MICROSEC
Számítástechnikai Fejlesztő Kft.

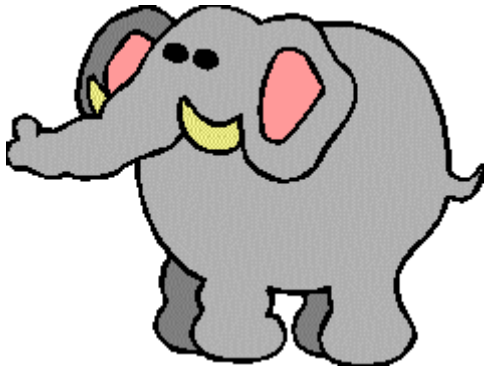
PKI gyakorlati kérdések, I

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

K+F igazgató
Microsec Kft.

Bevezetés

Elefánt



- Műszaki kérdések
- Gazdasági kérdések
- Jogi kérdések

PKI dióhéjban (1)

- Minden résztvevőnek van két kulcsa:
  - **magánkulcs** (csak ő ismeri)
  - **nyilvános kulcs** (bárki megismerheti)
- Ha magánkulcsunkkal kódolunk valamit, a nyilvános kulcsunkkal bárki ellenőrizheti, hogy a kódolást mi végeztük el. Ezt nevezzük **aláírás**nak, hitelesítésnek.
- Ha egy nyilvános kulccsal kódolunk valamit, azt kizárólag a hozzá tartozó magánkulccsal lehet visszafejteni. Ezt nevezzük **titkosítás**nak.

- Csak akkor támaszkodhatunk egy nyilvános kulcsra, ha tudjuk, hogy ki birtokolja a hozzá tartozó magánkulcsot.

PKI dióhéjban (2)

- A **hitelesítés szolgáltató**k olyan szereplők, akik aláírt igazolásokat állítanak ki arról, hogy egy adott nyilvános kulcs (és a hozzá tartozó magánkulcs) kihez tartozik. Ezen aláírt igazolásokat nevezzük **tanúsítvány**nak.
- A tanúsítványokat általában más tanúsítványok alapján ellenőrizhetjük, az ellenőrzést **gyökér** hitelesítés szolgáltatók nyilvános kulcsára vezethetjük vissza; e kulcsokat sokan ismerik és elfogadják.
- Az **időbélyegzés szolgáltató**k olyan aláírt igazolásokat bocsátanak ki arról, hogy egy adott dokumentum egy adott időpontban létezett.
- Jogszabály **bizonyító erő**t rendel
  - a minősített és a fokozott biztonságú aláírásokhoz és
  - a minősített időbélyegekhez.

Miért fontosak a jogszabályok?

- Titkosítás és authentikáció megvalósítható jogszabályok nélkül is.
- Az elektronikus aláírás értelmét az jelenti, hogy hitelességét jogszabály is elismeri.
- Titkosítás és authentikáció esetén is lehetne értelme a jogszabályoknak.
  - titkosítás: mikor szabad titkosítani, hogyan szabad? ki jogosult hozzáférni a dekódoló kulcshoz?
  - authentikáció: hogyan tudom meg, hogy ki az, aki authentikált, mennyire lehetek biztos benne, hogy ő tényleg az?
- Magyarországon: Eat.

PKI Magyarországon

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
- Felügyelet (Nemzeti Média- és Hírközlési Hatóság)
- A szolgáltatókra vonatkozó biztonsági követelmények, szolgáltatók felelőssége stb.

