PKI: EGY EMBER, EGY TANÚSÍTVÁNY?

Dr. Berta István Zsolt, istvan.berta@microsec.hu
Endrődi Csilla, csilla@microsec.hu
Microsec Kft.

1. Bevezetés

Elméletben jól ismerjük az alábbi modellt: A nyilvános kulcsú infrastruktúra (PKI, public key infrastructure) minden szereplőjének van egy nyilvános kulcsa és egy magánkulcsa. A nyilvános kulcsát mindenki nyilvánosságra hozza, míg a magánkulcsát mindenki titokban tartja. Ha ismerjük valakinek a nyilvános kulcsát, akkor biztonságosan (például titkosan, hitelesen) kommunikálhatunk vele. A nyilvános kulcsot hiteles módon kell megszereznünk, csak így lehetünk biztosak benne, hogy az valóban annak a nyilvános kulcsa, akivel kommunikálni szeretnénk. A nyilvános kulcsú infrastruktúrában ez általában úgy történik, hogy a nyilvános kulcsot tanúsítványba foglalva szerezzük meg, a tanúsítványban egy megbízható fél – egy hitelesítés szolgáltató – aláírásával igazolja, hogy az adott nyilvános kulcs kihez tartozik.

A gyakorlatban a helyzet nem ilyen egyszerű. A PKI szereplői általában rákényszerülnek, hogy nem egy, hanem több tanúsítványuk és kulcspáruk legyen. Aki kapcsolatba kerül a PKI-vel, gyakran szembesül azzal a problémával, hogy minden célra külön-külön tanúsítványt kell vagy kellene vásárolnia, mert meglévő tanúsítványát (esetleg tanúsítványait) valami miatt nem tudja máshol felhasználni.

Ezen okok egy része **alapvető biztonsági kérdésekre** vezethető vissza, és szabványokban, esetleg jogszabályokban is megjelenik. Másik részük **szerencsétlen, hibás megoldások**, szabványok közötti **ellentmondások** miatt fordul elő. Ezek vagy ismert, elterjedt alkalmazások hibái, korlátai vagy furcsaságai miatt kötött kompromisszumokban gyökereznek, vagy amiatt jelentkeznek, hogy a különálló PKI rendszerek tervezése során nem gondolták végig kellőképpen, hogy hogyan lehet majd őket összekapcsolni.

Cikkünkben ezen okokat tekintjük át.

2. Miért nem elég egy tanúsítvány? Ha már van tanúsítványom, miért nem használhatom akárhol?

2.1 Lejárt és visszavont tanúsítványok

A tanúsítványok nem örökké érvényesek. Ennek egyik oka, hogy a PKI szereplői – akár emberek, akár számítógépek – általában nem tudják tökéletesen biztonságosan őrizni a tanúsítványukhoz tartozó magánkulcsukat. Másik oka, hogy a tanúsítványban szereplő adataik, illetve a tanúsítvány által igazolt szerepköreik gyakran megváltoznak.

Ez a cikk a következő konferencián jelent meg: Networkshop 2008, Dunaújváros, 2008. március 17-19.

Egy tanúsítvány kétféle módon válhat érvénytelenné: **lejár** vagy **visszavonják**[1]. Mindkettő azt eredményezi, hogy a tanúsítvány birtokosa nem használhatja többé régi tanúsítványát, új tanúsítványra van szüksége.

Ha megnézzük egy hitelesítés szolgáltató tanúsítványtárát, nem kell csodálkoznunk rajta, ha valakinek több tanúsítványa található benne. Szét kell választanunk a lejárt, visszavont tanúsítványokat az aktuális, érvényes tanúsítványtól (vagy tanúsítványoktól).

2.2 Aláíró, titkosító és authentikációs tanúsítványok

A PKI eszköztárát alapvetően háromféle célra használhatjuk: aláírásra, titkosításra és authentikációra.

