatt (a felhasználási cél helyett).

74. ábra
A tanúsítvány főbb adatainak megjelenítése



75. ábra
A tanúsítvány adatainak részletes megjelenítése

Az **Issuer Statement** gomb automatikusan megjeleníti a szolgáltató szabályzatát (melyre a Certificate Policies toldalék mutat) egy böngészőablakban.

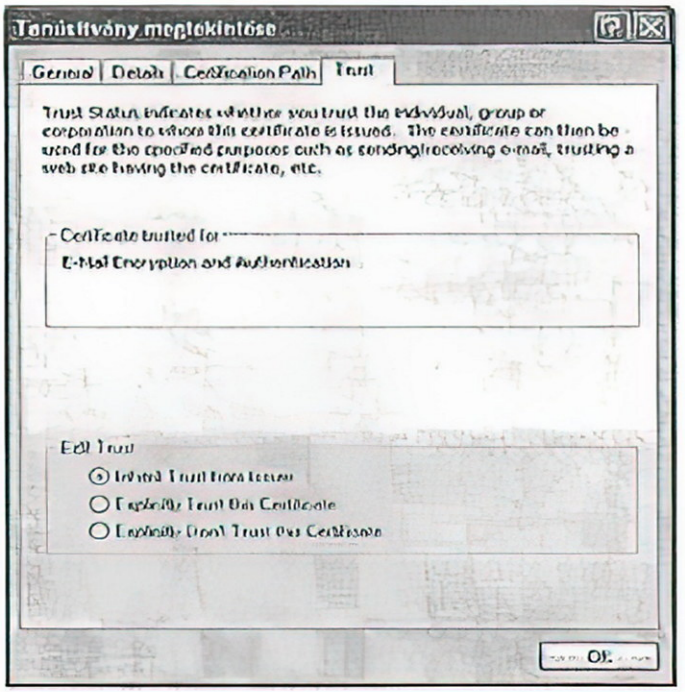
A második fül alatt a tanúsítvány mezőinek tételes tartalma jelenik meg. Ha a tanúsítvány tulajdonosának vagy kibocsátójának neve nem volt egyértelmű, akkor itt a teljes azonosító megtekinthető. Ugyanígy részletesebb (óra és perc) adatokkal van feltüntetve az érvényességi idő is, valamint itt lehet megtudni az algoritmus típusát és a kulcs erősségét.

A mezőnév mellett baloldalt szereplő jel mutatja, hogy a standard mezőről vagy toldalékról van-e szó, és a toldalék kritikus (felkiáltójel sárga háromszögben) vagy sem (zöld lefele mutató nyíl). A tulajdonságként (sárga ceruzával) feltüntetett mezők és értékeik olyan adatok, amelyek nem részei a tanúsítványnak, hanem a belső tanúsítványtárban mellette tárolódnak, vagy belőle következnek (például lenyomat). A mezőtípusokra a **Show** listában értéket választva szűrni is lehet (csak a kritikus toldalékokat megmutatva például). Egy adott mezőt kiválasztva a képernyő alsó felében megjelenik a mező tartalma részletesen.

A különböző típusú mezők eltérő módon jelennek meg (a 75. ábrán egy egyedi azonosító látható). Ha a **Windows** nem ismeri a tanúsítványba foglalt toldalékot (mert az nem szabványos, vagy „nem úgy" szabványos), akkor annak OID-ját írja ki, ellenkező esetben a mező nevét.

A harmadik oldal a tanúsítási lánc felépítését mutatja[24] és a tanúsítvány állapotát jelzi (a lánc azon tanúsítványának állapotát, amin állunk). Ha a tanúsítvány lejárt vagy más probléma van vele, itt nem a **This certificate is OK.**, azaz „tanúsítvány rendben" szöveg jelenik meg. A tanúsítási lánc valamely tanúsítvány tagján állva annak részletes adatait is megtekinthetjük a **View Certificate** gomb segítségével.

76. ábra
A tanúsítási lánc megjelenítése



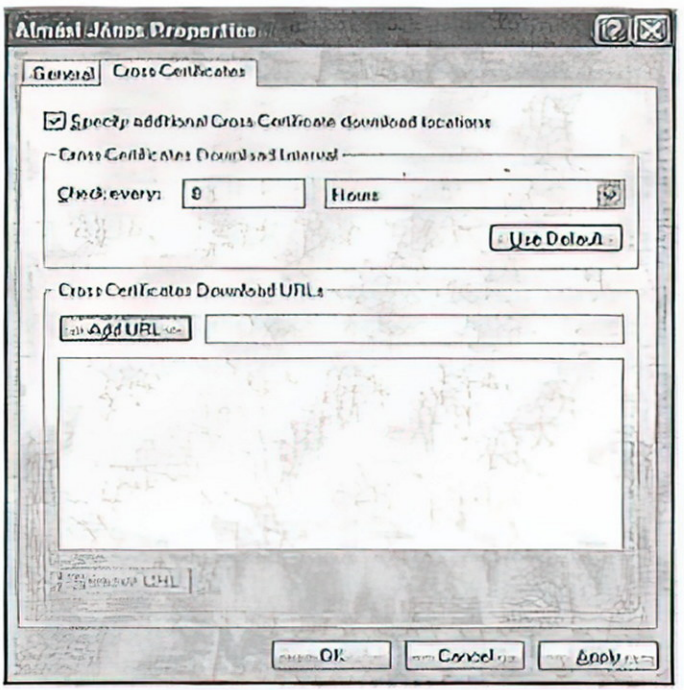
77. ábra
Tanúsítvány megbízhatósági beállításai

A negyedik és ötödik fül opcionális, megjelenésük a tanúsítvány típusától függ. A negyedik, **Trust** fül[25] opciói segítségével egyes tanúsítványokra lehet megadni, hogy azokban egyedileg is megbízzunk (akkor is, ha a kibocsátójában egyébként nem bízunk meg), vagy pont fordítva. Ez az információ a tanúsítvány mellett tárolódik a fájlban vagy a levélben (a tanúsítványtárban ilyen beállítási lehetőség nincs). Az ötödik fül a tanúsítvány **Address Book**-ban való rögzítésére ad lehetőséget.

A második oldalon található **Copy To File** gomb segítségével a tanúsítványt különböző formátumú fájlokba exportálhatjuk. Az ugyanitt elérhető **Edit Properties** gomb hatására a **Certificate Properties** (Tanúsítványtulajdonságok) ablak jelenik meg, ahol különböző beállítási lehetőségeink vannak a kérdéses tanúsítványra vonatkozóan (ezek az információk természetesen nem a tanúsítványba kerülnek be, hanem mellette tárolódnak). Beállíthatunk a tanúsítvány-

nak egy barátságos nevet, leírást írhatunk hozzá, és korlátozhatjuk a tanúsítvány Kiterjesztett kulcshasználat toldalékában feltüntetett felhasználási célokat. Akár le is tilthatjuk az összes ilyen felhasználási célt, s így az ezt ellenőrző alkalmazások számára megakadályozhatjuk a tanúsítvány elfogadását. Az **Add Purpose** gomb segítségével felhasználási célokat rendelhetünk azon tanúsítványokhoz, melyek nem rendelkeznek Kiterjesztett kulcshasználat toldalékkal.

78. ábra
Tanúsítványhoz rendelhető tulajdonságok



79. ábra
Kereszthitelesítésre vonatkozó attribútumok

Ugyanezen képernyő második fülén a kereszthitelesítéssel kapcsolatban határozhatunk meg attribútumokat. Ha a tanúsítványban nem szerepelne a kereszthitelesítésre vonatkozó cím, vagy a benne szereplő mellett újat is fel kellene venni, akkor az itt tehető meg, a kereszthitelesítő tanúsítvány ellenőrzési intervallumának megadásával együtt.

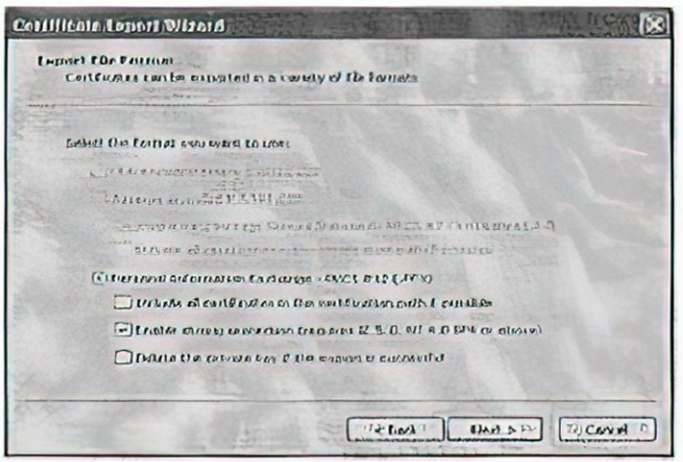
10.3.6 Tanúsítványok importálása és exportálása

A tanúsítványok belső tanúsítványtár kapcsán értelmezett (onnan, illetve oda történő) exportálása és importálása több helyről is kezdeményezhető (**MMC**, **Certificates** és **Certificate** program, **Intéző – Install Certificate** és **Install PFX** parancsok stb.). A művelet minden esetben ugyanazon varázslón keresztül történik. A kiválasztott állományformátumtól függően egy lépésben megoldható egy vagy több tanúsítvány mozgatása. Importálásnál megadható a tanúsítvány tárolásának logikai és fizikai helye (utóbbi a **Show physical stores** kontrollkocka beállításával). Amennyiben a magánkulcs importálására is sor kerül

80. ábra
Tanúsítványimportálás, fizikai tár megadása

(PKCS #12 és SST formátumok), meg kell adni a magánkulcs aktivizáló adatát, valamint az annak belső tárolására vonatkozó szabályokat (azt, hogy a magánkulcs később exportálható legyen-e, s használata során minden esetben figyelmeztessen-e, illetve jelszót kérjen).

Exportálásnál megadhatjuk, hogy a magánkulcsot is exportálni akarjuk-e a tanúsítvánnyal együtt (amennyiben azzal rendelkezünk, a kriptográfiai szolgáltató támogatja a kulcsexportot,[26] az export nincs letiltva[27], és van hozzáférési jogunk). Ennek hatására a varázsló különböző tanúsítványtárolási formátumokat ajánl fel. A formátumtól függően választhatunk a teljes lánc és a tanúsítvány önmagában történő exportálása között. Amennyiben a magánkulcs is exportálásra kerül, beállíthatjuk annak erősebb védelmi szintjét és azt, hogy ezek után a magánkulcs törlődjön-e a védett tárból.



81. ábra
Tanúsítványexportálási formátumok

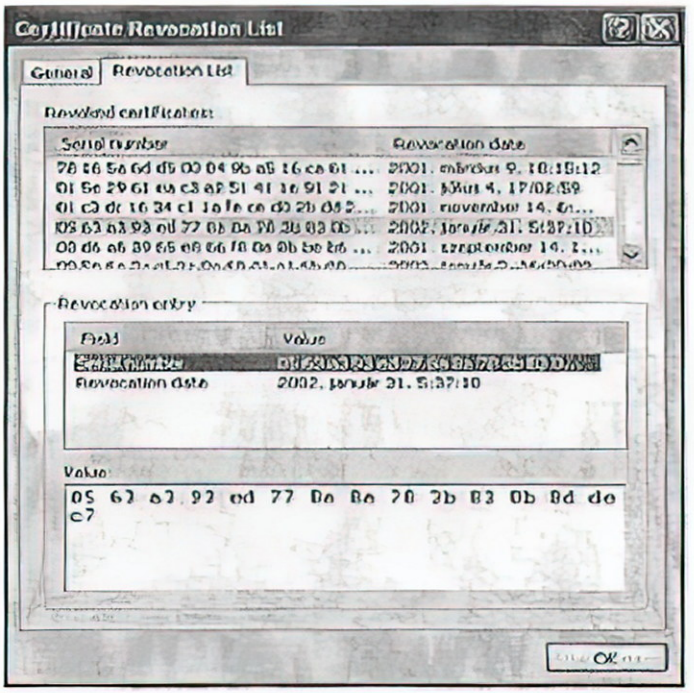
10.3.7 Visszavonási lista

Mivel a visszavonási lista automatikus ellenőrzése még nincs beépítve minden alkalmazásba, annak manuális ellenőrzésére gyakran szükség lehet. Visszavonási listát általában az erre a célra szolgáló weboldalon keresztül tölthetünk le az **Internet Explorer** segítségével. Miután a letöltött listát elmentettük a saját gépünkre, az **Intéző** segítségével importálhatjuk a belső tanúsítvány-nyilvántartásba. Az **Intéző** felismeri a CRL kiterjesztésű szabványos visszavonási listákat, és a jobb egérgomb hatására felkínálja annak importálását (**Install CRL**). Az importált visszavonási listák a tanúsítványtár felhasználói szegmensébe, a Registry HKEY_CURRENT_ USER\Software\Microsoft\SystemCertifica-

tes\CA\CRLs fejezetébe kerülnek.[28] A **Certificates** ablakban a belső tanúsítványtár visszavonási listái nem jelennek meg, azok csak az **MMC**-vel (**Intermediate Certification Authorities – Certificate Revocation List**) jeleníthetők meg. A listák tartalmának megtekintésére a **Windows** a **Certificate** ablakhoz hasonló felületet biztosít.

A P7B kiterjesztésű (PKCS #7 formátumú) visszavonási listákat az **Intéző** nem képes megkülönböztetni a tanúsítványoktól (mivel nem néz bele az állományba), így nem ismeri fel, hogy visszavonási listával van dolga, de az **Install Certificate** parancs hatására az is importálható a tanúsítványtárba. A PKCS #7 visszavonásilista-fájlok az **MMC** felületén keresztül, a CRL kiterjesztésű listaállományok közvetlenül jelennek meg megnyitás hatására a **Windows** visszavonási lista ablakában.

82. ábra
Visszavonási lista fejének megjelenítése



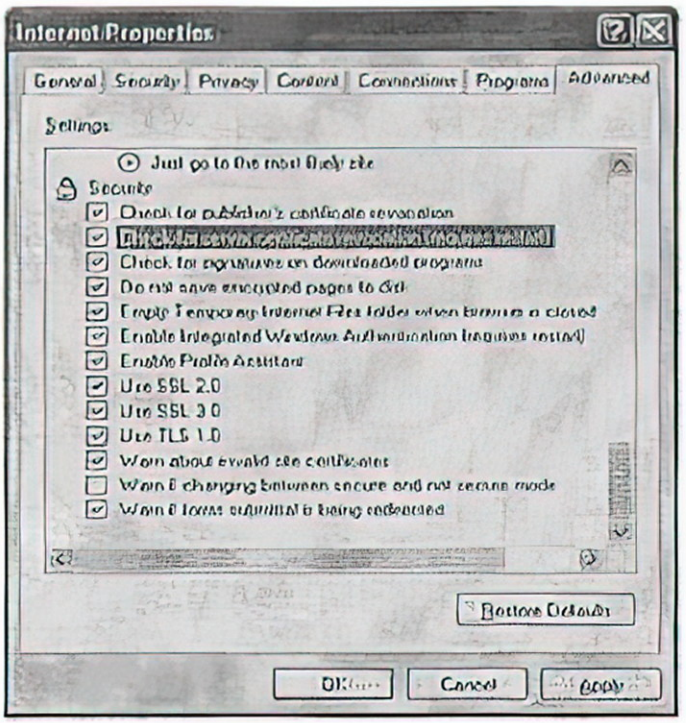
83. ábra
Visszavonási lista bejegyzéseinek megjelenítése

Az ablak első oldalán a lista fejadatai jelennek meg, második oldalán a visszavont tanúsítványok adatai: a tanúsítványok sorozatszáma és a visszavonás ideje, illetve a bejegyzések esetleges kiterjesztései. Sajnos keresési lehetőséget (az egyenkénti végigbogarászáson kívül) ez az ablak nem biztosít a bejegyzések között.

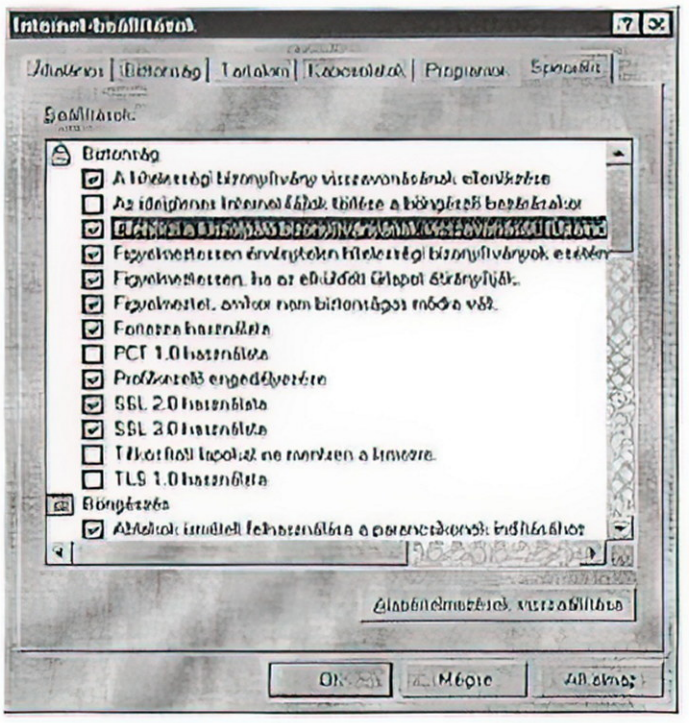
10.3.8 Internet Options

Az **Internet Explorer**-re vonatkozó (az **IE Tools** menüjén vagy a **Control Panel**-en keresztül elérhető) **Internet Options** képernyő több, az elektronikus aláírásra és titkosításra vonatkozó beállítási lehetőséggel bír. A belső tanúsítványtár adminisztrációja is innen érhető el, az SSL protokoll különböző verzióira va-

ló képességet is itt lehet érvényesíteni, a letöltött programok aláírásának ellenőrzése, valamint a visszavonási listák ellenőrzése is itt állítható be. A belső tanúsítványtárat más programok is használják, így az SSL-re és a visszavonási lista ellenőrzésére vonatkozó beállítások sem csak az **Internet Explorer**-re vonatkoznak (hanem például az **Outlook**-ra is). A visszavonási lista ellenőrzése a szoftverhitelesítők és az SSL-szerverek tanúsítványaival kapcsolatban különkülön állítható be.