Hazai piac

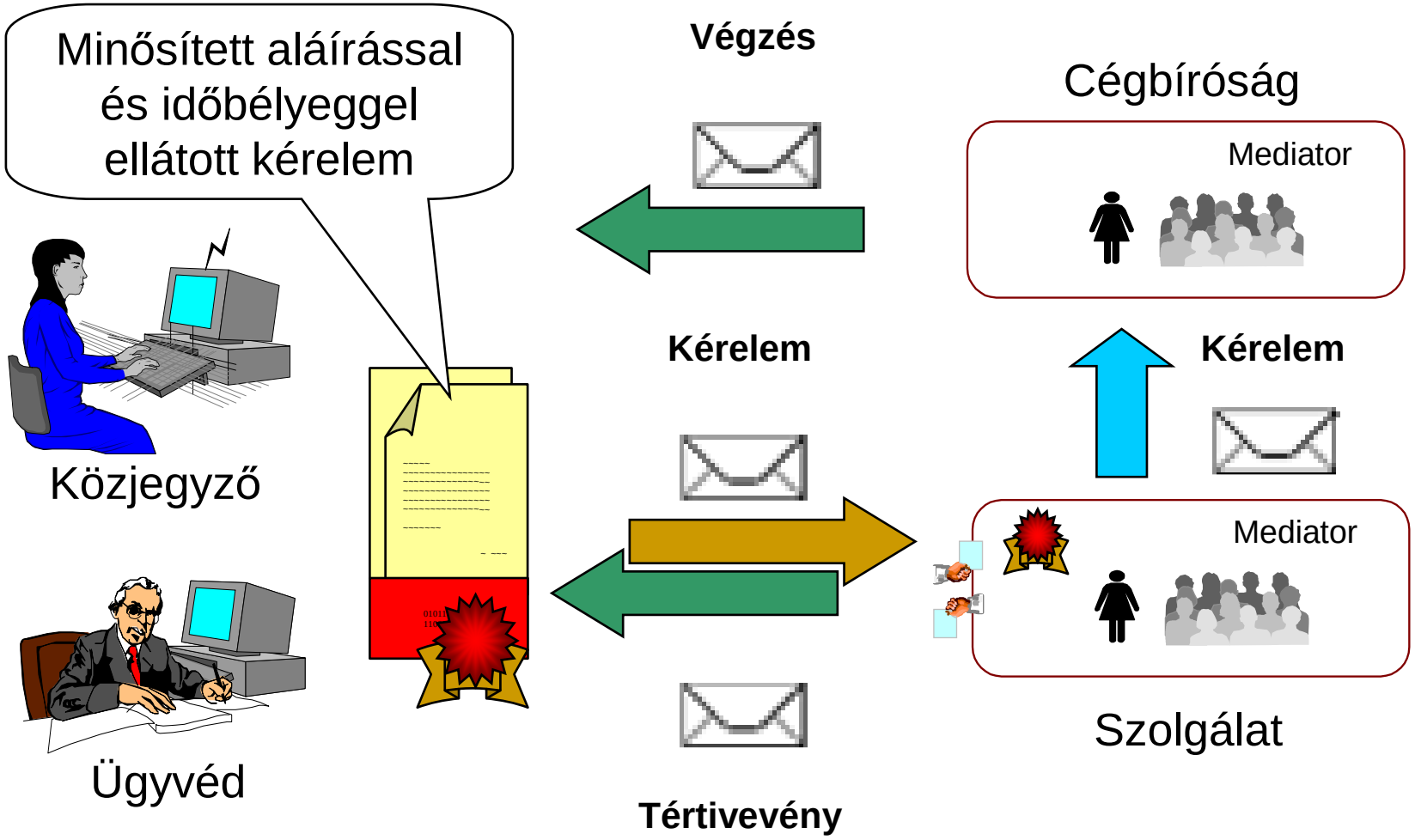
- A Nemzeti Média- és Hírközlési Hatóság felügyeli a szolgáltatókat
- Négy kereskedelmi hitelesítés szolgáltató működik Magyarországon:
  - Microsec, www.e-szigno.hu
  - Máv Informatika, www.mavinformatika.hu/ca
  - Netlock, www.netlock.hu
- Továbbá:
  - Educatio Kht. (működik, de csak nem minősített)
  - Siemens (csak archiválás)
  - GIRO, www.giro.hu (megszűnt)
  - Magyar Telekom, eszigno.t-systems.magyartelekom.hu (megszűnt)
  - IHM Biztonsági HSZ (nem működik)
  - KGYHSZ www.kgyhsz.gov.hu (csak gyökér)
- e-Cégeljárás, Ügyfélkapu, Magánnyugdíjpénztári bevallás

Felhasználási területek

- e-Cégeljárás, pl.
  - cégalapítás,
  - cég mérlegének benyújtása
  - APEH, KSH, bankok stb. egymás közötti kommunikációja
- Fizetési meghagyás
- Bírósái végrehajtók - bankok
- e-Számlázás, pénzügyi bizonylatok elektronikusan
  - pl: ELMÜ, UPC, Vatera, MALÉV, Budapest Bank stb.
  - Díjbeszedő (dbrt.hu),Távszámla (www.tavszamla.hu)
- Adatszolgáltatás hatóságok részére (NSZI, OEP stb.)
- Adatok archiválása
- (Ügyfélkapu)

- + amire papír alapú aláírást használunk

Cégbírósági beadványok



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

Minősített elektronikus aláírás

- Minősített elektronikus aláírás: olyan - fokozott biztonságú - elektronikus aláírás, amelyet az aláíró **biztonságos aláírás-létrehozó eszközzel** hozott létre, és amelynek hitelesítése céljából **minősített tanúsítványt** bocsátottak ki.
- „Teljes bizonyító erejű magánokirat”
- Minősített aláírást csak természetes személy készíthet.
- A CA aláírása is csak fokozott biztonságú lehet.

Hitelesítés szolgáltató

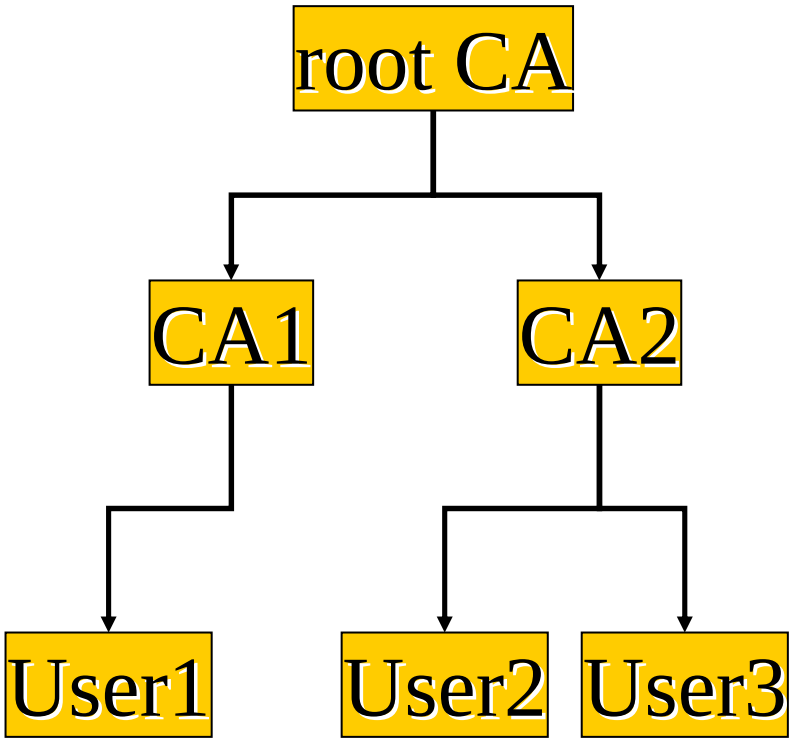
Mivel foglalkozik egy CA?