- **Aláírás** esetén saját magánkulcsunkkal kódoljuk az aláírandó dokumentumot, az így aláírt dokumentumról kimutatható, ha az aláírást követően megváltoztatták, és később az is bizonyítható, hogy ki készítette az aláírást[2]. (Az aláíró kiléte általában nem állapítható meg közvetlenül az aláírásból – az aláírás nem erre szolgál[3] – a bizonyítás általában a tanúsítványt kibocsátó hitelesítés szolgáltató nyilvántartása esetén lehetséges.)
- **Titkosítás** esetén a címzett nyilvános kulcsával kódolunk egy dokumentumot, amelyet a címzett később a saját magánkulcsával vissza tud fejteni, de más illetéktelen személy – aki nem rendelkezik a címzett magánkulcsával – nem tudja visszanyerni a nyílt dokumentumot.
- **Authentikáció** estén saját kilétünket igazolhatjuk kommunikációs partnerünk számára; ekkor egy tőle kapott, véletlen számot is tartalmazó adatblokkot (kihívást) kódolunk magánkulcsunkkal. Partnerünk a nyilvános kulcsunk alapján győződhet meg arról, hogy a kódolást valóban mi végeztük el. Az authentikáció során egyúttal közös szimmetrikus kulcsokban is megállapodhatunk, és titkosított, illetve hitelesített csatornát (például SSL vagy VPN) építhetünk ki. Partnerünk biztos lehet benne, hogy ha e csatornán kap üzenetet, az valóban tőlünk származik, de (ha az üzenet nincs pl. aláírva) ezt harmadik fél felé már nem tudja igazolni. Hasonlóan: e csatornán titkosítva haladnak ugyan az üzenetek, de (ha azok nincsenek külön titkosítva) a csatornából kivett üzenetet már akárki elolvashatja.

A szabványok elsősorban aláírás esetén hangsúlyozzák, hogy az aláíró kulcsot csak aláírásra használjuk [RFC3280], sőt, az elektronikus aláírásról szóló törvény is kimondja, hogy „*az aláíró az aláírás létrehozó adatot kizárólag az aláírás létrehozására használhatja*”. [EAT, 13. § (4)] Az authentikációt azért célszerű minden mástól elválasztani, mert ott a magánkulcs segítségével egy kívülről érkező „véletlen” blokkot kódolunk, így előfordulhatna, hogy egy cseles támadó authentikációkor aláírat vagy dekódoltat velünk egy üzenetet. (Megjegyezzük, hogy aláíráskor, titkosításkor és authentikációkor különböző padding megoldást szokás használni, amely nyújthat bizonyos fokú védelmet az ilyen támadások ellen.) A titkosítást szintén célszerű minden mástól elválasztani, ugyanis a dekódolásra szolgáló kulcsot letétbe szokás helyezni egy megbízható szolgáltatónál. (Lásd: 2.6. fejezet.) Aláírásra és authentikációra szolgáló kulcsokat nem szabad, nincs értelme letétbe helyezni (nem jelent

[1] A felfüggesztés a visszavonáshoz hasonló fogalom, a felfüggesztett tanúsítvány a visszavonthoz hasonlóan érvénytelennek minősül. Mindössze az jelenti a különbséget, hogy a felfüggesztés ideiglenes, a felfüggesztett tanúsítvány később megint érvényessé válhat. Jelen dokumentum szempontjából ennek nincs szerepe, így itt a felfüggesztést nem tekintjük külön kategóriának.

[2] Jelen dokumentumban szabványos (például [XAdES]) formátumú aláírást értünk aláírás alatt; az ilyen aláírás a dokumentum magánkulccsal kódolt lenyomatán túl további információkat is tartalmaz, például az aláíró tanúsítványát, a hozzá kapcsolódó tanúsítványláncot stb.

[3] Álneves tanúsítvány esetén például még a tanúsítvány alanyának az igazi neve sem derül ki a tanúsítványból. Lásd: 2.7. fejezet.

nagy kárt, ha az aláíró vagy authentikáló magánkulcs megsemmisül, viszont letétbe helyezésük súlyos visszaélésre adhatna lehetőséget).

Kimondhatjuk, **aláírásra, titkosításra és authentikációra külön-külön kulcspárt kell használni**, így e célra mindenkinek három külön kulcspárra és három külön tanúsítványra van szüksége.

