Informatikai biztonság

2002. március 5.

Nyilvános kulcsú rendszerek a gyakorlatban

Megvalósítás, problémák, megoldások...

Endrõdi Csilla

BME MIT Ph.D. hallgató

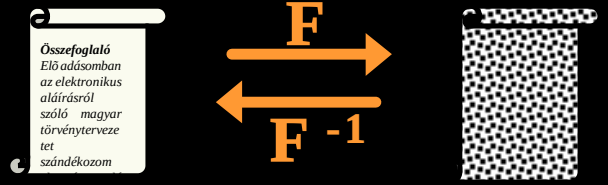
csilla@mit.bme.hu

Elõadásvázlat

- **Áttekintés – ismétlés**
  - *Nyilvános kulcsú kriptográfia*
  - *Felhasználási területei és hibái*
- **Gyakorlati alkalmazások**
  - *Kulcspárok, tanúsítvány*
  - *PGP, PKI (CA, CRL, TS, TSA)*
  - *Nyilvános kulcs nyilvánossága*
  - *Titkos kulcs titkossága*
  - *Idõkezelés*
  - *PKI elemei, szabványok, törvények*
- **Problémák**
  - *Idõkezelés, Tanúsítvány típusok, Ellenõrzési lánc, Kompatíbilitás, Országok közötti átjárhatóság, Algoritmus sajátosságok, Szöveg formátuma stb.*

Áttekintés – ismétlés

- **Rejtjelezés**

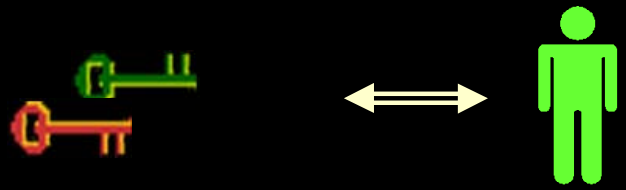


F_K: kulccsal paraméterezhetõ

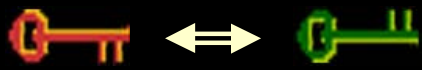
- **Aszimmetrikus kulcsú rejtjelezés** $F^{-1}_{K1} = F_{K2}$

- **Nyilvános kulcsú kriptográfia**

K1: nyilvános kulcs
K2: titkos kulcs



Speciális kapcsolat a kulcsok között:



- Egymás kiegészítõ párjai
- Egy kulcsnak csak egy párja van
- Egymásból gyakorlatilag kiszámíthatatlanok

Kulcsgeneráló eljárás garantálja

Nyilvános kulcsú kriptográfia

- Mindenki rendelkezik kulcspárral
- A nyilvános kulcsát mindenki nyilvánosságra hozza
- Titkos kulcsát szigorúan titokban tartja

Titkosítás:

Barbara

Barbara nyilvános kulcsa

Anna

Barbara titkos kulcsa

Kódolás Barbara *nyilvános* kulcsával

Dekódolás Barbara *titkos* kulcsával

Nyilvános kulcsú kriptográfia

- ***Rejtjelezés***

HIBA: ***Értelmes szöveg titkosítása***

➡ *Legfontosabb alkalmazása*

Helyes alkalmazás: *Nagy entrópiájú adat kódolására*
(pl. Session-key, Dokumentum lenyomat: lásd késõbbi példákban!)

◆

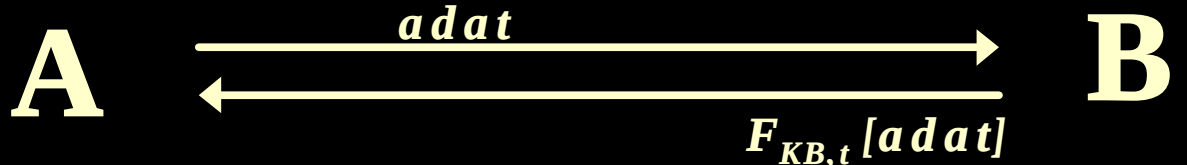
- ***Összetettebb adatbiztonsági funkciók:***
  - *Kulcsegyeztetõ protokollok*
  - *Partner azonosítás*
  - *Üzenet hitelesítés*
  - *Letagadhatatlanság*
  - *Digitális aláírás*
  - *Vak aláírás*
  - *Anonimitási protokollok*

