MICROSEC
Számítástechnikai Fejlesztő Kft.

Az elektronikus aláírás és gyakorlati alkalmazása

Dr. Berta István Zsolt <istvan.berta@microsec.hu>

Microsec Kft.

Elektronikus aláírás (e-szignó)

- Az elektronikus aláírás a **kódolás** egy fajtája
- Elektronikus aláíráskor ún. aláírás-létrehozó adat alapján kódoljuk az aláírt dokumentumot.
- A dokumentum hitelességét a kódolt (aláírt) dokumentum „szerkezete” garantálja.
- A kódolás az aláírás-létrehozó adat nélkül nem végezhető el, de bárki meggyőződhet róla, hogy az aláírás kinek az aláírás létrehozó adatával készült.
- Az elektronikusan aláírt dokumentumhoz bizonyító erő kapcsolódik.

Miről fogok beszélni?

- Kriptográfiai bevezető
- Tanúsítványok
- Elektronikus aláírás
- Hogyan jelenik meg mindez a gyakorlatban?
- Hol használják e technológiát?
- Összefoglalás

Kriptográfiai bevezető

Kriptográfia: A titkosírásokkal, rejtjelezésekkel, kódolásokkal és ezek megfejtésével foglakozó tudományág.

Információ védelme kódolással

- Érzékeny információinkat védenünk kell
- A védelem lehet
  - fizikai (pl. fal, páncélszerkény, fegyveres őr),
  - logikai (pl. tűzfalak, kódolási módszerek),
  - szabályzati (pl. eljárásrendek, jogszabályok)
- A továbbiakban arról lesz szó, ha az információt kódolással védjük

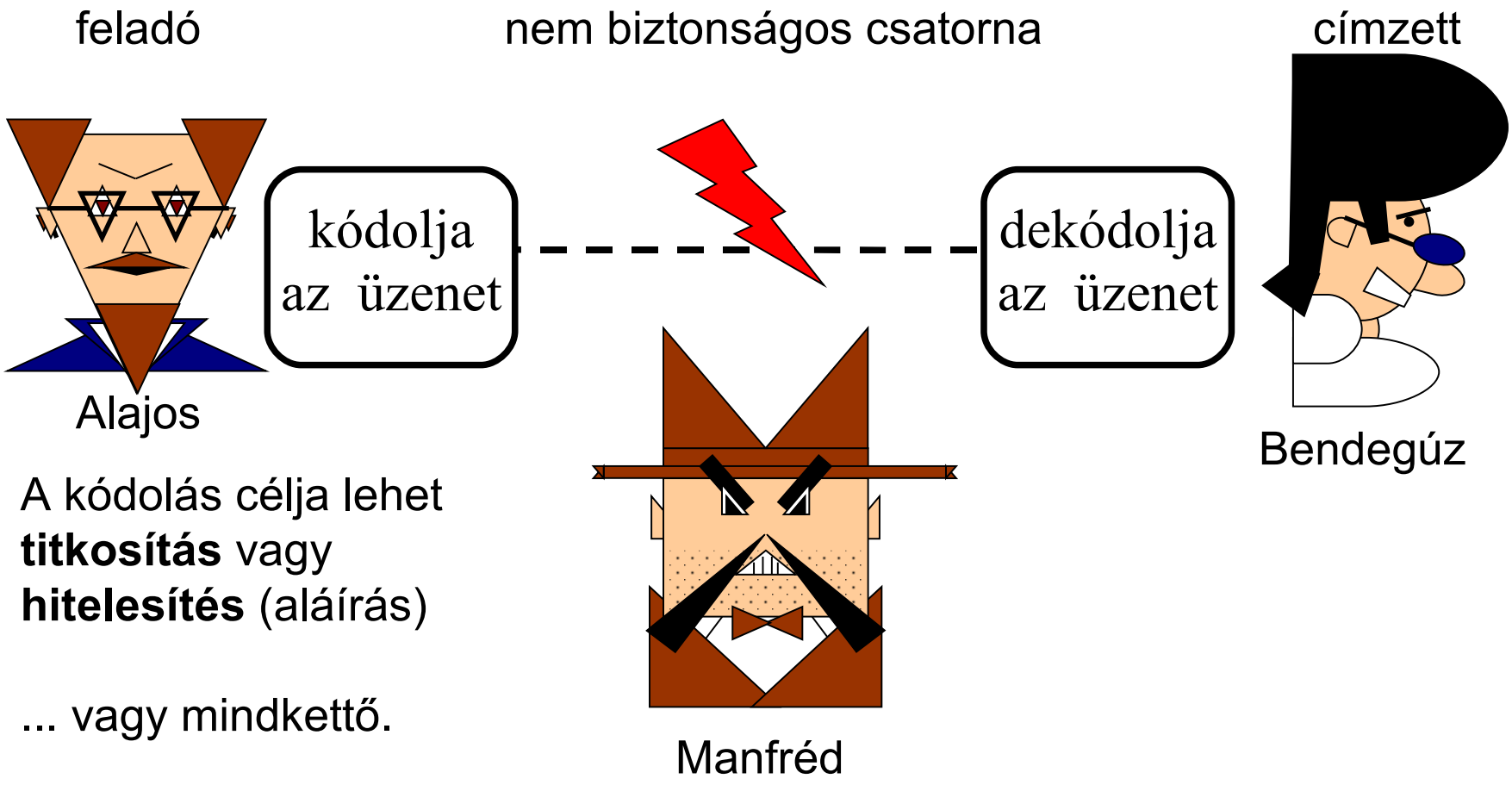
Milyen célt szolgálhat a kódolás?

- Tömörítés (forráskódolás)
  - az információ kisebb helyet foglaljon el
- Csatornakódolás
  - véletlen hibákkal szemben védekezünk
- Kriptográfiai kódolás (titkosítás, hitelesítés)
  - szándékos támadással szemben védekezünk

Kriptográfiai kódolás

- Az információt **szándékos támadással** szemben szeretnénk megvédeni.
- Ha azt szeretnénk, hogy illetéktelen felek
  - ne ismerhessék meg: **titkosítás**
    Megváltoztatjuk az információ szerkezetét.
    Pl.: **`ARANYALMA → BSBOZBMNB`**
  - ne módosíthassák észrevétlenül: **hitelesítés**
    Szabályosságot helyezünk el az információban.
    Pl.: **`ARANYALMA → ARANYALMA BSBOZBMNB`**
- Jellemzően arra épül, hogy egyes kódolásokat csak jogosult felek tudnak elvégezni.

Védelem a támadó ellen



- A kódolás célja lehet **titkosítás** vagy **hitelesítés** (aláírás)

  ... vagy mindkettő.

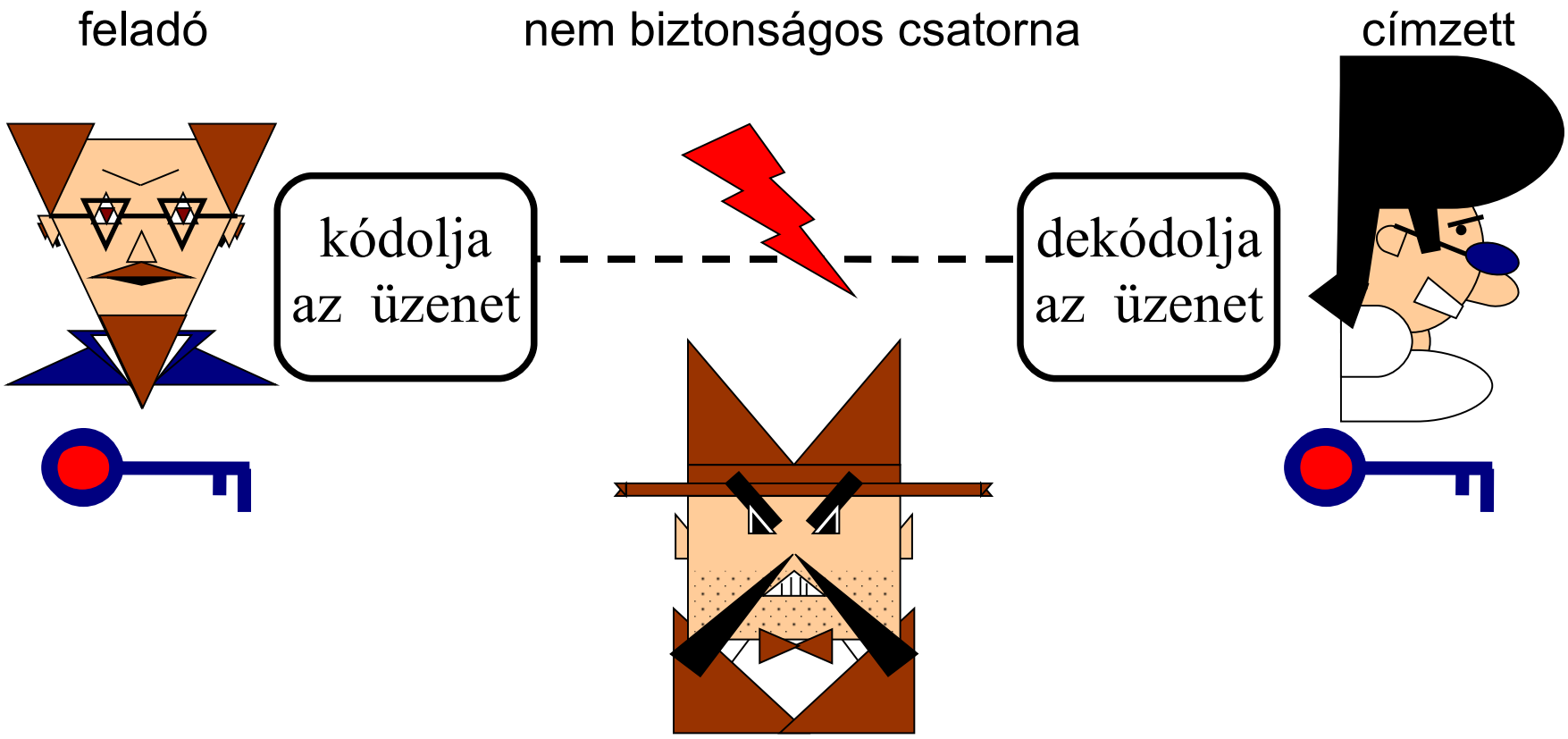
Ki végezheti el a kódolást?

- Bizonyos műveleteket csak a jogosult felek végezhessenek el. A támadó ne tudjon
  - kititkosítani (dekódolni),
  - hitelesíteni (pl.: aláírni jogosult fél nevében)
- Ötlet: Csak a jogosult felek ismerhessék az alkalmazott kódolási eszközöket (algoritmusokat).
- Hibái:
  - nagyon nehéz az algoritmust titokban tartani,
  - kevés „jó” algoritmust ismerünk.
- Nagyon rossz ötlet!

Kerckhoff feltétel (1883)

- A támadó ismerhesse az alkalmazott kódolási módszerek minden egyes részletét,
- kivéve a kódoló algoritmus egy paraméterét (ezt nevezzük „kulcs”-nak),
- a rendszer ekkor is legyen biztonságos.
- Ha a kódoló/dekódoló berendezések a támadó kezébe kerülnek, a kulcs cserélésével a rendszer tovább használható.
- A Kerckhoff feltétel alapvető, széles körben elfogadott alapelv.