2.3 A tanúsítvány használatának célja

Egy tanúsítványban feltüntethető, hogy milyen célra használható. Így kerülhető el például az, hogy valaki egy aláíró tanúsítványban lévő nyilvános kulccsal titkosítson egy üzenetet. A kulcshasználat célját a tanúsítvány KeyUsage mezejében lévő bitekkel szokás jelölni, és a tanúsítvány ExtendedKeyUsage mezejével lehet tovább szűkíteni.
A KeyUsage bitek nagyon sok kombinációt megengednek, és e téren gyakran ellentmondanak egymásnak az európai és az amerikai szabványok is. (Például, az amerikai szabványok szerint a DigitalSignature (DS) bit jelenti az aláírást, míg az európai szabványok a NonRepudiation (NR) bitet használják erre a célra. A hazai szabályozás szerint minősített tanúsítványban kizárólag NR bit szerepelhet, míg sok amerikai szoftver nem enged aláírni, ha a tanúsítványban nincs DS kulcshasználati bit.)
Előfordulhat, hogy egyes alkalmazások elvárják, hogy bizonyos kulcshasználati bitek szerepeljenek a tanúsítványban, illetve elvárják, hogy bizonyos bitek ne szerepeljenek (mert akkor a tanúsítvány biztosan más célra való). A különféle szabályozások, szabványok és alkalmazások miatt nem könnyű feladat, hogy egy tanúsítvány mindenhol használható legyen. (Például, ha a Windowsban chipkártyás beléptetéshez szeretnénk használni egy tanúsítványt, olyan egzotikus KeyUsage értéket kell beállítanunk, amely arra utal, hogy a tanúsítványt egyszerre használnánk authentikációra és titkosításra.) További nehézség, hogy a tanúsítványt kommunikáció védelmére szeretnénk használni, így nemcsak saját szoftverünk igényinek kell megfelelnünk, hanem kommunikációs partnerünk (vagy partnereink) szoftverének (szoftvereinek) is.
Bizonyos célokra a KeyUsage biteken túl ExtendedKeyUsage értékekre is szükség van a tanúsítványban. Például, ha azt szeretnénk, hogy az általunk fejlesztett alkalmazást ügyfeleink szoftverei megbízható helyről származó alkalmazásnak tekintsék, aláírásához CodeSigning ExtendedKeyUsage értéket tartalmazó tanúsítványt kell használni. Hasonló módon kell megjelölni a webszerverek tanúsítványait, az SSL kliensek tanúsítványait, a VPN tanúsítványokat stb.
Előfordulhat, hogy az egyes alkalmazások igényei miatt, illetve a speciális felhasználási célokra külön-külön tanúsítványokkal kell rendelkeznünk.

2.4 A tanúsítvány biztonsági szintje

A végfelhasználói tanúsítványok között az ún. **minősített tanúsítványok** képviselik a legmagasabb biztonsági szintet, ezek kibocsátását, kezelését az elektronikus aláírásról szóló törvény szabályozza. A minősített tanúsítvány alapján (biztonságos aláírás-létrehozó eszköz segítségével) minősített elektronikus aláírás hozható létre. A minősített tanúsítvány kizárólag aláírásra szolgálhat, „minősített titkosító” tanúsítvány nem létezik. Minősített tanúsítványt csak minősített hitelesítés szolgáltató bocsáthat ki, kizárólag személyes azonosítás alapján. A szolgáltatónak felelősséget kell vállalnia a tanúsítvánnyal okozott károkért, meghatározott pénzügyi követelményekkel, felelősségbiztosítással kell rendelkeznie stb. [EAT]
A minősített elektronikus aláíráshoz nemcsak szigorú szabályok és biztonsági mechanizmusok kapcsolódnak, hanem erős jogi vélelmek is, így **sok eljárásban kizárólag minősített elektronikus aláírással hitelesített dokumentum használható**.

