Elektronikus aláírás

Dr. Bakonyi Péter
c.docens

Mi az „aláírás”?

- Formailag valamilyen „szöveg” alatt, azt jelenti, hogy
  - valamit elfogadok
  - valamit elismerek
  - valamiről kötelezettséget vállalok
- Azonosítja az elfogadót, elismerőt
- Fontos: üres szöveget nem lehet aláírni!

Hagyományos aláírás - digitális aláírás

Nagy a hasonlóság:

1. van egy okirat
   digitális okirat - elektronikus eszközökkel megvalósítva
2. tartalmát elismeri, elfogadja az aláíró
   elektronikus tartalom változatlanságát (**integritását**) biztosítani kell
3. dátum szükséges
   ez a „timestamp” - amit a **date-server** biztosít
4. az aláírót ismerni kell
   egyértelmű azonosítás szükséges

Elektronikus aláírási törvény

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény (a továbbiakban: Eat.) hatálya az elektronikus aláírással kapcsolatos szolgáltatást végző, az elektronikus aláírással kapcsolatos szolgáltatást igénybe vevő, illetőleg elektronikus aláírást felhasználó természetes, illetve jogi személyre vagy jogi személyiség nélküli szervezetre, az elektronikus aláírással kapcsolatos szolgáltatásra és az elektronikus aláírás felhasználásának egyes kérdéseire terjed ki. A törvény szabályozza a hitelesítés-szolgáltatók tevékenységét, az időbélyegzést és az archiválást is, valamint az elektronikus iratkezelés alapvető kategóriáit. A törvény az elektronikus aláírásnak három fajtáját definiálja: az egyszerű-, a fokozott biztonságú- és a minősített elektronikus aláírást. Az aláírások és dokumentumok egyes típusaihoz fűződő jogkövetkezmények attól függően változnak, hogy az aláírás milyen biztonsággal azonosítja az elektronikus adatok szerzőjét és tartalmát. A családjogi és az öröklési jogi jogviszonyokra nem terjed ki a törvény hatálya.

1. A digitális okirat

- Digitális aláírás törvény
  - 2001. évi XXXV. törvény
- Ebben
  - elektronikus dokumentum: bármi
    - elektronikus irat: ami szöveges
      - elektronikus okirat: ami alá van írva

Digitális aláírás fajtái

- Egyszerű
  - csak azonosításra jó – nem alkalmas a biztonságos azonosításra
- Fokozott biztonságú
  - Alkalmas az aláíró azonosítására + integritás ellenőrzésére- nyilvános kulcsú technológiával készült
- Minősített – fokozott biztonságú-minősített tanusítvány-jogilag érvényesíthető
  - azonosításra + integritás ellenőrzésére
  - az aláíró „eszköz” biztonságát 3. fél garantálja

2. Integritás biztosítása

Egyszerű elv:

- minden dokumentumhoz egy fix hosszú ellenőrző szám
  - ami dokumentumonként **különböző**
  - dokumentum **méretétől nem függ**
  - biztonsággal **reprodukálható**
  - az ellenőrző számból **nem lehet visszafelé** a dokumentumot előállítani (egyirányú függvény)

Ellenőrző szám = „Üzenet kivonat”

- Más elnevezések
  - magyarul: **ujjlenyomat**
  - angolul: **message digest** vagy **hash**
- Több algoritmus létezik
  - MD5 a legelterjedtebb
  - mások: MD4, SHA, CRC
- MD5 lényege:
  - minden dokumentumhoz 128 bites (32 hexa) azonosító

Példa hash-re

There is $1500 in the blue box.

`05f8cfc03f4e58cbee731aa4a14b3f03`

There is $1100 in the blue box.

`d6dee11aae89661a45eb9d21e30d34cb`

The meeting last week was swell.

`050e3905211cddf36107ffc361c23e3d`

Mire jó a hash?

- Megváltozik a hash, ha
  - valaki **akár egyetlen betűt is átírt** a szövegben (lásd az 1500-1100 példát) vagy
  - valaki **akár egyetlen betűt hozzátett vagy elvett** a szövegből (amikor a végén nincs pont) vagy
  - valaki a **teljes szöveget kicseréli** (lásd amikor a szöveg teljesen más, mint az eredeti)

3. Dátumozás

- Alapkérdések
  - ki biztosítja a dátum-szervert (milyen cég)
  - hogyan lehet elérni
  - hogyan lehet megtudni a pontos időt :
  - Időbélyegző szolgáltató- műholdon, interneten vagy rádiókapcsolaton-
  - Minden egyes esetben el kell küldeni a szolgáltatónak, aki aláírva az időbélyegzőt visszaküldi az ügyfélnek

4. Azonosítás

- Szoros kapcsolatban a titkosítással
- Titkosítás fajtái
  - szimmetrikus (vagy egykulcsos)
  - nyilvános kulcsú (vagy két kulcsos)
    - sajátkulcs - nyilvános kulcs
- Ki „készíti” a kulcsot?
  - Egy cég --->> fokozott biztonságú
  - Egy cég --->> minősített

