Elektronikus aláírás

Miért van szükség elektronikus aláírásra?
A nyiltkulcsú titkosítás.
Az elektronikus aláírás működése.
Jogi háttér
Hitelesítő szervezetek.

Miért van szükség elektronikus aláírásra?

Elektronikus adóbevallás
Számlakibocsátás, -befogadás
Szövegszerkesztővel megírt szerződések aláírása
Megrendelések
Visszaigazolások
Átutalások
Kötelező statisztikák

Az elektronikus aláírás tulajdonságai

Csak egyetlen személy tudja létrehozni az aláírást, így az nem hamisítható és letagadhatatlan.

Könnyen létrehozható és ellenőrizhető.

Olyan módon kapcsolódik az aláírt dokumentumhoz, hogy az az aláírást követően már nem módosítható észrevétlenül (integritás védelem).

Nyilvános kulcsú titkosítás

- Titkos-nyilvános kulcspár
  - Egymás kiegészítő párjai
  - Egy kulcsnak csak egy párja van
  - Egymásból kiszámíthatatlanok

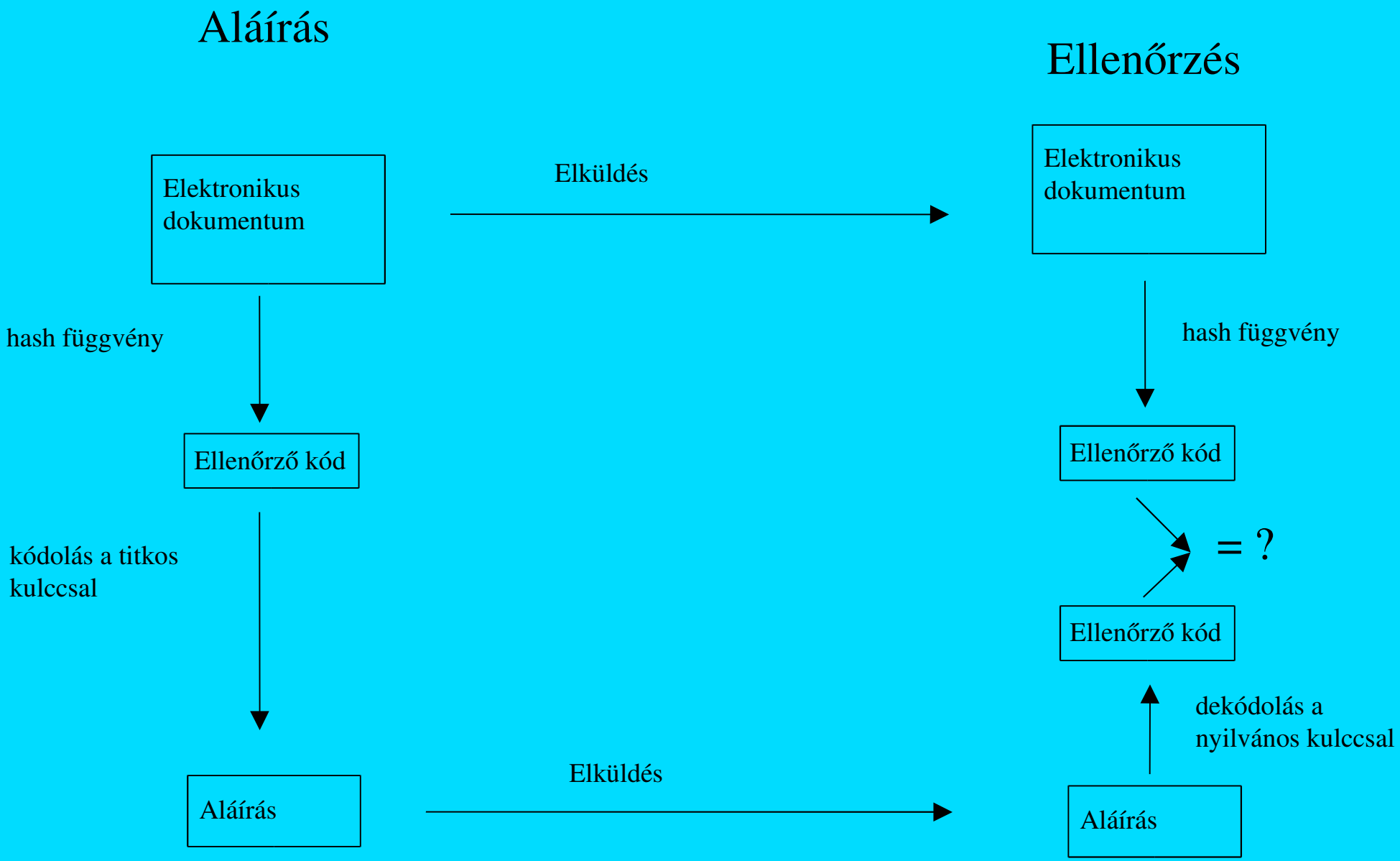
Nyilvános kulcsú titkosítás használata

- Rejtjelezés
  - Kódolás a titkos kulccsal
  - Dekódolás a nyilvános kulccsal
- Mindenki rendelkezik kulcspárral
  - A nyilvános kulcsát mindenki nyilvánosságra hozza
  - Titkos kulcsát szigorúan titokban tartja