A minősített tanúsítványokon belül is léteznek különböző fokozatok. A hitelesítés szolgáltató a tanúsítvány kibocsátásakor meghatározhatja, hogy az adott tanúsítvánnyal legfeljebb mekkora kötelezettség vállalható, ez az ún. **tranzakciós limit**. Így előfordulhat, hogy egy nagy értékű ügyletben valaki nem fogad el egy tanúsítványt, mert az adott tanúsítvány ekkora értékű ügyletben már nem használható, és baj esetén a tanúsítványt kibocsátó hitelesítés szolgáltató nem térítené meg a kárát. Még nem gyakori, hogy bizonyos célokra csak meghatározott tranzakciós limitű tanúsítványok lennének használhatóak, de a technológia terjedésével a tranzakciós limit várhatóan nagyobb jelentőséget kap majd.
A minősített tanúsítványok mellett léteznek **nem minősített tanúsítványok** is. Nem minősített tanúsítvány alapján legfeljebb fokozott biztonságú elektronikus aláírás hozható létre. A nem minősített tanúsítványokra (és a fokozott biztonságú aláírásokra) nagyon kevés szabály vonatkozik, ezért **különféle biztonsági szintek** fordulnak elő, és gyakran nagyon nehéz közöttük különbséget tenni[4]. Léteznek olyan nem minősített tanúsítványok, amelyeket már-már a minősített tanúsítványokéihoz hasonló szabályok szerint bocsátanak ki, más nem minősített tanúsítványok távolról, személyes találkozás nélkül is kibocsáthatóak.
Mivel a minősített aláírásokra nagyon merev szabályok vonatkoznak, sok esetben nem minősített tanúsítványt és fokozott biztonságú aláírást szokás használni. Ilyen például az elektronikus számlázás esete, amikor nagy mennyiségű aláírást kell gyorsan elkészíteni.
Mind a minősített, mind a nem minősített biztonsági szint értelemmel bír, és ezeken belül is különféle fokozatok képzelhetőek el. **Előfordulhat, hogy valakinek különböző biztonsági szintű tanúsítványai is vannak**; a magasabb biztonsági szint a nagyobb bizonyító erő, az alacsonyabb a rugalmas felhasználás miatt. A tanúsítványok kibocsátására és felhasználására vonatkozó szabályokat, így a tanúsítvány biztonsági szintjét az a **hitelesítési rend** határozza meg, amelynek megfelelően a tanúsítványt kibocsátották. Minden tanúsítványban szerepel azon hitelesítési rend azonosítója, amelynek a tanúsítvány megfelel. Tanúsítvány biztonsági szintjére talán a hitelesítési rend alapján a legcélszerűbb hivatkozni.

2.5 Magánkulcs tárolása

Ha egy tanúsítványt minősített aláírás létrehozásához szeretnénk használni, a hozzá tartozó magánkulcsnak mindenképpen **biztonságos aláírás-létrehozó eszközön** (pl. **chipkártyán**) kell lennie. A kulcs csak a chipkártyán létezik (gyakori, hogy a kártyán is keletkezett), soha nem hagyja el a kártyát, nem is lehet kinyerni a kártyából (azaz, nem lehet a kártyát „lemásolni"). Így a kártyabirtokos biztos lehet benne, hogy **amíg a kártya nála van, addig illetéktelen személy nem élhet vissza a kulcsával**.
Ha a magánkulcs nem (vagy nem csak) chipkártyán van, akkor „szoftveres kulcsról" beszélünk. **A szoftveres kulcs egy fájl egy számítógépen, így le lehet másolni**. Ezért sokkal nehezebb kézben tartani, hogy a szoftveres kulcsból hány másolat készül.
Ugyanakkor, a szoftveres kulcsoknak számos előnye is van. A kulcs birtokosa egyszerre több helyen, több gépen is használhatja, vagy biztonsági másolatot készíthet belőle. Általában minden alkalmazás támogatja a szoftveres kulcsokat, és a szoftveres kulcsok használatához nincs szükség az adott típusú chipkártya meghajtó programjára. (Előfordulhat, hogy egy adott típusú chipkártyát nem támogat egy alkalmazás, vagy a kártyához nincs olyan típusú meghajtóprogram, amelyet az adott alkalmazás támogatna stb.)

[4] Jogi szempontból egy minősített aláírás a fokozott biztonságú aláírásnál egyértelműen erősebb bizonyítékot jelent, de műszaki szempontból a helyzet nem ennyire egyszerű. Például, minősített aláírása csak természetes személynek lehet, így a minősített hitelesítés szolgáltató minősített tanúsítványon elhelyezett aláírása is fokozott biztonságúnak minősül. Ez jó példa arra, hogy egy fokozott biztonságú aláírás időnként sokkal szigorúbb biztonsági követelményeket is teljesít, és így akár erősebb biztonságot jelent, mint egy minősített aláírás.

