NOREG

IT biztonság

Hozzáférés-ellenőrzés és digitális aláírás I.

2020/2021 tanév

NOREG

Agenda

- Kriptográfiai alapok
- Elektronikus aláírás és aláírás ellenőrzés
- Tanúsítvány tartalma, főbb mezők, egy konkrét tanúsítvány elemzése
- Nyilvános kulcsú infrastruktúra alapjai, fő komponensek
- Regisztrációs módszerek
- Tanúsítvány visszavonás
- Időbélyegzés
- Kulcs archiválás, kulcsmenedzsment
- Néhány gyakorlati példa, alkalmazás

NOREG

Kriptográfiai alapfogalmak

NOREG

Kriptográfia története

- Görög eredetű - rejtett szó
- Caesar titkosító
- Enigma (rejtély, rejtvény) rejtjelző berendezés
- Manapság a mindennapi élet része

NOREG

„Kódolás”

- Nyílt információ + algoritmus + kulcs = Kódolt információ
- Kódolt információ + algoritmus + kulcs = Nyílt információ

NOREG

Kriptográfiai algoritmusok

- Szimmetrikus algoritmusok (RC4, DES, 3DES, Blowfish, Twofish, AES, …)
- Aszimmetrikus algoritmusok (RSA, ECC - elliptikus görbék, …)
- Hash eljárások (MD5, SHA-1, SHA-2)

NOREG

RSA algoritmus

- Ronald Rivest, Adi Shamir és Len Adleman fejlesztett ki
- IFP, azaz integer factorization problem - nem ismert hatékony algoritmus egy nagy egész szám prímtényezőinek meghatározására,
- azaz egy támadó *m* birtokában nem tudja kiszámítani *p* és *q* értékét.

NOREG

A kriptográfia biztonságos???

- 2012 évi adatok (a visszafejtés komplexitásának bemutatására):
  - 56 bit – 399 mp
  - 128 bit – 10^18 év
  - 256 bit – 3*10^37 év

- A kriptográfiai eljárások biztonsága a kulcsok biztonságán alapul !!!

NOREG

Szimmetrikus esetben

- NIST: 80 bites kulcsok 2010 után már nem elfogadottak [1]
- AES – 256 bit: még várhatóan jó ideig biztonságos marad

- [1] http://csrc.nist.gov/publications/nistpubs/800-131A/sp800-131A.pdf
- [2] http://arstechnica.com/old/content/2007/05/researchers-307-digit-key-crack-endangers-1024-bit-rsa.ars
- [3] http://www.pcworld.com/article/132184/researcher_rsa_1024bit_encryption_not_enough.html

NOREG

Aszimmetrikus esetben

- Az 1024-bites kulcsok halottak?
  - „The answer to that question is an unqualified yes.” [2]
  - NIST: 2013 végéig engedélyezett

NOREG

ECC - elliptic curve cryptography

- ECDLP (elliptic curve discrete logarithm problem) nevű matematikai problémára épülő kriptográfiai megoldások együttes elnevezése.
- ECC alatt több algoritmust is értünk:
  - aláírásra (pl. ECDSA),
  - titkosításra (pl. EC ElGamal)
  - autentikációra (pl. ECDH)

- Kisebb kulcsmérettel nyújtanak hasonló biztonságot, mint az RSA
  - 160 bites ECC kulcs == 1024 bites RSA kulcs
  - 224 bites ECC kulcs == 2048 bites RSA kulcs
- Ugyanakkor az ECC nem feltétlenül tekinthető gyorsabbnak, mint az RSA

NOREG

Hash-függvények

- MD5: már nem biztonságos használni
  - 2008: 200 PS3-mal sikerült hamis SubCA-t készíteni
- SHA-1: cserélni kell!
- SHA-2 család: (pl. SHA-256, SHA-512)
- SHA-3/KECCAK

NOREG

Kulcsméret és hash algoritmus váltás

- SHA-1 ☹ → SHA-2 család ☺
- 1024 bites RSA ☹ → 2048+ bites RSA ☺
- Alkalmazás integráció:
  - Microsoft
    - A Windows 2017. január 1-től nem fogadja el [1]
  - Google
    - Chrome: fokozatos figyelmeztetés [2]

[1] http://blogs.technet.com/b/pki/archive/2013/11/12/sha1-deprecation-policy.aspx
[2] http://googleonlinesecurity.blogspot.hu/2014/09/gradually-sunsetting-sha-1.html

NOREG

Kulcsméretek

- https://www.keylength.com/en/3/

Protection	Symmetric	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash
Legacy standard level *Should not be used in new systems*	80	1024	160	1024	160	160
Near term protection *Security for at least ten years (2019-2028)*	128	3072	256	3072	256	256
Long-term protection *Security for thirty to fifty years (2019-2068)*	256	15360	512	15360	512	512

All key sizes are provided in bits. These are the minimal sizes for security.

NOREG

Kulcsméret és hash algoritmus váltás

- KVANTUM számítógép - ha nagy kvantumszámítógépeket tudunk építeni, azok bizonyos feladatokat exponenciálisan gyorsabban tudnak megoldani, mint hagyományos számítógépeink.

NOREG

Kvantum számítógép

- Google confirms ‘quantum supremacy’ breakthrough
  - “Google says that its 54-qubit Sycamore processor was able to perform a calculation in 200 seconds that would have taken the world’s most powerful supercomputer 10,000 years.”

NOREG

Nem csak technológia

- A kriptográfiai algoritmusok önmagában nem elegendőek!!!
- Kell hozzá még:
  - Fizikai biztonság
  - Eljárások, szabályok
  - Felhasználó
  - Korrekt implementáció (kulcstér, TPM chip, ID cards)

NOREG

Rejtjelzés megvalósítása

- Szimmetrikus eljárás
  - Előny: gyors
  - Hátrány: kulcscsere
- Aszimmetrikus eljárás
  - Előny: kulcscsere
  - Hátrány: lassú

- Gyakorlatban a kettőt kombinálják !!!