Összetettebb adatbiztonsági funkciók

- ***Autentikáció***

„Amit az én nyilvános kulcsommal lehet dekódolni, az biztosan az én titkos kulcsommal készült.”

pl. ***Challenge & Response*** *módszere*



$$F_{KB,ny}\,[\,F_{KB,t}\,[adat]\,] \stackrel{?}{=} adat$$

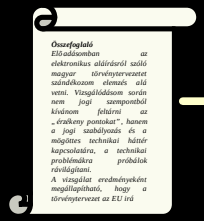
HIBA: *Undue signing*
Ha az „adat” jelentéssel bír.

Helyes alkalmazás: *Az „adat” kialakításában vegyen részt B is.*

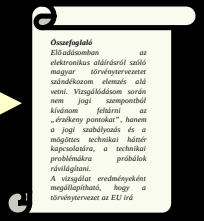
Letagadhatatlanság, a digitális aláírás

Aláíró fél

Ellenõrzõ fél



Megbízhatatlan hálózat

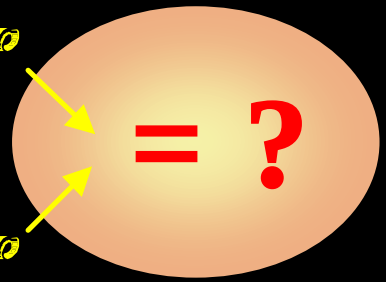


Lenyomatkészítés

Kódolás a titkos kulccsal

DIGITÁLIS ALÁÍRÁS

Lenyomatkészítés

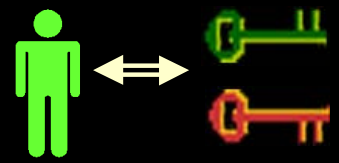


Dekódolás a nyilvános kulccsal

DIGITÁLIS ALÁÍRÁS

Gyakorlati alkalmazás

Nyilvános kulcsú kriptográfia



- *Mindenki rendelkezik nyilvános-titkos kulcspárral*
- *A nyilvános kulcsát mindenki nyilvánosságra hozza*
- *Titkos kulcsát szigorúan titokban tartja*

1. Nyilvános kulcs nyilvánossága

Kritikus pont:
A szereplõk nyilvános kulcsának közzététele **hiteles módon**.

- Személyes találkozás — **Nehézkes, bonyolult**
- Elektronikus formában elküldeni — **Támadás veszélye!**
- Megbízható harmadik fél által kiadott tanúsítvány

1. Nyilvános kulcs nyilvánossága

Megbízható harmadik fél (Trusted Third Party)
„Elektronikus igazolvány”: Certificate (Tanúsítvány)

Nyilvános kulcs és a személy összekapcsolása hitelt érdemlõ módon.

SZEMÉLYI IGAZOLVÁNY

Állandó adatok:
- név,
- anyja neve,
- szig. szám.

Biometriai adatok:
- fénykép, aláírás

Használat:
- biometriai adat ellenõrzése
- fizikai birtoklás: csak egyetlen darab létezik

Hitelesség bizonyítása:
- hatóság pecsétje,

Érvényesség:
- -tól, -ig

DIGITÁLIS IGAZOLVÁNY

Állandó adatok:
- név (*Common Name*),
- értelmezést segítõ adatok,
- serial number

Kriptográfiai adat:
- **nyilvános kulcs**

Használat:
- titkos kulcs birtoklása (kriptográfiai ellenõrzés)
- akármennyi létezhet

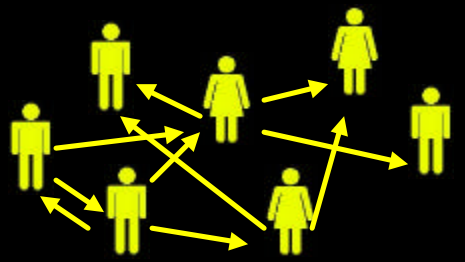
Hitelesség bizonyítása:
- hatóság digitális aláírása

Érvényesség:
- -tól, -ig

Tanúsítvány kiadása

PGP (Pretty Goog Privacy) / GPG (Gnu Privacy Guard)

- Open PGP: RFC 2440
- „Web of Trust” (Bizalmi háló)



- Bárki tanúsíthat.
- Egy kulcsot többen is tanúsíthatnak.