Így könnyen előfordulhat, hogy valakinek azonos célú, azonos adatokat tartalmazó érvényes tanúsítványai vannak, csak az egyik szoftveres, a másiknak a magánkulcsa pedig valamilyen intelligens kártyán van.

2.6 Hol van letétben a magánkulcs?

Titkosító tanúsítványok esetén a magánkulcsot letétbe szokás helyezni például arra az esetre, ha a dekódoló kulcsot tartalmazó kártyánk megsemmisülne, így a letétbe helyezett kulccsal a korábban kódolt adatok visszafejthetőek. Másik gyakori alkalmazás, hogy a titkosító tanúsítványát valaki egy szervezet munkatársaként használja, és a szervezet ragaszkodik ahhoz, hogy ő is hozzáférhessen a letétbe helyezett magánkulcshoz, így a dolgozó elbocsátása esetén annak közreműködése nélkül is hozzáférhet a hivatalos levelezéséhez. A szervezet ahhoz is szokott ragaszkodni, hogy más szervezet ne férjen hozzá a magánkulcshoz.
Ha valaki több szervezet nevében is folytat titkosított kommunikációt, előfordulhat, hogy az **egyes szervezetekhez külön-külön titkosító tanúsítványra** (és magánkulcsra) **van szükség**.

2.7 Tanúsítványban feltüntetett személyes adatok, szerepkörök

Minden tanúsítványban szerepel a tanúsítvány alanyának neve, amely az elektronikus aláírásról szóló törvény szerint **álnév** is lehet[5]. [EAT 9. § (4)] Ha aláíráskor az aláíró álneves tanúsítványt használt, az aláírásból még a valódi nevét sem lehet megállapítani, de később – a hitelesítés szolgáltató nyilvántartása alapján – mégis be lehet bizonyítani, hogy az aláírást ő készítette. Annak ellenére, hogy az álneves tanúsítványok alapján ellenőrizhető aláírások jogilag egyenértékűek a valódi nevet tartalmazó tanúsítványok alapján ellenőrizhető aláírással, álneves tanúsítványt a gyakorlatban szinte nem használnak. [B2006elf] Bizonyos felhasználási területeken (például a magyar közigazgatásban) egyáltalán nem fogadnak el álneves tanúsítványt.

Gyakori, hogy valakinek nem a nevéről, hanem a szerepköréről kell meggyőződnünk. Abban szeretnénk biztosak lenni, hogy valóban ott dolgozik-e, valóban van-e olyan jogosultsága, képzettsége, valóban az-e a hivatása stb. Ha egy tanúsítványban a tanúsítvány alanyának a nevén túl más információk is szerepelnek, a tanúsítvány ezen információkat is igazolhatja. Ez akkor jelent előnyt, ha a tanúsítványt vagy aláírást befogadó fél ezen információkat felismeri, és elfogadja. Igazolhatja például egy tanúsítvány, hogy az alanya közjegyző, vagy például egy adott cég nevében cégjegyzésre jogosult stb.
E megoldás korlátokkal is rendelkezik:

- Nem biztos, hogy a befogadó (vagy az általa használt automatizmus) megérti a tanúsítványban szereplő információkat. Ezen információk feltüntetésének módja szabványos ugyan [RFC3280], de a nemzetközi szabványban meghatározott mezőkben közel nem egyértelmű, hogy hogyan kell feltüntetni a speciális magyar adatokat (pl: TAJ szám). Emellett, a szabványban szereplő hierarchikus struktúra nem mindig alkalmazható a gyakorlati helyzetre. A különféle alkalmazások elvárásai itt is komoly problémát jelentenek. Például, sok levelezőprogram nem fogad el olyan tanúsítványt, amelyben nem szerepel az alany e-mail címe. Ugyanakkor, sokan nem szívesen tüntetnék fel e-mail címüket minden egyes aláírásukban.
- A tanúsítványt vagy aláírást befogadó fél nem mindig fogadja el a tanúsítványban szereplő adatokat, esetleg ezen adatokról nem a hitelesítés szolgáltató igazolása alapján szeretne meggyőződni.
- Akinek több szerepköre van, annak nem szerencsés, ha minden szerepköre ugyanabban a tanúsítványban jelenik meg. Egyrészt, így akivel csak kapcsolatba kerül, az minden