- A CA azonosítja, regisztrálja a felhasználót…
- Tanúsítványt bocsát ki a számára…
- Nyilvánosságra hozza a tanúsítványokat*…
- Nyilvánosságra hozza, ha a felhasználó visszavonja a tanúsítványt…
- Garanciát vállal (a saját működésére).
- Cserébe rendszeres (pl. éves) díjat kap a felhasználóktól

Tanúsítvány

- 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)

Mi a hitelesítés szolgáltató?



- Szervezet/vállalat?
- Szervezeti egység?
- Számítógép?
- HSM?
- Domain?
- Fizikai eszközök összessége?
- Tanúsítvány?
- Kulcspár?

Hitelesítési rend

- Sok, különböző biztonsági szintű tanúsítvány létezik.
- A tanúsítványokat befogadó „érintett felek” (relying party) meg kell, hogy tudják különböztetni őket.
- A hitelesítés szolgáltatók nyilvánosságra hozzák, hogy milyen követelményrendszerek szerint bocsátanak ki tanúsítványokat.
- A tanúsítványokban meghivatkozzák az adott tanúsítványra vonatkozó követelményrendszert.
- E követelményrendszer a hitelesítési rend (certificate policy)

A Hitelesítési Rend kritikus pontjai

- Milyen azonosítást végez a HSZ a tanúsítvány kibocsátása előtt?
  - történik-e személyes találkozás
  - ki végzi a személyes találkozást
- Milyen módon kérheti az ügyfél a tanúsítvány felfüggesztését/visszavonását?
- A HSZ mennyi idő alatt kell, hogy teljesítse a kérelmet?
- A HSZ mennyi idő alatt és milyen módon kell, hogy közzétegye a megváltozott visszavonási állapotot?
- Pontosan miért vállal felelősséget a HSZ, és milyen mértékben?

Azaz: mi alapján fogadhatunk el egy tanúsítványt, és mennyire bízhatunk meg benne.

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

Visszavonási állapot közzététele

- Visszavonási lista
  - a visszavont tanúsítványok sorozatszámát, és a visszavonás időpontját (és esetleg az okát) tartalmazza
  - RFC 5280
- Online tanúsítvány-állapot szolgáltatás
  - online kérés, amire aláírt válasz érkezik
  - RFC 2560

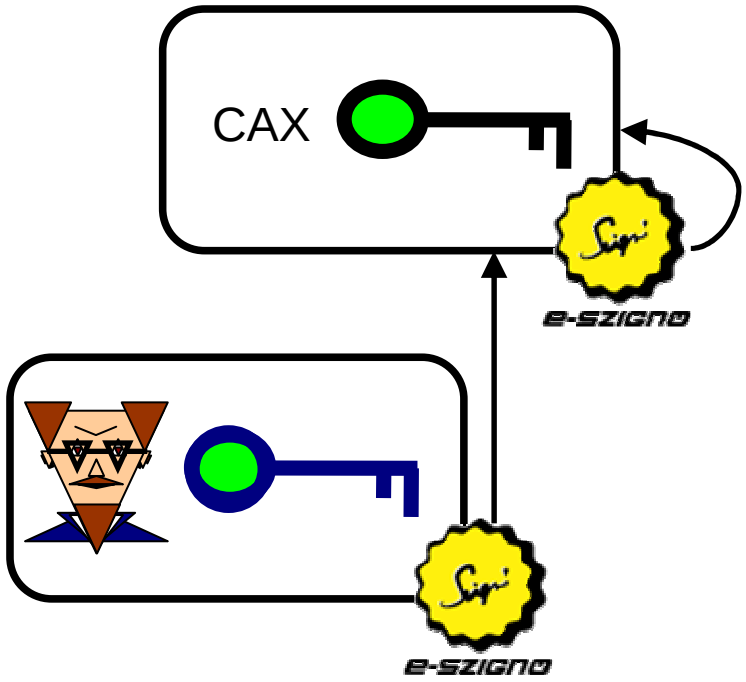
Visszavonási listák csoportosítása (1)

- Mikor bocsátja ki a HSZ?
  - Periodikusan (pl. 24 óránként)
  - A HSZ esetleg rendkívüli listát is bocsáthat ki
  - A HSZ esetleg kötelezettséget is vállalhat a rendkívüli lista kibocsátására
- Ki bocsátja ki, írja alá?
  - a HSZ a szolgáltatói kulcsával?
  - indirekt CRL: valaki más bocsátja ki (pl. azonos DN)
- A CRL vonatkozhat a HSZ összes tanúsítványára vagy csak bizonyos tanúsítványokra
  - ARL (authority revocation list, csak a CA tanúsítványokra vonatkozik)
- Delta CRL: a legutóbbi CRL-hez képest történt változásokat tartalmazza

Visszavonási listák csoportosítása (2)