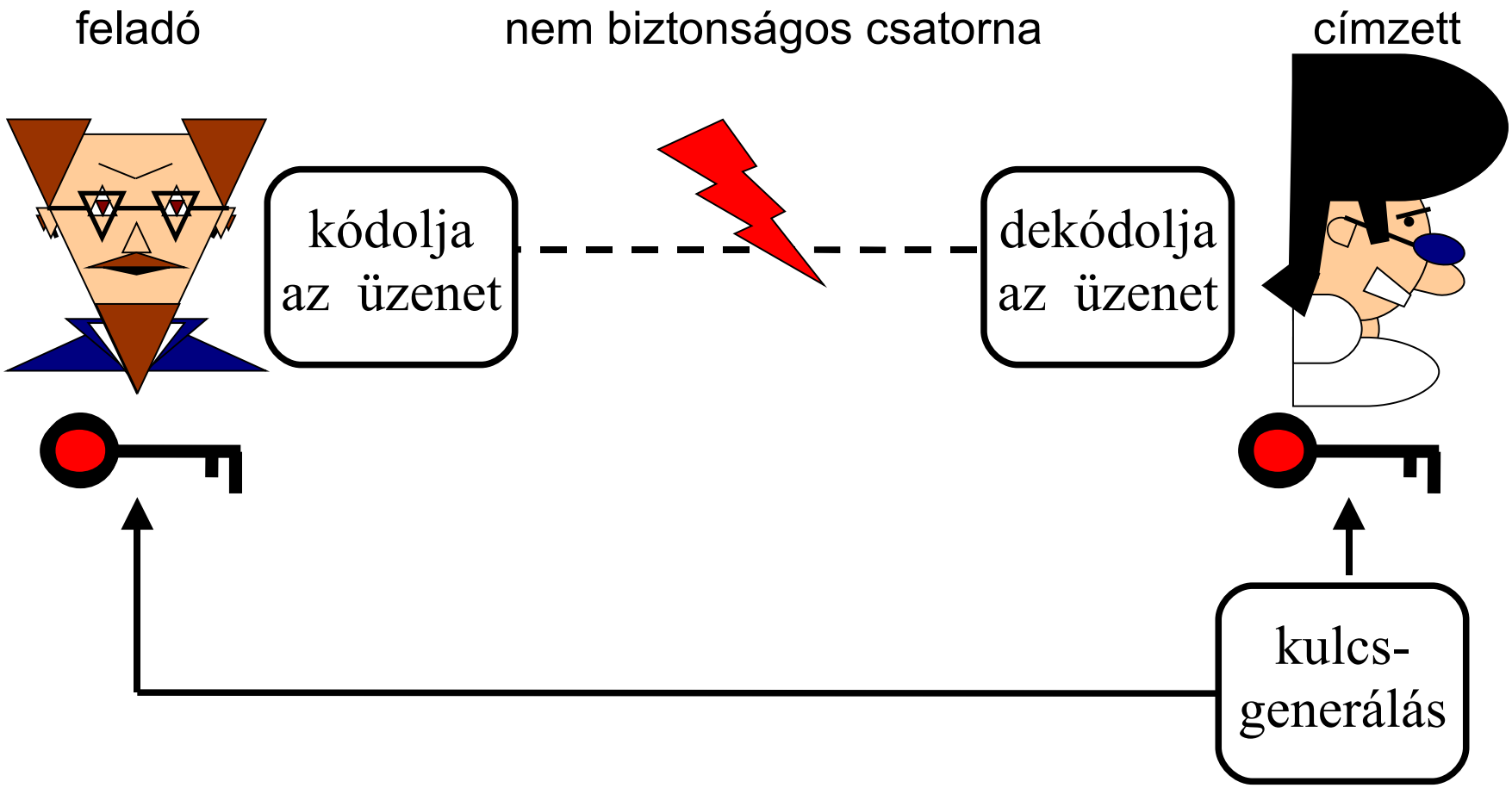
Kulcs


feladó
nem biztonságos csatorna
címzett
kódolja az üzenet
dekódolja az üzenet

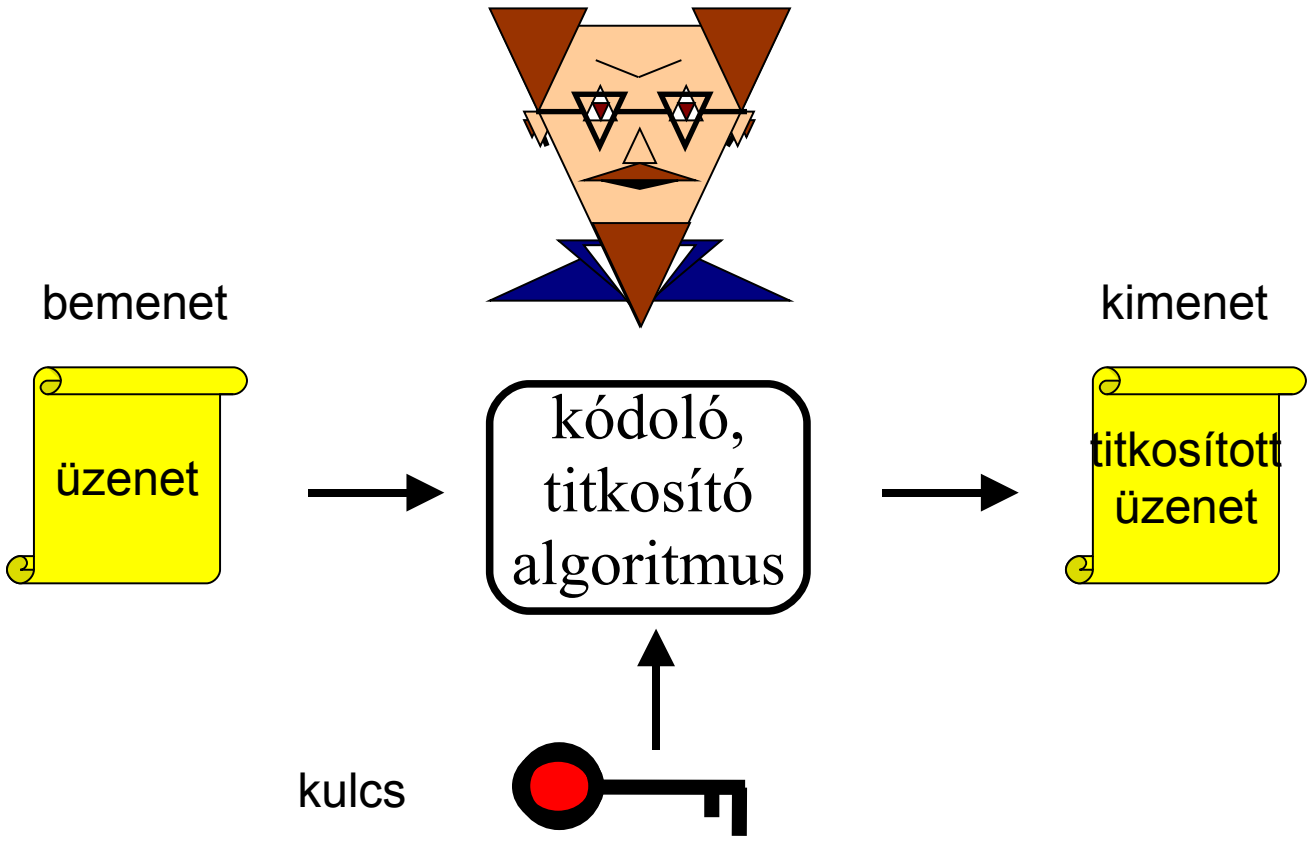
Kulcs

- A számítógépben minden információ (szöveg, kép, hang, videó stb.) megfeleltethető egy-egy számnak.
- A kódolás így egy matematikai műveletnek, a kulcs pedig egy számnak tekinthető.
- A támadó a kulcs kitalálásával megpróbálhatja megfejteni („megtörni”) a kódot, pl. végigpróbálhatja az összes lehetséges kulcsot.
- A kulcs hossza (kulcsméret) alapvetően meghatározza a rendszer biztonságát.
- A kulcsot véletlenszerűen kell kiválasztani, minden kulcs azonos eséllyel fordulhasson elő.

Szimmetrikus kulcsú kriptográfia



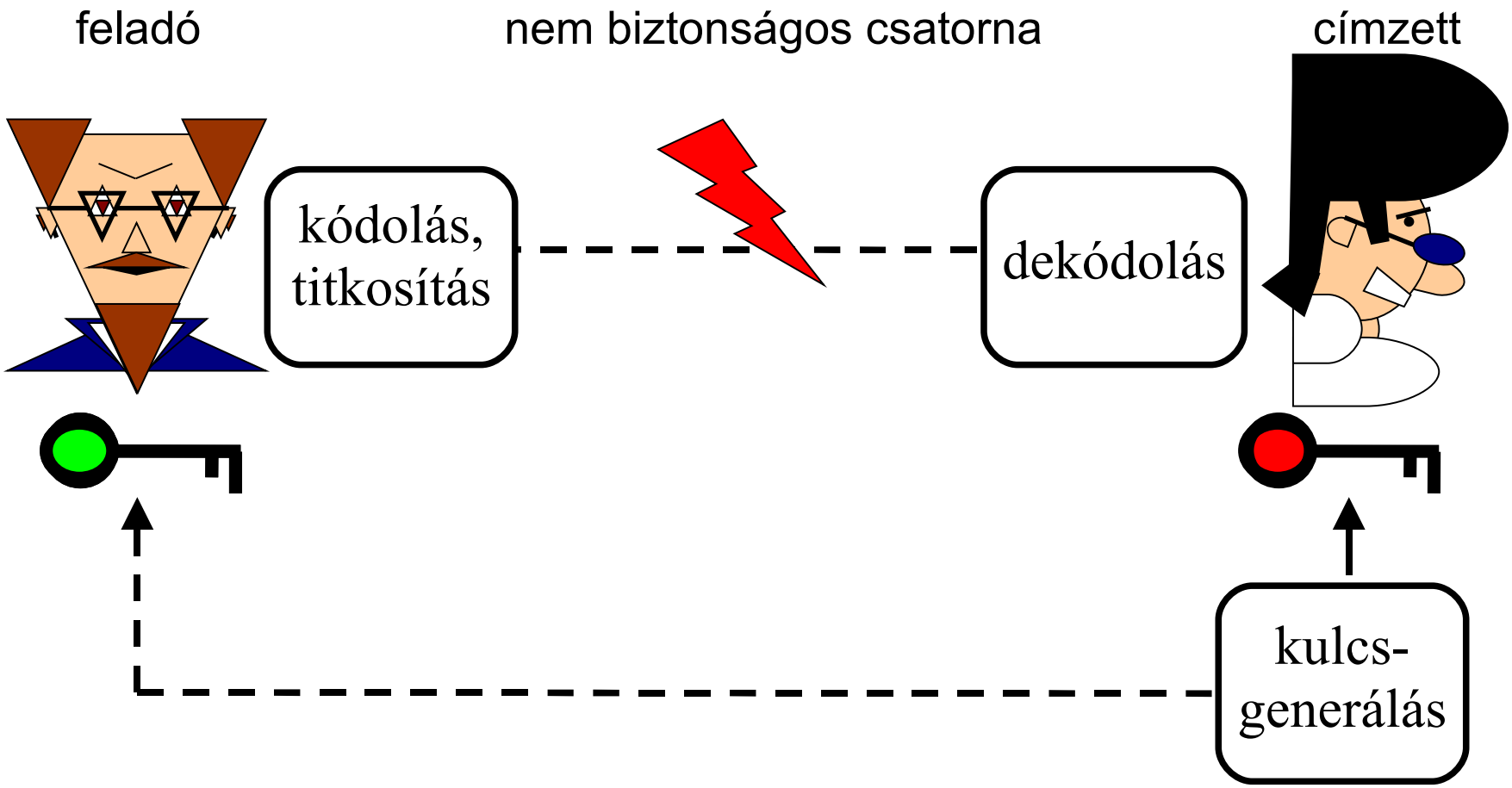
Pl. titkosítás



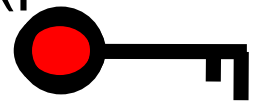
Szimmetrikus kulcsú kriptográfia

- Kódoláshoz és dekódoláshoz ugyanazt a kulcsot használjuk.
- A kulcs az egymással kommunikáló felek **közös titka**.
- A kulcsban biztonságos csatornán kell megegyezniük. (kulcstovábbítás, kulcscsere)
- A **kulcsot** titkosan kell eljuttatnunk, nem szabad, hogy a támadó megismerje.