NOREG

Elektronikus aláírás

NOREG

Elektronikus aláírás

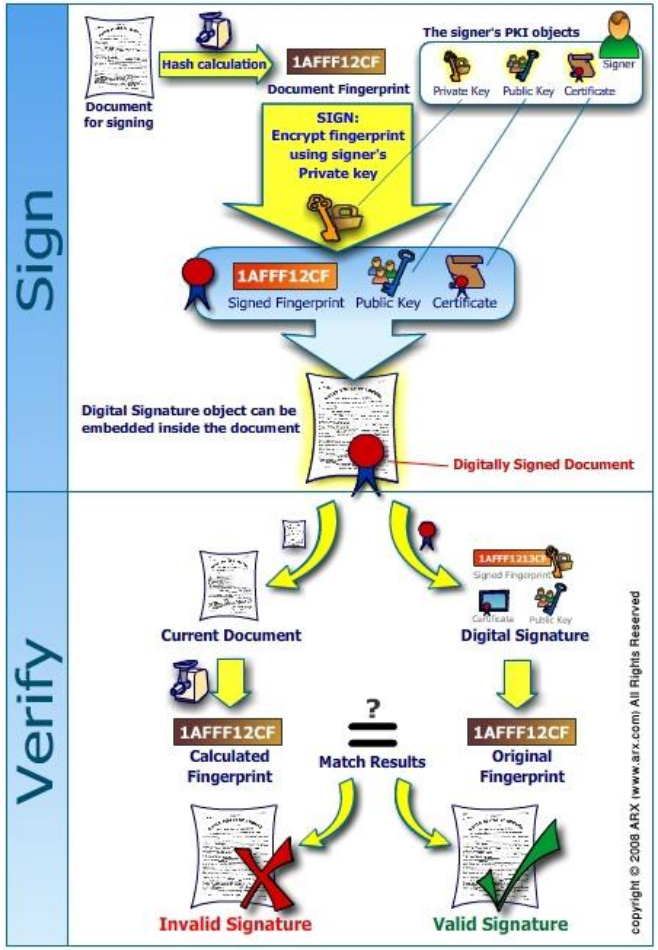
- Kapcsolódó eljárásokkal együtt alkalmas arra, hogy biztosítsa:
  - az aláíró egyértelmű azonosíthatóságát,
  - az aláírás tényének letagadhatatlanságát,
  - továbbá azt, hogy az elektronikus irat tartalma nem változott meg az aláírás művelete óta.

NOREG

Elektronikus aláírás

- Aláírás készítése:
  1. A dokumentumról (D) lenyomat (hash) számítás → H
  2. A hash titkosítása a privát kulccsal → S (signature)
  3. A dokumentum és az aláírás elküldése: {D, S}

- Ellenőrzése:
  1. A dokumentumról (D) lenyomat számítás → H'
  2. S visszafejtése a publikus kulccsal → H''
  3. Érvényes aláírás: H' == H''



Forrás: http://www.arx.com/files/Brochure-images/Digital-signatures2.jpg

NOREG

Elektronikus aláírás szabályozás

- 1993/93/EK irányelv
- Az elektronikus aláírásról szóló 2001. évi XXXV. törvény (eat.)
  - megteremtette az elektronikus aláírás jogszabályi hátterét
  - 1999/93/EK irányelvvel összeegyeztethető
  - módosította számos törvény és jogszabály egyes rendelkezéseit, hogy megteremtse az általuk szabályozott területeken az elektronikus dokumentumok felhasználásának lehetőségét.

NOREG

Elektronikus aláírás szabályozás

- 910/2014/EU rendelet (a továbbiakban: eIDAS rendelet)
- 2016. január 1-én bizonyos kivételekkel hatályba léptek az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól szóló 2015. évi CCXXII. törvény rendelkezései
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- A Bizalmi törvény 2016. július 1. napjától hatályon kívül helyezte többek között az elektronikus aláírásról szóló törvényt

NOREG

Elektronikus aláírás szabályozás

- eIDAS alapján:
  - elektronikus aláírást csak természetes személyek hozhatnak létre
  - jogi személyiségek csak elektronikus bélyegzőket adhatnak ki
- ez az uniós rendelet határozza meg Magyarországon az elektronikus tranzakciókat, az egész EU területére kiterjedően.
- Az elektronikus aláírás is érvényes, bizonyító erejű, és az unió egész területén elfogadott -> cél: várhatóan szélesedik mind az elektronikus aláírást létrehozó technikai megoldások, mind az ezeket felhasználó szolgáltatók köre

NOREG

Tanúsítvány alapok

NOREG

Tanúsítvány

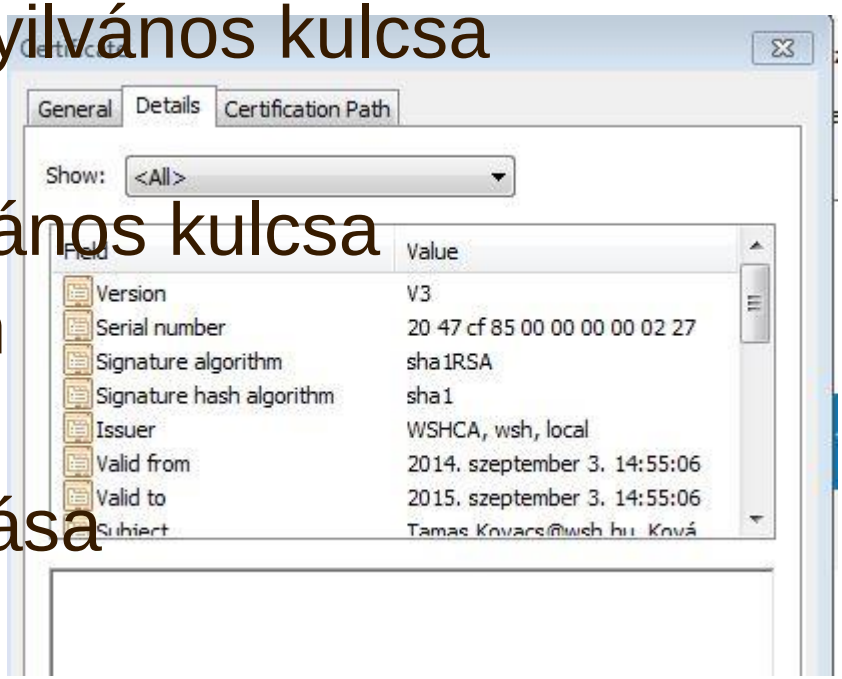
- „Kérdés 1”: Hogyan bízhatok meg egy nyilvános kulcsban?