PGP kulcs szerverek

Elfogadás: akihez az irányított gráf mentén el tudok jutni.

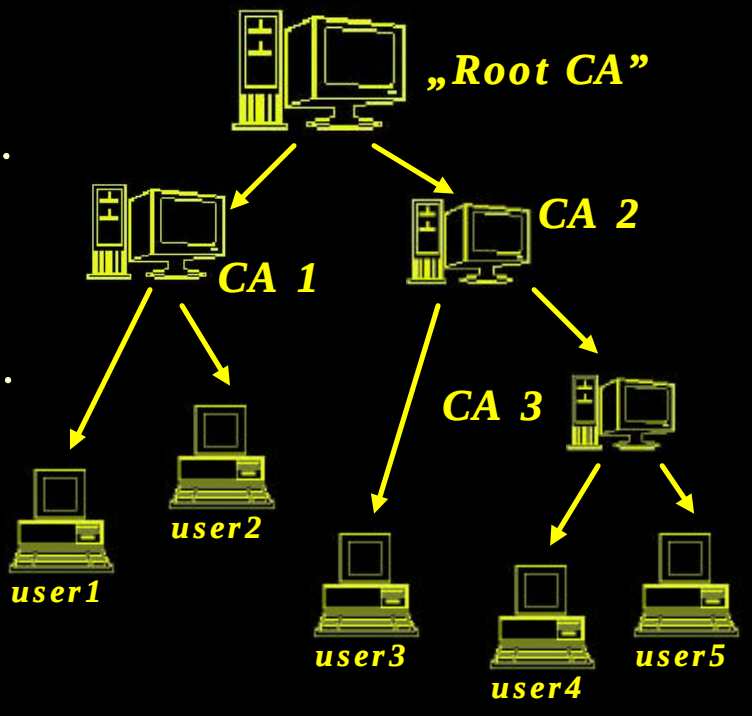
PKI (Public Key Infrastructure)

- ITU-T X.509, RFC 2459, 2510, 2511 stb.
- Certification Authority (CA)

- Csak CA bocsájthat ki tanúsítványt.
- Egy tanúsítványt pontosan egy CA ír alá.

! Root CA: bennük „megbízunk”