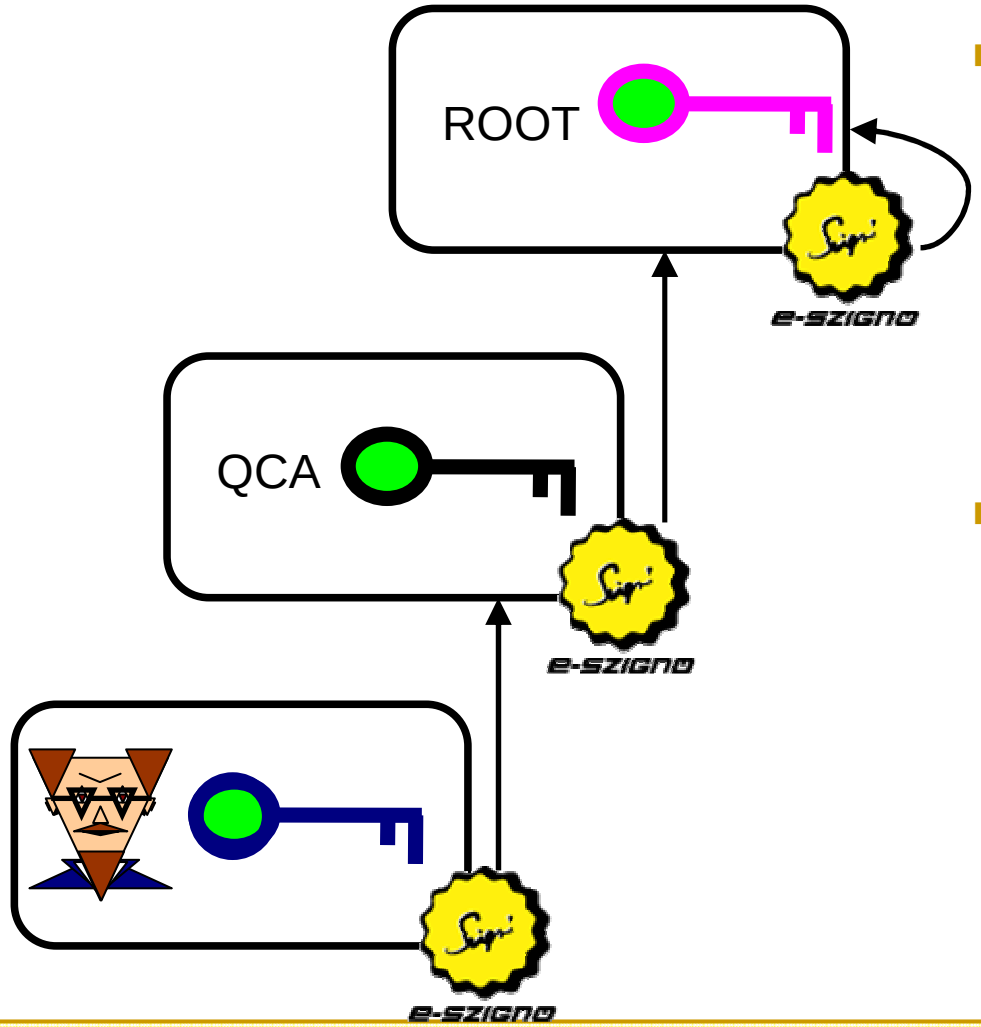
- A HSZ milyen csatornán fogadja a visszavonási kérelmeket?
  - fogadja napi 24 órában?
- Mekkora rendelkezésre állást vállal a HSZ?
- Mennyi idő alatt
  - bírálja el a visszavonási kérelem jogosságát?
  - dolgozza fel a visszavonási kérelmet?
  - teszi közzé az új visszavonási állapotot?
  - jut el az új információ az érintett félhez?
- Honnan derül ki, hogy milyen listáról van szó?
  - a HSZ szolgáltatási szabályzatából...

Tipikus megoldás (1)



- CAX az összes általa kibocsátott tanúsítványra vonatkozó visszavonási listát bocsát ki.
- Legalább 24 óránként bocsát ki visszavonási listát, de visszavonáskor 4 órán belül rendkívüli visszavonási listát bocsát ki.

Tipikus megoldás (2)



- A root legalább havonta bocsát ki visszavonási listát, az általa kibocsátott CA tanúsítványokra. CA visszavonása esetén haladéktalanul rendkívüli visszavonási listát bocsát ki.
- QCA legalább 24 óránként, a végfelhasználói tanúsítványokra bocsát ki visszavonási listát. Visszavonás esetén legalább 4 órán belül új listát bocsát ki.

Minősített HSZ biztonsági követelmények

- Pénzügyi (bankgarancia/felelősségbiztosítás)
- Szervezeti biztonság (ISO 9001,27001)
- Fizikai biztonság (2 helyszín stb.)
- Személyzeti biztonság (bizalmi munkakörök)
- Műszaki köv. (HSM, kettős ellenőrzés, naplózás stb.)
- Rendszeres auditok
- Szolgáltatás nyújtásának befejezése

Elektronikus aláírás

Letagadhatatlanság

- Elektronikus aláírás ~ letagadhatatlanság
- Eat.: bizonyító erőt rendel az aláírt dokumentumokhoz.
  - az érvényes aláíráshoz kapcsolódik,
  - ha az aláírás ellenőrzésének eredményéből más nem következik
- Aláírás műszaki ellenőrzése
  - az aláírás egy adott magánkulccsal készült-e?
  - a magánkulcshoz tartozó tanúsítvány érvényes volt-e az aláírás időpontjában?
- Jogi szempontból az aláírás érvényessége mást is jelenthet
  - az aláíró írta alá? valóban alá akarta írni? tisztában volt vele, hogy mit csinál?
- A letagadhatatlanság műszaki fogalom, az érvényes aláírást is meg lehet kérdőjelezni

Ha műszakilag érvényes az aláírás...

Lehet, hogy

- az aláíró kényszer alatt írta alá,
- az aláírót megtévesztették,
- az aláírótól elrabolták a magánkulcsát, és erőszakkal megakadályozták, hogy jelentse a kulcs kompromittálódását,
- hibás/rosszindulatú program készítette az aláírást

Ha műszakilag érvénytelen az aláírás...