Az ellenőrző kód (hash függvény)

- A dokumentum minden részlete befolyásolja az értékét.
- Az SHA-1 160 bites ellenőrző összeget állít elő $2^{160} \approx 10^{48}$

Elektronikus aláírás folyamata



Biztonságos aláíró eszközök

chipkártya olvasó

USB token

bővítőkártyák

Nyilvános kulcs közzététele

- Személyesen nehézkes
- Elektronikus úton könnyen támadható
- Megbízható harmadik fél által kiadott tanusítvány

Tanusítvány tartalma:

nyilvános kulcs
név, cím ...

Titkos kulcs elvesztése

- Akinél a kulcs van **hitelesnek tűnően** aláírhat az igazi tulajdonos nevében
- A kulcspár azonnali visszavonása
- A visszavonást megelőzően készített aláírásoknak érvényesnek kell maradniuk!
- Tanusítvány visszavonási lista
- Minden aláírás és a visszavonás időpontjának rögzítése

Az időkezelés problémája

- Ki rögzíti az időpontot?
  - Aláírást végző személy
    - Tévedés
    - Visszaélés
  - Megbízható harmadik fél
- Elosztott rendszerek időkezelése
  - Előbb történt
  - Később történt

Elektronikus aláírás törvény

2001. évi XXXV. törvény
az elektronikusan aláírt dokumentum meghatározott feltételekkel ugyanolyan bizonyító erővel rendelkezik, mint a hagyományos, papíron írt és aláírt irat.
A törvény három biztonsági fokozatot különböztet meg:
Az egyszerű elektronikus aláírásra példa egy elektronikus levél aláírása.
A fokozott biztonságú aláírás: alkalmasnak kell lennie az aláíró azonosítására, és egyedülállóan hozzá köthetőnek kell lennie. Csak olyan eszközzel hozható létre, amely kizárólag az aláíró befolyása alatt áll, és oly módon kell kapcsolódnia az aláírt dokumentumhoz, hogy azon az aláírást követő minden módosítás érzékelhető legyen.
A minősített elektronikus aláírásokkal szembeni további követelmény, hogy megfelelő technológiával rendelkező aláírás-létrehozó eszközzel állítsák elő, és hitelesítésére egy erre jogosult hitelesítés-szolgáltató tanúsítványt bocsásson ki. Ez a tanúsítvány igazolja, hogy az aláíró - akinek a személyazonosságát a hitelesítés-szolgáltató előzetesen ellenőrizte -, valóban az, akinek mondja magát.

Elektronikus számviteli bizonylat

A számviteli törvény 2002 januárjától hatályos módosítása alapján kizárólag az elektronikus aláírásról szóló törvény értelmében minősített elektronikus aláírással és időbélyegzővel ellátott elektronikus számla tekinthető érvényes számviteli bizonylatnak.

Az aláírás a kibocsátó egyértelmű azonosítására szolgál, az időbélyegző a bizolnylat utólagos módosítását zárja ki.

Az elektronikus aláírás jogi hatálya

Egyszerű aláírás:
az ilyen aláírás elfogadását megtagadni, bizonyító erejét kétségbe vonni önmagában azon az alapon, hogy elektronikus formában létezik, nem lehet.

Fokozott biztonságú aláírás:
úgynevezett egyszerű magánokirattal esik egy elbírálás alá bizonyító erő szempontjából: vagyis az irat hitelességét annak kell bizonyítania, aki hivatkozik rá.

Minősített biztonságú aláírás:
a minősített aláírással ellátott okirat viszont teljes bizonyító erejűnek minősül, tehát a benne foglalt nyilatkozat megtételét az ellenkező bizonyításáig valósnak kell tekinteni. Ekkor a bizonyítás azt terheli, aki az okirat tartalmának ellenkezőjét állítja.

Fokozott biztonságú szolgáltatók

GIRO Elszámolásforgalmi Rt.

Magyar Távközlési Részvénytársaság

Microsec Számítástechnikai Fejlesztő Kft.

MÁV INFORMATIKA Kereskedelmi, Szolgáltató és Tanácsadó Kft.

NetLock Informatikai és Hálózatbiztonsági Szolgáltató Kft.

Minősített szolgáltatók

MÁV INFORMATIKA Kereskedelmi, Szolgáltató és Tanácsadó Kft.

NetLock Informatikai és Hálózatbiztonsági Szolgáltató Kft.