A többi certificate ellenõrizhetõ



Certificate (X.509)

```
issuer :/C=HU/L=Budapest/O=NetLock Halozatbiztonsagi
Kft./OU=Tanusitvanykiadok/CN=NetLock Teszt Tanusitvanykiado
subject:/C=HU/ST=/L=Budapest/O=/OU=/CN=Endrodi
Csilla/Email=csilla@sch.bme.hu
serial :0100Certificate:    Data:        Version: 3 (0x2)
        Serial Number: 256 (0x100)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=HU, L=Budapest, O=NetLock Halozatbiztonsagi Kft.,
OU=Tanusitvanykiadok, CN=NetLock Teszt Tanusitvanykiado
        Validity            Not Before: Apr 20 14:48:40 2000 GMT
            Not After : May 20 14:48:40 2000 GMT
        Subject: C=HU, ST=, L=Budapest, O=, OU=, CN=Endrodi
Csilla/Email=csilla@sch.bme.hu
        Subject Public Key Info:            Public Key Algorithm:
rsaEncryption
            RSA Public Key: (512 bit)                Modulus (512 bit):
                    00:91:ac:d8:b7:49:2e:85:a8:f5:cb:01:00:6e:4c:
                    2b:cf:3d:73:f8:24:d2:61:3b:cd:4a:09:e4:c5:e6:
                    5c:df:f8:36:4c:58:76:e0:6a:ef:6f:37:32:1b:56:
                    f7:2a:0a:0e:bf:11:25:cf:51:72:3b:55:c0:60:75:
                    05:46:c5:0c:47                Exponent: 65537
(0x10001)
```

```
      X509v3 extensions:            Netscape Comment:
                FIGYELEM! Ezen tanusitvany a NetLock Kft. Altalanos
Szolgaltatasi Felteteleiben leirt eljarasok alapjan keszult. A
hitelesites folyamatat a NetLock Kft. termekfelelosseg-biztosita vedi.
A digitalis alairas elfogadasanak feltetele az eloirt ellenorzesi eljaras
megtetele. Az eljaras leirasa megtalalhato a NetLock Kft. Internet
honlapjan a https://www.netlock.net/docs cimen vagy kerheto az
ellenorzes@netlock.net e-mail cimen. IMPORTANT! The issuance and the use
of this certificate is subject to the NetLock CPS available at
https://www.netlock.net/docs or by e-mail at cps@netlock.net.
            Netscape Cert Type:                 0xA0
            X509v3 Basic Constraints: critical              0....
            X509v3 Key Usage: critical                  ....
    Signature Algorithm: md5WithRSAEncryption
        63:4c:ff:12:aa:64:19:1a:0e:b2:ae:5e:5e:2f:fe:48:d2:8e:
        f7:28:ff:ce:34:b5:0d:af:17:ed:aa:55:db:62:af:67:66:30:
        93:08:44:b9:21:7a:60:a2:47:d6:5d:6a:11:47:30:fe:22:82:
        f5:b0:b1:2b:a7:aa:ed:0c:73:7a:e7:d5:99:82:08:73:a2:0d:
        13:e5:5e:21:7f:a0:23:9b:1e:ed:1c:bf:75:1b:5b:60:27:60:
        f2:3d:9c:d7:1c:39:43:b1:f8:af:af:74:17:bd:77:ec:cc:21:
        e1:89:eb:e7:ca:f2:bd:92:e5:42:a8:cf:4b:c3:f7:7f:76:6e:
f7:be
```

```
-----BEGIN CERTIFICATE-----
MIIE3DCCBEWgAwIBAgICAQAwDQYJKoZIhvcNAQEEBQAwgY4xCzAJBgNVBAYTAkhV
MREwDwYDVQQHEwhCdWRhcGVzdDEnMCUGA1UEChMeTmV0TG9jayBIYWxvemF0Yml6
dG9uc2FnaSBLZnQuMRowGAYDVQQLExFUYW51c2l0dmFueWtpYWRvazEnMCUGA1UE
AxMeTmV0TG9jayBUZXN6dCBUYW51c2l0dmFueWtpYWRvMB4XDTAwMDQyMDE0NDg0
MFoXDTAwMDUyMDE0NDg0MFowfDELMAkGA1UEBhMCSFUxCTAHBgNVBAgTADERMA8G
A1UEBxMIQnVkYXBlc3QxCTAHBgNVBAoTADEJMAcGA1UECxMAMRcwFQYDVQQDEw5F
bmRyb2RpIENzaWxsYTEgMB4GCSqGSIb3DQEJARYRY3NpbGxhQHNjaC5ibWUuaHUw
XDANBgkqhkiG9w0BAQEFAANLADBIAkEAkazYt0kuhaj1ywEAbkwrzz1z+CTSYTvN
SgnkxeZc3/g2TFh24GrvbzcyG1b3KgoOvxElz1FyO1XAYHUFRsUMRwIDAQABo4IC
nDCCApgwggJgBglghkgBhvhCAQ0EggJRFoICTUZJR1lFTEVNISBFemVuIHRhbnVz
aXR2YW55IGEgTmV0TG9jayBLZnQuIEFsdGFsYW5vcyBTem9sZ2FsdGF0YXNpIEZl
bHRldGVsZWliZW4gbGVpcnQgZWxqYXJhc29rIGFsYXBqYW4ga2VzenVsdC4gQSBo
aXRlbGVzaXRlcyBmb2x5YW1hdGF0IGEgTmV0TG9jayBLZnQuIHRlcm1la2ZlbGVs
b3NzZWctYml6dG9zaXRhc2EgdmVkaS4gQSBkaWdpdGFsaXMgYWxhaXJhcyBlbGZv
Z2FkYXNhbmFrIGZlbHRldGVsZSBheiBlbG9pcnQgZWxsZW5vcnplc2kgZWxqYXJh
cyBtZWd0ZXRlbGUuIEF6IGVsamFyYXMgbGVpcmFzYSBtZWd0YWxhbGhhdG8gYSBO
ZXRMb2NrIEtmdC4gSW50ZXJuZXQgaG9ubGFwamFuIGEgaHR0cHM6Ly93d3cubmV0
bG9jay5uZXQvZG9jcyBjaW1lbiB2YWd5IGtlcmhldG8gYXogZWxsZW5vcnplc0Bu
ZXRsb2NrLm5ldCBlLW1haWwgY2ltZW4uIElNUE9SVEFOVCEgVGhlIGlzc3VhbmNl
IGFuZCB0aGUgdXNlIG9mIHRoaXMgY2VydGlmaWNhdGUgaXMgc3ViamVjdCB0byB0
aGUgTmV0TG9jayBDUFMgYXZhaWxhYmxlIGF0IGh0dHBzOi8vd3d3Lm5ldGxvY2su
bmV0L2RvY3Mgb3IgYnkgZS1tYWlsIGF0IGNwc0BuZXRsb2NrLm5ldC4wEQYJYIZI
AYb4QgEBBAQDAgCgMA8GA1UdEwEB/wQFMAMBAQAwDgYDVR0PAQH/BAQDAgCgMA0G
CSqGSIb3DQEBBAUAA4GBAGNM/xKqZBkaDrKuXl4v/kjSjvco/840tQ2vF+2qVdti
r2dmMJMIRLkhemCiR9ZdahFHMP4igvWwsSunqu0Mc3rn1ZmCCHOiDRPlXiF/oCOb
Hu0cv3UbW2AnYPI9nNccOUOx+K+vdBe9d+zMIeGJ6+fK8r2S5UKoz0vD9392bve+
-----END CERTIFICATE-----
```