[5] A tanúsítványból ekkor egyértelműen ki kell, hogy derüljön, ha álneves.

szerepkörét megismeri, másrészt, bármelyik szerepköre megváltozik, vissza kell vonni a tanúsítványát, és az új tanúsítványt esetleg csak az első kibocsátáshoz hasonló eljárás során kaphatja meg.

- Annak eldöntése is problémát jelent, hogy valaki éppen melyik szerepkörében használja a tanúsítványt, és használhatja-e a szerepköréhez tartozó (pl. közjegyzői) tanúsítványát magánszemélyként.

Előfordulhat, hogy azért van szükségünk több tanúsítványra, mert az egyes tanúsítványokban **különböző adatoknak kell szerepelnie**. Vagy mi nem szeretnénk, hogy minden adatunk ott legyen a tanúsítványunkban, vagy a különböző helyeken (például a szakmai kamarában, az egészségügyben vagy a közigazgatásnál) támasztanak egymásnak ellentmondó követelményeket a felhasználható tanúsítványok adattartalmával kapcsolatban.
Nem tartjuk szerencsésnek, hogy a tanúsítványban az alany nevén[6] kívül más információ is szerepeljen. Úgy gondoljuk, ezen információkat más módon, máshol kell nyilvántartani, és e nyilvántartásokat nem a PKI szolgáltatóknak kellene vezetnie, mert ez túlbonyolítja a PKI-t, és szigetmegoldásokat hoz létre. Ugyanakkor, sok PKI megoldás mégis ezt az utat választja, mert más módon nem tud könnyen építeni a tanúsítványok nyújtotta infrastruktúrára.

2.8 Melyik gyökértanúsítványt használjuk?

A tanúsítványt elfogadó félnek meg kell győződnie a tanúsítvány érvényességéről. Ehhez – többek között – vissza kell vezetnie a tanúsítványt egy általa elfogadott gyökértanúsítványra. Mely gyökértanúsítványokat fogadhatja el?

2.8.1 Jogilag elfogadott gyökerek

Dönthet úgy, hogy az [EAT] szerint elfogadott gyökereket fogadja el. Ilyenkor leggyakrabban a magyar hitelesítés szolgáltatók gyökereire gondolunk, de sok külföldi gyökér is ide tartozik. Mivel azonban nem létezik hiteles nyilvántartás ezen gyökerekről, ezek körét elég nehéz meghatározni.

2.8.2 Az alkalmazások által elfogadott gyökerek

Dönthet úgy, hogy az alkalmazása (vagy operációs rendszere) által támogatott gyökereket fogadja el. A legtöbb alkalmazásnak van tanúsítványtára, amelyben alapértelmezetten szerepelnek bizonyos gyökerek. Az alkalmazásfejlesztők általában valamilyen saját követelményrendszer szerint veszik fel ide a hitelesítés szolgáltatókat. A nemzetközi alkalmazások által elfogadott gyökértanúsítványok köre általában nem esik egybe Magyarországon jogilag is elfogadott gyökerek körével. Így előfordulhat, hogy a magyar hitelesítés szolgáltató tanúsítványa alapján létrehozott aláírást a külföldi partner nem fogadja el, mert nem ismeri a magyar gyökeret; vagy egy külföldi aláírást az alkalmazás elfogad, pedig a magyar jogszabályok szerint nem szabadna elfogadnia.

