MICROSEC
Számítástechnikai Fejlesztő Kft.

# PKI: egy ember, egy tanúsítvány?

Dr. Berta István Zsolt <istvan.berta@microsec.hu>
Endrődi Csilla Éva <csilla@microsec.hu>

Microsec Kft.

# PKI dióhéjban (1)

- Minden résztvevőnek van két kulcsa:
  - **magánkulcs** (csak ő ismeri)
  - **nyilvános kulcs** (bárki megismerheti)
- Ha magánkulcsunkkal kódolunk valamit, a nyilvános kulcsunkkal bárki ellenőrizheti, hogy a kódolást mi végeztük el. Ezt nevezzük **aláírás**nak, hitelesítésnek.
- Ha egy nyilvános kulccsal kódolunk valamit, azt kizárólag a hozzá tartozó magánkulccsal lehet visszafejteni. Ezt nevezzük **titkosítás**nak.

- Csak akkor támaszkodhatunk egy nyilvános kulcsra, ha tudjuk, hogy ki birtokolja a hozzá tartozó magánkulcsot.

# PKI dióhéjban (2)

- A **hitelesítés szolgáltató**k olyan szereplők, akik aláírt igazolásokat állítanak ki arról, hogy egy adott nyilvános kulcs (és a hozzá tartozó magánkulcs) kihez tartozik. Ezen aláírt igazolásokat nevezzük **tanúsítvány**nak.
- A tanúsítványokat általában más tanúsítványok alapján ellenőrizhetjük, az ellenőrzést **gyökér** hitelesítés szolgáltatók nyilvános kulcsára vezethetjük vissza; e kulcsokat sokan ismerik és elfogadják.
- Az **időbélyegzés szolgáltató**k olyan aláírt igazolásokat bocsátanak ki arról, hogy egy adott dokumentum egy adott időpontban létezett.
- Jogszabály **bizonyító erő**t rendel
  - a minősített és a fokozott biztonságú aláírásokhoz és
  - a minősített időbélyegekhez.

# A gyakorlatban ez nem ilyen egyszerű

- Nagyon sokféle tanúsítvány van.
- Egy szereplőnek is gyakran több tanúsítványa van.
- Nehéz különbséget tenni közöttük.
- Hogyan találjuk meg valakinek „a” tanúsítványát?
- Gyakori, hogy hiába van már egy tanúsítványunk, amit valahol használunk, máshol valami miatt már nem használhatjuk ugyanazt; hanem új tanúsítványra van szükségünk.

- ... miért?

# Miért nem elég egy tanúsítvány?

- Érdemi okok, fontos biztonsági szempontok
- Egyéb okok
  - szerencsétlen vagy hibás megoldások,
  - szabványok, specifikációk közötti ellentmondások,
  - elterjedt alkalmazások korlátai, „furcsaságai” miatt kötött kompromisszumok,
  - különálló PKI rendszerek tervezése során nem gondolták végig ezek későbbi összekapcsolását
  - ...

# Lejáró/visszavont tanúsítványok

- A tanúsítványok nem örökké érvényesek
  - A PKI szereplői nem tudják tökéletesen őrizni magánkulcsukat
  - A tanúsítványban szereplő adataik megváltozhatnak
- A tanúsítvány lejárta előre tervezhető, a visszavonása nem.

- Természetes, ha valakinek az érvényes tanúsítványa(i) mellett lejárt/visszavont tanúsítványai is vannak.

# Aláírás, titkosítás, authentikáció (1)

- Aláírás:
  - saját magánkulcsunkkal kódolunk,
  - észlelhető, ha az aláírt dokumentumot az aláírást követően megváltoztatták, és később az aláíró kiléte is bizonyítható
- Titkosítás:
  - a címzett nyilvános kulcsával kódolunk, a címzett (és csak ő) a saját magánkulcsával visszafejtheti az így kódolt dokumentumot.
- Authentikáció:
  - saját kilétünket igazoljuk
  - véletlen „kihívást” kódolunk a magánkulcsunkkal
  - szimmetrikus kulcsokban állapodunk meg, és egy biztonságos csatornát hozhatunk létre

# Aláírás, titkosítás, authentikáció (2)

- Miért kell hozzájuk különböző kulcspár?
  - Authentikációkor véletlen kihívást kódolunk a magánkulccsunkkal, és az eredményét elküldjük a partnerünknek. Egy támadó így akár aláírathat vagy dekódoltathat velünk valamit.
  - A titkosításhoz feloldásához használt kulcsot letétbe szokás helyezni. Aláíró és authentikációs kulcsot tilos és értelmetlen letétbe helyezni.
  - Törvény tiltja, hogy az aláírókulcsot aláíráson kívül bármi másra használjuk [Eat, 13. § (4)]
- Aláírásra, titkosításra és authentikációra külön-külön kulcspárt kell használni.

# Tanúsítvány használatának célja

- A tanúsítványban az ún. Key Usage bitek jelzik, hogy a tanúsítvány (és a magánkulcs) mire való.
  - eltérő európai és amerikai szabványok
  - egzotikus bitkombinációk
- A tanúsítvány használatának célja az Extended Key Usage mezővel szűkíthető
  - kód aláíró tanúsítványok,
  - webszerver tanúsítványok,
  - SSL, VPN tanúsítványok
- Egyes alkalmazások néha megkövetelnek, néha tiltanak bizonyos kombinációkat.