2. Titkos kulcs titkossága

Csak a tulajdonos használhassa! **(azonosítás)**
Jelszóval védett file, Smart card, Biometria

Kritikus pont: ***Titkos kulcs elvesztése/kompromittálódása***

Veszély: A kulcsot birtokló **hitelesnek tûnõen** aláírhat az igazi tulajdonos nevében.
A hamisíthatatlanság, egyediség, letagadhatatlanság megszûnik.

Teendõ:
A kulcspár használatának azonnali letiltása.

Tanúsítvány visszavonási lista
Certificate Revocation List (CRL)

A visszavonást megelõzõen készített aláírásoknak érvényesnek kell maradniuk!

Fontos: Minden aláírás és a visszavonás idõpontjának rögzítése.

3. Az idõkezelés

Ki rögzíti az idõpontot?

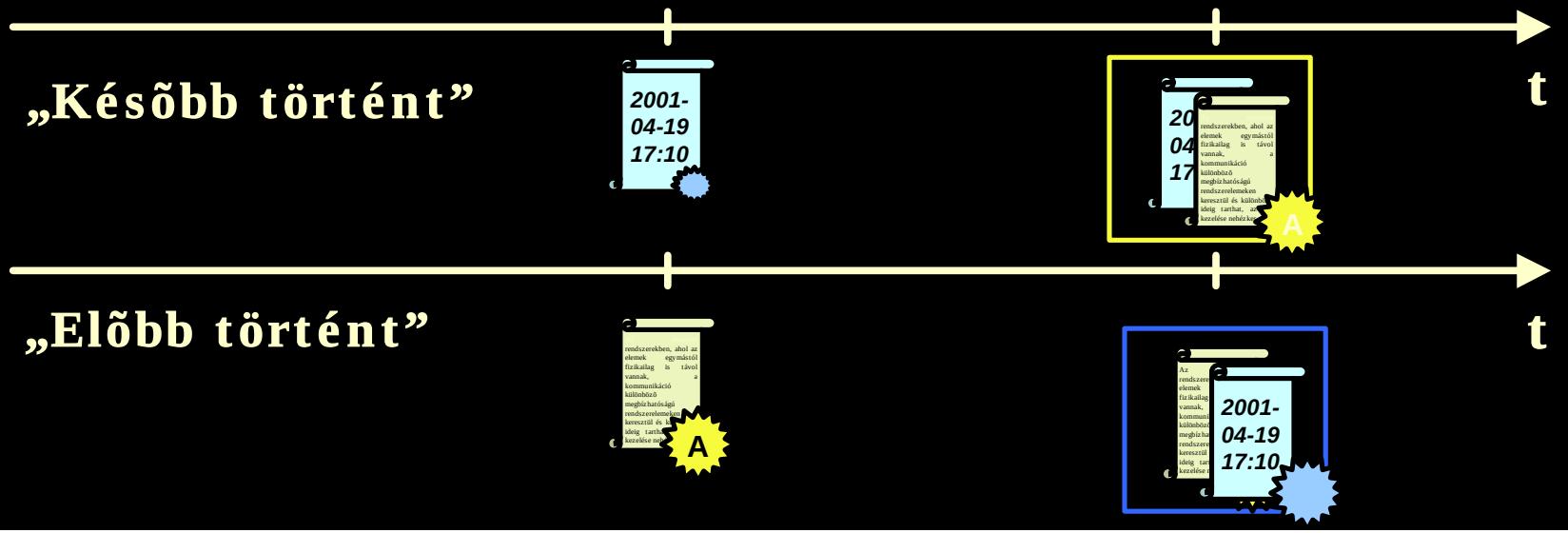
Aláírást végzõ személy

- Tévedés
- Visszaélés lehetõsége

Megbízható harmadik fél: Time Stamping Authority (TSA)

Idõbélyegzõ (Time Stamp, TS)

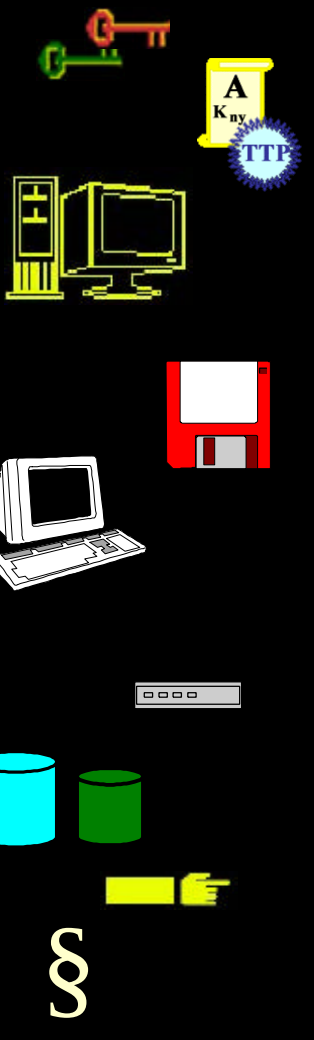
Elosztott rendszerekben az idõkezelés:



A Nyilvános Kulcsú Infrastruktúra (PKI)

Elemei

- A résztvevõk nyilvános-titkos **kulcspárjai**,
- A **tanúsítványok**,
- A hitelesítés szolgáltató (CA) és az idõbélyegzõ szolgáltató (TSA),
- A kulcsok létrehozásához és tárolásához, valamint az elektronikus aláírás létrehozásához és ellenõrzéséhez szükséges **szoftver** és **hardver eszközök**,
- A kommunikációhoz szükséges **hálózati elemek**,
- Az **adatbázisok**,
- A biztonsági **elõírások**,
- A **jogi szabályozás**



