Tanúsítványkezelés kihívásai napjainkban

Kovács Tamás
tamas.kovacs@noreg.hu

•1

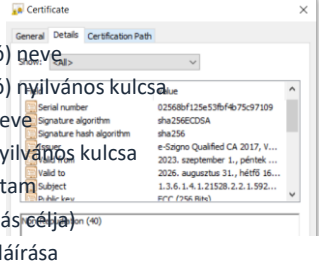
Az előadóról

- 20+ év tapasztalat az IT biztonsági területén
- ISACA membership
  - 2001 CISA
  - 2004 CISM
- Elektronikus aláírás szakértő
- Projektek:
  - Minősített szolgáltatások (hitelesítés, időbélyeg) kiépítése
  - Enterprise PKI megoldások bevezetése
  - Kapcsolódó szoftver fejlesztés
  - Szabályzatok kidolgozása

•2

X.509 tanúsítvány felépítése

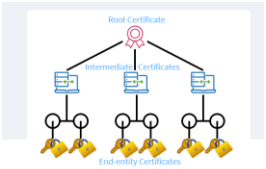
- X.509 certificate alapmezők
  - Serial number
  - Subject (felhasználó) neve
  - Subject (felhasználó) nyilvános kulcsa
  - Issuer (kibocsátó) neve
  - Issuer (kibocsátó) nyilvános kulcsa
  - Érvényességi időtartam
  - Key usage (kibocsátás célja)
  - Issuer (kibocsátó) aláírása



•3

Láncolt vagy Root CA

- Root CA: A saját certificate-jét maga írja alá
- Láncolt CA: A CA-t egy megbízható szervezet „hitelesíti”

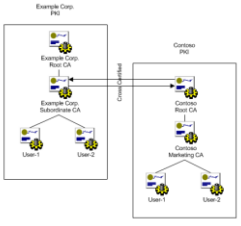


•4

Láncolt CA & Kereszt tanúsítás

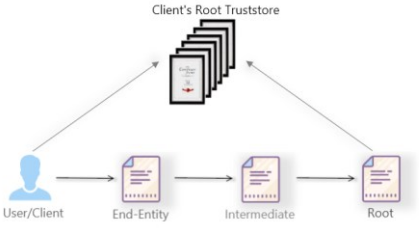
Abban az esetben, ha PKI rendszerünket nem csak belső, zárt környezetben használjuk:

- CA láncolás - HIERARCHIA kialakítása,
- Cross certification - két egyenrangú CA között alakul ki „trust” kapcsolat



•5

The chain of trust



•6

Tanúsítvány érvényesség - visszavonás

- Tanúsítvány visszavonás lehetséges:
  - véglegesen - visszavonás
  - ideiglenesen – felfüggesztés
- CRL (Certificate Revocation List – Tanúsítvány Visszavonási Lista)
- OCSP (Online Certificate Status Protocol)

•7

Ajánlások, szabályozások

- eIDAS (EU Trust List)
- https://eidas.ec.europa.eu/efda/tl-browser/#/screen/home
- CA/Browser forum
- https://cabforum.org/baseline-requirements-documents/
- Microsoft Trusted Root Program
- https://learn.microsoft.com/en-us/security/trusted-root/program-requirements
- Mozilla's CA Certificate Program
- https://wiki.mozilla.org/CA

•8

Felhasználói tanúsítványok

- Tanúsítvány felhasználás célja:
  - Aláíró
  - Autentikációs
  - Titkosító
  - “Kód aláírás”
- Törvényi, szerződéses kötelezettség

•9

Kihívások nagyvállalati környezetben

- Felhasználó (kezdeti) azonosítása
- Hiteles felhasználói adatok
- Tanúsítvány életciklus menedzselése
- Kulcshordozó eszközök (smartkártya, PKI token, VSC, OS store) menedzselése
- Mobil eszközök kezelése
- Titkosító kulcsok kezelése

- Átláthatóság: külső és belső tanúsítványokra

•10

Eszköztanúsítványok

- Miért más?
  - Más folyamatok, számosság
  - Ha lejár akkor azonnal megáll a szolgáltatás
  - Archiválás (HA pár, load balance)
  - Cserélni sem lehet bármikor (green zone)

•11

Átláthatóság

- Teljes nyilvántartás a tanúsítványokról
  - Külső szolgáltatóktól/partnerektől néhány darab
- Automatán igényelt tanúsítványok
  - Computer tanúsítvány (pl. NAC)
  - SCEP, ACME, ...
- Manuális kiadás
- Lejárati figyelmeztetés
  - Az igénylőt először, s ha nincs eredmény akkor a csoportot

•12

IoT “tanúsítványok”

- Mire használnak IoT eszközök nyilvános kulcsú kriptográfiát:
  - autentikáció
  - integritásvédelem
  - titkosítás
  - megbízható frissítés
- Speciális környezet
  - Méret (mikrokontroller, számítási kapacitás, RAM/ROM méret)
  - Fogyasztás
  - Sebesség
  - Fizikai védelem hiánya
  - Távolság és hozzáférés
  - Véletlen generálási problémák

•13

Köszönöm a figyelmet!

Kovács Tamás
tamas.kovacs@noreg.hu

•14