Nyilvános kulcsú kriptográfia (1)



Nyilvános kulcsú kriptográfia (2)

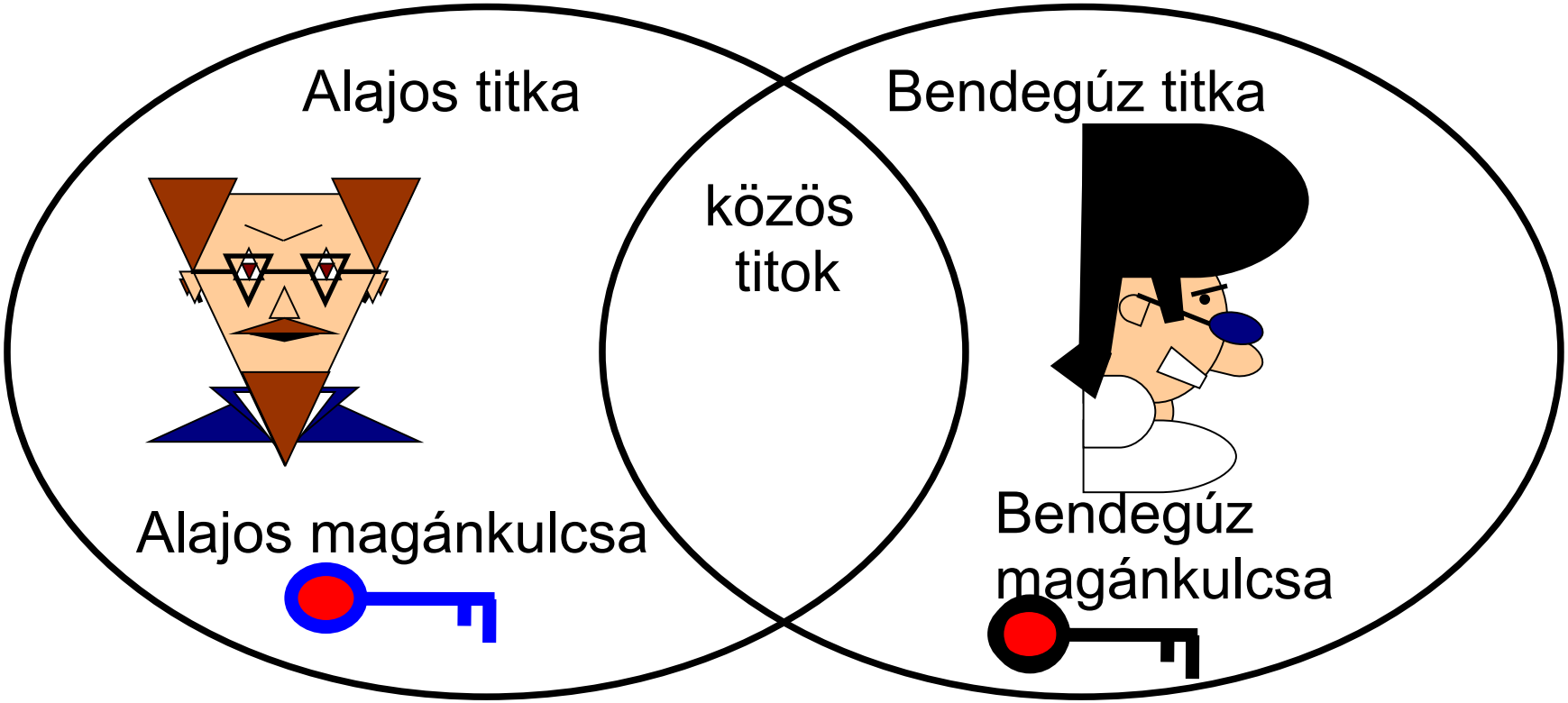
- Nyilvános kulcsú kriptográfiáról akkor beszélünk, ha a kódoláshoz és a dekódoláshoz nem ugyanazt a kulcsot használjuk.
- Elég az egyik kulcsot (pl. a dekódolót) titokban tartunk (magánkulcs), 
- a másik kulcsot (pl. a kódolót) akár nyilvánosságra is hozhatjuk (nyilvános kulcs). 
- Így nincs szükség közös titokra.
- A nyilvános kulcsot nem kell titkosan továbbítanunk, továbbíthatjuk nyilvános csatornán, de akár közzé is tehetjük.

Nyilvános kulcs és magánkulcs

- A nyilvános kulcs és a magánkulcs között matematikai összefüggés van,
- de a nyilvános kulcsból a magánkulcs nem számítható ki (hatékonyan).

- Titkosítás: kódolás a címzett nyilvános kulcsával, a címzett a saját magánkulcsával dekódolja.
- Aláírás: Kódolás a feladó magánkulcsával, a feladó nyilvános kulcsával bárki ellenőrizheti.

Minden résztvevőnek két kulcsa van

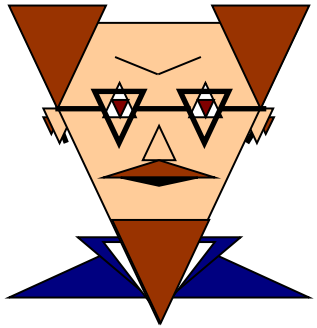


Titkosított üzenet küldése

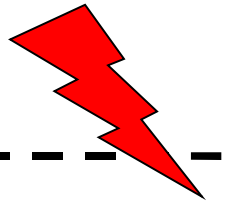
feladó

nem biztonságos csatorna

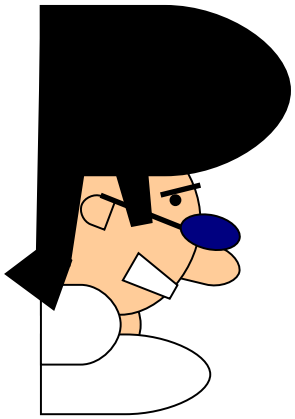
címzett

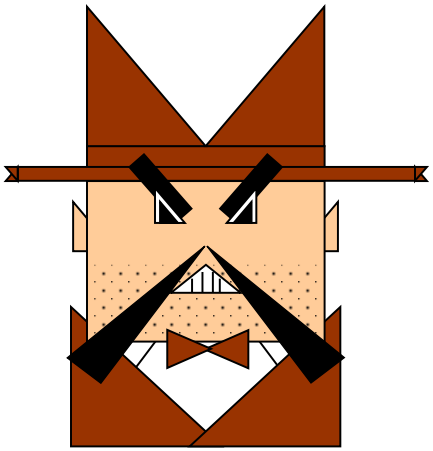


kódolja az üzenet



dekódolja az üzenet





kódolás a címzett nyilvános kulcsával

„titkosítás”

dekódolás a címzett magánkulcsával

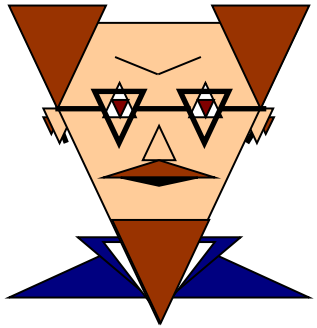
„visszafejtés”, dekódolás

Aláírt üzenet küldése

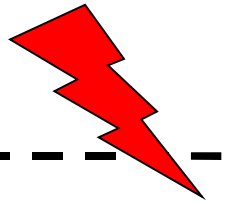
feladó

nem biztonságos csatorna

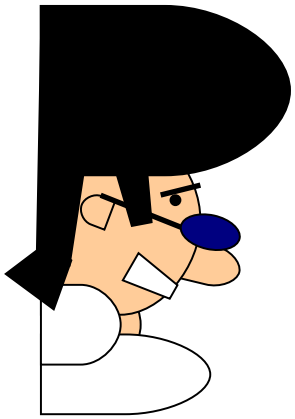
címzett

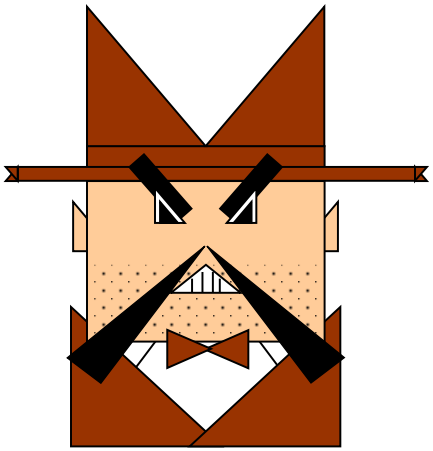


kódolja az üzenet

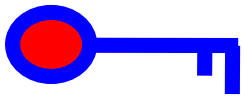


dekódolja az üzenet





kódolás a feladó magánkulcsával



„aláírás”

dekódolás a címzett nyilvános kulcsával

„aláírás ellenőrzése”

Összegzés

- Kriptográfiai kódolások segítségével szándékos támadások ellen védhetjük meg az információt.
  - Titkosság (illetéktelen fél ne ismerhesse meg),
  - Hitelesség (illetéktelen fél ne módosíthassa észrevétlenül)
- A nyilvános algoritmus valamilyen titkos információ (jelszó, szám) alapján működik. Ez a kulcs.
- Esetünkben kódoláshoz és dekódoláshoz különböző kulcsot használunk (nyilvános kulcsú kriptográfia)
  - Titkosítás: a címzett nyilvános kulcsával kódolunk, ő a saját magánkulcsával dekódol.
  - Aláírás: a saját magánkulcsunkkal kódolunk, mások a mi nyilvános kulcsunkkal ellenőrizhetik az aláírást.

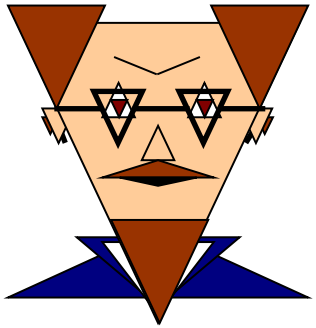
Tanúsítványok

A nyilvános kulcsot hitelesen kell megszerezni!

feladó

nem biztonságos csatorna

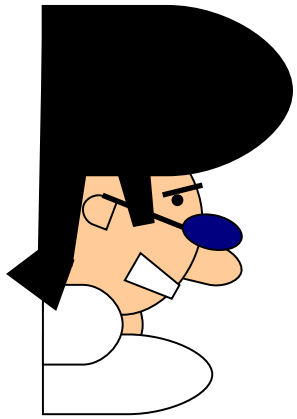
címzett



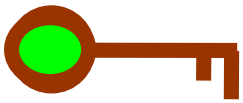
kódolja az üzenet

dekódolás + kódolás

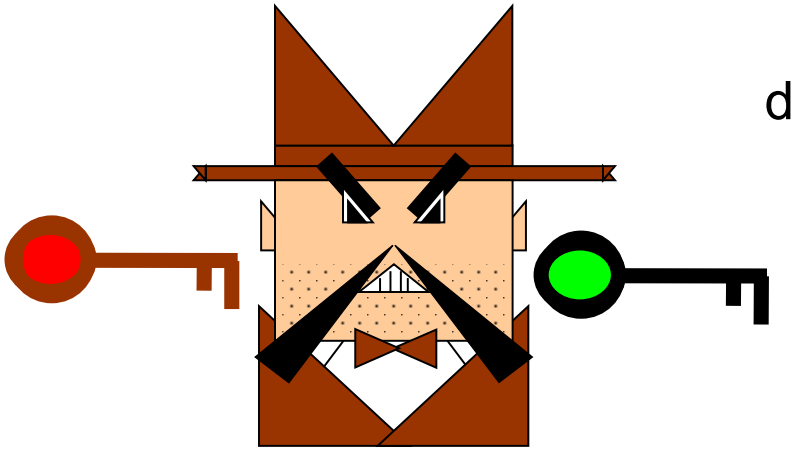
dekódolja az üzenet



kódolás a címzett nyilvános kulcsával



„titkosítás”

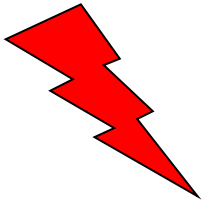


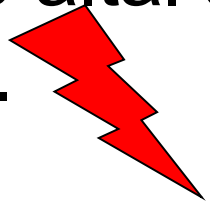
dekódolás a címzett magánkulcsával

„visszafejtés” dekódolás

Miért fontos a nyilvános kulcs hitelessége?