84. ábra
Internet biztonsági opciók
— angolul

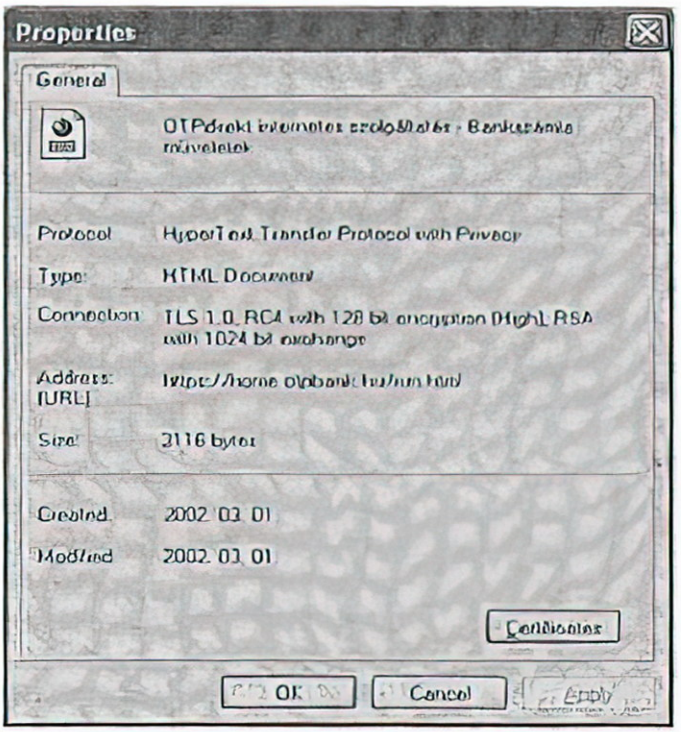


85. ábra
Internet biztonsági opciók
— magyarul

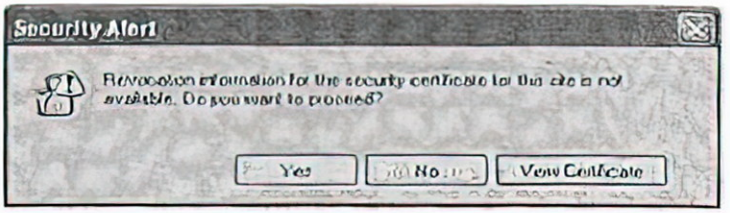
10.3.9 Internet Explorer

Az **Internet Explorer**-ben bármely weboldal kapcsán ellenőrizhető a kapcsolat biztonságának szintje. Az oldalon állva a jobb egérgombbal érhetjük el a **Properties** ablakon keresztül a kapcsolat protokolljára, az alkalmazott algoritmusokra és kulcshosszakra vonatkozó adatokat, és nézhetjük meg az SSL-szerver tanúsítványát (86. ábra).

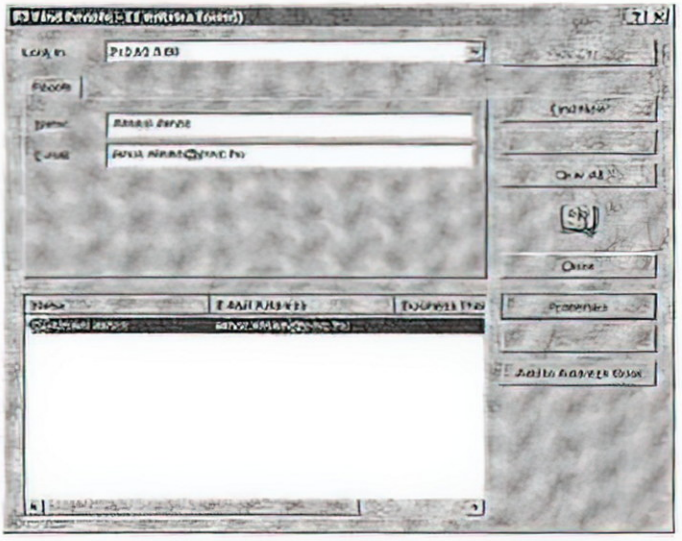
Az **Internet Explorer** akkor tudja a visszavonási listát ellenőrizni, ha a tanúsítvány tartalmazza a megfelelő kiterjesztésben (CRL Distribution Points) a lista elérhetőségének címét. Ha ennek ellenére mégsem képes a lista ellenőrzésére (mert például az nem elérhető, rossz formátumú), akkor a 87. ábrán látható üzenet jelenik meg.



86. ábra
Az internetkapcsolat biztonsági adatai



87. ábra
A visszavonási lista nem elérhető

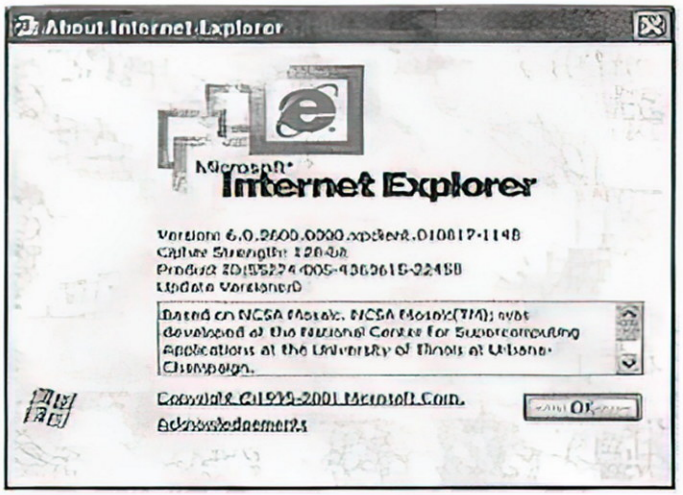


88. ábra
LDAP címtár lekérdezése Internet Expolrerrel

A tanúsítványtár LDAP protokollal történő eléréséhez gépeljük be az LDAP-szerver nevét vagy címét az **Internet Explorer Address** sorába (pl. LDAP://tar.giro.hu). Az ennek hatására megjelenő ablak segítségével a bejegyzés név (CN) és e-mail mezője alapján kereshetünk a címtárban. A találatok az ablak alsó találati részében válnak láthatóvá. A találaton állva a **Properties** gomb segítségével a bejegyzés részletes adatait tekinthetjük meg. A megjelenő ablak utolsó, **Digital ID** fülén állva a bejegyzés tanúsítványát jelenítheljük meg. Ugyanígy a visszavonási listára is rákereshetünk, de azt értelmes módon megjeleníteni innen sajnos nem tudjuk.

10.3.10 A kriptomodul erőssége

Az **Internet Explorer** kriptomoduljának (szimmetrikus algoritmusának) erősségét az **About** képernyő mutatja meg. Ez az **Internet Explorer** 6-os esetében a biztonságosnak számító 128 bit, régebbi változatoknál azonban 56 bites változat is előfordulhat. Utóbbit ingyenesen frissíteni lehet interneten keresztül erősebb változatra.

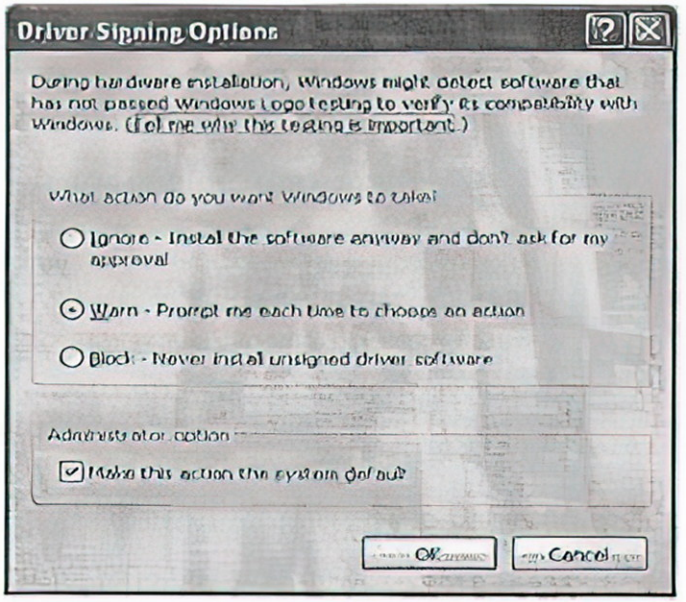


89. ábra
Az Internet Explorer kriptomodul erőssége

10.3.11 Aláírt programok

A Microsoft a **Windows**-nak az Authenticode rendszert fejlesztette ki a programok aláírására, mely digitális aláírással látja el a programokat. A programot annak fejlesztője írja alá saját nevében vagy a terjesztő, illetve a megrendelő nevében. Az aláírás ellenőrzését a szoftver felhasználójának kell elvégeznie, mielőtt elindítja a programot.

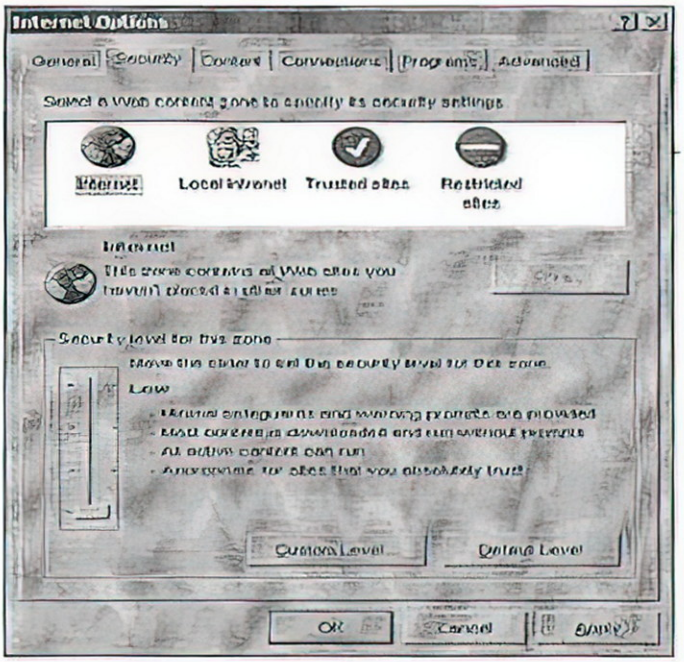
A **Windows** saját komponensei mind aláírtak (a telepítő-CD tartalma), s idegen szoftverek installálásakor is találkozhatunk aláírt programokkal. A Microsoft a **Windows** meghajtóprogramjait is ellátja elektronikus aláírással, hogy biztosak lehessük a meghajtószoftver eredeti és tesztelt mivoltában. Az aláírást a Microsoft helyezi el a meghajtóprogramon, attól függetlenül, hogy ki annak a gyártója (az **XP** esetében ez az aláírás össze van kapcsolva a „Designed for Microsoft Windows XP" programmal, s a program dobozokon és CD-ken megjelenő logójának virtuális párjaként funkcionál[29]). Azt, hogy ezen aláírásokat a **Windows** miként ellenőrizze, a **Driver Signing Options** ablakban (**Control Panel – System – Hardware – Driver Signing**) lehet beállítani.



90. ábra
Meghajtóprogramok aláírás-ellenőrzése

Aláírt programokkal találkozhatunk az interneten barangolva is, ahol aláírt ActiveX és Java programokba, valamint plug-inekbe (böngészőbe beépülő programok) egyaránt botolhatunk.[30] ActiveX esetében az aláírástól függően utasíthatjuk el, illetve engedélyezhetjük a program futását. Ha engedélyezzük számára a futást, akkor azzal mindent megengedünk, ami számunkra megengedett (saját

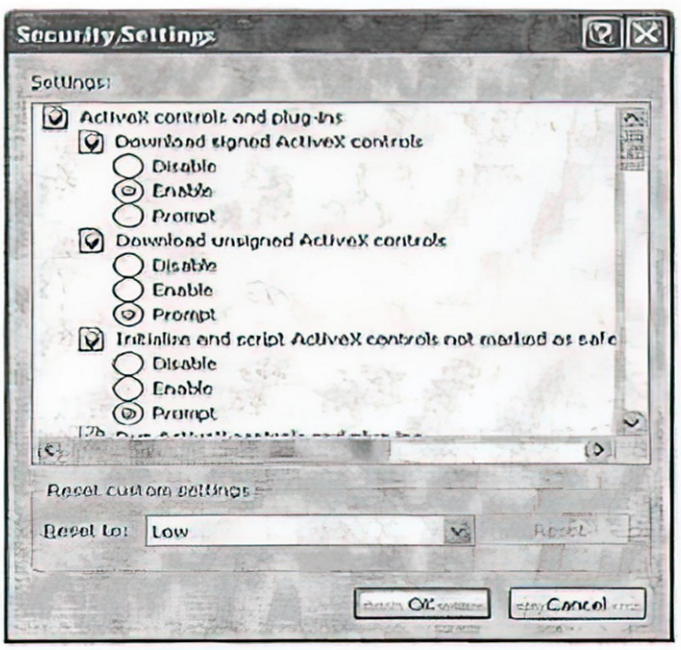
jogaink a gépen nem feltétlen korlátlanok). Hozzáférést adunk erőforrásainkhoz, írási-olvasási jogot háttértárunkra, ami éppen elég akár a gép rebootolásához vagy a winchester formázásához is. Ezért nagyon ajánlott körültekintő módon eljárni, mielőtt zöld lámpát adunk az ilyen programoknak. Java appletek esetében valamivel jobb a helyzet, mert az ő esetükben a jogosultságok finomhangolására is mód van. Megadhatjuk, mely erőforrásunkhoz milyen hozzáférést engedélyezünk.



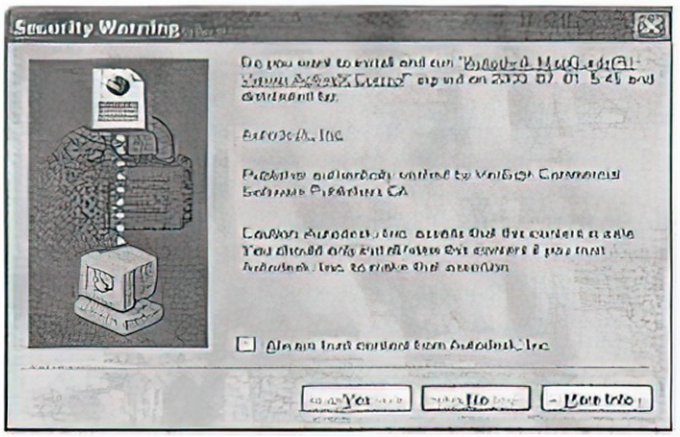
91. ábra
IE5 biztonsági szint beállítása

A weboldalak és levelek esetében az aláírásra használt tanúsítvány kibocsátójába koncentrálhatjuk bizalmunkat, s a hitelesítésszolgáltató kiléte alapján automatizálhatjuk az aláírás elfogadását (a szolgáltatói tanúsítvány felvételével a **Windows** belső tanúsítványtárába). A programok esetében nem a hitelesítésszolgáltatóba, hanem a program aláírójába kell a bizalmunkat helyezni (hiszen az előbbi túl általános feltétel lenne). A szoftverhitelesítők ennek megfelelően egy külön logikai egységbe szerveződnek a tanúsítványtárban.

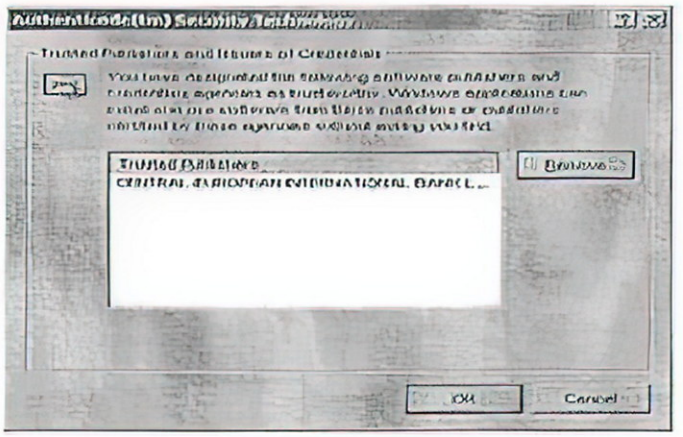
Jó tanácsként azt mondhatom, hogy minden programról egyedileg döntsünk, ne állítsuk be azt egy aláíró esetében sem, hogy programjait automatikusan elfogadjuk. Egyik zónára se állítsuk be az **Internet Explorer** biztonsági szintjét a legalacsonyabbra (**Internet Options – Security**). A **Low** szint esetében az ActiveX programok (**Windows 2000** esetében az aláírás nélküliek is) figyelmeztetés és engedélykérés nélkül elindulnak. A legfelsőbb szint a másik véglet: e beállítás esetében nem indíthatunk el egy ActiveX programot sem. Az **Office XP** részeként terjesztett **Internet Explorer** 6 esetében az ActiveX-re vonatkozó jogosultságok aprólékosabb hangolására van lehetőségünk, például az aláírt és nem aláírt programokra külön állíthatjuk be az ellenőrzést és a figyelmeztetést.