2.8.3 PKI közösség saját gyökere

Sok PKI közösségnek saját gyökere van, és csak az ide visszavezethető tanúsítványokat fogadja el. Ekkor a közösség minden számítógépén kizárólagosan ezt az egy gyökeret kell beállítani, így a közösség elfogadja az ez által felülhitelesített szolgáltatókat, illetve elutasítja, ha a gyökér visszavonja ezek tanúsítványait. Korlátja ennek a megoldásnak, hogy nehéz tovább szűrni ezen szolgáltatók tanúsítványai között, illetve a megoldás költséges, mert kell hozzá egy saját hitelesítés szolgáltató, amelyet biztonságosan kell üzemeltetni. Az is végiggondolandó, hogy a saját gyökér üzemeltetése növeli-e vagy éppen csökkenti a rendszer biztonságát.

[6] és természetesen valamely, a hitelesítés szolgáltató nyilvántartásában egyedi azonosítón

Egyazon kulcspárhoz több hitelesítés szolgáltató is bocsáthat ki tanúsítványt, ilyen esetben egy tanúsítvány több gyökérre is visszavezethető. Ha elzárkózunk ezen megoldástól, a kapott rendszer szigetmegoldássá válhat: Tegyük fel, hogy az „A" közösség csak a saját gyökere alá tartozó tanúsítványokat fogadja el, és „A" gyökere alá tartozó tanúsítvány nem tartozhat más gyökér alá. Ha a „B" közösség is ehhez hasonló követelményeket támaszt (csak „B" gyökere alá tartozó tanúsítványokat fogad el, és „B" gyökere alá tartozó tanúsítvány nem tartozhat más gyökér alá), akkor nem létezhet olyan tanúsítvány, amely „A" és „B" közösségben is használható; a két közösséghez külön-külön tanúsítványokat kell használni.
A magyar közigazgatás elkövette ezt a hibát: a közigazgatásban a [Ket] szerint a Közigazgatási Gyökér Hitelesítés Szolgáltató tanúsítványára visszavezethető tanúsítványokat szabad csak elfogadni, és a KGYHSZ nem engedi, hogy egy alá tartozó tanúsítvány más gyökér alá is tartozzon. A KGYHSZ gyökerét nem ismerik a nemzetközi alkalmazások, és a KGYHSZ által kibocsátott visszavonási információk (lásd: 2.9. fejezet) kevésbé rugalmasan érhetőek el, mint a kereskedelmi hitelesítés szolgáltatók esetén, így a közigazgatási tanúsítványok elszigetelődtek.
A saját gyökér egy másik buktatót is rejt. Így könnyen beleesünk abba a csapdába, hogy összemossuk a tanúsítvány érvényességét (azt, hogy a magánkulcs a tanúsítvány alanyának birtokában van) a közösséghez való tartozással (vagy más jogosultságokkal), és nehéz lesz más közösségből származó tanúsítványt befogadni a rendszerünkbe.

2.9 Visszavonási információk elérhetősége

Vannak tanúsítványok, amelyek visszavonási állapota könnyebben, gyorsabban ellenőrizhető, és bizonyos esetekben ilyen tanúsítványokat lehet jól használni. Aláírás ellenőrzésekor arról kell meggyőződnünk, hogy az aláíró tanúsítványa, illetve az aláíró tanúsítványához tartozó tanúsítványlánc minden egyes elme (kivéve a gyökértanúsítványt), érvényes volt-e az aláírás pillanatában[7]. Ehhez olyan visszavonási információkra – visszavonási listákra (CRL), online tanúsítvány-állapot válaszokra (OCSP) – van szükség, amelyeket az aláírás pillanatát követően bocsátottak ki. Egyes hitelesítés szolgáltatók esetén ezen információkat esetleg csak hosszú idő után lehet beszerezni. Például, sok gyökér csak havonta, vagy még annál is ritkábban bocsát ki visszavonási listát, így esetleg csak hónapok múlva lesz a birtokunkban olyan visszavonási információ, amely igazolná az aláírás érvényességét. [M2005OCSP]
Itt két külön problémával álluk szemben: egyrészt, meg kell győződnünk róla, hogy a szolgáltató nem vonta vissza a tanúsítványt, és ez alapján döntést kell hoznunk. Másrészt, igazolnunk kell, hogy a döntést milyen információk alapján hoztuk. Van olyan szolgáltató, amely esetén a döntést viszonylag gyorsan meghozhatjuk (látjuk, hogy nem jelent meg új visszavonási lista), de nem tudjuk ezt bizonyítani (a nem létező visszavonási listát nem tudjuk felmutatni).
Könnyen előfordulhat, hogy az aláírásunk jogilag érvényes ugyan, de az aláírást befogadó fél nem tudja, vagy csak nagyon hosszú idő után tudja ellenőrizni (és igazolni) az érvényességét. Így bizonyos célokra (például, ha archiválás szolgáltatónál akarjuk archiválni az aláírást, akkor a szolgáltatót jogszabály kötelezi arra, hogy 3 napon belül minden bizonyítékot összegyűjtsön az aláírás érvényességéről) olyan tanúsítványt kell választani, amelyhez rugalmasan érhetőek el visszavonási információk.