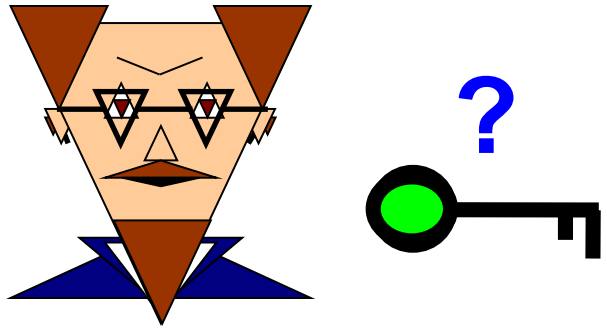
- Tudnunk kell, hogy kinek a nyilvános kulcsát használjuk, különben lehet, hogy éppen a támadóval kommunikálunk „biztonságosan”.
- Ha a támadó nyilvános kulcsával titkosítunk, a titkosított üzenetet a támadó tudja majd visszafejteni.
- Ha a támadó nyilvános kulcsával ellenőrzünk egy aláírást, a támadó által aláírt üzeneteket fogadjuk el hitelesnek.



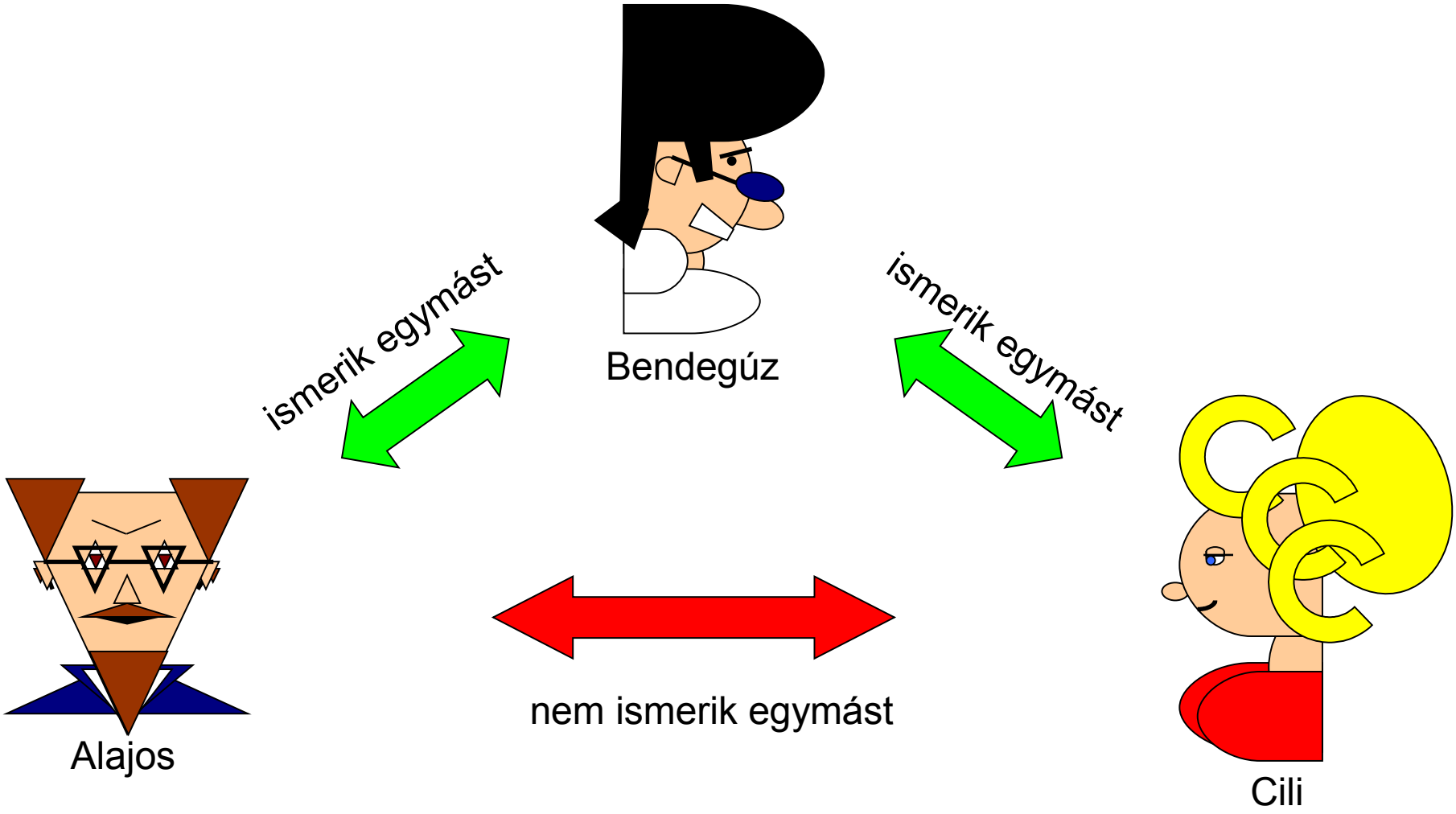


A nyilvános kulcs hitelessége

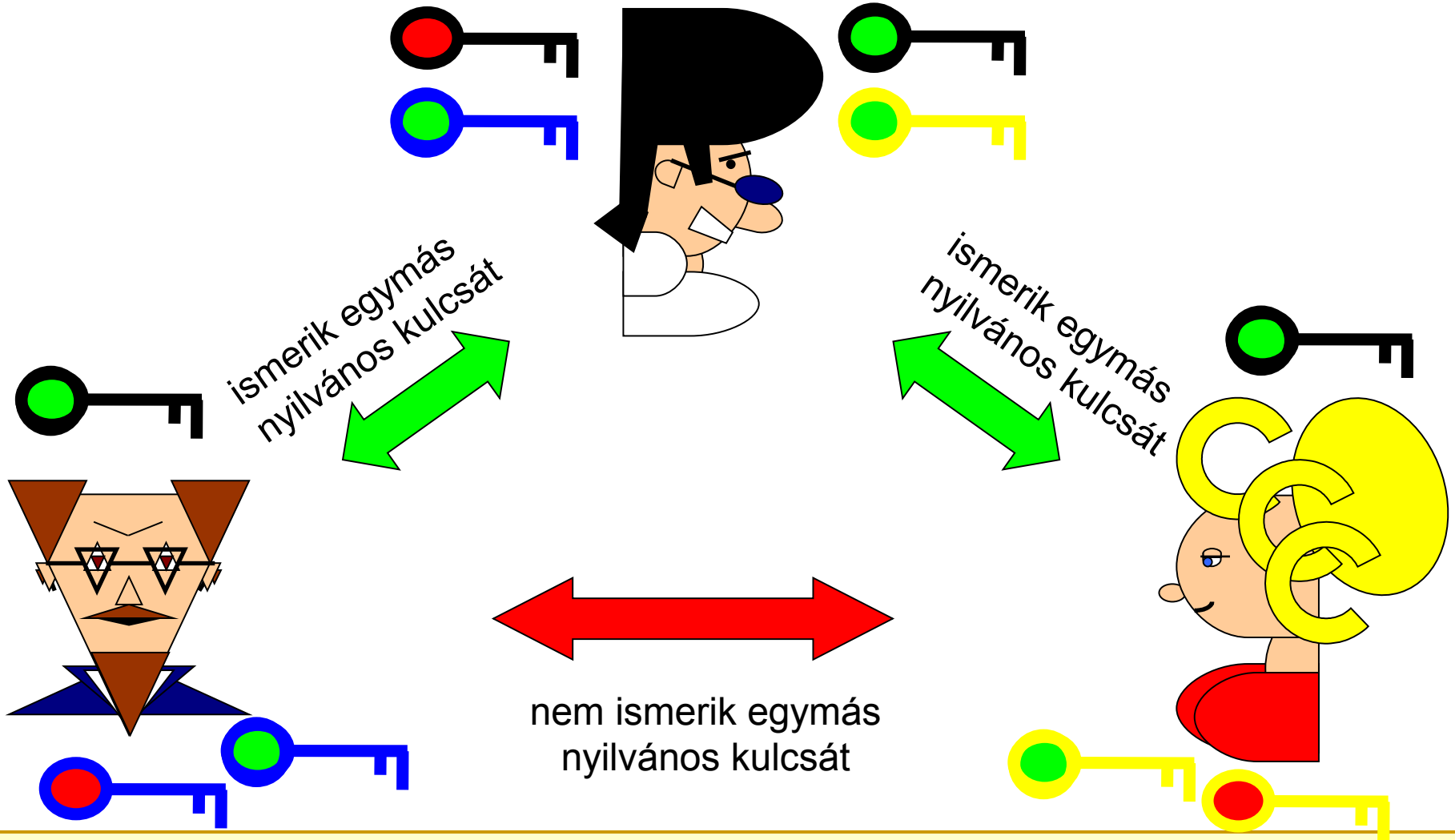
- Ha ismerjük valakinek a nyilvános kulcsát
  - titkosított üzenetet tudunk küldeni neki
  - ellenőrizni tudjuk az aláírását
  - stb.
- Hogyan jutunk hozzá valakinek a nyilvános kulcsához?
- Honnan tudjuk, hogy valóban az az ő nyilvános kulcsa?