92. ábra
IE6 biztonsági szint beállítása



93. ábra
ActiveX program engedélyezése



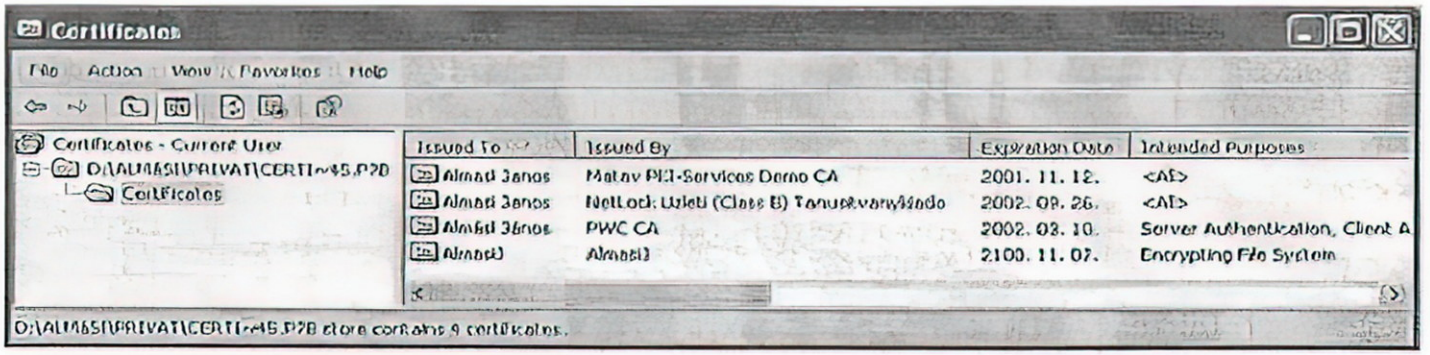
94. ábra
Szoftverhitelesítők listája – Windows 2000

Az ábrákon mutatott beállításokat internetes környezetre semmilyen körülmények között ne állítsunk be!

A 93. ábrán látható képernyő egy ActiveX program engedélyezését mutatja be (az 52. ábrán bemutatott Java applet engedélyezéssel ellentétben itt nincs lehetőség jogosultságok beállítására). A fejlesztő cég nevére kattintva megjelenik a szoftverhitelesítő tanúsítvány. Az **Always trust Content from...** kontrollkocka beállításával szaporodik a megbízható szoftverhitelesítők listája (ezt nem ajánlottam gyakori használatra). A lista **Windows 2000** esetében külön képernyőn jelenik meg, **Windows XP** esetében pedig a tanúsítványtár **Trusted Publishers** füle alatt.[21] E tanúsítványokra a visszavonási lista ellenőrzése az **Internet Options** ablakban állítható be (lásd a 10.3.8 fejezet).

10.3.12 Intéző

Az **Intéző** felismeri a **Windows** által kezelt tanúsítványformátumokat, és különböző műveleteket ajánl fel velük kapcsolatban. A CER formátumú állományra kattintva megjelenik a tanúsítvány tartalma a **Certificate** program segítségével. Ha egy P7B kiterjesztésű fájlra bökünk (PKCS #7 tanúsítványtárra), akkor az **MMC** indul el, megmutatva a fájl tartalmát, ami több összefogott ta-



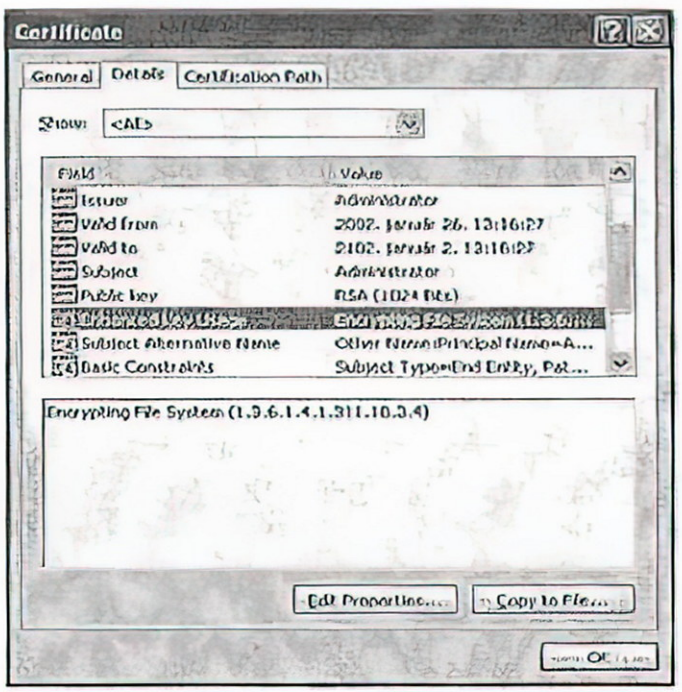
95. ábra Egy PKCS #7 állomány tanúsítványainak megtekintése

núsítvány is lehet, egymástól függetlenek vagy egy tanúsítási lánc tagjai, illetve visszavonási listát is tartalmazhat. PKCS #12 tanúsítványok esetén felkínálja a tanúsítvány importálását, s a tanúsítvány tartalma csak ezek után tekinthető meg. A CRL kiterjesztésű visszavonásilista-állományokat a CER kiterjesztésű tanúsítványokhoz hasonlóan azonnal megjeleníti.

10.3.13 EFS

Említettem a könyv elején, hogy rejtjelezett adatainkat érdemes rejtjelezett könyvtárakba szervezni. Ha egy könyvtárt kívánunk rejtjelezni, akkor választhatunk a könyvtár rejtjelezése és a könyvtár alatt lévő összes információ rejtjelezése között (ugyanígy az **Intéző** az állomány rejtjelezése esetén is rákérdez a teljes könyvtár rejtjelezésére). Az előbbi esetben a könyvtár alatt az attribútum állításának pillanatában lévő állományok nem rejtjeleződnek, csak a később oda kerülők (például másolással) és ott létrejövők. Az egyszer rejtjelezett állományok viszont nem rejtjelezett NTFS-könyvtárba[32] mozgatva is megőrzik rejtjeles attribútumukat, sőt törlés-visszaállítás után is. Ez azt is jelenti, hogy ugyanazon kötetben mozgatva, másolva az állományokat, az mindig titkosított marad. Nem EFS-képes állományrendszerbe (FAT-be, azaz például floppyra vagy NT4 NTFS-be) másolva viszont elveszítik rejtjelezett voltukat, amire üzenet figyelmeztet[33]. Az EFS gondoskodik arról is, hogy egy rejtjelezett fájlnak minden ideiglenes (NTFS-egységen létrejövő) változata is rejtjelezett legyen.[34]

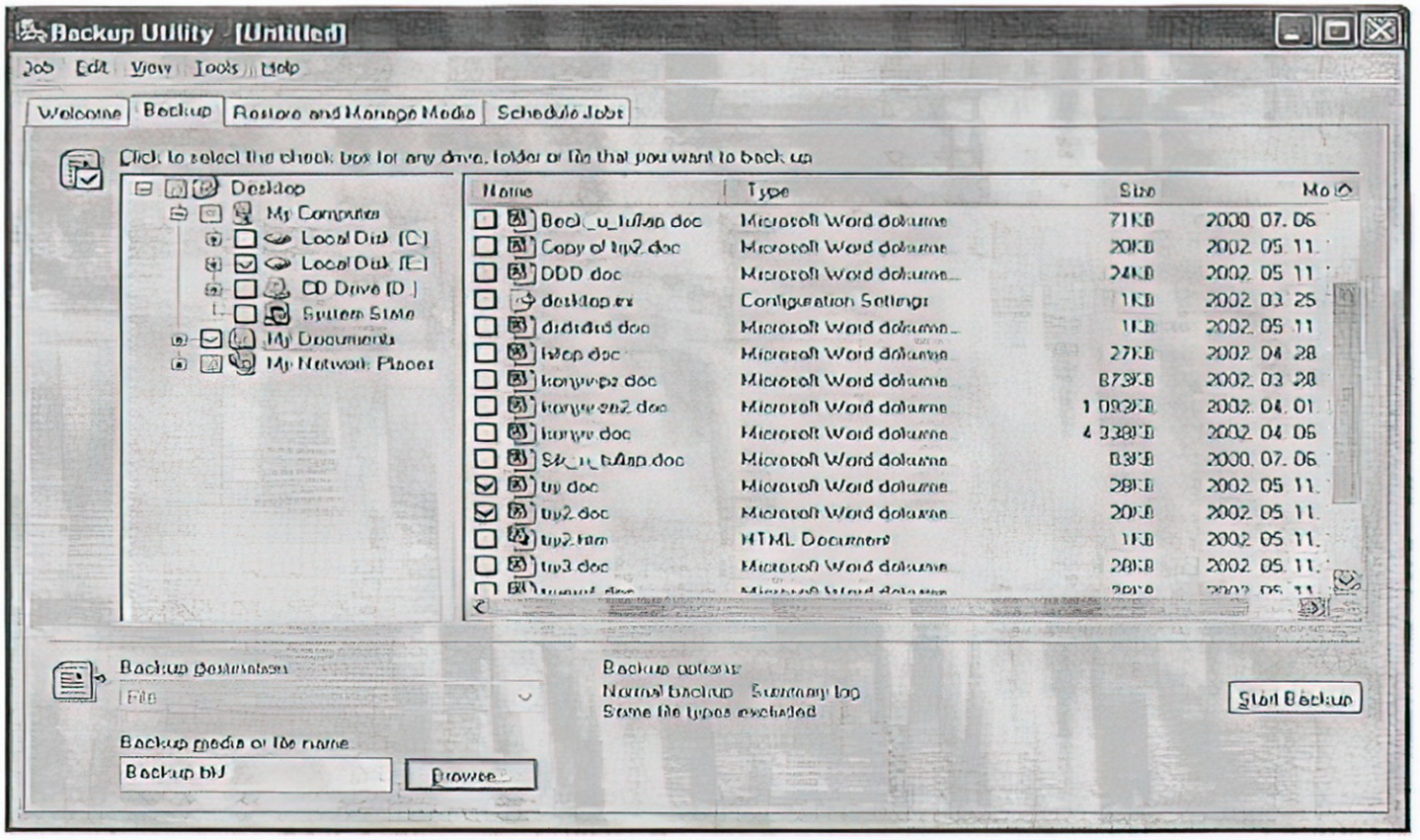
Tipikusan rejtjelezésre született könyvtár a My Documents (amennyiben valóban az szolgál személyes dokumentumaink tárolására), de kár lenne elfelejtkezni a Temp könyvtárról is, ahova sok árulkodó anyag kerülhet ideiglenesen vagy hosszabb távra, nem is beszélve a Favoritesról, ami kedvenc webhelyeink titkát tárolja. Ugyanez igaz lehet a Cookies, a teljes Local Settings könyvtárra, Temporary Internet Files-ostól, Historystól, és minden olyan könyvtárra, amiben előfordulhatnak ténykedéseink mivoltára utaló jelek. A könyvtárak titkosításával elkerülhető, hogy az ott létrejövő ideiglenes és munkaállományok, valamint utólag bekerülő kész anyagok mások számára hozzáférhetők legyenek.



96. ábra
EFS tanúsítvány

A rejtjelezés első használatkor az operációs rendszer a felhasználó részére generál egy tanúsítvány magánkulcs párt száz év érvényességgel. Ez a tanúsítvány a **Certificates** ablakban is megjelenik a tanúsítványok között. A tanúsítvány tulajdonosaként és kibocsátójaként az aktuálisan bejelentkezett felhasználó, felhasználási céljaként az EFS van megjelölve.

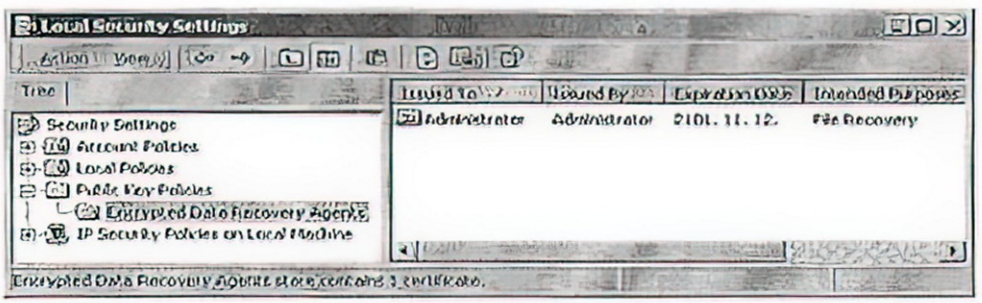
Ajánlatos észben tartani ugyanakkor, hogy az állományok titkosításával olykor a magunk orra alá is könnyen borsot törhetünk. Saját feledékenységemből okulva javaslom mindenkinek, hogy készítsen másolatot a titkosítótanúsítványról és magánkulcsáról egy floppyra vagy CD-re. Ez legegyszerűbben a **Certificates** ablakban hajtható végre az **Export** paranccsal. Ha ezek után bármikor szükség lesz a magánkulcsra (például mert megszűnik az a tartomány (domain), ahova a felhasználó tartozik, és így annak tagjaként már nem tud többet belépni), akkor az ugyanezen képernyőn beimportálható. Mivel az operációs rendszer a több kulcs közül magától megtalálja, melyikre van szüksége, ugyanezen módszerrel eleve megosztható a titkosítás-visszafejtés lehetősége több user között. Ha több gépet használva akarunk a gépek között rejtjelezett állományokat mozgatni, és az operációs rendszer csak úgy nem engedi ezt (például különböző tartományok között), akkor a legérdemesebb backupolni, és visszatölteni a fájlokat.[35] A **Backup** programmal létrehozott állomány titkosított formában tartalmazza a titkosított állományokat, így ez az állomány nyugodtan másolható akár floppyra is. Ha rendelkezünk barangolóprofillal (roaming user profile), akkor még az előbb leírt tanúsítványexportra és -importra sincs szükségünk ahhoz, hogy a visszaállított állományt új helyén megnyissuk.



97. ábra Titkosított állományok biztonsági mentése[36]

Az EFS akkor különösen hasznos, ha valaki az operációs rendszer védelmi és jogosultsági mechanizmusait megkerülve képes a diszkhez férni. Ez a megoldás még az adminisztrátori joggal rendelkező felhasználók elől is képes elrejteni az elrejteni valónkat, egyetlen kivétel van csak, aki elől még a rejtjelezés sem véd meg minket: a Data Recovery Agent. Ő lokális gép esetében az adminisztrátor, tartományba kapcsolt gépek esetében a tartomány adminisztrátora, és akkor jön létre, mikor az első fájltitkosítás történik a gépen. Szerepe az, hogy ha a felhasználó elvesztené lehetőségét titkosított állományainak visszafejtésére (mert magánkulcsa megsemmisül), akkor a segítségére tudjon lenni.[37] Ha nincs DRA, akkor az EFS nem használható.[38] Ezt a tulajdonságot kihasználva (a csoportszabályzatból kivéve a DRA-t) szokták letiltani a tartományi gépek esetében az EFS használatát. A DRA sem fér hozzá viszont a titkosító magánkulcsunkhoz, csak az állomány titkosítására használt szimmetrikus kulcsot tudja visszafejteni, ami az ő nyilvános kulcsával is le lett kódolva.

A DRA a **Control Panel – Administrative Tools – Local Security Policy** képernyő **Public Key Policies – Encrypted Data Recovery Agents** beállításainál található meg (az **MMC**-ből is előcsalható ugyanez a képernyő).



98. ábra
Encrypted Data Recovery Agent

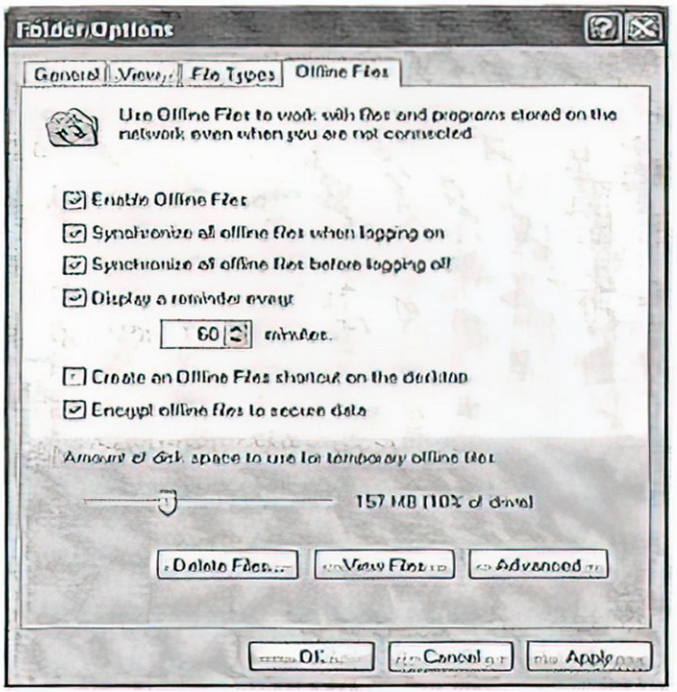
Egy állományt több felhasználó is titkosíthat (például egy kiszolgáló adott könyvtára csak a cég férfi dolgozói számára visszafejthető), és több DRA-t is felvehetünk a rendszerbe. Az állomány ez esetben is csak egyszer lesz rejtjelezve a szimmetrikus kulccsal,[39] s csak ez a kulcs lesz titkosítva minden egyes felhasználó és a DRA nyilvános kulcsával. E titkosított kulcsok az állomány Data Decryption Field és Data Recovery Field mezőiben tárolódnak.