Nyilvános kulcsú titkosítás

- A kulcsokat egyszerre készítik, mert
  - a két kulcs függ egymástól
- Kulcskezelés
  - egyik kulcs: sajátkulcs (vagy titkoskulcs)
    - szigorúan védeni kell - pl. chipkártyán
  - másik kulcs: nyilvánoskulcs
    - publikálni - feltenni kulcsszerverre, átküldeni másnak

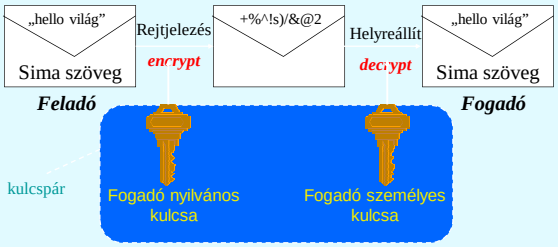
Digitális aláírás =

üzenet-kivonat sajátkulccsal titkosítva

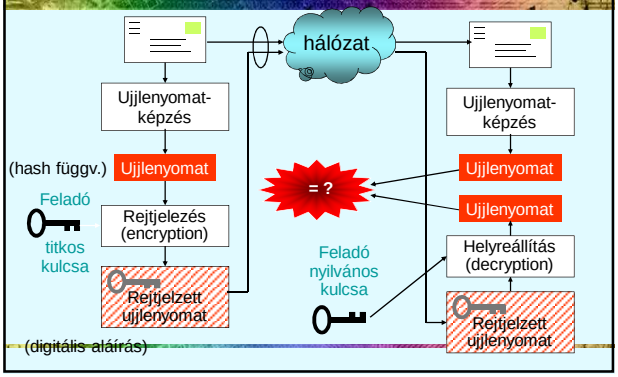
PKI alapok

Nyilvános kulcsú kriptográfia

Rejtjelezés aszimmetrikus kulcspárral



PKI alapok - digitális aláírás



Záró megjegyzések

- RSA algoritmus a nyilvános kulcsú titkosítás kulcsainak előállítására- lényege prim tényezőkre bontás-faktorizálás
- Az algoritmus a kulcspár előállításához használja a prímszámokat
- Biztonság „mérete”
  - 40 bites kódolt számhoz 1 millió körüli prím kell
  - 128 biteshez 20 számjegyű prím kell

Minden együtt: hogyan írunk alá digitálisan?

- 0. Van egy kulcspárunk
- 1. Elkészítjük az elektronikus okiratot
- 2. Elkészítjük az okirat hash-ét
- 3. Ezt a hash-t titkosítjuk a sajátkulcsunkkal

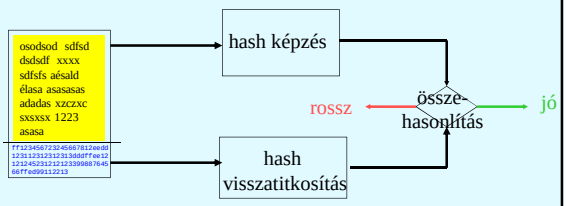
... ÉS KÉSZ !!!!

Hogyan ellenőrízzük a digitális aláírást?

- 0. Megtudjuk a készítő publikus kulcsát
  - pl. „kulcstartó szerverről” vagy az illető átküldi nekem
- 1. Beolvassuk az elektronikus okiratot
- 2. Elkészítjük az okirat hash-ét
  - ezt eltároljuk - ez MD5 esetén 32 db. hexa szám
- 3. Beolvassuk a küldött (és kódolt) hash-t
- 4. Ezt visszakódoljuk a készítő publikus kulcsával
- 5. A 2. és a 4. pontbeli értékeket összehasonlítjuk

... ÉS KÉSZ !!!!

Ellenőrzés ábrán



Mi rossz, ha rossz?

- valaki hozzányúlt az okirat szövegéhez (hozzáírt, kihúzott, átírt)
- nem az igazi aláíró kódolta a hash-t a saját kulcsával

PKI alapok - tanúsítvány

- Saját kulcs - nyilvános kulcs: egyikkel rejtjelzett üzenet csak a másikkal fejthető meg.
- Digit aláírás: doku ujjlenyomata saját kulccsal rejtjelezve. Csak egy személytől származhat.
- Bizalom alapja: egyértelmű kapcsolat a kulcspár és tulajdonosa között.
- Tanúsítvány: egyértelmű kapcsolatot bizonyít a nyilvános kulcs és tulajdonosa között.
- Hitelesítő központ - CA (Certification Authority)
  Az általa aláírt tanúsítvánnyal a CA igazolja a benne foglalt adatok valódiságát:
  - a nyilvános kulcs tulajdonosát,
  - a kulcs érvényességi idejét

Hitelesítő-szolgáltatás (CSP)

- Kulcskezelés (CA)
  - Kulcspár előállítás
  - Chipkártya előállítás
- Hitelesítő központ (CA)
  - Tanúsítvány kiadás
- Regisztráció (RA)
  - Azonosítás
- Címtár (DS)
  - Kulcs, tanúsítvány
  - Kulcsvisszavonás (CRL)
- Időbélyegző (TSA)
  - Hiteles idő
- Biztonságos archiválás

Köszönöm a figyelmet!