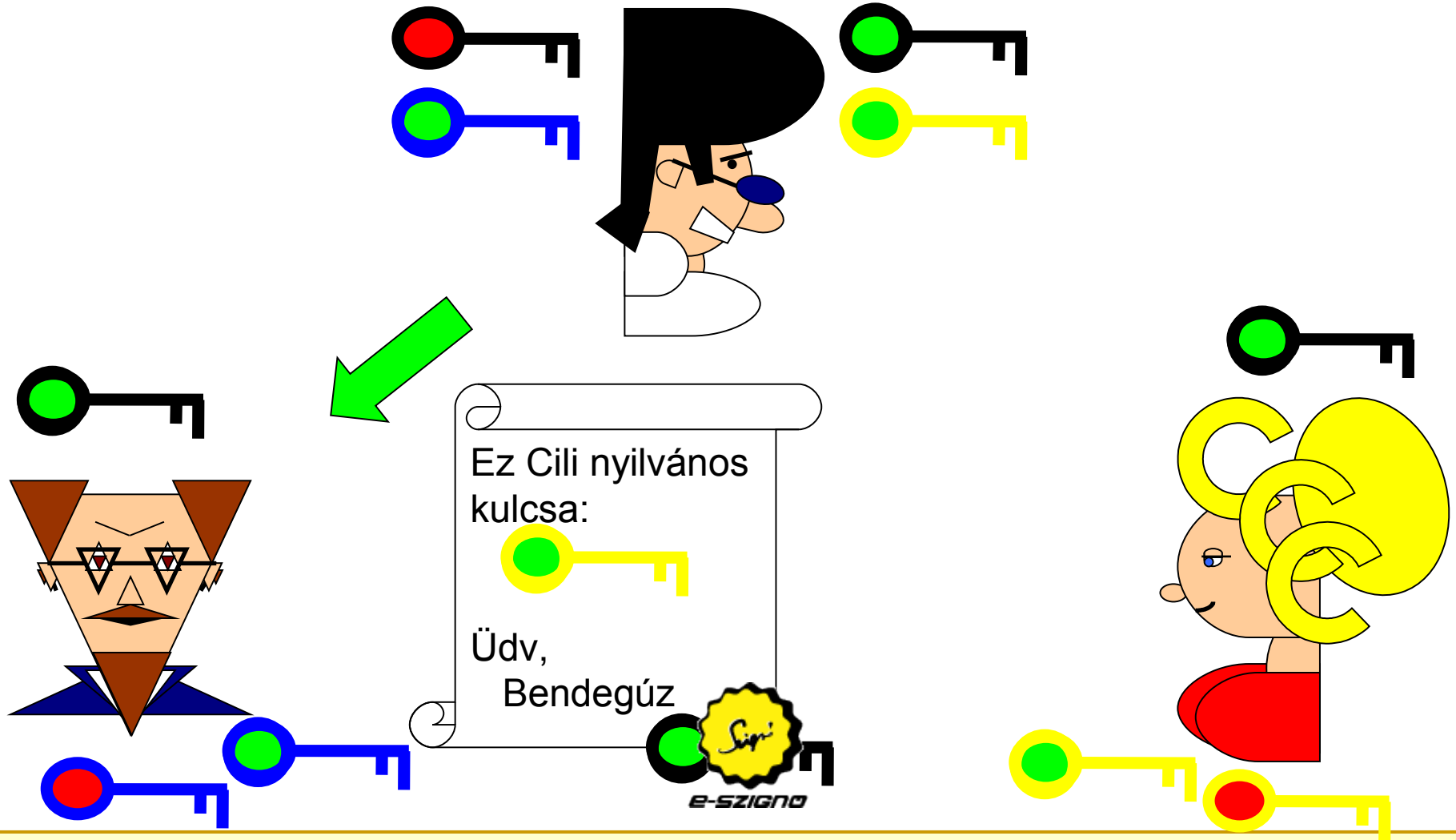
Közös megbízható ismerős



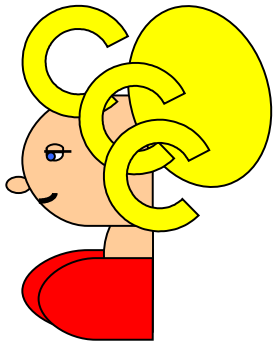
Megbízható harmadik fél (1)



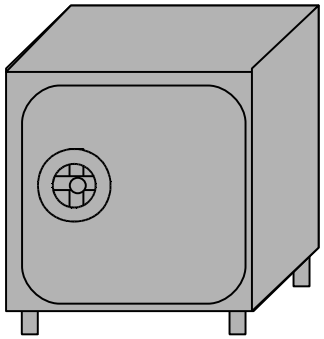
Megbízható harmadik fél (2)



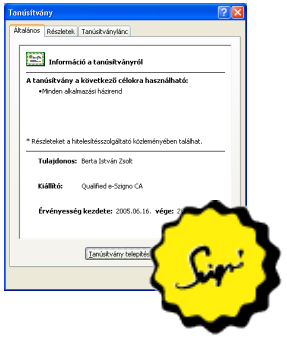
Hitelesítés szolgáltatás (Eat)

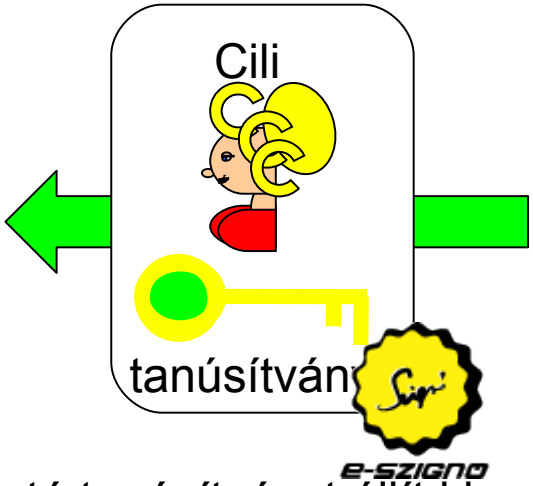


Cili



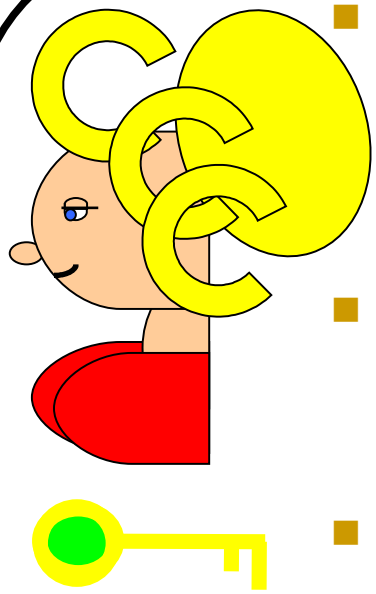
hitelesítés szolgáltató
(minősített /
nem minősített)





a hitelesítés szolgáltató tanúsítványt állít ki

Tanúsítvány

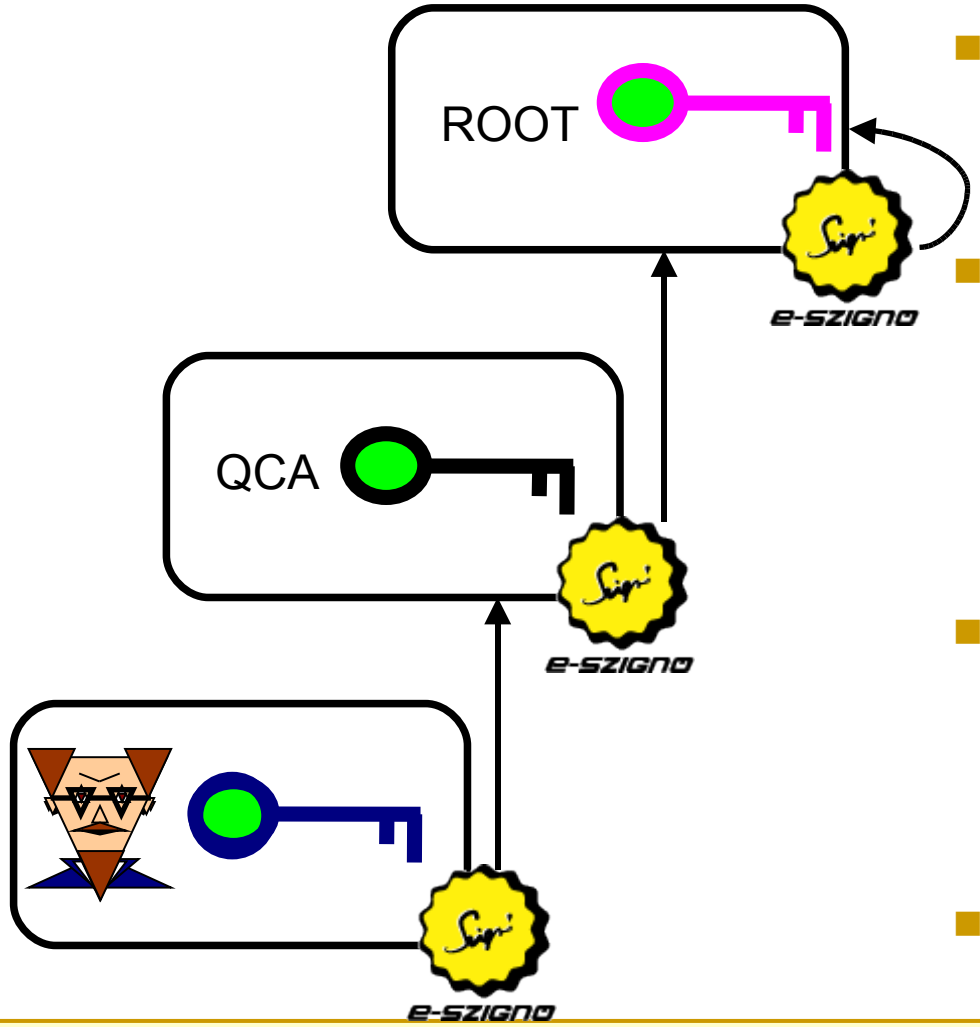


- Ez Cili nyilvános kulcsa, őnála van a hozzá tartozó magánkulcs.
- Ez a kulcs aláírások ellenőrzésére használható.
- ...
- A fenti adatokat a Microsec ellenőrizte, és vállalja értük a felelősséget.

e-SZIGNO

- A hitelesítés szolgáltató a saját magánkulcsával aláírja a tanúsítványt.
- A tanúsítvány ellenőrzéséhez a hitelesítés szolgáltató nyilvános kulcsa kell.
- És azt honnan tudom meg?

Tanúsítványlánc, Gyökértanúsítvány



- A végfelhasználó aláírását a tanúsítványa alapján ellenőrizhetjük.
- A végfelhasználó tanúsítványán lévő aláírást a hitelesítés szolgáltató tanúsítványa alapján ellenőrizzük.
- A hitelesítés szolgáltató tanúsítványán lévő aláírást egy másik HSZ tanúsítványa alapján ellenőrizhetjük.
- Gyökértanúsítvány

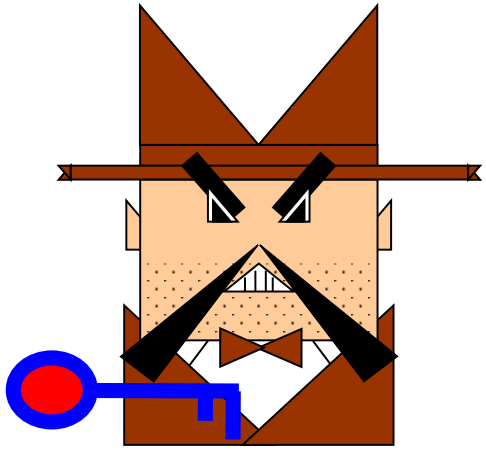
Aláírás, titkosítás, authentikáció

- Aláíró tanúsítvány
  - elektronikus aláíráshoz
- Titkosító tanúsítvány
  - titkos üzenetek küldéséhez
- Authentikációs (partner hitelesítésre szolgáló) tanúsítvány
  - biztonságos bejelentkezéshez
  - pl. webszerver tanúsítvány

- E három területre külön-külön tanúsítvány szükséges, az egyik célra használható tanúsítványt nem szabad más célra használni!