Tudni kell, hogy tökéletes védelmet az EFS sem biztosít. Mivel a magánkulcs a védendő diszken van, ahhoz megfelelő szakértelemmel hozzá lehet férni, és ez esetben vissza lehet fejteni a rejtjelezett állományokat. Ezért üzleti és politikai értelemben fokozottan védendő információk védelmére olyan rejtjelező megoldást tartok csak megfelelőnek, ami a kulcsot biztonságos környezetben tárolja, semmiképp sem ugyanott, ahol a védendő adatokat.

Az EFS használatakor a következő korlátozásokkal kell együtt élnünk:

- Csak NTFS fájlrendszeren működik, kizárólag nem tömörített állományokkal.
- System-állományok nem rejtjelezhetők.
- A rejtjelezés nem véd az állomány törlése vagy átnevezése ellen (ezek a jogosultságok beállításaival korlátozhatók).

– Lehet hálózati számítógép NTFS-egységén is titkosítani – ha az engedélyezett –, de az így megnyitott állomány a hálózaton már nyílt formában utazik.



99. ábra
Offline állományok titkosítása

A **Windows XP** esetében az EFS beállítható az offline állományok[40] tárolására vonatkozóan is, de nem fájlonként vagy könyvtáranként, csak generálisan az összes offline állományra. A beállítás elérhető az **Intéző Tools – Folder Options** menüpontjain keresztül, az **Encrypt Online files to secure data** kontrollkocka kipipálásával.

10.3.14 Kártyás bejelentkezés

A **Windows XP** esetében lehetőségünk van szakítani a már jól ismert jelszavas belépéssel, s ehelyett elektronikus aláírásunkkal azonosíthatjuk magunkat a gépbe (és tartományba) történő bejelentkezéskor (az elméletet lásd a 3.5.6. fejezetben). Ilyen esetben felhasználói nevünk és jelszavunk helyett egyszerűen csak be kell helyeznünk a kártyánkat a kártyaolvasóba (amit a rendszer a CTRL-ALT-DEL-hez hasonlóan kezel), és meg kell adnunk a PIN-kódunkat. Pont úgy, ahogy az ATM-eknél tesszük készpénz felvételekor.

Az eljárás a PKINIT protokollon keresztül csatlakozik a Kerberos hitelesítési rendszerhez, aminek segítségével single sign-on (azaz egyszeri bejelentkezés) szolgáltatással is ki lehet egészíteni a kártyás belépést.

Ahhoz azonban, hogy ezek a funkciók egy vállalati környezetben használhatók legyenek, a rendszergazdáknak sokat kell dolgozniuk. Helyi címtárat kell létrehozniuk az Active Directory segítségével; a hitelesítésszolgáltató tanúsítványát közzé kell tenniük a címtárban[41]; intelligens kártyakiadó állomást kell felállítani, aminek a kezeléséhez beiktató ügynök szükséges; be kell állítaniuk a felhasználóra vonatkozó szabályzatot; kulcsot kell generálni a kártyára, a szolgáltatói tanúsítványt is el kell rajta helyezni stb.

10.3.15 Virtuális magánhálózat

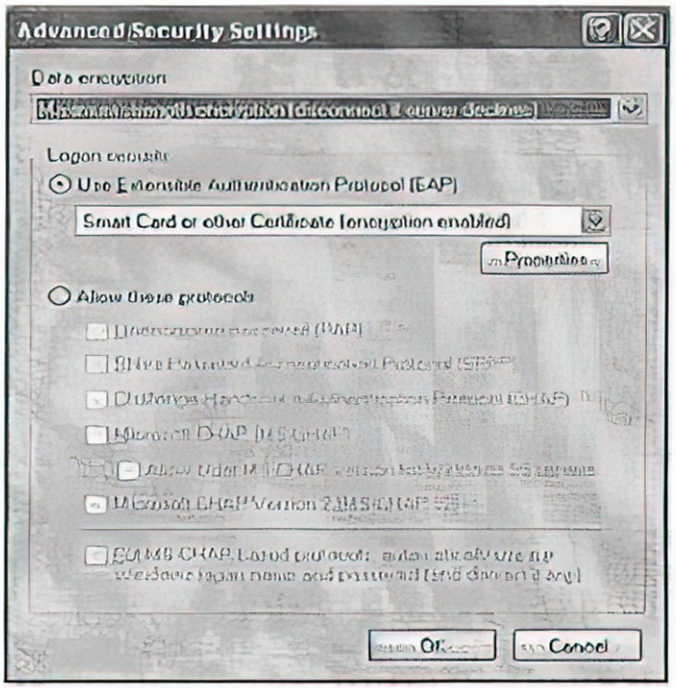
Virtuális magánhálózat létesítésére akkor van szükség, amikor egy egyébként nem biztonságos hálózati kapcsolaton keresztül akarunk biztonságos kommuni-

kációt folytatni. Például cégünk hálózatára távolról akarunk felkapcsolódni telefonvonalon vagy interneten keresztül (otthonról, ügyféltől vagy mert megtaláltak minket a nyaralásunk alatt). Olyan esetekben is használható, amikor egy sok telephellyel, kirendeltséggel rendelkező vállalat egyes fiókjai között akarunk biztonságos kapcsolatot. Sőt lokális hálózatokon is eredményesen használható a belső támadások kivédésre. A VPN leginkább abban különbözik a már ismertetett védelmi módszerektől, hogy nem az alkalmazásban (például levelezőprogram), hanem a hálózati protokoll valamelyik szintjén biztosítja a biztonságot. Ez azt jelenti, hogy egy ilyen módon biztosított kapcsolatot használva bármely alkalmazás biztonságosan tud kommunikálni[42]: Pago Pago pálmafái alól a helyi internetszolgáltató segítségével felcsatlakozhatunk a cég adatbázisára, és rendbe tehetjük az adatbázis korrumpálódott tábláit, letölthetjük leveleinket, és szétnézhetünk az intraneten, mintha csak bent lennénk az irodában.

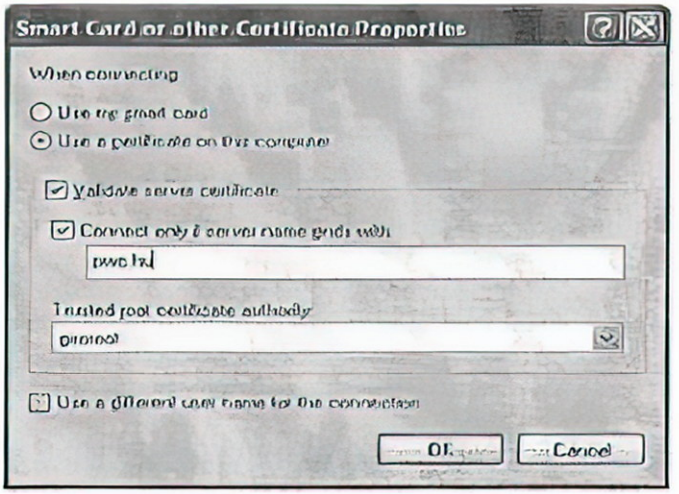
A **Windows 2000** és **XP** operációs rendszerek több módszerrel is rendelkeznek VPN létrehozására. Az IPSec protokoll segítségével a hálózati rétegben, az L2TP és PPTP protokollok[43] segítségével pedig az adatkapcsolati rétegben hozhatjuk létre a szükséges biztonságot. Az IPSec (lásd a következő fejezetet) a számítógépet hitelesíti, a felsőbb szinteken működő protokollokkal viszont felhasználói szintű hitelesítést is tudunk használni. Ezeket a protokollokat és használatukat nem kívánom részletesen ismertetni, mert messze túlmutatnak a könyv keretein, csak az eddig tárgyalt témákhoz való kötődésükre hívnám fel a figyelmet.

A PPTP az RC4 algoritmust használja a kapcsolat rejtjelezésére, a kulcs rendszeres cseréjével. Az L2TP protokoll – saját ilyen irányú képességek hiányában – az IPSec titkosító képességeit hasznosítja. A felhasználók hitelesítésére mindkét protokoll több módszerrel is képes. A PAP ezek közül a legprimitívebb: a felhasználónév és jelszó kódolatlan továbbítását takarja. A CHAP protokoll szintén felhasználónév és jelszó alapú hitelesítést jelent, de ez esetben mindkettőnek csak (az MD5 algoritmussal képzett) lenyomata közlekedik, megspékelve egy – a hitelesítő féltől kapott – kapcsolati azonosítóval és véletlenszerű karakterlánccal. A legfejlettebb azonosítási módszer az EAP, ami nyilvános kulcsú módszereket használ mindkét résztvevő hitelesítésére. Ez akkor is működik, ha a felhasználó a magánkulcsát és tanúsítványát intelligens kártyán tárolja.

A fentiek kipróbálásához fel kell vennünk egy VPN-kapcsolatot a **Control Panel** segítségével (**New Connection Wizard – Connect to the network at my workplace – Virtual Private Network connection** – stb.), majd annak tulajdonságai közül (jobb egérgomb – **Properties**) a **Security** fület, azon belül is az **Advanced** beállításokat kell választanunk. Itt megadhatjuk a rejtjelezés szintjeit: tilos, opcionális és kötelező. Az első esetben akkor nem jön létre kapcsolat, ha a másik fél megköveteli a rejtjelezést, a kötelező opció esetében pedig akkor nem, ha a másik fél nem képes a rejtjelezésre. Opcionális szintet választva a kapcsolat felépítését nem kockáztatjuk. Ez esetben akkor kapunk rejtjelezést, ha a másik fél is képes arra (nem tiltotta le).



100. ábra
VPN biztonsági beállítások



101. ábra
VPN hitelesítési beállítások

Az EAP protokollt választva beállíthatjuk, hogy intelligens kártyán vagy belső tanúsítványtárban tárolt magánkulcsot és tanúsítványt akarunk-e használni (a bennük szereplő név különbözhet a felhasználónévtől). Partnerünk hitelesítése kapcsán megkövetelhetjük az ő aláírásának és tanúsítványának az ellenőrzését is. Megadhatjuk, hogy melyik szolgáltató által kibocsátott tanúsítványokat fogadjuk el, s szűrhetünk a tanúsítványban szereplő név szerint is (partnerünk domainneve vagy annak vége alapján). Például a pwc.hu címet megadva az összes, erre a címre végződő kiszolgálóval kapcsolatot tudunk teremteni.

10.3.16 IPSec

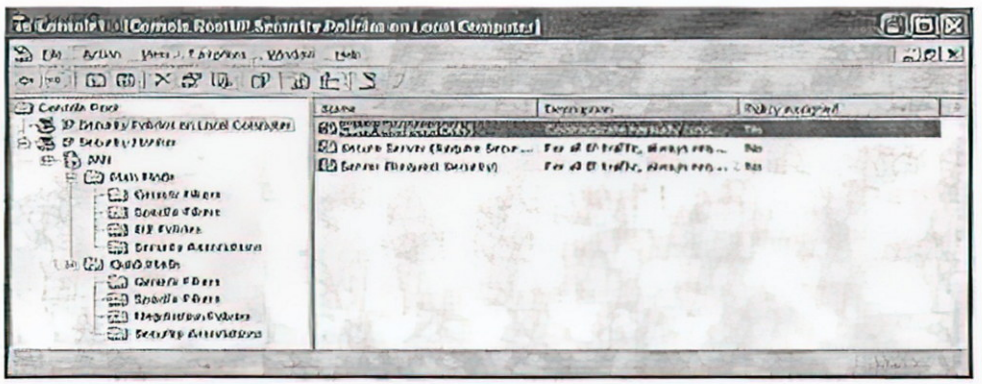
Az 3.7.8 fejezetben ismertetett IPSec protokollt a **Windows** is kezeli, annak szolgáltatásaira épülve egy olyan biztonsági rendszert valósít meg, amelyet bármely program ki tud használni. Az IPSec windowsos változatában sok mindennel találkozhatunk az elméletben már megismert módszerek közül:

A kulcskicserélési műveletek során a Diffie-Hellman eljárással, ami itt az Oakley kulcsmeghatározó protokoll részeként jelenik meg; a DES és 3DES algoritmusokkal, amik az adatcsomagok rejtjelezéséről gondoskodnak, az ESP protokoll részeként; hash-algoritmusokkal, amelyek a csomagok sértetlenségéért felelősek s az AH protokollba épülnek be; s nyilvános kulcsú tanúsítványokra alapozott elektronikus aláírási műveletekkel is, melyek a részt vevő felek hitelesítéséért felelősek (szintén az Oakley protokoll részeként). Az említett protokollok további biztonsági szolgáltatásokat is biztosítanak, így védenek a csomagok ismétlése ellen, a rejtjelező kapcsolati kulcsokat állandóan cserélik, Kerbe-

ros alapú és előre megegyezett kulcsok alapján történő hitelesítést is támogatnak.

Az IPSec szolgáltatásait beállíthatjuk egyes gépekre (természetesen legalább két gép esetén van csak értelme, a köztük lévő kommunikáció biztosítására), egy tartományra vagy szervezetre, illetve szervezeti egységekre egyaránt. A gépek közötti hálózati egységeknek nem feltétlen kell támogatni az IPSec protokollt, mivel azok hagyományos IP-csomagokba vannak csomagolva. A nyilvános kulcsú hitelesítéshez azonban magánkulccsal és tanúsítvánnyal kell hogy rendelkezzen a számítógépünk is, hiszen a védett kapcsolat nem személyek, hanem gépek között valósul meg, s így hitelesíteni sem a személyeket, hanem a gépeket kell.[44]

Az IPSec-re vonatkozó beállításokat az **MMC** felületén adhatjuk meg. Ehhez az **MMC** elindítása után fel kell vennünk az IP Security Policy Management modult a konzol felületére (**Add/Remove snap-in – Standalone – Add...**), megadva, hogy a lokális gépre, egy másik gépre vagy egy tartományra vonatkozóan akarjuk-e konfigurálni a szolgáltatást.

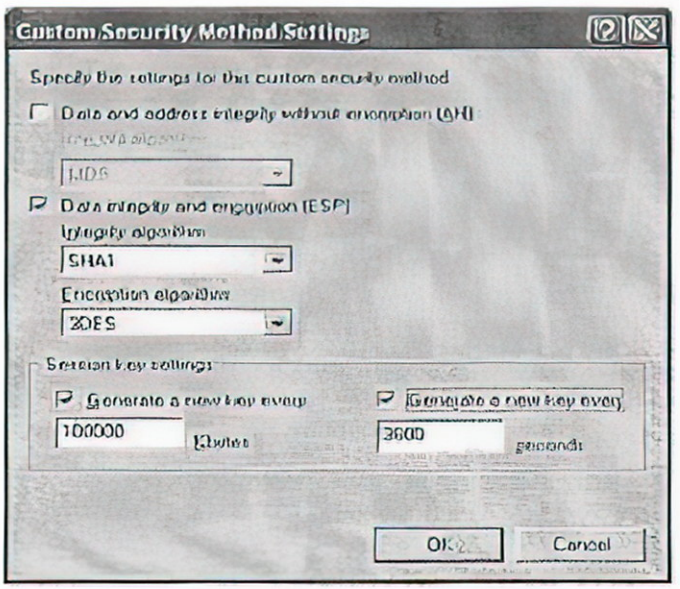


102. ábra IPSec szabályzati beállítások

Kettőt kattintva bármely szabályzatra, megjelennek az adott szabályzat beállításai. Itt felvehetünk új szabályokat (**Rules – Add...**), vagy módosíthatjuk a jelenlegieket (dupla kattintás). Ez utóbbi esetben csak a számunkra különösen érdekes biztonsági és hitelesítési szabályok jelennek meg. A biztonsági szabályoknál beállíthatjuk, hogy csak a sértetlenség ellenőrzését (AH) vagy a bizalmasság biztosítását is (ESP) kérjük-e, s megadhatjuk az ezt biztosító algoritmusokat: Az MD5 és SHA-1 hash-algoritmusokat, valamint a DES és 3DES rejtjelező algoritmusokat. Ugyanitt megadhatjuk, hogy az átvitt adatmennyiségtől és időtől függően milyen gyakran generáljon új kapcsolati kulcsot a protokoll.

Hitelesítési szabályként az említett tanúsítvány és Kerberos alapú, valamint az előre megegyezett kulcsok alapján történő hitelesítést tudjuk felvenni. A Kerberosszal történő hitelesítés egy (vagy több, egymással bizalmi viszonyban lévő) tartományban lehet működőképes. A tanúsítvány alapú módszer internetes környezetben is működik, olyan partnerekkel is, akik nem tagjai a tartománynak. A megegyezett kulcsok módszere a legegyszerűbb, de a legkevésbé biztonságos. Mivel a kulcs nyílt formátumban tárolódik, ezért csak lokális használata elfogadható (egyébként a címtárban is megjelenne a kulcs értéke). Tanúsítvány alapú hitelesítés esetén azt a szolgáltatót kell megadnunk (a megjelenő

gyökér szolgáltatói tanúsítványok listájából kiválasztva), amelynek a tanúsítványait elfogadjuk a partner hitelesítésére. Saját tranzakcióink a gép magánkulcsával lesznek aláírva, s így partnereinknek a számítógépünk tanúsítványát kiadó szolgáltatót kell hasonló módon felvenniük saját szabályzatukba.