Lehet, hogy

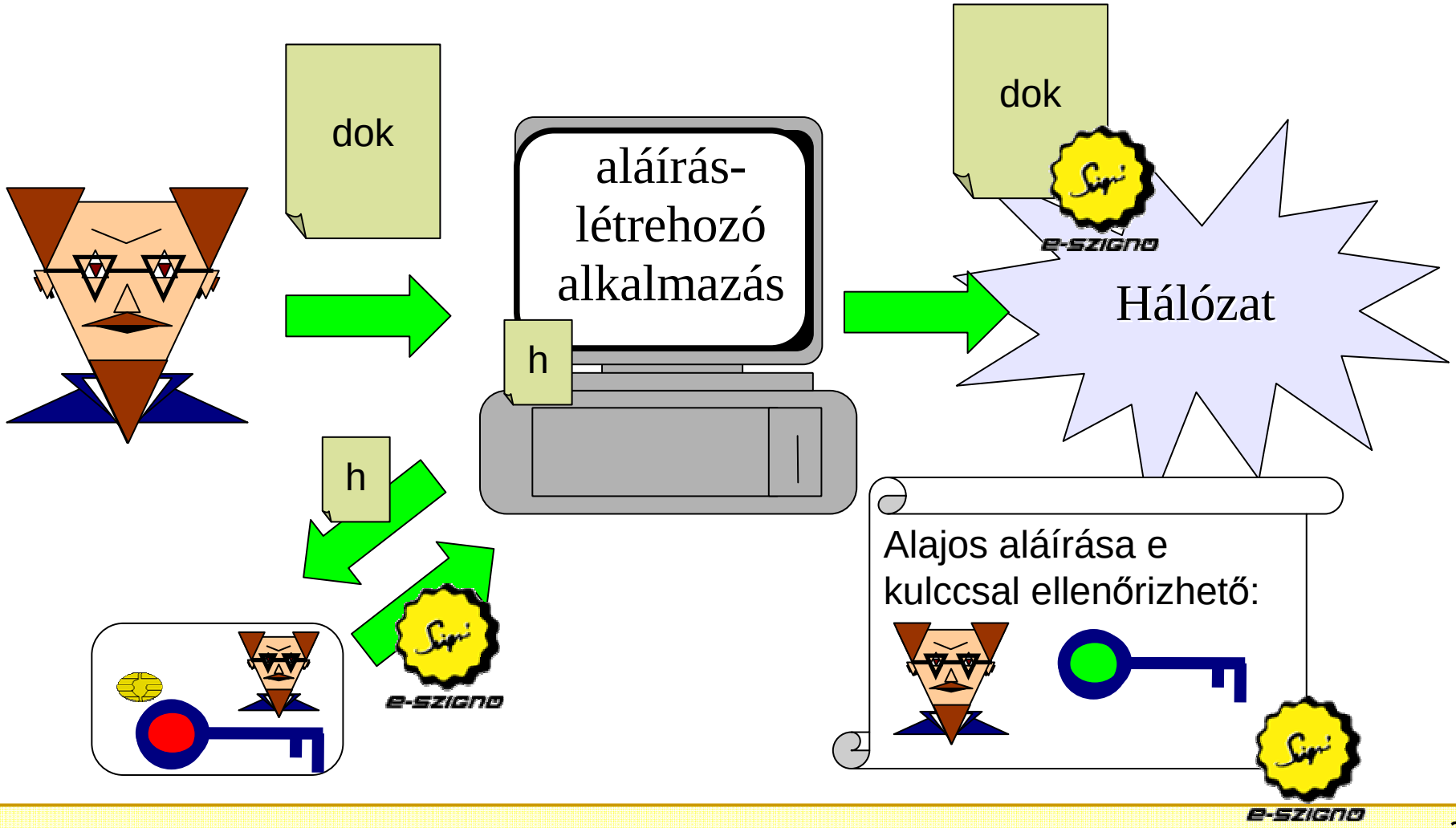
- az aláíró valóban aláírta a dokumentumot,
- de a tanúsítványa ekkor már érvénytelen volt,
- és a befogadót ez egyáltalán nem zavarja.