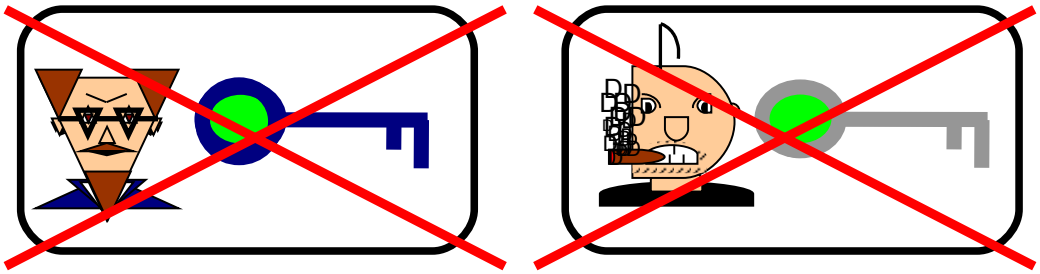
Tanúsítvány visszavonása

- Egy tanúsítvány csak a benne meghatározott ideig érvényes.
- Soron kívül is érvénytelenné válhat
  - ha a magánkulcs illetéktelen kezekbe kerül (a támadó megszerzi)
  - ha a benne szereplő adatok megváltoznak
- Felfüggesztés (ideiglenes), Visszavonás (végleges)
- A hitelesítés szolgáltató közzéteszi a visszavonást.



Visszavonási lista (CRL)

Az alábbi tanúsítványokat visszavontuk, már nem érvényesek. Ne használjátok a bennük szereplő nyilvános kulcsokat.



Aláírás:

e-Szignó HSZ

A hitelesítés szolgáltató a saját magánkulcsával aláírja a visszavonási listát, és közzéteszi a honlapján.

Mit hoz nyilvánosságra a HSZ?

- Magát a tanúsítványt, ha az aláíró beleegyezik
- A tanúsítvány visszavonási állapotát
  - a CRL a tanúsítvány sorozatszámát tartalmazza
  - egy adott tanúsítványról megállapítható, hogy visszavonták-e
- Jogszabályban meghatározott esetekben (pl. bíróságnak) a HSZ köteles kiadni bizonyos információkat

Összegzés

- A tanúsítványban a hitelesítés szolgáltató igazolja:
  - egy adott nyilvános kulcs egy adott személyhez tartozik, és
  - a tanúsítványban feltüntetett adatokat ellenőrizte.
- A hitelesítés szolgáltató mindezért felelősséget vállal, és
- szükség esetén visszavonja a tanúsítványt (pl.: adatváltozás esetén, vagy ha az ügyfél jelenti, hogy elvesztette a magánkulcsát)

Elektronikus aláírás

Elektronikus aláírás (e-szignó)

- Az elektronikus aláírás a **kódolás** egy fajtája, aláíráskor ún. aláírás-létrehozó adat (magánkulcs) alapján kódoljuk az aláírt dokumentumot.
- A dokumentum hitelességét a kódolt (aláírt) dokumentum „szerkezete” garantálja.
- A kódolás a magánkulcs nélkül nem végezhető el.
- Az aláírást bárki ellenőrizheti, ehhez az aláíró tanúsítványa szükséges, amelyet hitelesítés szolgáltató bocsát ki.
- Az elektronikusan aláírt dokumentumhoz bizonyító erő kapcsolódik.

Mire jó az e-szignó?

- Az elektronikusan aláírt dokumentum **hiteles**, tehát bizonyítható, hogy
  - az aláírást valóban az aláíró készítette (az aláíró magánkulcsával készült),
  - az aláírt dokumentum nem változott meg az aláírás óta.

- Az aláírt dokumentum **minden „másolata” eredeti**!

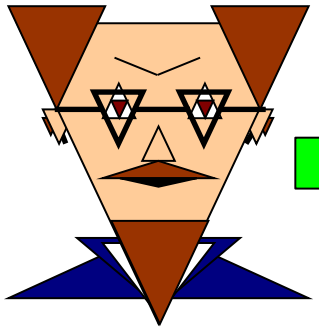
2001. évi XXXV tv. az elektronikus aláírásról

- EU direktíva (1999/93) az elektronikus aláírásról
- Elektronikus aláírással kapcsolatos szolgáltatások meghatározása
  - hitelesítés szolgáltatás (tanúsítvány-kibocsátás)
  - időbélyegzés szolgáltatás
  - eszköz szolgáltatás
  - archiválás szolgáltatás
- Minősített és nem minősített szolgáltatók, és a szolgáltatásaikhoz kapcsolódó bizonyító erő
- Nyilvántartás, felügyelet (Nemzeti Hírközlési Hatóság)
- A szolgáltatókra vonatkozó biztonsági követelmények, szolgáltatók felelőssége stb.

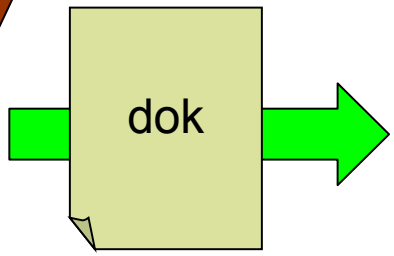
Fokozott biztonságú ↔ minősített aláírás

- **Minősített elektronikus aláírás**
  - minősített hitelesítés szolgáltató által kibocsátott minősített tanúsítvány
  - személyes megjelenéshez kötött
  - biztonságos aláírás-létrehozó eszköz (BALE)
  - szigorú szabályozás a tanúsítvány kibocsátására és a hitelesítés szolgáltató felelősségvállalására
  - teljes bizonyító erejű magánokirat hozható létre
- **Fokozott biztonságú elektronikus aláírás**
  - azonos kriptográfiai algoritmusok (kódolási módszerek)
  - sokkal kevesebb szabály
  - írásba foglaltnak minősülő dokumentum hozható létre
  - nehéz megfeleltetni valamely biztonsági szintnek

Hogyan készül az elektronikus aláírás?

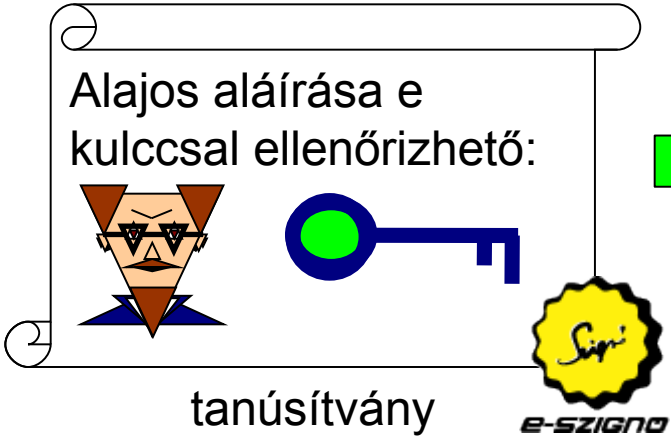


aláíró



aláírás-létrehozó eszköz

aláírt dokumentum



tanúsítvány

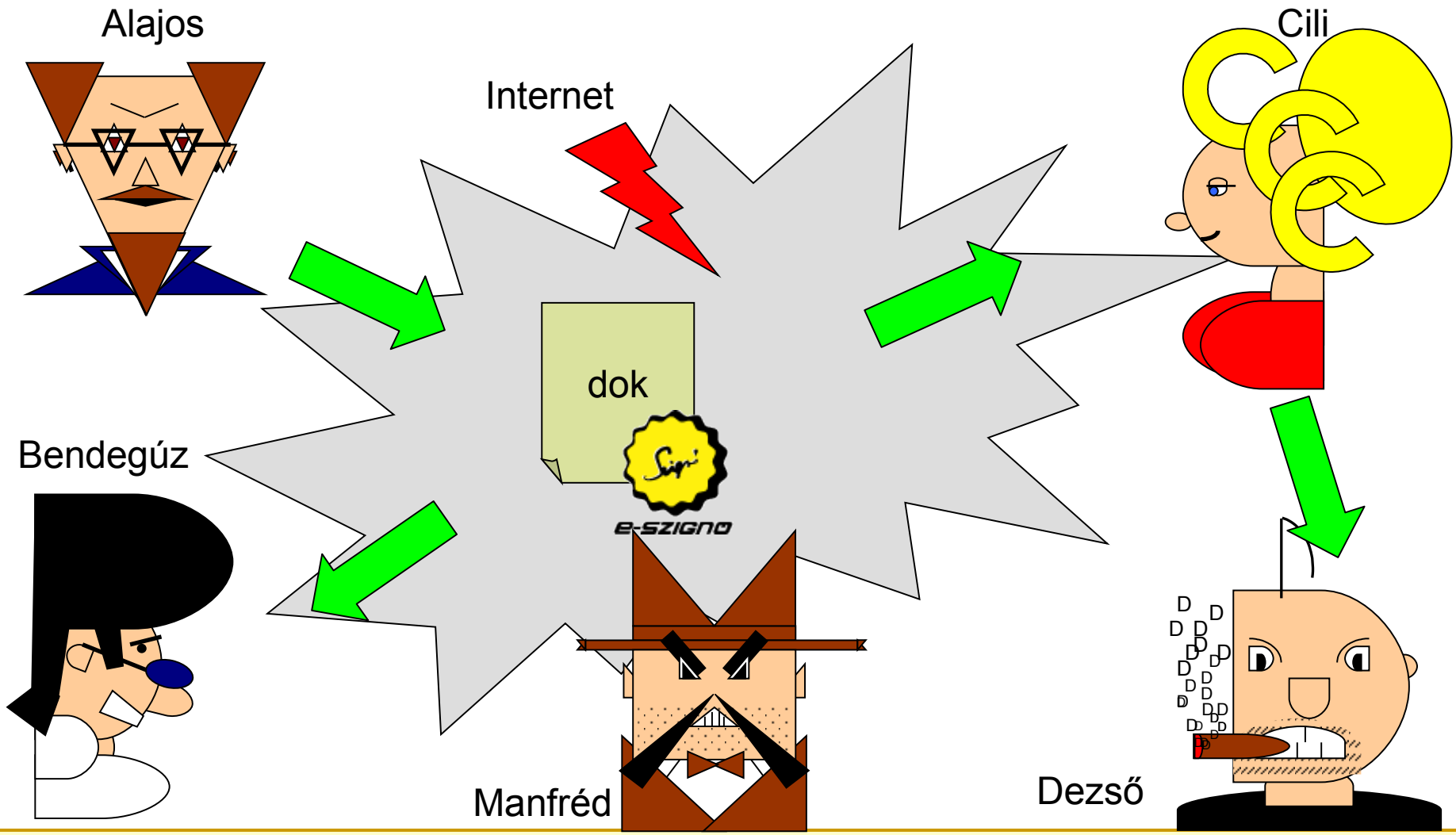
Az aláírt dokumentumról a tanúsítvány alapján egyértelműen megállapítható, hogy melyik aláíró magánkulcsával írták alá.

aláíró tanúsítvány ~
elektronikus aláírási címpéldány

Aláírás készítése

- Az **aláíró** megtekint egy dokumentumot, majd úgy dönt, aláírja.
- Az aláíró átadja a dokumentumot **aláírás-létrehozó alkalmazás**ának.
- Az aláírás-létrehozó alkalmazás átadja a dokumentumot (vagy annak lenyomatát) az **aláírás-létrehozó eszköz**nek
- Az aláírás-létrehozó eszköz az aláírás-létrehozó adat segítségével **kiszámítja az aláírást**, és visszaadja az aláírást az aláírás-létrehozó alkalmazásnak.
- Az aláírás-létrehozó alkalmazás csatolja az aláírást a dokumentumhoz, és esetleg az aláírtást a dokumentummal együtt egy ún. e-aktába foglalja.