103. ábra
IPSec biztonsági szabályok beállítása

104. ábra
IPSec hitelesítési szabályok beállítása

Ha minden szükséges konfigurációt elvégeztünk, akkor a szabályzaton állva az **Assign** paranccsal (kapcsoló ikon) állíthatjuk érvényesre a beállításokat.

10.3.17 A CryptoAPI és a CSP-k

A Microsoft CryptoAPI-ja – ahogy a neve (Cryptographic Application Programming Interface) is mutatja – egy programozási felület, ami így elsősorban fejlesztők számára lehet érdekes. A CryptoAPI egységes elérési felületet kínál a CSP-k által nyújtott kriptoszolgáltatásokhoz. A gyártó- és eszközfüggő CSP-k valósítják meg ténylegesen a kriptográfiai műveleteket, ezek a szolgáltatásaik azonban erősen eltérőek lehetnek. Léteznek szoftveres és hardveres CSP-k, az utóbbiak például intelligens kártyákon, illetve annak meghajtóprogramján lehetnek implementálva.[45] A Microsoft a **Windows**-ba eleve több CSP-t is beépített. A CSP-k határozzák meg – többek között – a magánkulcsok és tanúsítványok tárolását, exportálását, importálását és egyéb menedzsmentjét (például barangolóprofilok használatát[46]), valamint azt, hogy milyen típusú és erősségű algoritmusok állnak rendelkezésünkre. Így például egy intelligens kártya CSP-je megmondhatja, hogy a magánkulcs és a tanúsítvány is a kártyán kell hogy tá-

rolódjon, a magánkulcs azt nem is hagyhatja el, s aktivizálásához PIN-kódot kell megadni. Ezért van az, hogy a magánkulcs aktivizáló adatát a CSP előírásainak megfelelően, a CryptoAPI által biztosított felületen kell megadni (lásd: 10. ábra). Ha egy új intelligens kártyát akarunk a rendszerhez csatlakoztatni, az a kártya CSP-jének telepítésével járhat együtt, s ugyanígy egy CSP telepítésével adhatunk új algoritmusokat a kriptográfiai rendszerhez.

A CryptoAPI szolgáltatásai között megtalálhatók a könyvben leírt valamennyi fontosabb eljárás: elektronikus aláírás és titkosítás, aláírás ellenőrzése és visszafejtés, X.509 tanúsítványok és visszavonási listák kezelése, a PKCS szabványkészlet eljárásainak és adatformátumainak támogatása stb. Maga a **Windows** és az **Office**-programok is a CryptoAPI segítségével valósítják meg PKI-szolgáltatásaikat, így például az Authenticode, az EFS és más rendszerkomponensek is erre épülnek. A programozók Javából, C-ből, VBScriptből és más fejlesztőrendszerekből egyaránt elérhetik a CryptoAPI eljárásait.

10.3.18 Támogatott kártyák és kártyaolvasók

A **Windows 2000** a Gemplus GemSAFE és a Schlumberger CryptoFlex intelligens kártyáit támogatja. A **Windows XP** a Gemplus GemSAFE 4k és 8k, az Infineon SICRYPT v2 és a Schlumberger Cryptoflex 4k, 8k és Cyberflex Access 16k kártyáit támogatja. E kártyák CSP-i a **Windows** standard részeként az operációs rendszerrel vannak szállítva. Ettől eltérő kártyákat akkor lehet a **Windows**-zal használni, ha annak gyártója (a SmartCard SDK segítségével) elkészítette hozzá a megfelelő CSP-t.

Kártyaolvasóból többet is támogat a **Windows**, de óvatosnak kell lenni, mert az olvasókon jelzett PC/SC megfelelőségi jelzés még semmire sem garancia. Ha biztosra akarunk menni, akkor keressük fel a www.microsoft.com/hcl/ oldalt, ahol a Smart Card Reader terméktípust kiválasztva megjelenítheljük a különböző **Windows** operációs rendszerek által garantáltan támogatott olvasók listáját.[47] Ezen olvasók közül jó pár meghajtóprogramja része a **Windows XP**-nek[48], míg a többi esetében a gyártó szállítja a meghajtóprogramot. Előbbi esetben nincs más dolgunk, mint rácsatlakoztatni az olvasót a soros vagy USB-portra (esetleg a PCMCIA-slotra), s a telepítési eljárást megvárni (ez láthatatlanul lezajlik a háttérben), az utóbbi esetben viszont az **Add Hardware Wizard**-dal találkozunk. Ha nem így történik, az azt jelenti, hogy nem plug and play olvasóval van dolgunk. Ilyet nem ajánlatos a **Windows**-zal együtt használni. A varázsló el fogja indítani a **Windows** intelligens kártya szolgáltatását is, amit mi manuálisan a **Services** programban (**Control Panel – Administrative Tools**) tehetünk meg a **Smart Card** szerviz megfelelő konfigurálásával.

10.3.19 Outlook 2000 és 2002

Az **Internet Explorer** és az operációs rendszer sokat vitatott összenövése érhető tetten abban, hogy az **Outlook** a visszavonási listákat az **Internet Explorer**től kapja. Ő maga nem is tölti le minden alkalommal újra a listát, mivel azt az **Internet Explorer** web gyorsítótárában tárolja. Ez azzal jár, hogy az **Outlook**nak az **Internet Options**-nál bemutatott beállításokra szintén szüksége van. De nem csak arra. A visszavonási lista kezelése érdekében és az egyéb biztonsági és elektronikus aláírási lehetőségek életre keltése, konfigurálása végett további beállításokat is el kell végezni. Ezeket a Registryben tudjuk megtenni az alábbiakban ismertetett mezők segítségével.

Az **Outlook 2000** esetén a tanúsítványok korrekt kezeléséhez az **Outlook** SR1 biztonsági bővítéseit kell bekapcsolnunk. Ezt a HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office\9.0**Outlook**\Security\EnableSRFeatures kulcs felvételével és 1-re állításával tehetjük meg. A tanúsítvány érvényességének automatikus ellenőrzése érdekében a HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Cryptography\{7801ebd0-cf4b-11d0-851f-0060979387ea}\PolicyFlags kulcsot kell felvennünk, és 0x10000-re (hexadecimális 10000, decimálisan 65536) állítanunk. Ennek hatására az **Outlook** a levélhez csatolt tanúsítványban szereplő szétosztási pont alapján lekérdezi, és ellenőrzi a visszavonási listát.[49]

Ezeket és az alább felsorolt beállításokat hálózatba kapcsolt gépek esetében csoportszabályzat segítségével érdemes teríteni. Egyébként rendszer-adminisztrátori joggal saját magunk is állíthatjuk őket. A táblázatban bemutatott kulcsok mindegyikét **Outlook 2002** esetében a HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\10.0\Outlook\Security fejezet alatt kell felvennünk, és beállítanunk a Registryben (alaphelyzetben szinte mindegyik érték hiányzik).[50] **Outlook 2000** esetében nagyon hasonló beállítási lehetőségeink vannak a HKEY_LOCAL_MACHINE\Software\Microsoft\Office\9.0\Outlook\Security fejezet alatt.[51]

Mezőnév	Jelentés	Értékek
UseCRLChasing	Visszavonási lista ellenőrzése	0: Alapérték 1: Ellenőrizze a CRL-t, kapcsolat esetén 2: Nem ellenőriz
AlwaysEncrypt	Levelek titkosítása	0: Nem titkosít 1: Titkosít
AlwaysSign	Levelek aláírása	0: Nem ír alá 1: Aláír
ClearSign	Aláírt levelek nyílt aláírt levélként való küldése	0: Nem nyílt aláírt levél 1: Nyílt aláírt levél

Mezőnév	Jelentés	Értékek
RequestSecure-Receipts	Az aláírt S/MIME levelekről visszaigazolás kérése	0: Nem kér visszaigazolást 1: Kér visszaigazolást
ForceSecurity-Label	Az aláírt S/MIME levelek biztonsági címkézésének megkövetelése[52]	0: Címkézés nem kötelező 1: Címkézés megkövetelése
SigStatusNoCRL	Hiányzó visszavonási lista jelzése	0: Jelzés figyelmeztetésként 1: Jelzés hibaként
PromoteErrorsas-Warnings	Aláírással kapcsolatos hibák figyelmeztetésként való jelzése[53]	0: Jelzés hibaként 1: Jelzés figyelmeztetésként
PublishToGAL-Disabled	A **Publish to GAL** gombhoz való hozzáférés beállítása[54]	0: Gomb elérhető 1: Gomb nem elérhető
FIPSMode	FIPS 140-1 módban való futás	0: Nem FIPS mód 1: FIPS mód
WarnAbout-Invalid	Érvénytelen aláírások jelzése	0: Felhasználó döntése alapján 1: Mindig figyelmeztet 2: Nem figyelmeztet
DisableContinue-Encryption	Visszafejtési hibák esetében a **Folytatás** gomb elrejtése	0: Gomb feltüntetése 1: Gomb elrejtése
RespondToReceipt-Requests	Visszaigazolás küldése	0: Üzenet megnyitása, ha nem tud visszaigazolást küldeni 1: Visszaigazolás küldése előtt figyelmeztet 2: Soha nem küld biztonságos visszaigazolást 3: Az üzenetet nem nyitja meg, ha nem tud visszaigazolást küldeni
NeedEncryption-String	Üzenet megjelenítése, ha nem talál tanúsítványt a kapott üzenet visszafejtéséhez	*üzenet értéke (max. 255 karakter)*

10.4 Hitelesítésszolgáltatók Magyarországon

Könyvem írásának pillanatában Magyarországon három hitelesítésszolgáltató működik, mindhárman fokozott biztonságú szolgáltatást nyújtva. Minősített szolgáltatás indítását a NetLock és a GIRO tervezi a közeljövőben. Időbélyegzés szolgáltatással jelenleg egyikőjük sem rendelkezik, de a NetLock 2002-ben szándékozik ilyet indítani. Állami szervek (mint például az IM, az APEH vagy a vámosok) is rendelkeznek zárt körben használatos szolgáltatással, és kormánydöntés született egy központi kormányzati tanúsítványkiadó központ beindításáról is (a

már említett KEAR). Ezenkívül zárt körben számos cég és szervezet használ tanúsítványokat belső szabályzatok vagy egyedi szerződéses feltételek alapján.

A három nyilvános szolgáltató tipikusan egyéves érvényességű, 1024 bites RSA kulccsal felszerelt aláíró- és titkosítótanúsítványok kártyára vagy floppyra történő kibocsátását nyújtja. Aktuális árlistájuk, szabályzataik, szerződéses feltételeik elérhetők saját web oldalaikon keresztül vagy a Hírközlési Felügyeletnél.[55]

A kézirat zárásakor vette a HÍF nyilvántartásba negyedik hitelesítészolgáltatásként a Microsec Számítástechnikai Fejlesztő Kft. fokozott biztonságú e-szigno hitelesítésszolgáltatását (www.e-szigno.hu).

10.4.1 A NetLock Kft. és hitelesítésszolgáltatása

A NetLock Kft. 1996. október 25-én alakult, alig másfél évvel a Verisign után, pont akkortájt, amikor magam is első, elektronikus aláírással felvértezett alkalmazásaimat írtam. A hárommillió forintos alaptőkéjű cég magyar magánszemélyek és társaságok, tíz százalékban pedig egy angol befektető tulajdonában van.

A cég három lábon áll. A tanúsítványkiadási tevékenység ezek közül a legismertebb. A második, PKI-integrációnak nevezett láb a legerősebb, mely PKI alapú fejlesztéseket, intelligenskártya-megoldások implementálását és saját hitelesítőközpont-technológiájuk vállalati bevezetését takarja. Ezek mellett kezd feljönni a harmadik lábként definiált PKI tanácsadási tevékenység, melybe beletartozik rendszertervek, tanulmányok és ajánlások készítése is.

A NetLock Kft. saját gyártású rendszert üzemeltet, melyet az OpenSSL-re, egy nyílt kódú kriptokészletre alapozva fejlesztett ki (és fejleszt tovább jelenleg is) saját igényeinek megfelelően. A szolgáltatói kulcsok biztonságáról egy hardveres kriptográfiai egység gondoskodik, melynek beszerzésére az exporttilalom feloldása után nyílt alkalmuk. 1999. október 6-án, azóta is egyetlen magyar, sőt kelet-európai tanúsítványkiadóként gyökér tanúsítványaik bekerültek a Microsoft operációs rendszereibe.

A NetLock Kft. a törvény szerinti fokozott biztonságú szolgáltatását 2001. október 26-án indította (ekkor a törvényt megelőző szolgáltatásuk már évek óta működött). Ezt a szolgáltatást az Ernst & Young auditálta nemzetközi standardok (a WebTrust ajánlása) alapján. Ugyanezen cég végezte a szolgáltatás fizikai biztonság auditját is. Ezenkívül rendelkeznek ISO 9001:2000 minőségbiztosítási tanúsítvánnyal is, melyet a Moody International adott ki. A cég harmincmillió forintos felelősségbiztosítással rendelkezik az AXA-Colonia Biztosító Rt.-nél.

A NetLock termékpalettája C (Expressz), B (üzleti), A (közjegyzői) és teszt tanúsítványosztályok, valamint személyes, meghatalmazásos, szervezeti, SSL-szerver, VPN, WAP-szerver, láncolt szolgáltató tanúsítványtípusokból áll. C osztályú tanúsítvány esetén ötvenezer forint, B osztályú tanúsítvány esetén ötszázezer forint, A osztályú tanúsítvány esetén ötmillió forint pénzügyi garancia jár a tanúsítványokkal.

Ha valaki NetLock-tanúsítványt szeretne igényelni, felkeresheti a cég oldalait, és regisztráció után on-line igényelhet magának tesztcélú vagy A, B, C osztályú ta-

núsítványt. Tesztcélú tanúsítványnál (ahogy azt bemutattam) mindent el tud intézni interneten keresztül. C osztályú tanúsítványnál sem kell kimozdulnia otthonról, de faxon vagy levélben adatokat kell szolgáltatnia. B osztályú tanúsítvány beszerzése már nem megy otthonról: vagy a NetLockhoz, vagy a 3200 postahivatal egyikébe be kell fáradnia a kedves ügyfélnek. A osztályú tanúsítvány megkaparintásához viszont egyenesen egy közjegyzőt kell felkeresni. Az igénylőnek az A, B és C osztályú tanúsítványok esetében eltérő szintű személyes regisztráción kell átesnie.

Cég: NetLock Informatikai és Hálózatbiztonsági Kft.
Cím: 1023 Budapest, Zsigmond tér 10 Telefon: 345-2255
Web: www.netlock.net E-mail: info@netlock.net

10.4.2 Matáv e-Szignó

A Matávot – úgy hiszem – nem kell bemutatnom senkinek. A több mint százhárommilliárd forint alaptőkéjű cég egészen más súlycsoportban versenyez, mint riválisai. A távközlési rt. részvényeinek 59 százaléka a Deutsche Telekomé, 41 százaléka nyilvános forgalomban, egy aranyrészvény pedig a magyar állam kezében van.

Az e-Szignó-nak nevezett hitelesítésszolgáltatás alapját adó hitelesítő-központ Németországban található. Magyarországon a hozzáférési felületek honosítását és regisztrációs környezetek kialakítását, valamint a szolgáltatás helyi üzleti menedzsmentjét végzik. Vagyis a CompanyPass nevű termékre alapozott megoldás voltaképpen nem is a Matávé, hanem annak anyukájáé, a Deutsche Telecomé, s imigyen tekintve már többéves tapasztalat áll mögötte. Szóval igazi német minőséggel van dolgunk, jelentsen ez bármit a Holstentől a Dáridóig bezárólag. Bár a Schumacher-hívők biztos erre indulnának be, le kell hűtenem a felforrósodó kedélyeket. A 2001. október 1-jén indított szolgáltatás (a HÍF-regisztráció időpontja 2001. december 21.) még nem hozzáférhető egyszerű halandók számára. Egyelőre csak vállalati körben való terjesztésről van szó, melynek keretében az ügyfél cég maga végzi a tanúsítványkérelmek elbírálását, továbbá a tanúsítványok regisztrációját és menedzsmentjét, vállalva a regisztrációs adatok helytállóságáért a felelősséget a Matáv felé. Ma még ez a helyzet, de mire e könyvet olvassák, már lehet, megjelent a cég a piacon az igazi felhasználói tanúsítványokkal is, melyeket várhatóan a MatávPontokon (a Matáv ügyfélszolgálati irodáin) keresztül lehet majd igényelni.

A K&H Bank e-bank-rendszerében vizsgázott szolgáltatás auditját a PricewaterhouseCoopers, az aláíró eszköz műszaki tanúsítását a HunGuard Kft. végezte.

Az e-Szignó szolgáltatás keretében tipikusan kliens oldali SSL és S/MIME tanúsítványok kibocsátását kérhetjük, a kriptomodultól függően 512, 768 vagy 1024 bit kulcshosszal, de egyedi szerződéses feltételek mellett mód van IPSec tanúsítványok és USB tokenen tárolt tanúsítványok beszerzésére is.

Cég: Magyar Távközlési Rt. Cím: 1013 Budapest, Krisztina krt. 55.
Telefon: 481-7317 Web: www.matav.hu/vilag/aktualis/eszigno.html
E-mail: kovari.ferenc1@ln.matav.hu

10.4.3 A GIRO hitelesítésszolgáltatása

Az 1989-ben alapított GIRO Rt. valószínűleg kevésbé ismert olvasóim előtt. Pedig a két és fél milliárd forint alaptőkéjű, magyarországi pénzintézetek által tulajdonolt cég kiemelt szerepet játszik a hazai pénzügyi életben: ő működteti a fizetési rendszer egyik ütőerének számító bankközi elszámolási rendszert.