⇨ Hitelesíttetni kell a kulcsot (kell egy CA)

NOREG

X.509 tanúsítvány felépítése

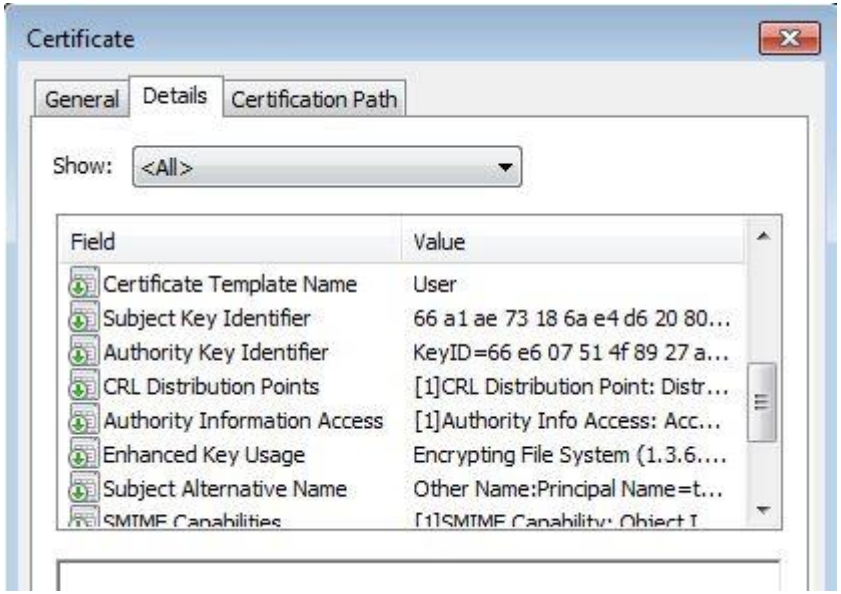
- X.509 certificate alapmezők
  - Serial number
  - Subject (felhasználó) neve
  - Subject (felhasználó) nyilvános kulcsa
  - Issuer (kibocsátó) neve
  - Issuer (kibocsátó) nyilvános kulcsa
  - Érvényességi időtartam
  - Kibocsátás célja
  - Issuer (kibocsátó) aláírása



NOREG

X.509 tanúsítvány felépítése

- X.509 certificate bővítések:
  - Certificate Policy
  - Extended Key Usage
  - Basic Constraints
  - CRL Distribution Points
  - Netscape Extensions
  - Generic Extensions



NOREG

Tanúsítványok „osztályozása”

- Tanúsítvány fajták
  - Magánszemélyek
  - Szervezeteket képviselő személyek
  - Eszközök
- Tanúsítvány típusok
  - Alap biztonságú
  - Fokozott biztonságú
  - Minősített biztonságú

NOREG

Tanúsítvány - Gyakori félreértés

- Kérdés 2: „Egy tanúsítvány felmutatása bizonyítja a személyazonosságot?”

- Ez nem igaz!!! - A személyazonosságot a titkos kulcs korrekt használatának ellenőrzése biztosítja.

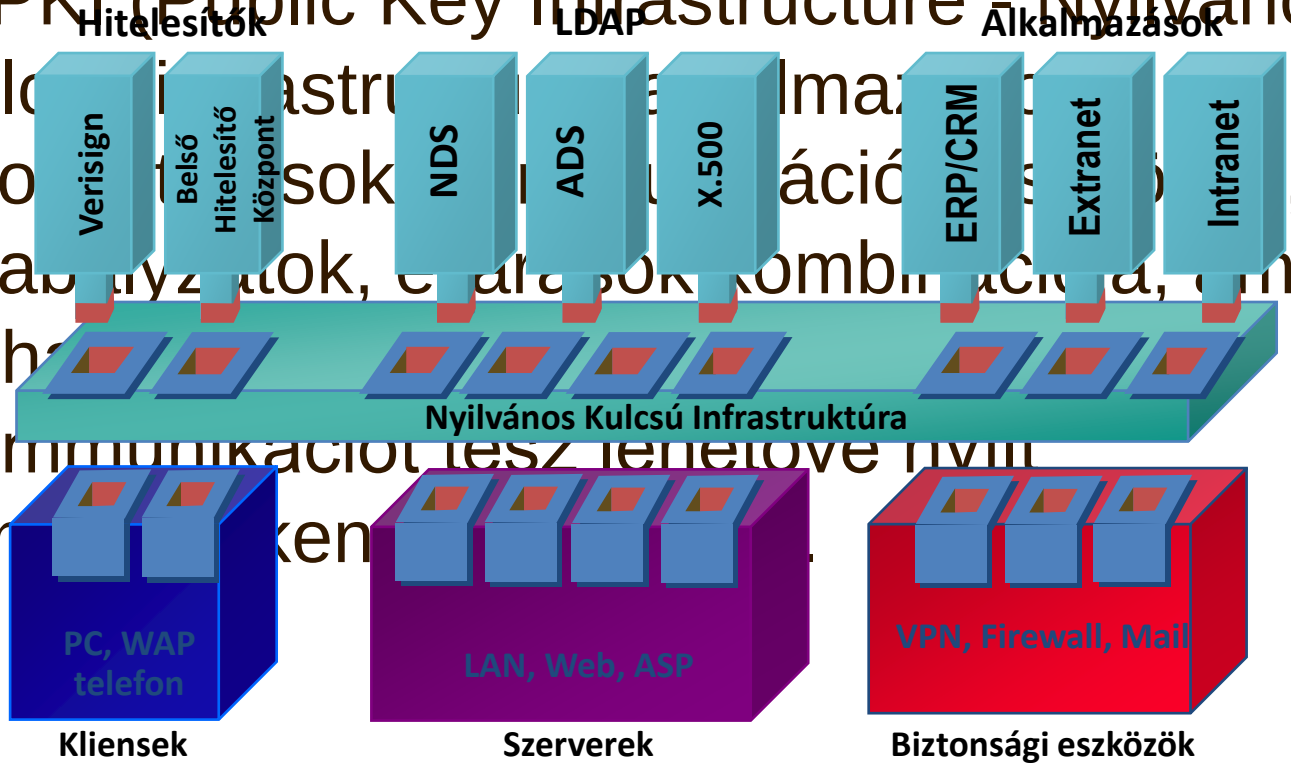
NOREG

Nyilvános kulcsú infrastruktúra

NOREG

Nyilvános kulcsú infrastruktúra

A PKI (Public Key Infrastructure – Nyilvános kulc[illegible]astru[illegible]lmaz[illegible] szo[illegible]sok [illegible]áció[illegible], szab[illegible]ok, e[illegible]ok kombi[illegible], ami a felh[illegible] kommunikációt tesz lehetővé nyílt ren[illegible]ken.



