A digitális aláírás alapjai és használata Linux rendszeren

Mátó Péter <atya@fsf.hu>

A digitális kor kihívásai

- A digitális dokumentumok
  - könnyen másolhatók
  - könnyen módosíthatók
  - a kommunikáció lehallgatható
- Meg kellene oldani az alábbiakat
  - letagadhatatlanság
  - a dokumentum sértetlenségének ellenőrzése
  - bizalmasság megőrzése

A digitális aláírás működési elve

- A digitális aláírás az aszimmetrikus titkosításon alapul
  - Nagyon nehezen megoldható matematikai problémán alapul
  - Egyelőre nem megoldható belátható időn belül, ezért most megfelel
  - A leggyakrabban használt algoritmus: RSA
- Két kulcs van, az egyiket csak a tulajdonosa ismerheti, a másikat mindenkinek odaadja

A kulcsok felhasználása

- A titkos kulcs felhasználható
  - aláírásra
  - titkosítás visszafejtésére
- A nyilvános kulcs felhasználható
  - aláírás ellenőrzésére
  - titkosításra (valójában egy szimmetrikus kulcsot titkosítanak vele)

Kulcs párok készítői

- Problémák
  - Ki csinálja őket?
  - Honnan lehet tudni, hogy a készítő tényeg az, akinek mondja magát
- Saját gyártású kulcsok
  - ellenőrzés nagyon fontos - újjlenyomatok
- Az igazi megoldás: harmadik, megbízható fél
  - A CA-k (Certifitate Authority) ellenőrzötten adnak ki kulcspárokat

Tanúsítványok típusai I

Mátó Péter <atya@fsf.hu>
A digitális aláírás használata Linux rendszeren

Tanúsítványok díja

Fokozott biztonságú tanúsítványok

	NetLock Expressz (Class C)Tanúsítványkiadó	NetLock Üzleti (Class B)Tanúsítványkiadó	NetLock Közjegyzői (Class A)Tanúsítványkiadó
Személyes	4.800 Ft/év	7.800 Ft/év	9.000 Ft/év
Munkatársi	9.600 Ft/év	15.600 Ft/év	18.000 Ft/év
Munkatársi csomag (5 db)	28.800 Ft/év	46.800 Ft/év	54.000 Ft/év
Szervezeti	9.600 Ft/év	15.600 Ft/év	18.000 Ft/év
SSL (szerver)	19.200 Ft/év	31.200 Ft/év	36.000 Ft/év
Láncolt tanúsítványkiadó (LHSz)	Érdeklődjön!	Érdeklődjön!	Érdeklődjön!

Minősített tanúsítványok

	NetLock Minősített Közjegyzői (Class QA) Tanúsítványkiadó	
	Személyes tanúsítvány	Munkatársi tanúsítvány
Ügyleti érték: 5 millió Ft	20.000 Ft/év	30.000 Ft/év
Ügyleti érték: 20 millió Ft	30.000 Ft/év	50.000 Ft/év
Ügyleti érték: 50 millió Ft	40.000 Ft/év	70.000 Ft/év

Tanúsítványok típusai II

- A osztály: közjegyző által hitelesített, szigorú ellenőrizési lépések (személyes megjelenés és dokumentumok bemutatása)
- B osztály: a szolgáltató által hitelesített, szigorú ellenőrizési lépések (személyes megjelenés és dokumentumok bemutatása)
- C osztály: korlátozottan ellenőrzött (dokumentum másolatok beküldése) - csak kis kockázatú műveletekhez ajánlott

Tanúsítványok

- A tanúsítvány egy adatcsomag, amely tartalmazza a nyilvános kulcsot és egyéb, CA által hozzátett információkat
- Minden tanúsítvány tartalmazza a tanúsítvány szolgáltató aláírását
- Minden tanúsítvány egyedi azonosítóval van ellátva
- Tanúsítvány érvényességét
- Tanúsítvány visszavonási lista helyét

Tanúsítványok ellenőrzése

- Megfelelő-e a kiállító aláírása?
  A tanúsító szervezet nyilvános kulcsát be kell szerezni hozzá
- Érvényes-e a tanúsítvány?
  A tanúsítvány tartalmazza az érvényességének idejét
- Nem vonták-e vissza a tanúsítványt?
  Szükséges hozzá a CA friss CRL-je (Certificate Revocation List)

A tanúsítványok felhasználása

- Digitális aláírásra és annak ellenőrzésére
- Adatok titkosítására és visszafejtésére
- Szerverek azonosítására az interneten
- Felhasználók azonosítására az interneten

Felhasználás a gyakorlatban

- Levelezés: Thunderbird levelező program
  - aláírás
  - aláírás ellenőrzése
  - titkosítás
  - visszafejtés
- Felhasználó azonosítása
  - Firefox böngésző, stunnel program...
- Szerverek azonosítása: Az SSL protokoll-t ismerő szervereknél használható (pl https)

Köszönöm a figyelmet

(az előadás kiegészített, szöveges változata hamarosan elérhető lesz a http://kolab.fsf.hu oldalon)

A digitális aláírás alapjai és használata Linux rendszeren

Mátó Péter <atya@fsf.hu>