A 2001 legvégén hiteles védjegy alatt megkezdett szolgáltatás alapja a Baltimore Technologies SUN vason és Solaris operációs rendszer alatt futó UniCERT szoftvere, a szintén Baltimore-gyártású nagy megbízhatóságú kulcstároló egységek, valamint a SUN iPlanet LDAP könyvtárrendszere. A rendszer kiépítése során belső auditori tevékenységet is magában foglaló tanácsadást látott el a PwC Consulting.

Bár a GIRO szolgáltatása nyilvános, ahhoz, hogy egy tanúsítvány büszke tulajdonosai lehessünk, egy pénzintézet ügyfelévé kell válnunk, és olyan szolgáltatást kell igényelnünk, amely a tanúsítványokat hasznosítja. A szereposztás szerint ugyanis a pénzintézetek a GIRO hitelesítő-központjának regisztrációs szervezeteként funkcionálnak, s így a szolgáltatások előfizetők felé való közvetítését ők intézik. Az igénylőknek így nem közvetlenül a GIRO Rt.-hez kell fordulni hitelesítésért. Azt csak e partnerintézményeken keresztül tudják intézni, amelyek a tanúsítványok és szolgáltatások értékesítését a saját üzletpolitikájuk szerint, különböző feltételeket szabva végzik. A pénzintézet a tanúsítványt – valószínűleg – határozott céllal fogja kibocsátani, vagyis az elsődlegesen csak arra a célra, abban a környezetben lesz felhasználható, mint az említett szolgáltatás (bár az ettől eltérő felhasználás gyakorlatilag nemigen akadályozható meg, a GIRO Rt. felelősségvállalása nyilvánvalóan csak a szabályzatoknak megfelelő felhasználásra terjed ki, amit határozottan ajánlanék a majdani elfogadók figyelmébe).

Azok számára, akik a feltételeknek eleget tesznek, számos tanúsítványtípussal kedveskedik a cég: a személyes és szervezettípusok mellett eszköztanúsítványokkal is. Míg az előbbihez jelenleg ötvenezer forint pénzügyi garancia jár tanúsítványonként, az utóbbi két típusnál 250 ezer forint a garancia mértéke.

Cég: GIRO Elszámolásforgalmi Rt.
Cím: 1054 Budapest, Vadász utca 31. Telefon: 428-5600
Web: http://www.giro.hu/hiteles E-mail: kerdes@hiteles.giro.hu

10.5 Aláírás és aláírás-ellenőrzés

A könyv bejezéseként emlékeztetőül összefoglalnám az aláírás megtételével és ellenőrzésével kapcsolatos legfontosabb tevékenységeket, illetve a hitelesítésszolgáltatók előírásait a magánkulcs és a tanúsítvány birtoklásával és fel-

használásával kapcsolatosan. A szolgáltatók kártérítési felelősséget vállalnak az általuk kibocsátott tanúsítványok tekintetében, de ez csak akkor érvényesíthető, ha a károsult fél igazolja, hogy mindenben úgy járt el az elektronikus aláírási vagy aláírás-ellenőrzési tevékenységében, illetve a magánkulcs birtoklása során, ahogy azt a rá vonatkozó szabályzatok és jogszabályok előírják, valamint ahogy az az adott helyzetben a szükséges műszaki, jogi ismeretek birtokában és a józan ész szerint is elvárható lett volna. Remélem, a fejezet végén minden olvasó elmondhatja, hogy ezen ismereteknek birtokába jutott, és így megfontoltsága biztos alapokra építkezhet az elektronikus aláírás felhasználásakor.

10.5.1 Az aláíró kötelezettségei

Az aláíró kötelességei között legfőbb helyen a magánkulcs lehető legnagyobb gondossággal való kezelését, védelmét szokták kiemelni. Ez a kötelezettség egyetemben vonatkozik a magánkulcs aktivizáló adatára és az aláíró eszközre, illetve a kulcs hordozójára. Ritkán említik, de ugyanígy megfelelő védelemben kell részesíteni a teljes aláíró környezetet is a már említett, az aláírás menetébe beleavatkozó fenyegetések ellen. Ha bármilyen komoly kétség merülne fel az aláírás-létrehozó vagy annak aktivizáló adatának biztonságát illetően, az aláírónak azonnal intézkednie kell a tanúsítvány visszavonása végett.

Az aláírónak, mint a tanúsítvány tulajdonosának, saját érdekében is ügyelnie kell arra, hogy a tanúsítványban valódi és érvényes adatok legyenek feltüntetve (különösképpen az azonosítómezőben). A tanúsítvány igénylésekor ilyen adatokat kell megadnia, első használat előtt ellenőriznie kell ezeket, és később új tanúsítványt kell igényelnie, ha az adatok érvényüket vesztenék.

Az előírások nemcsak az aláíró kulcsokkal és tanúsítványokkal kapcsolatosan értelmezettek, hanem eltérő módon mindenfajta tanúsítvánnyal kapcsolatban. Így a magánkulcsok felhasználása tekintetében a felhasználónak be kell tartania az arra vonatkozó korlátozásokat is. Ez egyaránt vonatkozik a felhasználási célra, érvényességi időre, pénzügyi korlátokra és egyebekre.

Mindezeket a kötelességeket és a felhasználó egyéb feladatait a szolgáltatók szabályzatai részletesen tárgyalják, s annak érdekében, hogy ezekkel a felhasználó tisztában legyen, előírják számára e szabályzatok megismerését.

10.5.2 Elektronikus aláírás megtétele

Az elektronikus aláírás megtétele mindezek után igen egyszerű. Az aláírónak ki kell választania azt a magánkulcsát (annak tanúsítványán keresztül), amivel az aláírást meg kívánja tenni, meg kell győződnie arról, hogy azt írja alá, amit valóban alá akar írni, és ki kell adnia a parancsot az aláírásra. Az aláíráskor lehetséges, hogy különböző aláírás-attribútumok beállítása is szükséges. Ilyen lehet például az aláírási szabályzatra való hivatkozás vagy a kötelezettségvállalás típusa. Az aláírás ellenőrzéséhez szükséges tanúsítvány, illetve az aláírás idejét igazoló időbélyegző is ilyen attribútumként utazhat az aláírással együtt. Az alá-

írás attribútumait, azok értelmezését és beállítását, az aláírásra vonatkozó egyéb szabályokat az aláírási szabályzat határozza meg.

10.5.3 Az ellenőrző kötelezettségei

Számos előírás létezik az aláírás ellenőrzésének tekintetében is. Ezek célja, hogy minimalizálják annak lehetőségét, hogy az ellenőrző nem érvényes aláírást fogad el, illetve ennek felelősségét az ő nyakába varrják. A szolgáltatói szabályzatok elsősorban a tanúsítvány ellenőrzését tárgyalják. Így előírják az aláíró személyéről és a szolgáltató kilétéről való meggyőződést a tanúsítvány azonosító mezői alapján (s ha az nem elégséges, egyéb módszerekkel is), a tanúsítvány érvényességének ellenőrzését a tanúsítványban feltüntetett érvényességi idő és egyéb érvényességi információk (CRL, OCSP) alapján, és a tanúsítvány felhasználási céljának, korlátjainak ellenőrzését is. Elvárják a tanúsítvány sértetlenségének vizsgálatát is a szolgáltatói tanúsítvány segítségével, az említett ellenőrzések megismétlését a szolgáltatói tanúsítványra, valamint a teljes tanúsítási láncra vonatkozóan.

A szolgáltatók elvárják a szabályzatok megismerését és betartását az ellenőrző felek részéről is, és magam is azt tudom tanácsolni mindenkinek, hogy a szabályzatok rájuk vonatkozó részével ismerkedjenek meg minél hamarabb.

10.5.4 Az elektronikus aláírás ellenőrzése

Az elektronikus aláírás ellenőrzése első lépcsőben annak algoritmikus ellenőrzését jelenti: az aláíró tanúsítványba foglalt nyilvános kulcsával való visszafejtését, és az aláírt adat sértetlenségének megvizsgálását. Ez az algoritmikus ellenőrzés minden alkalmazás esetében automatizált. Részben automatizált a tanúsítvány és a tanúsítási lánc ellenőrzése: az érvényességi idő megvizsgálása például általában ilyen. A lánc ellenőrzésének addig kell tartani, míg egy korábban ellenőrzött és biztonságosnak minősített tanúsítvánnyal nem találkozunk (saját nyilvántartásunkban). Automatizálható a kibocsátó- és aláíró-azonosítók, a szabályzatazonosító, a pénzügyi korlátok ellenőrzése is (erre főleg tranzakciós rendszerek esetében van példa). A tanúsítvány állapotának ellenőrzése a tanúsítvány sorozatszáma vagy egyéb azonosítója alapján történhet, de ehhez előbb be kell szerezni a visszavonási listát. Ez történhet az alkalmazás, illetve az operációs rendszer saját nyilvántartásából vagy a tanúsítványtárból LDAP lekérdezés segítségével (amennyiben a vállalati rendszergazdák nem állnak ennek útjába). A listában való keresés előtt ellenőrizni kell a listán lévő aláírást, a lista saját kibocsátási idejét és a következő lista kibocsátásra vonatkozó időt. Ha a következő lista kibocsátásának idejét túlhaladtuk, akkor le kell tölteni az azóta kibocsátott listákat, illetve a legutolsó listát[56], és abban kell elvégezni a tanúsítványra vonatkozó keresést. Ezek a lépések ugyan automatizálhatók az alkalmazások által (de ezen automatizmusokban csak akkor bízzunk meg, ha mű-

ködésüket ellenőriztük), az ellenőrzőnek azonban magának kell dönteni a tanúsítvány elfogadásáról, illetve visszautasításáról, ha a visszavonási listában felfüggesztési vagy visszavonási bejegyzés található. Ilyen esetben az aláírás és a visszavonás idejének összehasonlítása is szükséges lehet. Az ellenőrzés során használt dátumnak az aláírás idejét kell alapul vennie (nem az ellenőrzés idejét). Az elektronikus aláírás ellenőrzéséhez hozzá tartozik ezen túl az aláírás attribútumainak vizsgálata is, az aláírási szabályzatnak megfelelően.

A kezdeti ellenőrzés után – különösen az aláírás elfogadása esetén – hasznos lehet az ellenőrzés során felhasznált adatok – az üzenet, az aláírás, a tanúsítvány és a visszavonási lista (vagy OCSP válasz) – archiválása a későbbi ellenőrzésekhez és a letagadhatatlanság biztosításához (még akkor is, ha ezen adatok egy része később a szolgáltatótól is beszerezhetők).[57]

Az ellenőrzőt leginkább fenyegető, legvalósabb veszély az azonosítókkal való visszaélés: a szolgáltató megtévesztésével hamis azonosító szerzése, félreérthető azonosító igénylése, esetleg saját tanúsítvány legyártása hamis szolgáltatói (de valódi felhasználói) azonosítóval. Könnyen elképzelhető még a visszavonás-kezeléssel való visszaélés is: a visszavonás időzítéseinek kihasználásával még érvényesnek látszódó aláírás készítése (vissza lehet élni például azzal, ha az ellenőrzőnek késik a rendszerórája). Nem árt a saját tanúsítvány-nyilvántartásunkra való ügyelés sem (a gépünkhöz való ellenőrizetlen hozzáférések megakadályozásával), nehogy valaki belecsempésszen egy olyan szolgáltatói tanúsítványt, amit magunktól nem minősítenénk megbízhatónak.

Ezek a veszélyek megfelelő kontrollal kezelhetők, nem is kívánnak tudományos szintű műszaki ismereteket, mindössze az alapvető veszélyeket ismerő tudatos és felelősségteljes magatartást, ami arányban van egy hamis aláírás elfogadásából származó esetleges veszteséggel.

JEGYZET

1 Erre az USB tokeneknél általában nincs mód.

2 Szótár adatbázisok pár százezres szóállományát akár pár óra alatt is végig lehet próbálni.

3 A gyakrabban használt száz különböző karakterrel számolva.

4 Az OSI specifikációja kapcsán lett kifejlesztve, az ITU X.208 szabvány írja le.

5 Mindegyik az ASN.1 által leírt objektumok platformfüggetlen kódolását szabályozza. Az ITU X.209, X.690 és ISO/IEC 8825 szabványok által leírva.

6 Lásd: IETF RFC 1341 és RFC 2633.

7 A P7C kiterjesztésű fájlokat Digital ID File-ként ismeri fel az **Intéző**.

8 A bekerüléshez a szolgáltatóktól a WebTrust tanúsítását követelik meg. Bővebb információ: http://www.microsoft.com/technet/security/news/rootcert.asp és http://www.webtrust.org/certauth.htm

9 A **Netscape**-nek hasonló nyilvántartása van, hasonló gyengeségekkel.

10 A **Windows 2000** és a régebbi operációs rendszerek esetében a felhasználók a Windows Update website segítségével tehetik meg ezt manuálisan. A lista szervezetek esetében, az Active Directory használata esetén csoportszabályzattal is bővíthető. Fejlesztők figyelmébe ajánlom további lehetőségként az Internet Explorer Administration Kitet, a CAPICOM scriptelési lehetőséget és a CertEnroll vezérlőelem weblapról történő meghívását.

11 **Windows 2000** esetében kevesebb logikai egység létezik.

12 Kétdimenziós tárként lehet elképzelni: az egyik dimenzió a szegmenseké, a másik a logikai egységeké.

13 Az **MMC** segítségével ezt magunk is kipróbálhatjuk. Csak arra kell vigyázni, hogy az **MMC** ezt az öröklést nem mutatja. Ennek hatása csak a **Certificates** ablakban fedezhető fel.

14 Group Policy: egy hálózati tartomány felhasználóira együttesen vonatkozó szabályok, melyeket a tartomány adminisztrátora állít be.

15 Nem árt azonban fenntartásokkal kezelni az itt megjelenítetteket, mert saját tapasztalataim ellentmondanak az **MMC** által mutatott adatoknak. Például az **MMC** a saját tanúsítványokat a Registryben jelzi, én ezzel szemben csak a fájlrendszerben bukkantam rájuk, a szolgáltatói tanúsítványok előre definiált részét pedig a fájlrendszerben jelzi, én viszont csak a Registryben találkoztam velük!

16 Magyar nyelvű operációs rendszer esetén a könyvtárnevek értelemszerűen különböznek.

17 **Windows 2000** esetében a **Control Panel – Users and Passwords – Advanced – Certificate Management / Certificates** útvesztő is ugyanide vezet.

18 **Run MMC** parancsal indítható a **Windows Start** menüjéből, megfelelő jogosultságok birtokában.

19 Az **MMC** ettől függetlenül is képes más képet mutatni a tanúsítványtárról, mint a **Certificates** ablak. Ennek egyik oka, hogy az **MMC** az öröklési jellegű szabályokat nem mutatja (a gép gyökér tanúsítványai közül törölt elemeket megjeleníti a felhasználó tárában is, pedig azok nem élnek ott), de praxisomban találkoztam olyan jelenséggel, hogy **Certificates** ablak nem mutatott létező, a Personal könyvtárt gazdagító tanúsítványokat, azok csak az **MMC**-vel és más alkalmazásokkal váltak láthatóvá.

20 E két üzemmódtól eltérő működést is be lehet állítani a rendszer szabályzati moduljának átszabásával.

21 Nem vállalati nyilvános szolgáltató esetében ez a módszer sajnos nem működik.

22 A toldalék kritikus voltától függően a felhasználási cél csak ajánlás vagy kötelezően betartandó előírás.

23 Ilyenek például az önhitelesített EFS tanúsítványok is (lásd 96. ábra).

24 Az ablak mögött álló minialkalmazás többfajta tanúsítványformátumot kezel, olyanokat is, amelyek egy lánc elemeiként több tanúsítványt fognak össze, illetve képes az ismert szolgáltatói tanúsítványok láncba szervezésére.

25 P7C típusú tanúsítványokkal sikerülhet előbújtatni, az **Intéző**-ből, valamint **Outlook**-beli levelezés alkalmával találkozni vele.

26 Hardveres CSP-k nem támogatják.

27 A magánkulcs exportját lehetőleg ne engedélyezzük, mert ezt kihasználva illetéktelenek is másolatot készíthetnek kulcsunkról.

28 A gép szegmense a HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\SystemCertificates\CA\CRLs bejegyzés már eredetileg is tartalmaz visszavonási listát.

29 Bővebb információ: www.microsoft.com/winlogo

30 A Java appletek nem feltétlen Authenticode módszerrel vannak aláírva. Nem windowsos környezetben, nem az IE JVM-je (Java Virtual Machine) alatt ez a módszer nem működik.

31 Az ilyen aláírók a Registry HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing\Trust Database kulcsa alatt találhatók.

32 Ez egymással bizalmi viszonyt ápoló gépek esetén, egy másik gép NTFS-egységére is igaz, amennyiben az engedélyezi a titkosítás használatát.

33 Ez a figyelmeztetés nem biztos, hogy minden verzióban, minden körülmények között megjelenik, ezért ajánlott a manuális ellenőrzés.

34 Az EFS kódja a **Windows** magjában található. A magánkulcsokat soha nem tárolja lapozható memóriaterületen, így azok lapozófájlba véletlenül sem kerülhetnek. Az EFS a DES algoritmust használja a rejtjelezéshez.

35 Ez sem segít azonban, ha 128 bites titkosítással rendelkező gépről próbálunk 56 bitesre mozdulni. Ilyen esetben a titkosítórendszer frissítése a megoldás.