Az aláírt dokumentum továbbítása

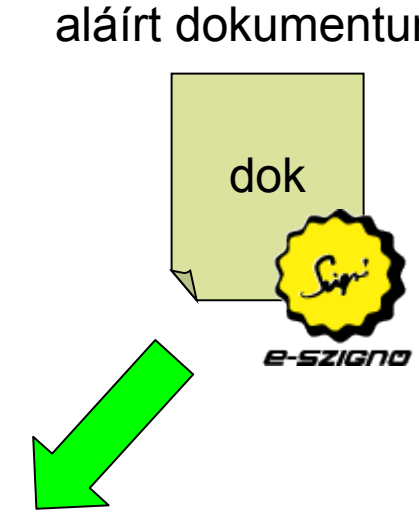


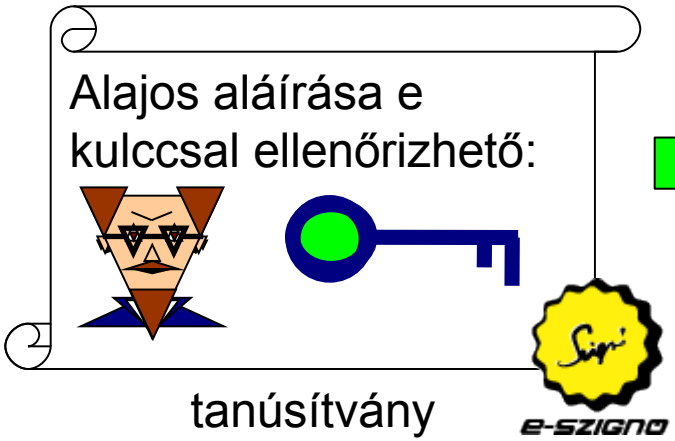
Aláírás ellenőrzése

- Összetartozik-e az aláírás és az aláíró nyilvános kulcsa?
- Az aláírás időpontjában érvényes volt-e az aláíró tanúsítványa (amely az adott nyilvános kulcsot tartalmazza)?
  - visszavezethető-e a tanúsítvány valamely megbízható gyökértanúsítványra? (tanúsítványlánc)
  - a tanúsítványlánc minden eleme érvényes volt-e az aláírás időpontjában? (nem járt-e el? nem vonták-e vissza?)

Aláírás és aláírt dokumentum összetartozása

- Ha a dokumentumon lévő aláírást kódoljuk az aláíró tanúsítványában lévő nyilvános kulccsal, visszakapjuk-e a dokumentum lenyomatát?

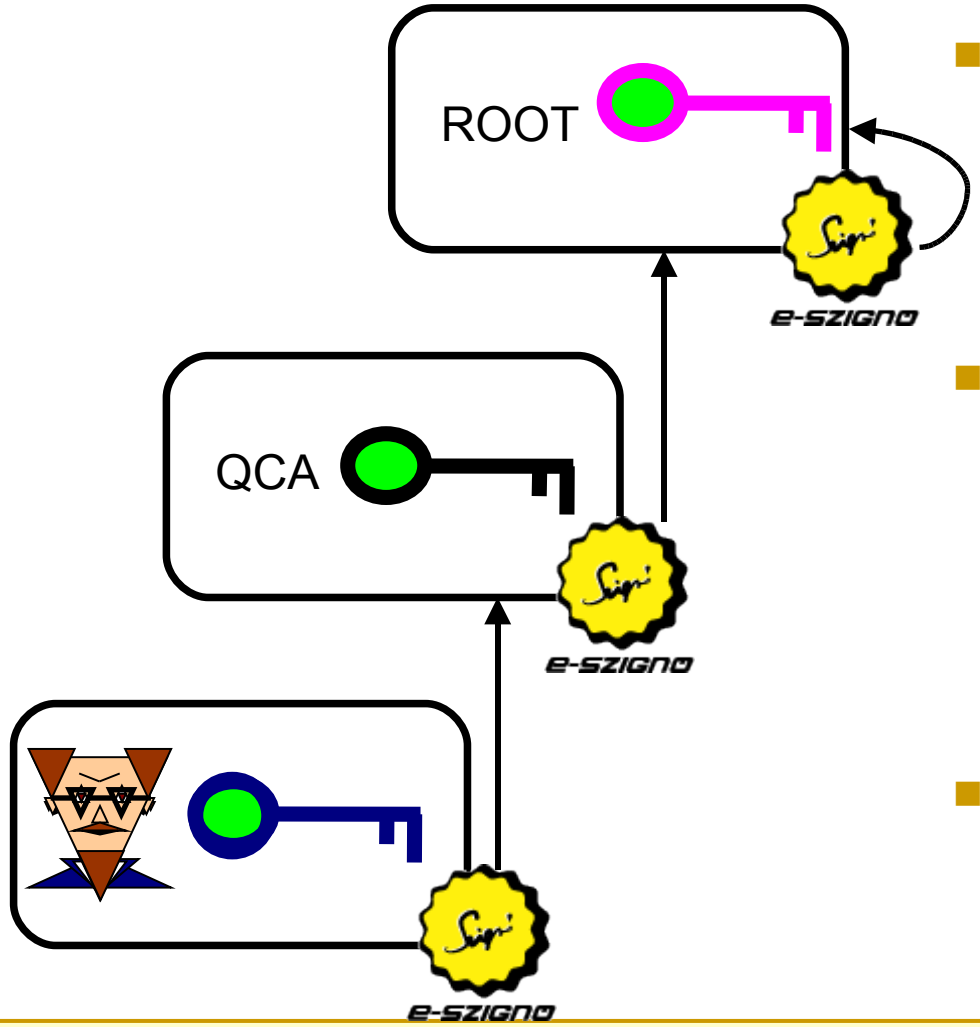




Az aláírt dokumentumról a tanúsítvány alapján egyértelműen megállapítható, hogy melyik aláíró magánkulcsával írták alá.

aláíró tanúsítvány ~
elektronikus aláírási címpéldány

Tanúsítványlánc felépítése + ellenőrzése

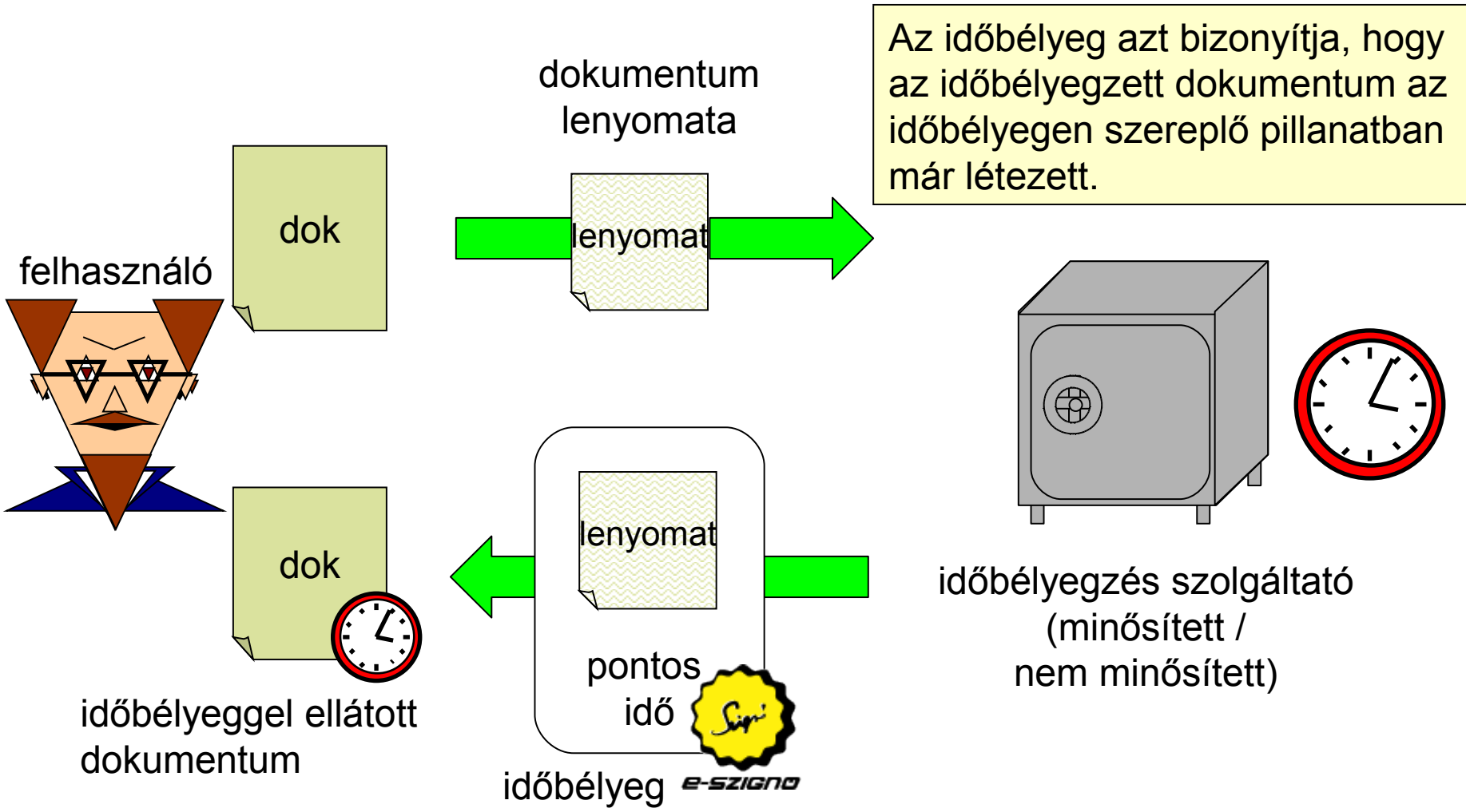


- Keresünk egy olyan tanúsítványláncot az aláíró tanúsítványától egy megbízható gyökérig, ahol
- az aláírás időpontjában a lánc minden tanúsítványa érvényes volt, és egyiket sem vonták vissza.

- Mikor készült az aláírás?

Időbélyegzés szolgáltatás (Eat.)

Az időbélyeg azt bizonyítja, hogy az időbélyegzett dokumentum az időbélyegen szereplő pillanatban már létezett.



Mi állapítható meg az aláíróról a tanúsítványból?

- Valódi nevet tartalmazó tanúsítvány esetén:
  - az aláíró neve,
  - (szerepköre, hivatása vagy beosztása),
  - (az e-mail címe),
  - (szervezetének neve),
  - + bármi más, amihez az aláíró hozzájárult.
- „Álneves” tanúsítványok
- A tanúsítványból önmagában nem állapítható meg, hogy az aláíró kicsoda!

A tanúsítvány és az aláíró összekapcsolása

- Az aláíró járuljon hozzá, hogy az adatai szerepeljenek a tanúsítványban...
  - milyen adatai? miért pont azok?
    mi van, ha mégsem járul hozzá?
- Viszontazonosítás...
- Attribútum tanúsítvány?
- Miért kell összekapcsolni őket?
  - Miért nem elég az az információ, ami egy kézzel írott aláírásban szerepel?
  - Jogvita esetén a hitelesítés szolgáltatónak ki kell adnia az aláíró adatait.

Mitől válhat egy aláírás érvénytelenné?

- A kötelezettségvállalás nem válik érvénytelenné.
  Az fordulhat elő, hogy már nem bizonyítható, hogy a kötelezettségvállalás valóban megtörtént.
- Mi okozhatja ezt?
  - Ha már nem bizonyítható, hogy az aláíró tanúsítványa érvényes volt akkor, amikor az aláírás készült;
    (e probléma időbélyeggel orvosolható)
  - Időbélyegzés szolgáltatók tanúsítványának lejárta;
  - Időbélyegzés szolgáltatók meghibásodása vagy a magánkulcsának kompromittálódása;
  - A tudomány vagy a technológia hirtelen, ugrásszerű fejlődése.