Fokozott biztonságú vs. minősített aláírás

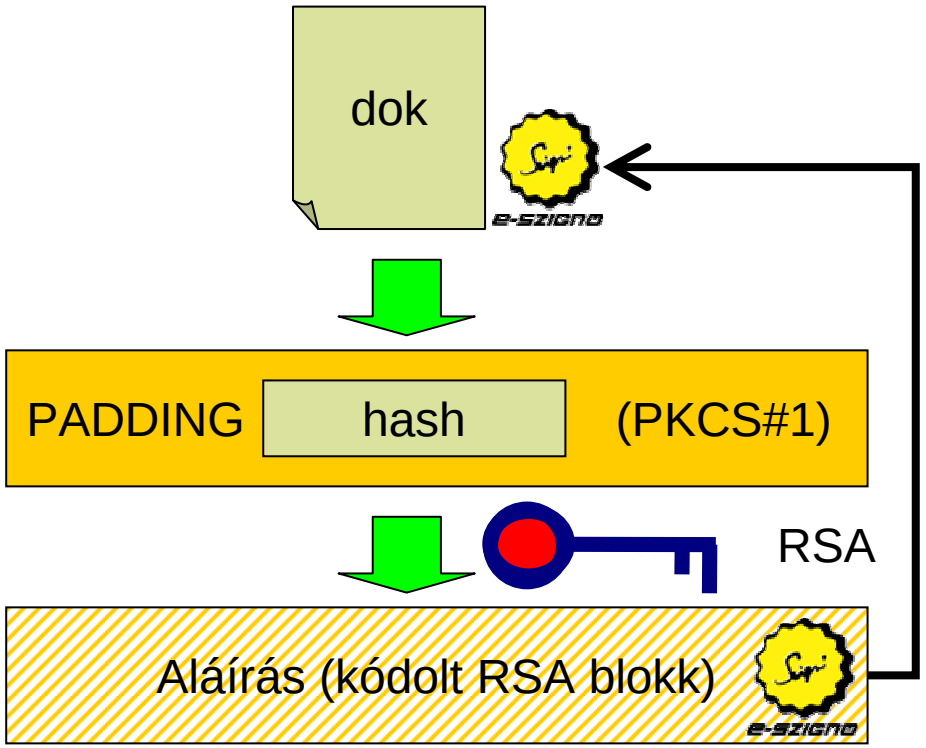
- Az elektronikus aláírásról szóló törvény szerint:
  - a fokozott biztonságú elektronikus aláírással hitelesített dokumentum írásba foglaltnak minősül;
- A polgári perrendtartásról szóló törvény szerint:
  - a minősített elektronikus aláírással hitelesített dokumentum **teljes bizonyító erejű magánokirat** (~ közjegyző vagy két tanú előtti aláírás)

- Ezek jogi kategóriák, azonos technológia húzódik meg mögöttük. A különbség:
  - a bizonyító erő
  - a hitelesítés szolgáltató felelősségvállalása
  - a szabályozás a tanúsítvány kibocsátására, használatára

Aláírás készítése

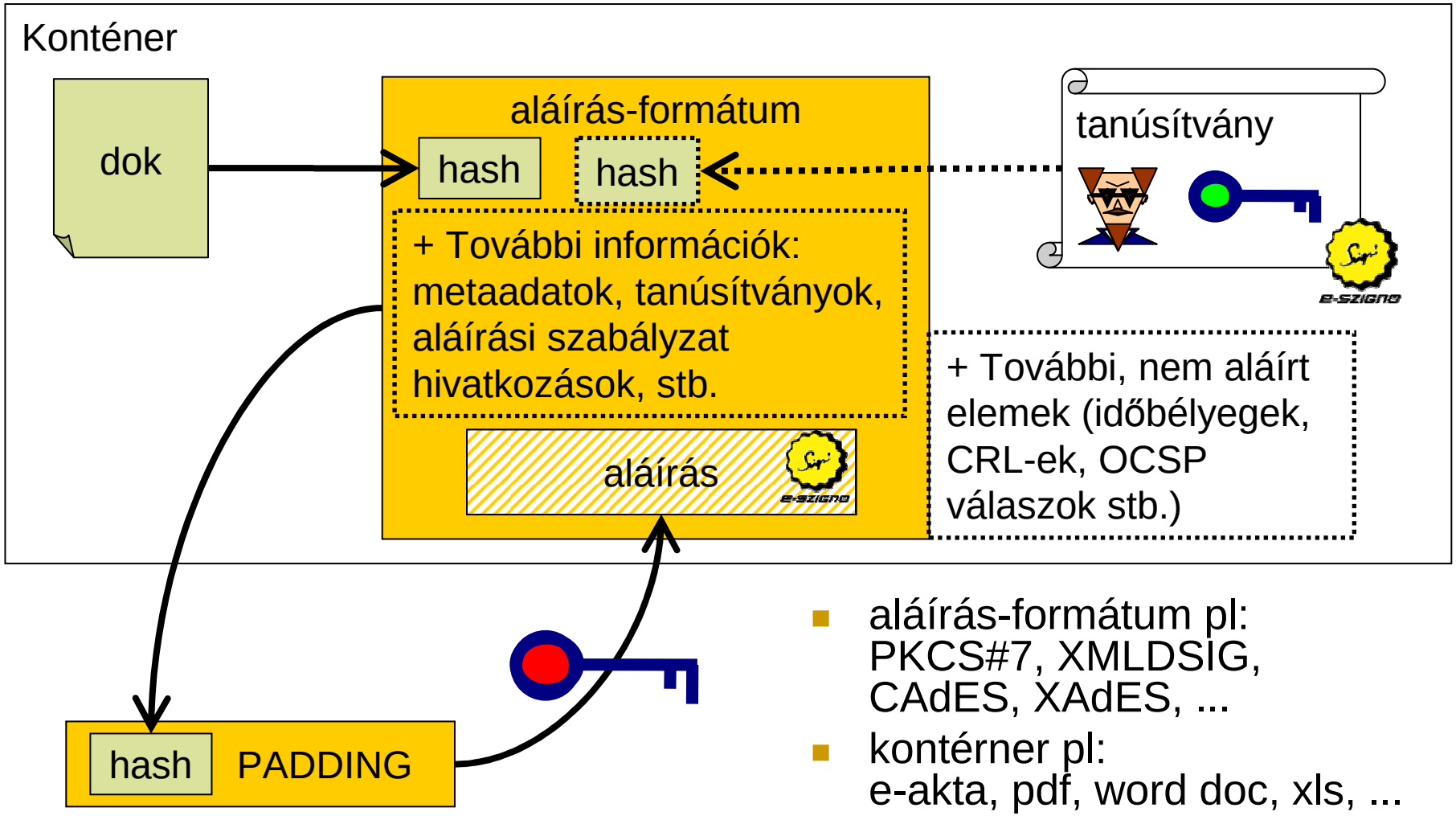


Hogyan készül az aláírás (egyszerű ábra)?