NOREG

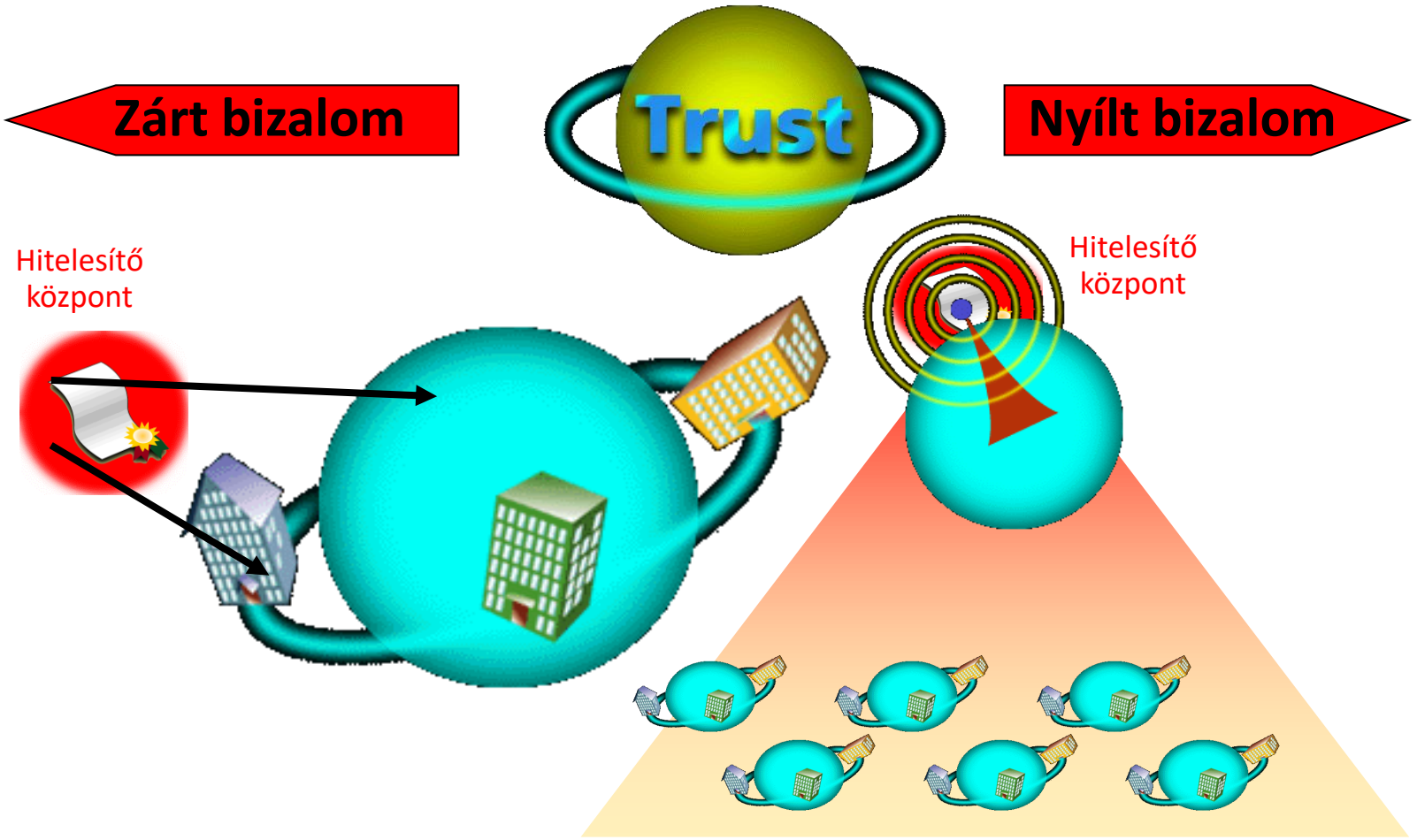
Nyilvános kulcsú infrastruktúra

- „Kérdés 3”: Hogyan bízhatok az elektronikus közjegyzőben?

- Tanúsítvány lánc segítségével

NOREG

Nyilvános kulcsú infrastruktúra



NOREG

Láncolt vagy Root CA

- Láncolt CA:
  - A CA-t egy megbízható szervezet „hitelesíti” - akkor kell, ha a certificate-ket a külvilággal is el akarja fogadtatni.
- Root CA:
  - A saját certificate-jét maga írja alá

NOREG

Láncolt CA & Kereszt tanúsítás

- Abban az esetben, ha PKI rendszerünket nem csak belső, zárt környezetben használjuk:
  - CA láncolás - HIERARCHIA kialakítása,
  - Cross certification - két egyenrangú CA között alakul ki „trust” kapcsolat