36 A **Backup** program ablakában a titkosított állományok nem eltérő színnel jelennek meg.

37 Ha ilyen kellemetlenség történne velünk, akkor a DRA-nak kell elküldenünk titkosított állományunkat. Ezt az előbb ismertetett backup mentést követően akár e-mailben is megtehetjük. A DRA által visszafejtett adatokat azonban érdemesebb nem nyílt levélben visszajuttatni.

38 Állítják legalábbis a dokumentációk, de saját tapasztalásaim ennek ellentmondanak.

39 FEK, azaz File Encryption Key. Ez a kapcsolati kulcs szisztémához hasonlít.

40 A lokális gépen másolati formában tárolt hálózati állományok, amik így hálózati kapcsolat nélkül is elérhetők, módosíthatók, s melyek tartalma rendszeresen egyeztetve van a hálózati verzióval.

41 Használható e célra szolgáltatói (nem a vállalati MS Certificate Server által létrehozott) tanúsítvány is, de az ilyen tanúsítványnak sok feltételnek meg kell felelnie, és bizonyos mennyiségű buherálást igényel a feladat.

42 Ezzel véletlenül sem kívánom azt az érzést kelteni, hogy ez a módszer előnyösebb az alkalmazás szintű biztonsági megoldásoknál. Az igazság ennek pont az ellenkezője, viszont ha az alkalmazásunknak nincsenek ilyen képességei, akkor nagyon is jól jön ez a módszer.

43 A PPTP csak IP-hálózaton működik, és csak egyetlen csatornát tud létrehozni. Az L2TP az IP-n kívül ATM, Frame Relay és X.25-ös hálózatokon is működőképes, több csatorna egyidejű kezelésével.

44 Ez azzal jár, hogy mindenki, aki be tud jelentkezni a gépünkre (összes helyi és tartomány felhasználó, meg aki fel tudja törni az operációs rendszer védelmét), az a gép magánkulcsához is hozzáfér, s így az IPSec-es kommunikációt is használni tudja.

45 A hardveres CSP-ket nevezik SCSP-nek és SCCP-nek is.

46 A CSP-k barangolóprofilokon keresztül támogatják a felhasználók barangolását, azaz hogy a felhasználó bármely tartományi gépen hozzáférjen magánkulcsaihoz, tanúsítványaihoz és egyéb biztonsági beállításaihoz. Intelligens kártyák használata esetén a magánkulcsot persze kézzel kell a felhasználási helyére szállítani.

47 Hasonló listát kaphatunk az XP-hez a Windows Catalogban is (www.microsoft.com/windows/catalog **Hardware – Input Devices – Smart Card Reader**), sőt a www.microsoft.com/hwtest oldalról egy test kitet is letölthetünk a kompatibilitás tesztelésére.

48 Ezek listáját lásd: www.microsoft.com/TechNet/prodtechnol/winxppro/proddocs/sag_SCusereader.asp

49 Bővebb információ az Exchange 2000 Release Notes-ban: http://www.microsoft.com/exchange/techinfo/productdoc/2000/E2KReleaseNotes.doc

50 Bővebb információ az **Office XP** Resource Kit-ben: http://www.microsoft.com/office/ork/xp/two/admb05.htm

51 Bővebb információ: http://www.microsoft.com/office/ork/2000/download/Out2000SR-1.doc

52 A levél fejlécében jelölhetjük az üzenet érzékenységét s azt, hogy ki nyithatja meg, továbbíthatja az üzenetet.

53 Hibák: ismeretlen aláírási algoritmus, aláíró-tanúsítvány nem található, hibás attribútumkészlet, kibocsátótanúsítvány nem található, visszavonási lista nem található, lejárt tanúsítvány, gyökér megbízhatósági hiba, lejárt tanúsítványbizalmi lista.

54 A tanúsítvány Exchange Global Address List-be történő közzétételéhez.

55 Bár cégem, a PwC Consulting (a PricewaterhouseCoopers vezetési tanácsadó részlege) és személyem ezer szállal kötődik a nevezett cégekhez, s szolgáltatásaik kiépítésében is valamilyen módon mindegyikőjüknél szerepet vállaltunk, az ismertetőt igyekeztem mindenfajta részrehajlás nélkül összeállítani.

56 Delta CRL esetében az összes, azóta kibocsátott listát le kell tölteni.

57 Az alkalmazásokban ezen adatok nagy része általában automatikusan megőrződik, hacsak direkt ki nem töröljük őket.

Melléklet

Fogalomtár

A korábbiakban sokkal slendriánabb módon használt kifejezések ellenpontozásaként az alábbi fogalomtárban a könyvben szereplő fontosabb szakkifejezések, fogalmak szinonimáit, angol megfelelőjét és „hivatalos" definícióját mutatom be. Azoknál a fogalmaknál, amelyeket a könyv nem tárgyalt minden részletében, rövid magyarázat is található. A fejezetet a közigazgatási fogalomtár alapján állítottam össze (minimális változtatásokkal), amely a törvényi definíciók és egyéb szabványok figyelembevételével készült.* A fogalomtár teljes tartalma a http://www.fogalomtar.hu/ címen érhető el.

Kriptográfia, kriptológia, kriptoanalízis
A görög kripto szótőből származó kapcsolódó elnevezések. Kriptológia: rejtjelezés-tudomány; kriptográfia: rejtjelrendszerek tervezése; kriptoanalízis: rejtjelrendszerek elemzése. – A rejtjelezés a szöveg (adatsor) olyan átalakítása, mely után az átalakítás módjába be nem avatottak számára (az algoritmus és/vagy kulcs ismeretének hiányában) az átalakított szöveg (adatsor) nem visszaállítható.

Nyilvános kulcsú infrastruktúra – Public Key Infrastructure (PKI)
Azoknak a berendezéseknek, szoftvereknek, emberi erőforrásoknak és eljárásoknak az együttese, melyek a nyilvános kulcsú kriptográfián alapuló tanúsítványok előállításához, menedzseléséhez, tárolásához, szétosztásához és visszavonásához szükségesek.**

Lenyomat – Fingerprint, Hash-code, Message Digest
Egy elektronikus dokumentumból előállított rövid karaktersorozat, amely gyakorlatilag egyértelműen jellemző az adott dokumentumra.

Hash-függvény – Hash Function
Olyan egyirányú függvény, mely tetszőleges hosszúságú szövegből olyan, rögzített hosszúságú bitsorozatot (lenyomatot) állít elő, mely egyértelműen jellemző az adott szövegre.

Aláírás-létrehozó adat, magánkulcs – Signature Creation Data
Olyan egyedi adat (jellemzően kriptográfiai magánkulcs), melyet az aláíró az elektronikus aláírás létrehozásához használ.

---

* A fogalomtárat a Hunguard Kft. készítette a MEH IKB részére.

** Az IETF PKIX munkacsoportjának definíciója

Aláírás-ellenőrző adat, nyilvános kulcs – Signature Verification Data
Olyan egyedi adat (jellemzően kriptográfiai nyilvános kulcs), melyet az elektronikus iratot vagy dokumentumot megismerő személy az elektronikus aláírás ellenőrzésére használ. A gyakorlatban az aláírás-ellenőrző adatot általában egy tanúsítvány tartalmazza.

Aktivizáló adat – Activation Data
Az aláírás-létrehozó adat felhasználásához szükséges adat, melyet csak az aláíró (aláírás-létrehozó adat tulajdonosa) ismerhet.

Elektronikus aláírás, digitális aláírás – Electronic Signature
Elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt és azzal elválaszthatatlanul összekapcsolt elektronikus adat, illetőleg dokumentum.

Aláíró – Signer, Subscriber
Az a természetes személy, akihez a hitelesítésszolgáltató által közzétett aláírás-ellenőrző adatok jegyzéke szerint az aláírás-ellenőrző adat kapcsolódik.

Ellenőrző – Verifier
Az a személy vagy automatizmus, aki vagy amely az aláírás-ellenőrző adat felhasználásával meggyőződhet az aláírás és így az elektronikus úton aláírt irat hitelességéről, az aláíró személyéről.

Aláírás-létrehozó eszköz – Signature Creation Device
Olyan hardver-, illetve szoftvereszköz, melynek segítségével az aláíró az aláírás-létrehozó adat felhasználásával az elektronikus aláírást létrehozza.

Elektronikusan történő aláírás
Olyan folyamat, amelynek során az elektronikus aláírás hozzárendelése, illetve logikailag való hozzákapcsolása az elektronikus adathoz megtörténik.

Aláírt adat – Signed Data Object
Az aláíró dokumentuma és az aláírás-jellemzők, amelyeket együttesen írtak alá.

Kötelezettségvállalás-típus – Commitment Type
Aláírás-jellemző az elektronikus aláírás pontos szándékának az aláíró által kiválasztott jelzésére. Akkor van rá szükség, ha egy aláírási szabályzat egynél több kötelezettségvállalás-típust határoz meg, melyek különböző jogi értelmezéssel látják el az aláírási szándékot (például: származás igazolása, átvétel igazolása, létrehozás igazolása).

Többszörös aláírás – Multiple Signatures
Különböző, egymástól független aláírások elhelyezése egy elektronikus dokumentumon. Például akkor alkalmazzák, ha a dokumentum fontossága több személy együttes aláírását igényli.

Azt írsz alá, amit látsz – What You Present is What You Sign
Elv, melynek érvényre jutása garantálja, hogy az aláíró valóban az aláírásra szánt adatot írja alá. Az aláírandó dokumentumot valósan, egyértelműen meg kell mutatni az aláíró részére.

Aláírás-létrehozási környezet – Signature Creation Environment
Az a fizikai és rendszerkörnyezet, melyben az aláírási folyamat lezajlik, és amely egy aláírás-létrehozó rendszert tartalmaz az aláírás-létrehozó eszközzel és az aláíró által kezelt rendszerelemekkel.

Aláírás-létrehozó rendszer – Signature Creation System
Az a rendszer, illetve alkalmazás az aláírás-létrehozási környezeten belül, amelyik egy aláírás-létrehozó eszközt használ fel fokozott biztonságú elektronikus aláírás létrehozásához.

Elektronikus aláírás ellenőrzése – Signature Verification
Az elektronikus dokumentum aláíráskori, illetve ellenőrzéskori tartalmának összevetése, továbbá az aláíró személyének azonosítása a dokumentumon szereplő, illetve a hitelesítésszolgáltató által közzétett aláírás-ellenőrző adat és a tanúsítvány felhasználásával.

Aláírás-ellenőrzési folyamat – Verification Process / Validation Process
Olyan folyamat, amely érvényesít egy elektronikus aláírást az aláírási, hitelesítési vagy szolgáltatási szabályzat követelményeinek megfelelően. – Az ellenőrzési folyamat eredménye lehet befejezetlen ellenőrzés, sikeres ellenőrzés, sikertelen ellenőrzés. Az ellenőrzési folyamatnak két típusa különböztethető meg: kezdeti ellenőrzés, utólagos ellenőrzés.

Sikertelen ellenőrzés – Failed Verification
Az ellenőrzés eredménye azt jelzi, hogy vagy az aláírás formátuma, vagy a digitális aláírás értéke nem megfelelő, vagy az aláírás nem felel meg az aláírás-ellenőrzési szabályzatnak, vagy pedig az aláíró tanúsítványát visszavonták.

Sikeres ellenőrzés – Passed Verification
Az ellenőrzés eredménye azt jelzi, hogy az aláírás ellenőrzése sikeres volt, és megfelel az aláírás-ellenőrzési szabályzatnak.

Befejezetlen ellenőrzés – Incomplete Verification
Az aláírás-ellenőrzési folyamat akkor szolgáltat „befejezetlen ellenőrzés" eredményt, ha mind az aláírás formátuma, mind a digitális aláírás ellenőrzése sikeres volt, de mégsem áll rendelkezésre elegendő információ ahhoz, hogy az aláírási szabályzat alapján az aláírás érvényességét meg lehessen határozni. – Például elindítottak egy tanúsítvány-felfüggesztési kérelmet, melynek hitelességét a szolgáltató még nem ellenőrizte. Ekkor lehet, hogy kérvényezhető az aláírás egy későbbi időpontban való újraellenőrzése, amikorra a (még szükséges) kiegészítő érvényesítő információ már rendelkezésre fog állni. Befejezetlen ellenőrzés esetében az alkalmazás vagy a felhasználó számára olyan információkat lehet hozzáférhetővé tenni, melyek segítségével az alkalmazás vagy a felhasználó el tudja dönteni, hogy mit kezdjen a részben érvényes elektronikus aláírással.

Kezdeti ellenőrzés – Initial Verification
Egy ellenőrző által végrehajtott folyamat, melyet egy aláírás létrehozása és ellenőrzőhöz juttatása után minél hamarabb kell megtenni. – A kezdeti ellenőrzés

célja, hogy azok az információk megszerezhetők legyenek, melyek az ellenőrzőnek szükségesek, és utólagos ellenőrzésekhez alkalmassá teszik az aláírást.

Utólagos ellenőrzés – Usual Verification
Egy ellenőrző (vagy döntőbíró) által végrehajtott folyamat, melyet hosszú idővel egy aláírás létrehozása után is végre lehet hajtani, s amelyhez nincs szükség több adat megszerzésére, mint amit a kezdeti ellenőrzés során már megszereztek.

Tanúsítványállapot-ellenőrzés – Certificate Status Verification
Az a folyamat, amelynek során megvizsgálják a tanúsítványállapot-információt.

Tanúsítványérvényesség-ellenőrzés – Certificate Validation Verification
Az a folyamat, amelynek során megvizsgálják a tanúsítvány érvényességét. – A tanúsítványérvényesség-ellenőrzés az állapotellenőrzésnél átfogóbb folyamat. Egyrészt jelenti a tanúsítványba foglalt érvényességet befolyásoló adatok ellenőrzését (például érvényességi idő), magában foglalja a tanúsítványra vonatkozó állapot ellenőrzését, és ezenfelül tartalmazhat a szabályzatokra vonatkozó ellenőrzéseket is (például hitelesítési szabályzat azonosítójának ellenőrzését). Az előbbi ellenőrzéseket nem csak a tanúsítványra, de a teljes tanúsítási lánc érvényességére vonatkozóan is elvégzi. A folyamat végrehajtását érvényességi szolgáltató is nyújthatja.

Érvényesítési adat – Validation Data
Olyan kiegészítő adat, melyet az aláíró és/vagy egy ellenőrző gyűjt össze, és amely annak eldöntéséhez szükséges, hogy egy elektronikus aláírás megfelel-e az aláírási szabályzat követelményeinek. – Tartalmazhat tanúsítványokat, visszavonási állapotinformációkat (az aláíróra és a hitelesítésszolgáltatóra vonatkozóan), továbbá időbélyegzés-szolgáltatóktól származó időbélyegzéseket. Az érvényesítési adatnak igazolnia kell azt, hogy az aláírás létrehozásakor az ott felhasznált teljes tanúsítási lánc érvényes volt.

Hitelesítésszolgáltatás – Certification Service
A hitelesítésszolgáltatás keretében a hitelesítésszolgáltató azonosítja az igénylő személyét, tanúsítványt bocsát ki, nyilvántartásokat vezet, fogadja a tanúsítványokkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a tanúsítványhoz tartozó szabályzatokat, az aláírás-ellenőrző adatokat és a tanúsítvány aktuális állapotára (különösen az esetleges visszavonására) vonatkozó információkat.

Tanúsítvány-létrehozási szolgáltatás – Certificate Generation Service
A hitelesítésszolgáltató egyik kötelező tevékenysége, amelynek során a tanúsítványokat előállítja. A tanúsítvány előállítása az aláírás-ellenőrző adat és a tanúsítvány egyéb adatainak együttes aláírását jelenti. A kriptográfiai kulcspár generálása része lehet ennek a tevékenységnek.

Tanúsítványkibocsátás, tanúsítványszétosztási szolgáltatás – Dissemination Service
Olyan szolgáltatás, amely az aláíróknak eljuttatja a saját tanúsítványukat, hozzájárulásuk esetén pedig szétosztja azt az elfogadó felek között is.

Regisztrációs szolgáltatás – Registration Service
Olyan szolgáltatás, mely ellenőrzi egy aláíró személyazonosságát és – ha létezik – más egyedi jellemzőit is. Eredményeit a rendszer a tanúsítvány-létrehozási szolgáltatás felé továbbítja.

Egyedinév-szolgáltatás – Naming Service
Olyan szolgáltatás, melynek feladata a nyilvános kulcsú infrastruktúra környezetén belül egyedi nevek előállítása.

Biztonságos adattárolási szolgáltatás – Secure Storage Service
Olyan kötelező adattárolási szolgáltatás, mellyel egy minősített hitelesítésszolgáltató biztosítja, hogy a regisztráció során felvett és a tanúsítványhoz kapcsolt adatok meghatározott ideig és módon megismerhetők legyenek.

Visszavonás-kezelési szolgáltatás, tanúsítvány-visszavonási szolgáltatás – Revocation Management Service
Olyan szolgáltatás, mely feldolgozza a visszavonással kapcsolatos kérelmeket és bejelentéseket a szükséges teendők meghatározása érdekében. Eredményei a visszavonási állapot szolgáltatáson keresztül kerülnek kiosztásra. – A tanúsítvány-visszavonási kérelmek mellett ez a szolgáltatás kezeli a tanúsítványfelfüggesztési és a felfüggesztett tanúsítványokra vonatkozó visszahelyezési (újraérvényesítési) kérelmeket is.

Aláírás-létrehozó eszköz ellátó szolgáltatás – Subscriber Device Provision Service
Olyan szolgáltatás, mely az aláírók számára aláírás-létrehozó eszközt készít elő és biztosít.