Aláírt dokumentumok hiteles megőrzése

- Ha azt szeretnénk, hogy egy aláírás érvényessége később is bizonyítható legyen, helyezzünk el időbélyeget az aláíráson.
- Ha az aláírás érvényességét hosszú távon (évtizedekig) is meg szeretnénk őrizni, néhány évente gondoskodnunk kell a rendszeres időbélyegzésükről.
  Ezt pl. archiválás szolgáltatóval tehetjük meg.

Archiválás szolgáltatás (Eat.)

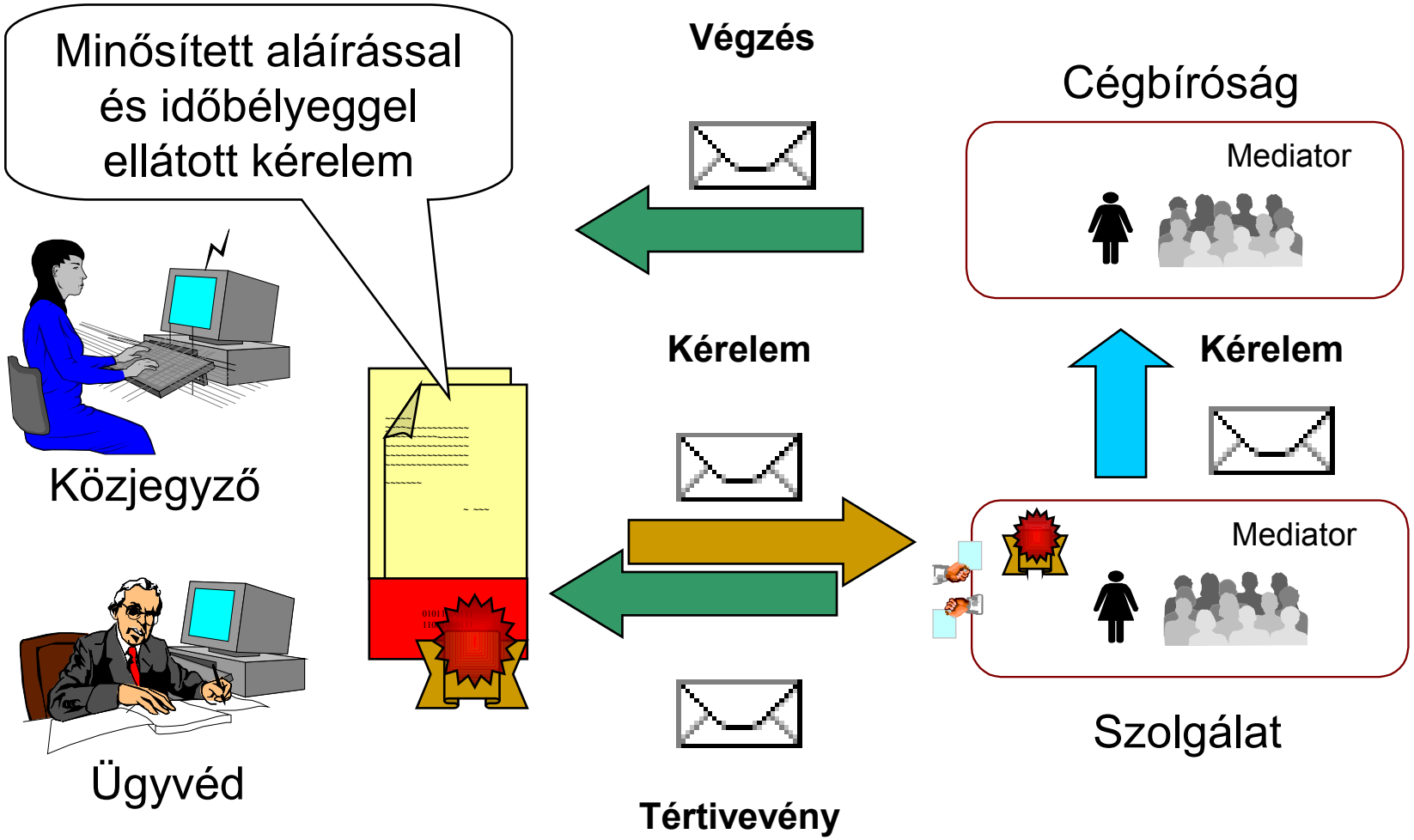
- Az archiválás szolgáltató megbízható rendszerrel ellenőrzi, és biztonságos módon eltárolja az archiválandó aláírást.
- Az archiválás időtartama alatt a jogszabályi előírások szerint folyamatosan biztosítja az archivált aláírások hitelességét.
- Ügyfelei kérésére igazolást állít ki arról, hogy egy adott aláírás érvényes.
- Ha minősített archiválás szolgáltató archivál egy aláírást, vélelmezni kell, hogy az aláírás érvényes.
- A szolgáltatást az Eat. definiálja.
- A minősített archiválás szolgáltatókról a Nemzeti Hírközlési Hatóság vezet nyilvántartást.

Bemutató

Bemutató

- Mire van szükség hozzá?
- Hogyan működik?
  - Tanúsítványtár a Windowsban
  - Elektronikus aláírás készítése
  - Elektronikus aláírás időbélyegzése
  - Elektronikus aláírás ellenőrzése
- Mire használják?
  - Elektronikus számla
  - Elektronikus cégkivonat

Bejegyzési kérelmek elektronikus kezelése



Az e-Cégeljárás számokban

- hetente ~6000 elektronikusan aláírt beadvány
  - ebből ~2000 szerződésmintát használ („1 órás”)
- hetente ~7000 elektronikusan aláírt végzés
  - ennek 95-97%-át elektronikusan veszi át az ügyvéd
- havi ~10 millió forint megtakarítás kizárólag a postaköltségen

Összefoglalás

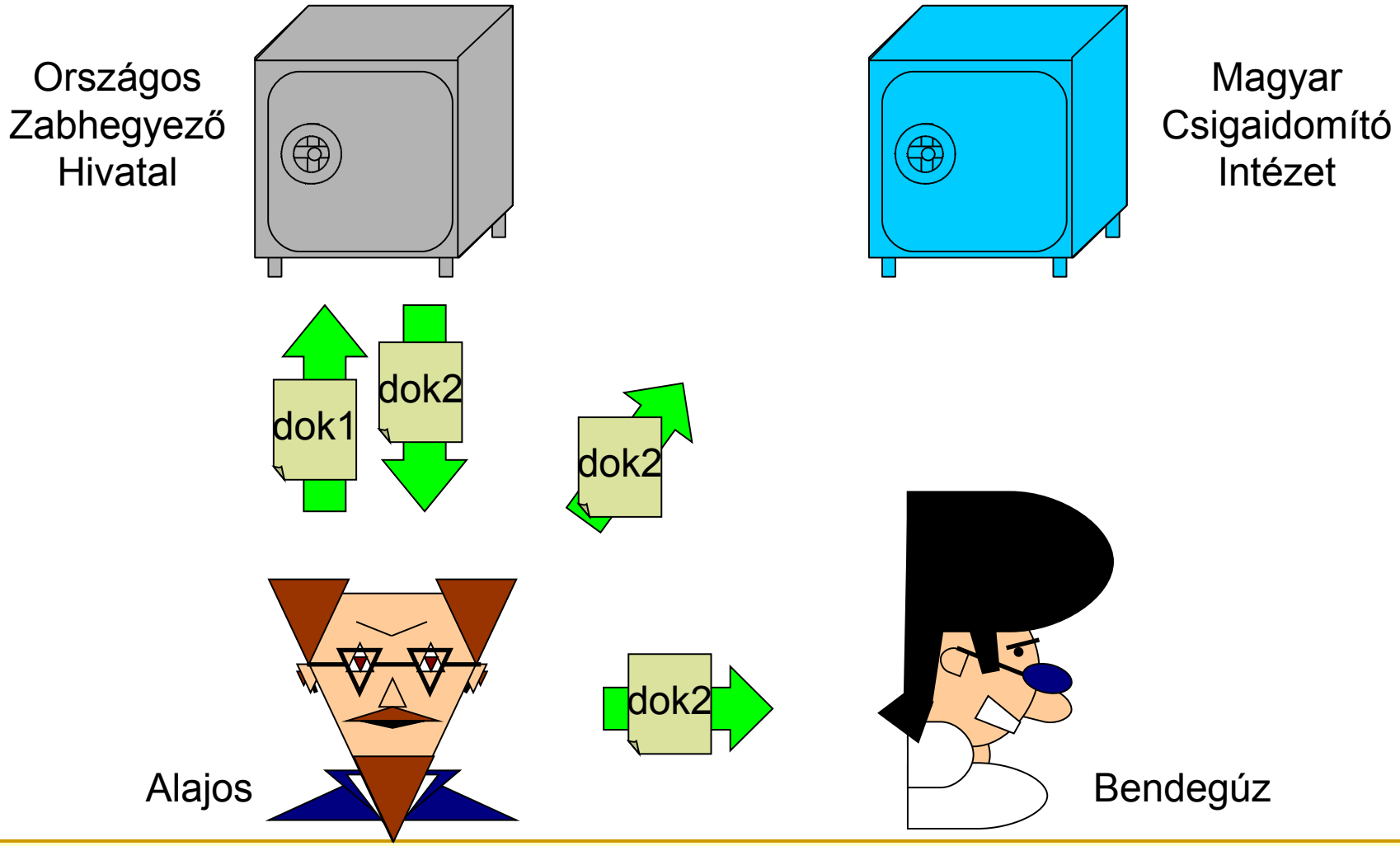
Elektronikus aláírás (e-szignó)

- Az elektronikus aláírás a **kódolás** egy fajtája
- Elektronikus aláíráskor ún. aláírás-létrehozó adat alapján kódoljuk az aláírt dokumentumot.
- A dokumentum hitelességét a kódolt (aláírt) dokumentum „szerkezete” garantálja.
- A kódolás az aláírás-létrehozó adat nélkül nem végezhető el.
- Az aláírást bárki ellenőrizheti, ehhez az aláíró tanúsítványa szükséges, amelyet hitelesítés szolgáltató bocsát ki.
- Az elektronikusan aláírt dokumentumhoz bizonyító erő kapcsolódik.

Mire jó?

- Az elektronikusan aláírt dokumentum hitelessége független attól, hogy a dokumentum hol van.
- Az elektronikusan aláírt dokumentum minden másolata is hiteles.
- Hiteles dokumentumok gyorsan és olcsón továbbíthatóak, hitelességük gyorsan ellenőrizhető.

Hol segítenek az aláírt dokumentumok?



Egy megbízható rendszer...

- Aláírja a kimenő dokumentumokat
  - így más is ellenőrizheti a kiküldött dokumentumok hitelességét
- Érdemi utasítást aláírt formában fogad el, és megőrzi az aláírt utasításokat
  - így felelősségre vonható, minden egyes műveletéről igazolni kell tudnia, hogy milyen utasítás hatására végezte el
- A befogadott dokumentumokra aláírt tértivevényt ad válaszul
  - így ügyfelei később elszámoltathatják, hogy az egyes beküldött utasításokat valóban végrehajtotta-e

Hasznos linkek

- További információk:
  www.e-szigno.hu/?lap=tudasbazis
- Aláírás-létrehozó alkalmazás:
  https://www.e-szigno.hu/e-Szigno_bemutato
  (ingyenes letöltés)
- Ingyenes teszt tanúsítványok:
  http://www.e-szigno.hu/?lap=teszt_bevezeto
- Az előadásom diái elérhetőek lesznek a
  www.berta.hu oldalon.

Köszönöm a figyelmet!

MICROSEC
Számítástechnikai Fejlesztő Kft.

Az elektronikus aláírás és gyakorlati alkalmazása

Dr. Berta István Zsolt <istvan.berta@microsec.hu>

Microsec Kft.