NOREG

Nyilvános kulcsú infrastruktúra építőelemek

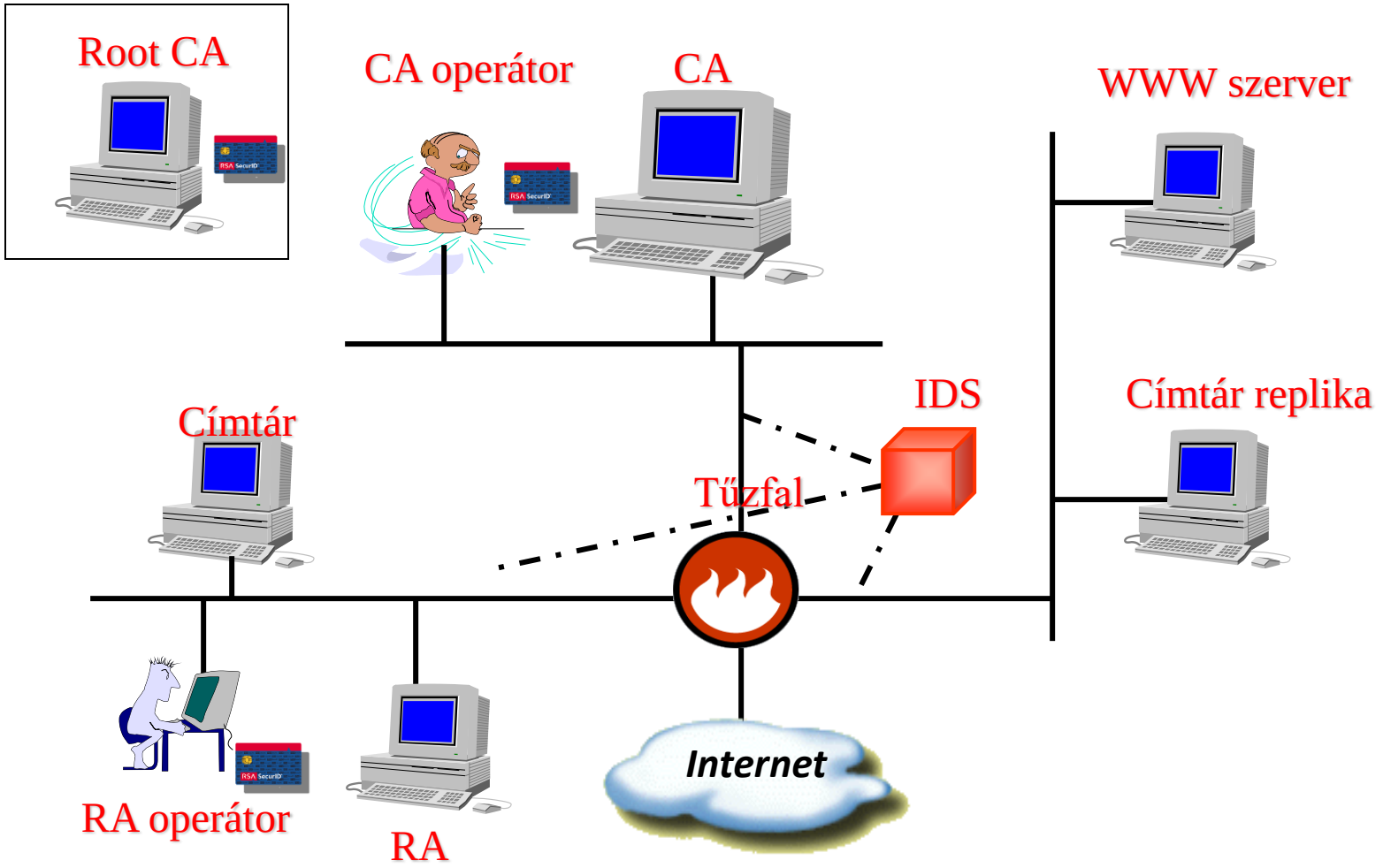
NOREG

PKI építőelemek

- Hitelesítő központ (Certification Authority - CA)
- Regisztrációs központ (Registration Authority – RA)
- Címtár szolgáltatás (vagy webes publikáció)
- Hardver biztonsági eszközök
- Szabályzatok
- PKI alkalmazások
- Biztonsági megoldások (pl. Tűzfal, IPS eszközök)

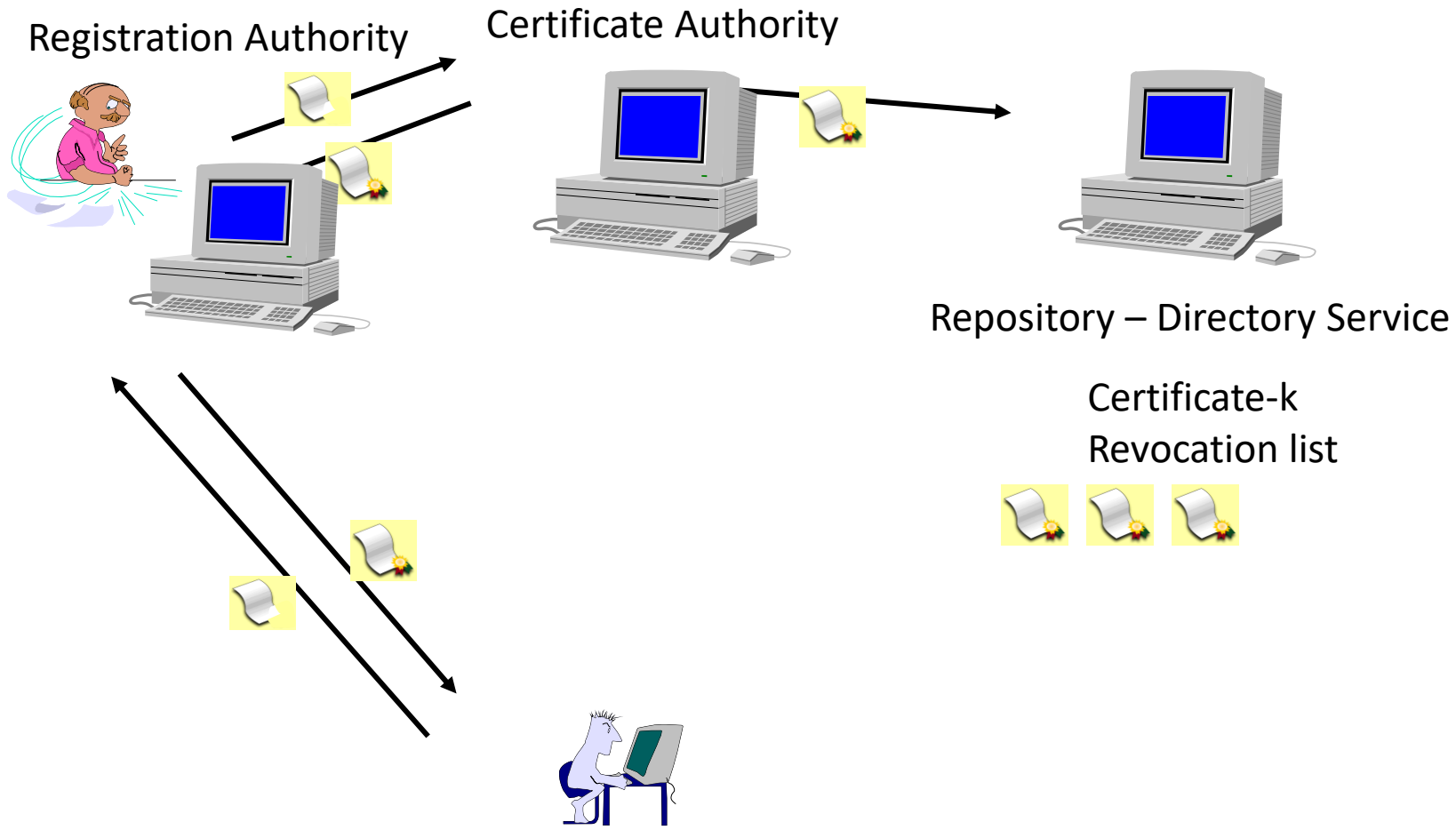
NOREG

PKI architektúra



NOREG

Tanúsítványkiadás folyamata



NOREG

CA – Certificate Authority

- Tanúsítvány előállítás
- Tanúsítvány kiadás és publikálás
- Tanúsítvány visszavonás
- Kulcs mentés és visszaállítás