Visszavonási-állapot szolgáltatás – Revocation Status Service
Olyan szolgáltatás, mely a tanúsítvány visszavonási állapotáról információt biztosít az elfogadó felek számára. Lehet valós idejű, vagy alapulhat egy rendszeres időközönként frissített tanúsítvány-visszavonási listán.

Érvényességi szolgáltató – Validation Authority
Olyan szolgáltató, amely a tanúsítványra és a teljes tanúsítási lánc érvényességére vonatkozó információt kiadja.

Hitelesítésszolgáltató – Certification Service Provider
Olyan személy (szervezet), mely tanúsítványokat bocsát ki, vagy az elektronikus aláíráshoz kapcsolódó egyéb szolgáltatást nyújt.

Időbélyegző – Time Stamp
Egy elektronikus irathoz, illetve dokumentumhoz végérvényesen hozzárendelt, illetőleg az irattal vagy dokumentummal logikailag összekapcsolt igazolás, amely tartalmazza a bélyegzés időpontját. A dokumentum tartalmához technikailag olyan módon kapcsolódik, hogy minden – az igazolás kiadását követő – módosítás érzékelhető.

Szakirodalom

Az alábbiakban pár hasznos szakirodalmat szeretnék azon olvasóim figyelmébe ajánlani, akiket nem sikerült elrémítenem. A lista vegyesen tartalmaz magyar és angol nyelvű, kriptográfiával, tanúsítványokkal és PKI-val foglalkozó könyveket, leginkább újabb kiadású átfogó műveket, de pár régi klasszikust is. Többjüket magam is forgattam, és eredményesen alkalmaztam szellemem pallérozása céljából.

1 *Simon Singh: Kódkönyv – A rejtjelezés és rejtjelfejtés története* – Park Könyvkiadó, 2001
2 *Révai Zoltán: Titkosírások* – LAZI Bt., 2001
3 *Nemetz Tibor, Vajda István: Algoritmusos adatvédelem* – Akadémiai Kiadó, 1991
4 *Ködmön József: Kriptográfia* – ComputerBooks, 1999/2000
5 *Németh József: Adatvédelem a számítógépes és hírközlő rendszerekben* – Számalk, 1984
6 *Gács Péter, Lovász László: Algoritmusok* – Tankönyvkiadó, 1987
7 *Lovász László: Algoritmusok bonyolultsága* – Tankönyvkiadó, 1989
8 *Vasvári György: Biztonsági rendszerek szervezése* – PRO-SEC Kft., 1999
9 *Cormen, Leiserson, Rivest: Algoritmusok* – Műszaki Könyvkiadó, 1998
10 *Pulai, Sziklássy, Tóth, Udvaros: Védd magad az Interneten* – Kossuth Kiadó, 1997
11 *Ian McLean: Windows 2000 Biztonság* – Kiskapu, 2001
12 *Diffie, W. M.E. Hellman: New Directions in Cryptography* – IEEE Transactions on Information Theory, 1976 november, 644–654 oldal
13 *Rivest, Shamir, Adleman: On Digital Signatures and Public Key Cryptosystems* – MIT Laboratory for Computer Science, Technical Report, 1979 január
14 *R. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems* – http://theory.lcs.mit.edu/~rivest/rsapaper.pdf
15 *Robert D. Silverman: A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths* – http://www.rsasecurity.com/rsalabs/bulletins/bulletin13.html
16 *L. Blum, M. Blum and M. Shub: „A Simple Unpredictable Pseudo-Random Number Generator"* – SIAM Journal of Computing 15(2) : 364–383, 1986.
17 *Bruce Schneier: Applied Cryptography* – John Wiley & Sons, 1996

Warwick Ford, Michael S Baum: Secure Electronic Commerce – Prentice Hall, 1997
18 *Adams, Lloyd, Kent: Understanding the Public-Key Infrastructure* – New Riders Publishing, 1999
19 *Tom Austin: PKI : A Wiley Tech Brief* – John Wiley & Sons, 2000
20 *Russ Housley, Tim Polk: Planning for PKI* – John Wiley & Sons, 2001
21 *Jalal Feghhi, Peter Williams, Jalil Feghhi: Digital Certificates: Applied Internet Security* – Addison Wesley, 1999
22 *Nash, Duane, Brink, Joseph: PKI: Implementing & Managing e-Security* – RSA Press
23 *Stefan A. Brands: Rethinking Public Key Infrastructures and Digital Certificates* – MIT Press, 2000
24 *W. Rankl, W. Effing:Smart Card Handbook* – John Wiley & Sons, 1997
Catherine A. Allen, Ron Schultz: Smart Cards – McGraw-Hill, 1996

Tárgymutató

3

3DES, Triple DES algoritmus 83, 86, 97, 274

A

Active Directory 127, 252, 254, 257, 272
ActiveX 154, 266, 267, 268
Advanced Encryption Standard 83
aktivizáló adat ..... 28, 31, 79, 91, 111, 123, 128, 152, 157, 161, 165, ... 167, 193, 228, 249, 250, 262, 277, 283, 294
aláíró környezet 111, 193, 194, 201, 283
ALE, aláírás-létrehozó eszköz 165, 170, 195, 208, 239, 242, 292
álvéletlen 87, 88
ARL 153
ASN.1 ..... 251, 286
Authentication Header, AH 93, 274
Authenticode 266, 277, 287

B

babrálásálló 201
babrálásbiztos 165, 177, 194, 201
BALE, biztonságos aláírás-létrehozó eszköz 195, 208, 237, 242, 245
barangolóprofil 270, 276, 288
Base64 251
Béla 103
Kovács 119, 121, 139, 161, 183, 185
BER 251
biometrikus azonosítás 77, 78, 104, 111, 141, 176

C

CAST algoritmus 83
CBC, ECB, CFB, OFB 86, 189
CER 61, 251, 268, 269, 282
Certificate Store 251, 252, 256
Certificate Trust List 251, 252
CHAP protokoll 273

Cisco 94, 166
Common Name 139, 258
CRL 130, 134, 136, 142, 154, 221, 226, 252, 257, 262, 269, 284, 287
  delta 133, 144, 145, 153
  distribution points 132
  indirekt 112, 133
  kiterjesztésű fájl 268, 286
CryptoAPI 255, 276, 277
Cryptographic Message Syntax Standard 251

CS

csoportszabályzat 255, 271, 278, 286

D

DAP protokoll 152
Data Encryption Standard 82
Data Recovery Agent 271
DER 251
DES algoritmus 82, 274, 287
Diffie-Hellman 91, 94, 142, 274
Digital Signature Standard 82, 98
DNS 77, 142, 143
domainnév 49, 61, 120, 141
DoS támadás 153
DSA 69, 85, 90, 96, 98, 114, 116, 151

E

EAP protokoll 272
ECDSA 69, 85
EFS 49, 61, 62, 142, 254, 269, 270, 271, 272, 277, 287
egyedi név 126, 139
  tanúsítvány 153, 154, 164
  visszavonási lista 133
Encapsulating Security Payload 93
érvényességi szolgáltató 171, 294, 295

F

faktorizálás 84, 85, 97
feltörés
  algoritmus 32, 79, 82, 83, 86, 194, 238, 245
  rendszer 61, 77, 251
  üzenet 26
floppy 50, 123, 150, 192, 269, 270, 280
FTP 92

G

gateway 93
Gemplus 199, 277
GIRO 61, 128, 189, 265, 279, 282

H

hash
  algoritmus, eljárás 69, 75, 82, 96, 141, 274, 275
  függvény 69, 70, 96, 152, 291
HÍF 234, 243, 245, 280, 281
HMAC 92
HSM, Hardware Security Module 111, 151, 199, 200
HTTP 90, 92, 137, 148, 153, 166, 211

I

IDEA 83
időbélyegző 33, 52, 57, 66, 102, 114, 132, 142, 189, 209, 221, 241, 283, 295
  szolgáltatás 171, 172, 177, 208, 279
  szolgáltató 95, 171, 239, 240, 294
időforrás 162, 171, 177
infravörös port 198
Internet Explorer ..... 48, 60, 128, 252, 255, 262, 263, 264, 265, 266, 267, ... 278, 286
Intéző 50, 54, 61, 255, 261, 262, 263, 268, 269, 272, 286, 287
IPSec protokoll 93, 94, 273, 274, 275
ITU 136, 154, 207, 210, 228, 286

J

James Bond 26, 174
Java applet 267, 268, 287
Java cardlet 197
Java Virtual Machine 287

K

kapcsolati kulcs 74, 91, 94, 244, 274, 275, 287
KEAR 234, 280
Kerberos 79, 272, 274
kereszthitelesítés 182, 183, 185, 187, 261
közösség 71, 72, 73, 103, 104, 105, 151, 158, 159, 215, 216, 220, 224, 225
kriptoanalízis 32, 80, 81, 106, 291
kriptográfiai szolgáltató, CSP 41, 61, 253, 262, 276, 277, 287, 288

L

L2TP protokoll 273
LDAP 92, 126, 127, 128, 130, 134, 137, 152, 153, 211, 264, 282, 284
lenyomat 67, 69, 70, 75, 92, 102, 152, 171, 193, 194, 209, 259, 273, 291

M

magánkulcs-kompromittálódás ..... 94, 106, 128, 129, 131, 132, 133, 135, ... 144, 145, 173, 226, 227, 241
Matáv 189, 281
MD5 algoritmus 69, 82, 96, 141, 273, 275
Message Digest 96, 290
Microsoft Certificate Server 187, 257, 258
MIME 93, 211, 251
MMC 256, 257, 258, 261, 263, 268, 271, 275, 286
mobiltelefon 27, 30, 31, 65, 66, 76, 195, 198

N

National Security Agency 86
NetLock 17, 40, 41, 42, 59, 189, 279, 280, 281
Netscape
  böngésző 61, 83, 286
  cég 90, 209
  tanúsítványtípus 258
NTFS 49, 50, 61, 249, 269, 271, 272, 286

O

Oakley protokoll 274
objektumazonosító, OID 141, 142, 219, 258, 260
OCSP
  megoldás, protokoll 136, 137, 153, 221, 284
  szerver, válasz 136, 153, 285
OpenSSL 280
Outlook 32, 43, 44, 45, 47, 61, 252, 264, 278, 287

P

PAP protokoll 273
PCI slot 194
PCMCIA 195, 198, 277
PDA 31, 194, 195
PGP 35, 150, 154
PIN kód 76, 78, 111, 196, 198, 250, 251, 272, 277
PKCS
  #1 ..... 82, 141, 210

#10 166
#11 199
#12 ..... 251, 252, 262, 269
#15 ..... 199, 210
#7 ..... 166, 251, 252, 263, 268
szabványkészlet 93, 209, 210, 252, 277
PKI 34, 78, 79, 176, 188, 207, 252, 277, 280, 291, 296, 297
PKIX 207, 210
munkacsoport 207, 291
pontosidő-szolgáltató 171, 189
PPTP protokoll 273
protokoll .....
hálózati 126, 131, 199, 211, 273
kripto 15, 26, 27, 32, 81, 88, 89, 90, 91, 95

R

RC2 algoritmus 83, 86
RC4 algoritmus 83, 97, 273
RC6 algoritmus 83
Registry 255, 262, 278, 286, 287
replikáció 128, 162
RIPEMD algoritmus 69, 82
RSA
algoritmus 69, 79, 84, 85, 86, 96, 116, 141, 252, 280
cég 83, 97, 199, 208, 210, 251, 297

S

S/MIME 43, 46, 90, 93, 98, 147, 154, 251
SCEP 166
Schlumberger 199, 277
SCVP 153
SHA-1 algoritmus 69, 82, 96, 252, 275
S-HTTP 90, 211
SIM-kártya 196, 199, 200
single sign-on 31, 272
SMTP 137
sorozatszám 126, 138, 143, 144, 146, 263, 284
SSL protokoll 43, 61, 79, 90, 92, 93, 153, 211, 263
szabályzat 215, 276
aláírási 95, 149, 171, 218, 221, 223, 284, 285, 292, 294
hitelesítési 151, 171, 208, 218, 220, 222, 258
szolgáltatási 151, 218, 219, 222, 293
szabályzatok 16, 34, 139, 152, 157, 159, 162, 165, 187, 216, 224, 241, 283

szoftveraláírás 114, 194
szoftverhitelesítő 252, 254, 264, 267, 268

T

tanúsítási lánc ..... 117, 125, 126, 132, 141, 142, 149, 151, 171, 182, 185, ... 187, 221, 251, 260, 269, 284, 294, 295
tanúsítványbizalmi lista 251, 253, 288
tartomány 61, 252, 270, 271, 272, 275, 286, 288
TCP/IP 92, 94, 128, 211
  cím 120, 141
  csomag 93, 275
titokmegosztó protokoll 91, 189
TLS protokoll 92
trójai faló 76, 194, 198, 250
tűzfal 31, 32, 66, 114, 120, 137, 195, 249

U

UNIX 50, 79
USB
  port 198, 200, 277
  token 195, 200, 201, 281, 286
útválasztó 31, 66, 93, 114, 195

V

véletlen 87, 88, 98
Verisign 40, 58, 60, 166, 209, 253, 280
vírus 32, 35, 56, 57, 176
Visual Basic 56, 197
VPN 94, 273, 274, 280

W

webböngésző 142
weboldal 17, 32, 40, 41, 48, 78, 148, 149, 163, 210, 245, 258, 262, 267
webszerver 31, 32, 49, 66, 79, 92, 93, 94, 98, 114, 120, 142, 148, 154, 236
WebTrust 280, 286
WTLS protokoll 92

X

X.500
  címtár 127, 211
  névformátum 138, 139, 141, 144, 146, 166
  szabvány 127, 210, 211

X.509
szabvány 127, 137, 140, 143, 146, 205, 229, 251
tanúsítvány 138, 141, 154, 208, 252, 277
visszavonási lista 143, 277
XML 194

A **GIRO Elszámolásforgalmi Rt.** az elektronikus pénzügyi szolgáltatások általános elterjedésére tekintettel a pénzügyi intézmények és ügyfeleik egymással történő kapcsolattartásának

biztonságos,
hiteles,
letagadhatatlan

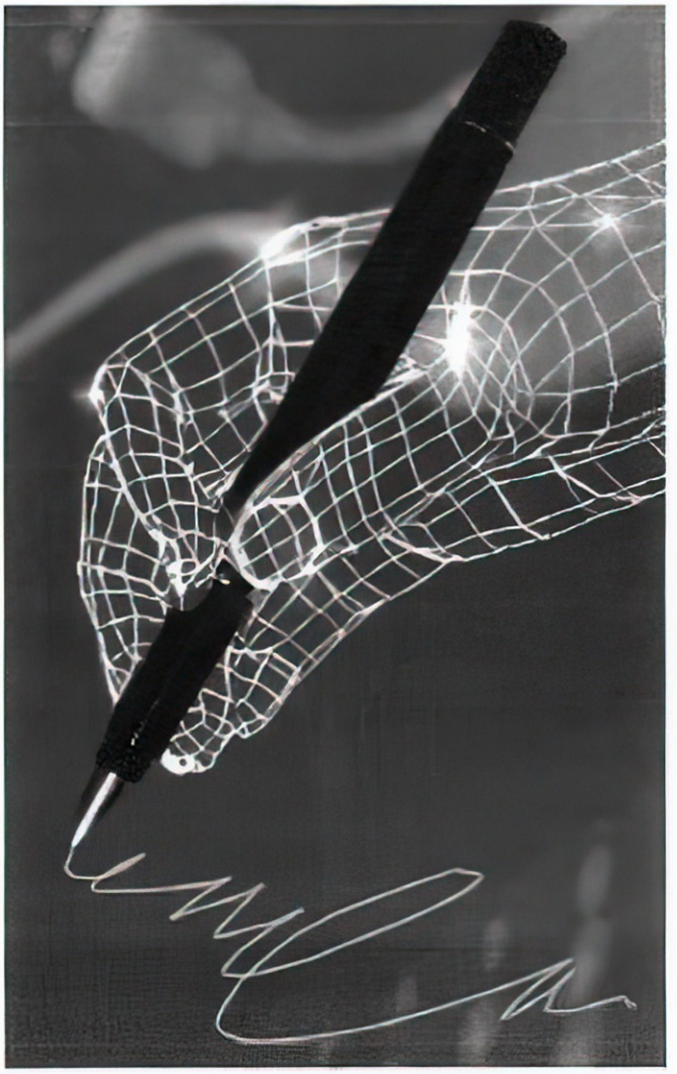
voltának biztosítása érdekében nyilvános kulcsú hitelesítési eljáráson alapuló „fokozott biztonságú" szolgáltatást nyújt.

A tanúsítványok felhasználhatóak:

- magánszemélyek,
- valamely szervezet nevében eljáró természetes személyek, vagy
- szervezet által üzemeltetett eszközök által előállított adatállományok aláírására, így többek között
  - ✔ elektronikus banki kapcsolattartás
  - ✔ elektronikus levelezés
  - ✔ irodai környezetben készített fájlok hitelesítésére.

GIRO Elszámolásforgalmi Rt.
1054 Budapest, Vadász utca 31.
Telefon: 428-5600
Fax: 269-5458

A hit@les szolgáltatás a **GIRO Rt.** és az együttműködő intézmények, mint regisztrációs szervezetek szabályozott együttműködésével valósul meg.



hit@les

honlap: www.giro.hu/hiteles
e-mail: kerdes@hiteles.giro.hu
szabályzatok:
www.giro.hu/hiteles/szabályzat
HIF regisztrációs szám:
FA 7717-1/2001