RSA blokkméret pl: 2048 bit

Hogyan készül az aláírás (valójában)?

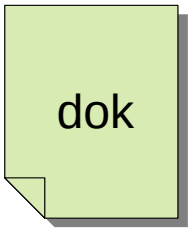


- aláírás-formátum pl:
  PKCS#7, XMLDSIG,
  CAdES, XAdES, ...
- kontérner pl:
  e-akta, pdf, word doc, xls, ...

XAdES aláírások

- XML Advanced Electronic Signature
- W3C által kidolgozott formátum
- ETSI TS 101 903 szabvány
- Többfajta aláírást definiál, van közöttük egyszerű, időbélyeggel ellátott, és hosszú távon letagadhatatlan is

„Alap” elektronikus aláírás (-BES)

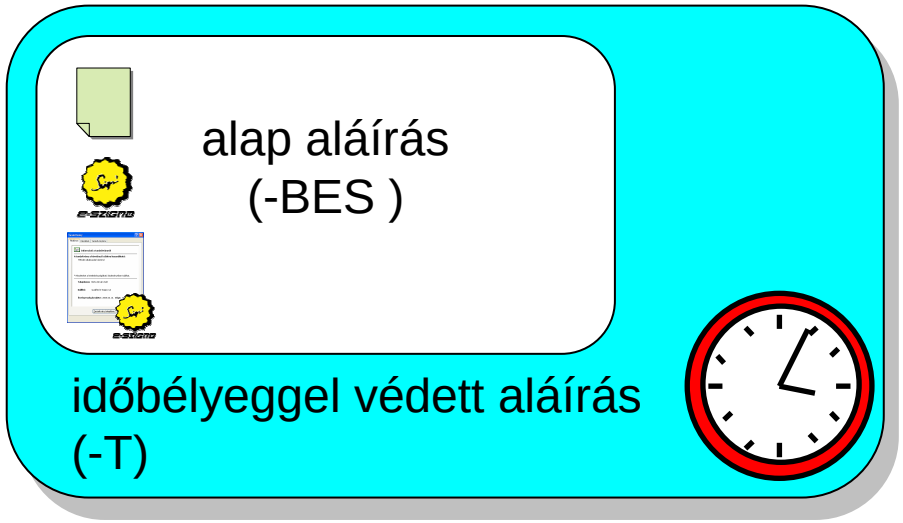


a dokumentum, amelyet aláírtunk

a dokumentumra vonatkozó elektronikus aláírás

az aláíró tanúsítványa, amelyet egy hitelesítés szolgáltató írt alá

Időbélyeggel védett aláírás (-T)