NOREG

CA működése

- Root CA, mint PKI infrastruktúra központja
  - Root CA által hitelesített tanúsítványok
  - Működtetésének alapelvei
- SubCA
  - Kapcsolata a Root CA-val
  - Működtetésének alapelvei

NOREG

Tanúsítvány előállítás, kibocsátás

- Általában policy segítségével
- Itt határozódik meg milyen információt tartalmazzon a tanúsítvány
- Vannak kötelező és opcionális elemek

NOREG

Tanúsítvány publikálás, disztribúció

- Tanúsítvány disztribúciója:
  - azon az útvonalon, ahol beérkezett a kérelem
  - szabványos fájl formátumban publikálással
- Tanúsítványok publikálása:
  - X.500 címtár
  - LDAP
  - File-, vagy webszerver

NOREG

Regisztráció

NOREG

RA – Registration Authority

- Az RA fogadja:
  - Beérkező remote regisztrációs és visszavonási kéréseket
  - Regisztrációs operátor generálja a face-to-face regisztrációs kéréseket
- Az RA, mint regisztrációs központ felel a tanúsítvány hitelesítési kérelmek továbbításáért a CA felé

- Regisztrációs folyamat
  - Adatgyűjtés
  - Jogosultság ellenőrzés
  - Regisztrációs döntés
  - Opcionális kulcsgenerálás és kulcs és tanúsítvány disztribúció
- Visszavonás

NOREG

Regisztráció

- Regisztrációs modellek közös jellemzői:
  - Azonosítani kell a felhasználót
  - Fogadni kell a felhasználó adatait
  - Le kell generálni a szükséges kulcsokat
  - El kell készíteni a tanúsítvány kérelmet
  - A CA elkészíti és hitelesíti a tanúsítványt
  - A tanúsítvány terjesztés

NOREG

Regisztráció

- Face-to-face
  - Az RA operátor személyesen találkozik a felhasználóval
  - Kulcsgenerálást az operátor végzi tipikusan
  - Operátor vagy a felhasználó választ PIN-t.
  - A kulcs és a tanúsítvány továbbításra kerül a felhasználó gépére
- Remote
  - Az RA operátor távolról kell „ellenőrizze” a felhasználó személyazonosságát
  - Kulcsgenerálás a felhasználónál
  - RA szoftver nem kontrollálja a kulcsgenerálást
  - A privát kulcs nem hagyja el a felhasználó gépét

NOREG

Tanúsítvány visszavonás

NOREG

Tanúsítvány visszavonás

- „Kérdés 4”: Honnan értesülök arról, hogy a tanúsítvány már nem érvényes?
- Legelterjedtebb módja: CRL (Certificate Revocation List – Tanúsítvány Visszavonási Lista)
- Tanúsítvány visszavonás lehetséges:
  - véglegesen - visszavonás
  - ideiglenesen - felfüggesztés

NOREG

Tanúsítvány visszavonás

- CRL terjesztése a felhasználók közt
  - elhelyezzük mindenki számára elérhető helyre – zártkörű felhasználás
  - CDP (CRL Distribution Point) - X.509 v3 certificate-ek tartalmazhatnak CDP bejegyzést, amely meghatározza a CRL helyét a rendszerben

NOREG

Tanúsítvány visszavonás

- Minden CRL tartalmazza az alábbiakat:
  - Verziószám (meghatározza a CRL formátumát)
  - Aláírás
  - Kibocsátó
  - Utolsó frissítés időpontja
  - Következő frissítés időpontja
  - Visszavont tanúsítványok listája

NOREG

Tanúsítvány visszavonás

- A visszavonási tanúsítványok listája tartalmazza az alábbiakat:
  - A tanúsítvány sorszámát
  - A visszavonás dátumát
  - Opcionális kiegészítések melyek a visszavonás körülményeire vonatkozhatnak

NOREG

CRL

- CRL lehet:
  - Teljes (master) CRL - Minden visszavont tanúsítvány sorszámát tartalmazza
  - Részleges CRL - Csak az adott feltételnek megfelelőkét

NOREG

CRL – Reason code

- Visszavonás oka lehet:

```
CRLReason ::= ENUMERATED {
     unspecified                (0),
     keyCompromise              (1),
     cACompromise               (2),
     affiliationChanged         (3),
     superseded                 (4),
     cessationOfOperation       (5),
     certificateHold            (6),
          -- value 7 is not used
     removeFromCRL              (8),
     privilegeWithdrawn         (9),
     aACompromise              (10) }
```

NOREG

Online Certificate Status Protocol

- Revocation Checker” – ként működik a felhasználói alkalmazások számára
- Gyorsabb válaszidőt biztosít azáltal, hogy nem a CRL-t ellenőrzi, csak az adott certificate érvényességét
- Azonnal, on-line frissül az adatbázisa (!!!)
- Egyidejűleg több CA rendszert is ki tud szolgálni

NOREG

Online Certificate Status Protocol

- Az OCSP szerver az alábbi lehetséges válaszok valamelyikét adja lekérdezés esetén:
  - Revoked – A certificate visszavonásra került
  - Not revoked – A certificate érvényes
  - Do not know – Az adatbázisa nem tartalmazza a kért információt

NOREG

Kulcs archiválás

NOREG

Kulcs archiválás

- A tanúsítványok felhasználása:
  - Aláírás
  - Azonosítás
  - Titkosítás
- Mi történik, ha megsemmisül a privát kulcs???
  - Digitális aláírás - későbbi hitelesítése OK
  - Rejtjelezett állományok - nem lesznek elérhetőek

NOREG

Kulcs archiválás

- A felhasználó privát kulcsáról készült másolatot tárol:
  - A kulcsokat fel kell „készíteni”
  - A távoli kéréskor generált kulcsokat – tipikusan - nem lehet archiválni
- Gondok:
  - Kulcs generálása nem központilag történik
  - On-board kulcsgenerálás