3. Összefoglalás

Látható, hogy könnyen előállhat olyan helyzet, amikor egy új környezetben, új alkalmazásban már nem tudjuk használni a meglévő tanúsítványunkat, hanem új tanúsítványra van szükség.

[7] Az aláírás pontos időpontját nem mindig ismerjük, az ellenőrzéseket az aláíráson elhelyezett időbélyegen szereplő időpontra vonatkozóan szokás elvégezni.

E jelenség bizonyos okai a PKI alapvető elveiből következnek; ilyenek például a lejáró és visszavont tanúsítványok, az aláíró, titkosító és authentikációs tanúsítványok, és a tanúsítványokhoz tartozó biztonsági szintek. Más okok viszont tervezési hibák vagy a PKI technológia gyermekbetegségeinek tekinthetők, ezek egy része megfelelő tervezéssel, szabályozással orvosolható.
Úgy látjuk, hogy a PKI gyakorlati elterjedése szempontjából létfontosságú, hogy egy tanúsítvány sok helyen, sok PKI közösségben használható. Így nem kell minden közösséghez külön-külön tanúsítványt vásárolnunk, így a PKI összességében olcsóbbá válhat.

Mire ügyeljünk PKI-re épülő rendszerek tervezésénél?

- Tudomásul kell vennünk, hogy a tanúsítványok nem érvényesek örökké, így számolnunk kell azzal a jelenséggel, hogy a PKI szereplőinek a tanúsítványai időben változnak.
- El kell különíteni egymástól az aláíró, titkosító és authentikációs tanúsítványokat, és az ezeket felhasználó funkciókat. Figyelembe kell vennünk, hogy az aláíró, titkosító és authentikációs tanúsítványok gyökeresen eltérő kulcsmenedzsmentet igényelnek.
- Hangsúlyt kell fektetnünk a szabványos tanúsítványok használatára, hogy a nálunk használható tanúsítványt más rendszer is befogadhassa.
- Meg kell határoznunk, hogy a rendszer milyen biztonsági szintű tanúsítványokat fogad be, és hogyan győződik meg a tanúsítványok biztonsági szintéjről.
- Végig kell gondolnunk, hogy rendszerünk később hogyan fog kapcsolatba kerülni más PKI-re épülő rendszerekkel. Hogyan fogjuk elfogadni a máshonnan származó tanúsítványokat, és hogyan állapítjuk meg a hozzájuk tartozó felhasználók jogosultságait.
- A tanúsítvány érvényessége mindössze annyit kellene, hogy jelentsen, hogy a kulcs az adott személy birtokában van, és ne mossuk ezt össze a felhasználók jogosultságaival.
- Kerülnünk kell, hogy a tanúsítványban az alanyok nevén kívül bármilyen más adat is szerepeljen.

4. Hivatkozások

[B2006elf] Berta István Zsolt – Mi alapján fogadhatunk el egy elektronikus aláírást? Híradástechnika, 2006, vol. LXI, 2006, in Hungarian, 2006. http://www.e-szigno.hu/anyagok/Berta2006eaelf.pdf

[Eat] 2001. évi XXXV. törvény az elektronikus aláírásról

[Ket] 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól

[M2005OCSP] Berta I. Zs. – A CRL és az OCSP technológiák összehasonlítása, Microsec White Paper, http://www.e-szigno.hu/wp_crl_vs_ocsp.html

[RFC3280] RFC 3280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[XAdES] ETSI TS 101 903 – XML Advanced Electronic Signatures (XAdES)