Szabványok, ajánlások

- Information Telecommunication Union (ITU)
  X.509 *Public-key and attribute certificate frameworks*
- Internet Engineering Task Force (IETF)
  Public Key Infrastructure X.509 (PKIX) Working Group
  X.509 v3, CRL v2 Certificate and CRL Profile (RFC 2459)
  Certificate Management Protocol (CMP, RFC 2510)
  Online Certificate Status Protocol (OCSP, RFC 2560)
  Certificate Management Request Format (CRMF, RFC 2511)
  Time Stamp Protocols (TSP, **RFC 3161**)

Elektronikus aláírás törvény

- EU direktíva (1999/93/EK)
  Haladék: 2001. júliusáig
- *Magyarországon: 2001. nyár*
  - Technológia független
  - X.509-et veszi alapul
- *Végrehajtási utasítások kidolgozás alatt*

Érdekes problémák

1. CA-k hibázása

Kritikus pont a felhasználó adatainak ellenõrzése!

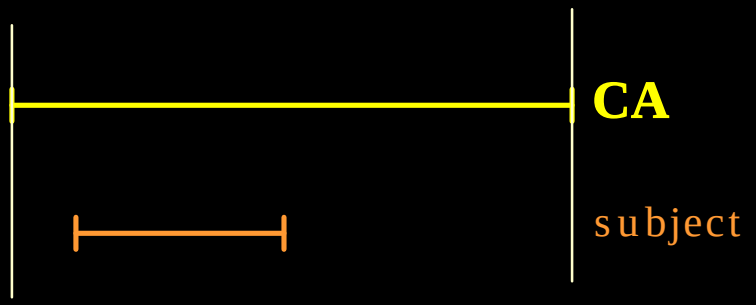
2. CRL vizsgálata

Sok esetben nem használják, ha igen, mikori, honnan származik… ?

3. Idõkezelés

Kettõs idõbélyeg

Szûkülõ idõintervallumok



4. Tanúsítvány típusa

Magánszemély / beosztás

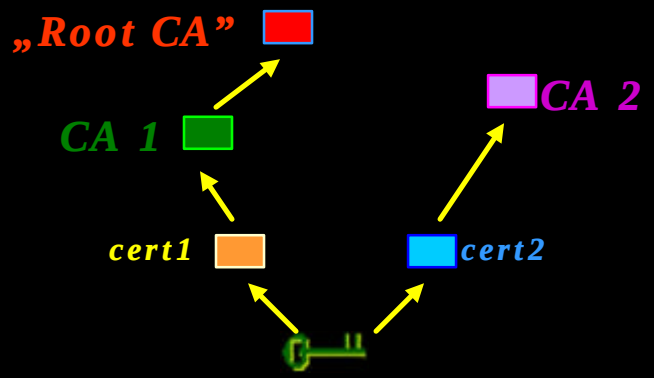
Nem csak embereknek lehet rá szüksége

Érdekes problémák

5. Certificate ellenõrzése

Ellenõrzási lánc nem egyértelmû

Kapott / tárolt certificate-ek



6. Kulcsgenerálás

Ki generálja a kulcsot?

User / központ

7. Algoritmus típusának ellenõrzése

RSA/ECC: más biztonságos kulcsméret

8. Certificate-ek kompatíbilitása

Országspecifikus attributumok

9. Mit írtunk alá… ?

„Csak szöveg”: Mit jelent pontosan? (Word document, Rich Text Format, makrók?)

„Rejtett” mezôk

Záró szavak

- A nyilvános kulcsú kriptográfia által létrehozható szolgáltatásokra szükségünk van
  - Elektronikus kereskedelem
  - Kommunikáció
  - Állami ügyintézés stb.
- Rendkívül sok hibalehetõség!
  - Rendkívül sok téveszme
  - Leggyengébb láncszem elve (hiányzó láncszemek...)
- Fel kell még hozzá nõni...
  - Hamis biztonságérzet, alaptalan veszélyérzet: egyik sem jó.
  - Sok feladat vár még ránk!

Endrõdi Csilla

<csilla@mit.bme.hu>