NOREG

Kulcs archiválás

- A kulcsokat a Kulcs Archiváló Szerver segítségével lehet helyreállítani különböző formátumokban:
  - PKCS#12
  - PSE fájl formátum
  - Bináris PKCS#1 privát kulcs

NOREG

Hardware Security Modul

NOREG

Hardware Security Modul

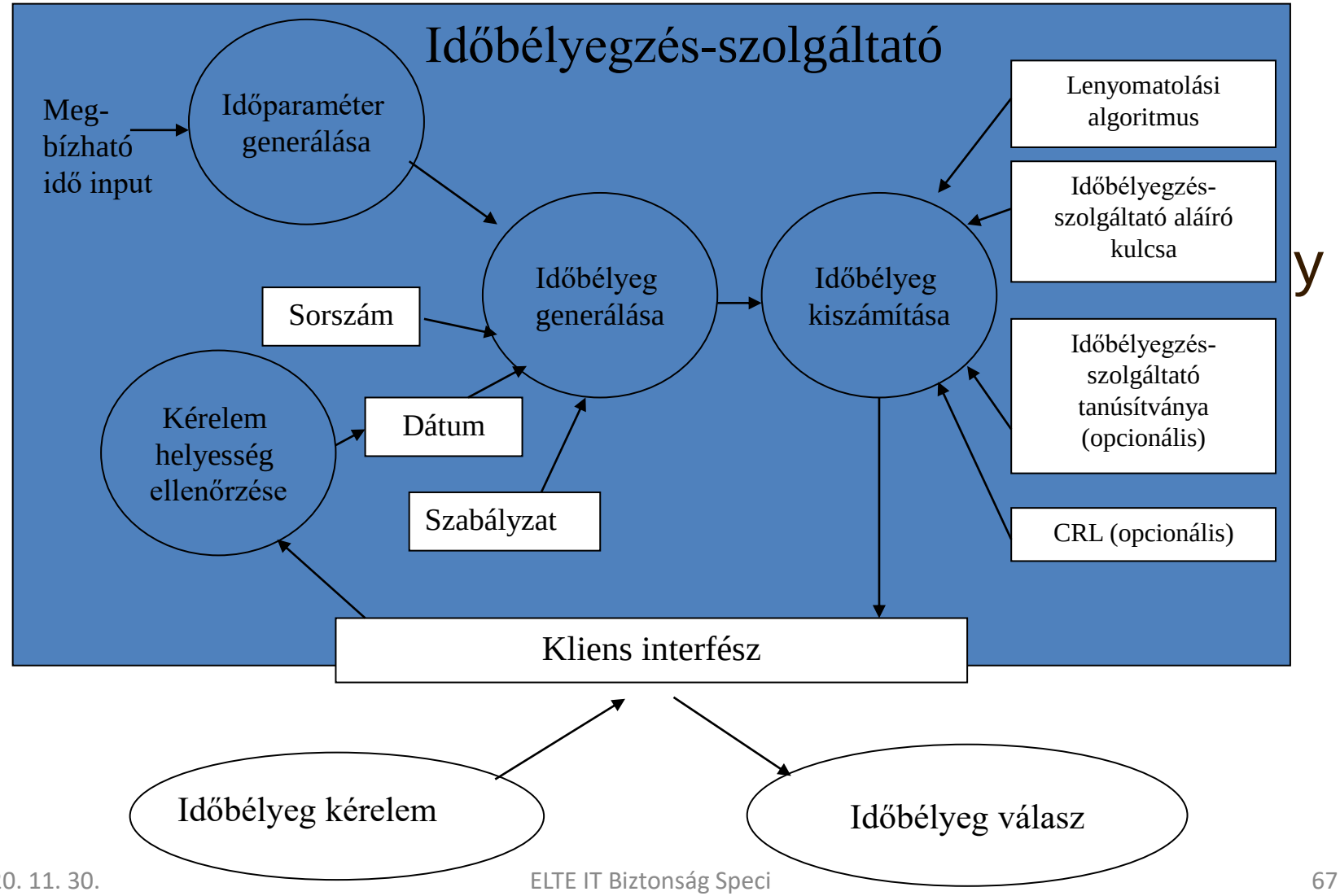
- Cél : kulcsok biztonságos **tárolása** és **generálása** - a privát kulcs nem hagyja el az eszközt
- A legtöbb rendszer támogatja a szabványos megoldásokat (PKCS#11)
- Lehet:
  - PCI illetve hálózati felületen csatlakozó eszköz

NOREG

Időbélyeg

NOREG

Timestamp - időbélyeg



NOREG

Kártya és kulcsmenedzsment

NOREG

Tanúsítványt honnan?

- Szolgáltatótól vs. saját CA(k)
- Szempontok:
  - Előírások
  - Elfogadottság
  - Ár
  - Üzemeltetés