# A tanúsítvány biztonsági szintje

- Minősített tanúsítványok (csak aláírás)
  - erős bizonyító erő
  - szigorú szabályozás, sok megkötés, néhol nagyon körülményesen használható
- Nem minősített tanúsítványok („fokozott”)
  - alig van szabályozás, nehéz eldönteni, hogy mennyire biztonságos
  - sokkal rugalmasabban használható
- Előfordulhat, hogy valakinek különféle biztonsági szintű tanúsítványokra van szüksége.

# Magánkulcs tárolása

- Ha a magánkulcs chipkártyán van, amíg nálam a kártya, addig más nem élhet vissza a kulcsommal.
  - Ez szigorú korlátokat jelent.
- A „szoftveres” kulcs egy fájl, le lehet másolni.
  Sokkal rugalmasabban használható:
  - biztonsági másolatot készíthetek a kulcsról
  - több gépen egyszerre is használhatom
  - olyan alkalmazást is tudok használni, amely nem támogatja az én kártyámat

- Gyakran mindkettőre szükség van...

# Hol van letétben a magánkulcs?

- A titkosító tanúsítványokhoz tartozó magánkulcsot letétbe szokás helyezni, hogy ha a kulcs megsemmisül, ne vesszen el a kulccsal titkosított összes adat.
- Szervezeti titkosító tanúsítványok esetén általában a szervezet is hozzáférhet a dolgozói magánkulcsához.
- A szervezet ekkor ragaszkodhat hozzá, hogy más szervezet ne férjen hozzá ehhez a magánkulcshoz.
- Ha valaki több szervezet nevében is használ titkosító tanúsítványt, lehet, hogy különböző tanúsítványokra van szüksége.

# Személyes adatok a tanúsítványban

- A tanúsítványban szerepel a tanúsítvány alanyának a neve, de ez álnév is lehet.
  - Az álneves aláírás elvileg egyenértékű a nem álnevessel
  - Sok helyen (pl. a közigazgatásban) mégsem fogadnak el álneves tanúsítványt
- Ha más adat szerepel a tanúsítványban...
  - a befogadó fél hogyan találja meg ezen információkat?
  - a befogadó fél elfogadja a hitelesítés szolgáltató állítását?

# Szerepkör a tanúsítványban

- Gyakran nem valakinek a nevéről, hanem szerepköréről, jogosultságáról, tulajdonságáról kell meggyőződnünk
- Hogy állapítható ez meg?
- Biztos, hogy jó, ha a szerepkör a tanúsítványból derül ki?
  - minden szerepkörhöz külön tanúsítvány szükséges?
  - különben honnan tudom, hogy mikor melyik szerepkörömben használom a tanúsítványomat?
  - különben bármelyik szerepköröm megváltozik, vissza kell vonni a tanúsítványt?
  - különben minden aláírásomból kiderül, hogy pontosan milyen szerepköreim, jogosultságaim vannak?
- A tanúsítvány a kulcspár és az entitás összetartozását igazolja, másra lehetőleg ne használjuk.

# Melyik gyökeret használjuk?

- A tanúsítványt elfogadó fél valamely gyökér alapján ellenőrzi a tanúsítvány érvényességét. Melyik gyökeret, gyökereket használja?
  - A jogilag elfogadott [Eat] szerinti gyökereket? Mely hazai és mely külföldi gyökerek tartoznak ide?
  - Az ellenőrző alkalmazás által elfogadott gyökereket? Biztos, hogy ez jó megoldás???
  - A PKI közösség saját gyökerét?
    Ha rosszul csinálják (egy tanúsítvány csak egy gyökérhez tartozhat), az elszigetelődéshez vezet...

# Visszavonási információk elérhetősége

- A tanúsítványt elfogadó félnek ellenőriznie kell a tanúsítvány visszavonási állapotát.
- A különféle tanúsítványok esetén különböző módon, és különböző rugalmassággal érhetőek el a visszavonási információk.
- Példa: archiválás szolgáltatás
  - a jogszabály szerint 3 napon belül össze kell gyűjteni minden visszavonási információt
  - sok hitelesítés szolgáltató esetén akár hónapok is eltelhetnek, amíg a szükséges visszavonási listák megjelennek...

# Miért nem elég egy tanúsítvány?

- A PKI alapvető elveiből következik pl.:
  - lejáró/visszavont tanúsítványok
  - aláírás, titkosítás, authentikáció
  - biztonsági szintek

- Sok más ok hibáknak, illetve a PKI gyermekbetegségeinek a következménye

# Összefoglalás

- Vegyük figyelembe, hogy a szereplők tanúsítványai változnak, a tanúsítványok nem örökké érvényesek
- Különítsük el az aláíró, titkosító és authentikációs tanúsítványokat, funkciókat
- Hangsúlyt kell fektetnünk a szabványos tanúsítványok használatára (és megkövetelésére)
- Meg kell határoznunk, hogy milyen biztonsági szintű tanúsítványokat fogad el a rendszer
- Végig kell gondolnunk, hogy hogyan kerülünk majd kapcsolatba más PKI-re épülő rendszerekkel
- Ne mossuk össze a tanúsítványt a szereplő jogosultságaival
- Kerüljük, hogy a tanúsítványban az alany nevén kívül bármilyen más információ szerepeljen

MICROSEC
Számítástechnikai Fejlesztő Kft.

# PKI: egy ember, egy tanúsítvány?

Dr. Berta István Zsolt <istvan.berta@microsec.hu>
Endrődi Csilla Éva <csilla@microsec.hu>

Microsec Kft.