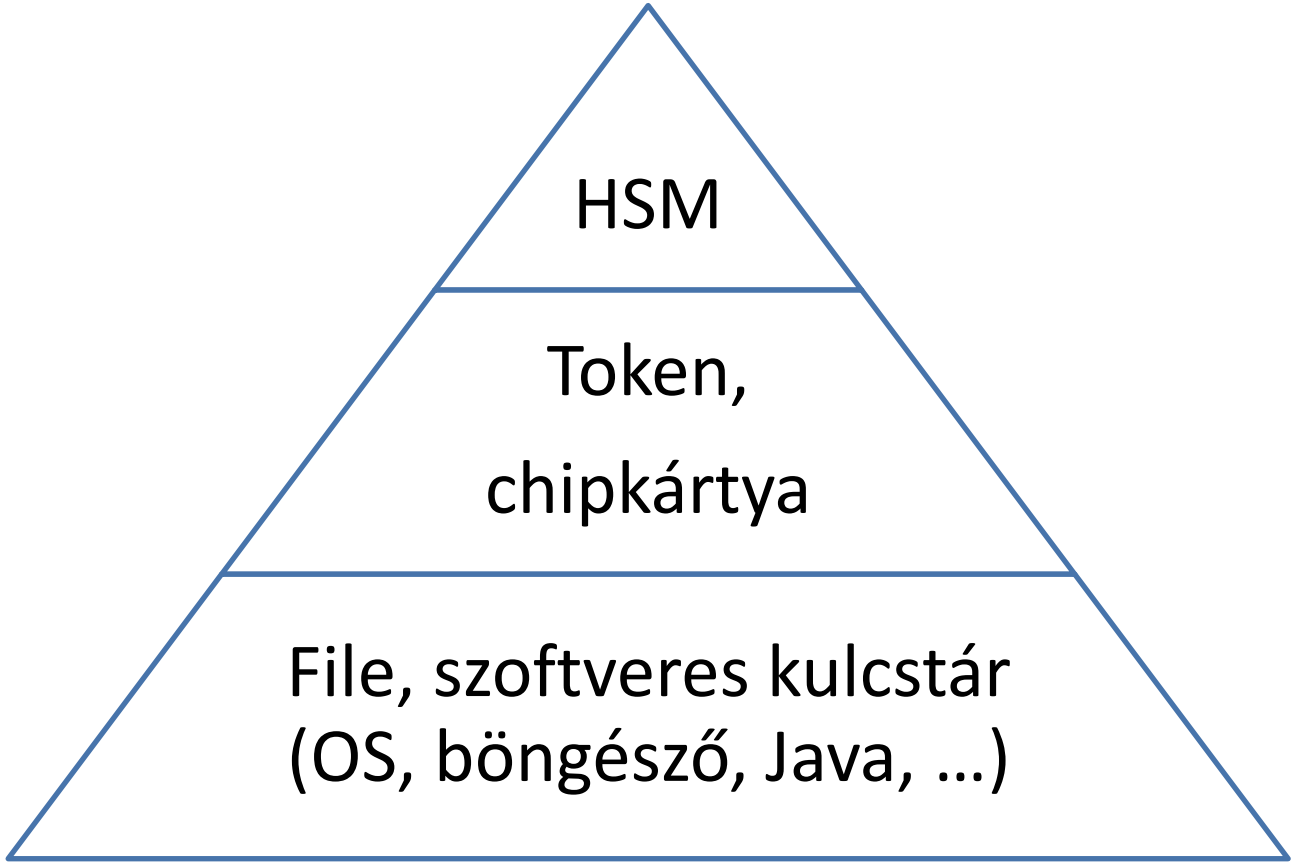
NOREG

Hány tanúsítványt?

- 3 fő felhasználói tanúsítványtípus:
  - Autentikációs
  - Aláíró
  - Titkosító
- 3 különböző kulcsot javasolt használni
  - A titkosító kulcsokat menteni kell!

NOREG

Hol tároljuk a kulcsokat?



NOREG

Hardver kulcstároló eszközök

- Kulcshordozó eszköz lehet file és hardver (pl. Smart kártya, Token)

- A hardver eszközök előnyei:
  - Hardveres véletlenszám-generátor
  - A kulcs nem hagyja el az eszközt
  - PIN-kód, PIN-policy
  - Egyéb védelmek: fizikai felépítés, zaj-generátorok, stb.

- Bárhol is tároljuk a különböző célú kulcsokat, azokat célszerű együtt kezelni.

- Az eszközök, s a többféle tanúsítvány menedzselése komplex folyamatokból áll, a PKI rendszernél magasabb szinten.

NOREG

A kártyák, tokenek előnyei

- Biztonságos (minősítések)
- Egyéb kétfaktorú technológiákkal szemben:
  - Egyszerűen megújítható
  - Újrafelhasználható
    - Nem jár le az eszköz érvényessége
    - Nincs elem, nem merül le
    - Törölhető
  - Egyszerűen visszavonható
  - Nincs folyamatos tranzakciós költség

Hogyan menedzselhetők a tanúsítványok, kártyák?

- A tanúsítványok számától függően:

10

100

>100

PKI kihívások nagyvállalati környezetben

- Felhasználó azonosítása
- Felhasználó és tanúsítvány összerendelése
- Tanúsítvány életciklus menedzselése
- Hardver eszközök menedzselése
- Folyamatok menedzselése (megújítás, csere)
- Mindezt compliance elvárásoknak megfelelően!!!

PKI kihívások nagyvállalati környezetben

- A hiteles adatforrás és a kártyák/tokenek életciklusának kezelése számos problémával jár, ha csak önmagában PKI (CA) rendszer van.

NOREG

PKI funkciók kiterjesztése

- Elosztott, távoli működés lehetséges
- Kártya életciklus-kezelés
- Több CA kezelése
- Regisztráció (akár IDM nélkül), (RA – Registration Authority) funkciók

NOREG

Kártyamenedzsment feladatok

- Kártyák/tokenek gyártása, kezelése, nyilvántartása
  - Elektronikus (és vizuális) megszemélyesítés
- PKI rendszerek kezelése
- Adatforrások kezelése
  - IDM
  - Címtár
- Profilok, sablonok támogatása
- Kártyafolyamatok (csere, elvesztés, megújítás, letiltás) menedzselése
  - Titkosító kulcsok visszaállítása, korábbi tanúsítványok törlése
  - PIN feloldás
- Szoft-token támogatás
- Regisztrációs feladatok
    - Szervezeti hierarchia, Felhasználó, Telephely, Címadatok, stb.
  - Riport funkciók
  - Mindezt biztonságosan!

NOREG

Menedzsment funkciók

- Kártya/token folyamatok kezelése
  - új kártyák kiadása, megszemélyesítése
  - visszavonás, felfüggesztés, visszavétel
  - megújítás, csere, otthonhagyott kártya
  - elfelejtett jelszó feloldása
- S még sok más
  - alapadatok kezelése, riportolás, leltár, …
  - változások kezelése (pl. + 1 tanúsítvány)

NOREG

A mindennapi gyakorlatban

- Konkrét példa: 3 tanúsítványt tartalmazó kártya kiadása
  - Autentikációs, aláíró és titkosító tanúsítványok – szokásos, ajánlott konfiguráció
- MS CA saját eszközeivel a gyártás kb. 5 perc
  - 3 külön folyamat, felhasználó és kártyák kiválasztása minden esetben
  - A titkosító kulcsot kézzel kell importálni. Jelszókezelés, tárolás!
- Kártyamenedzsment rendszerrel: kb. másfél perc
  - Egy integrált folyamat

NOREG

Gyakorlati alkalmazások

- Levelezés aláírása/titkosítás
- Elektronikus számlázás
- VPN kapcsolatok
- SSL elérés
- Elektronikus cégeljárás

NOREG

Gyakorlati alkalmazások - IoT

- IoT – Internet of Things speciális környezet
  - Méret (mikrokontroller, számítási kapacitás, RAM/ROM méret)
  - Fogyasztás
  - Sebesség
  - Fizikai védelem hiánya
  - Véletlen generálási problémák

NOREG

Köszönöm a figyelmet