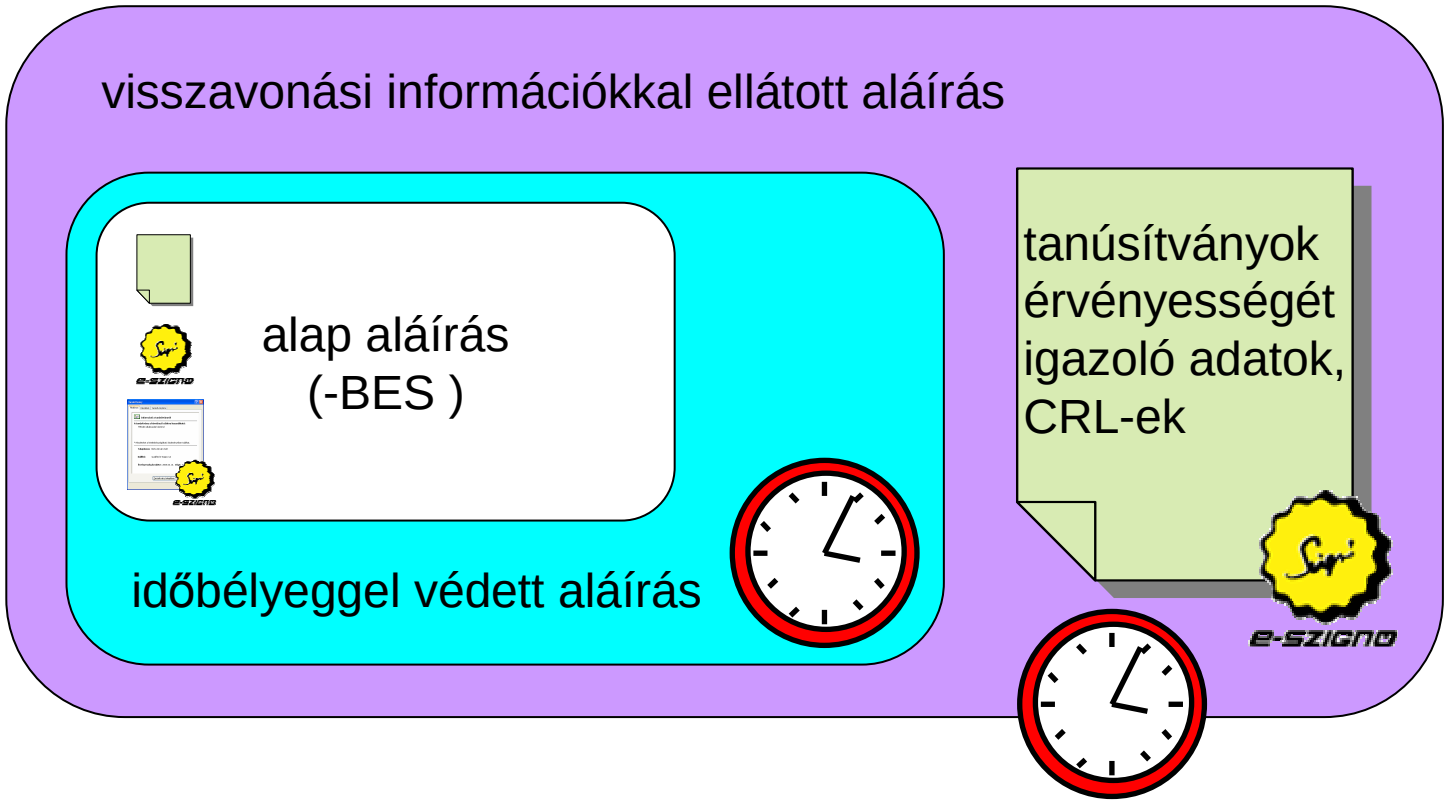


Ha az aláírást az aláírás pillanatában időbélyeggel látjuk el, bizonyíthatóvá válik, hogy pontosan mikor írtuk alá a dokumentumot, így bizonyítani lehet, hogy a tanúsítványunk akkor még érvényes volt.

Az időbélyeggel védett aláírás akkor is érvényes marad, ha

- a tanúsítvány később lejár
- a tanúsítványt később visszavonják

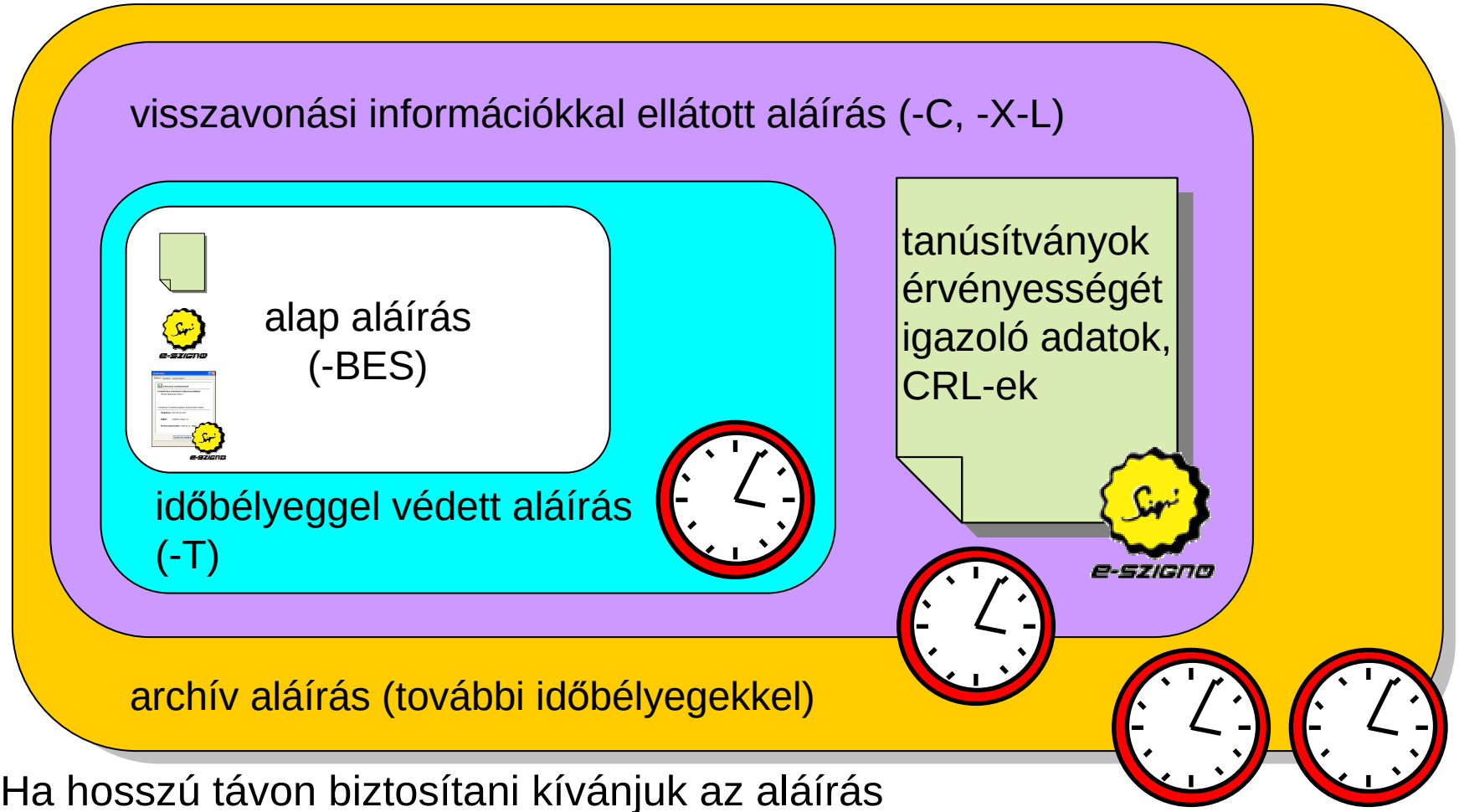
Visszavonási információk csatolása



Az az időbélyegzett aláíráshoz visszavonási információk vagy azok referenciája is csatolható (-C).

A visszavonási információkon időbélyeget is elhelyezhetünk (-X-L)

Archív aláírás (-A)



Ha hosszú távon biztosítani kívánjuk az aláírás érvényességét, rendszeresen újabb időbélyegekkel kell ellátni.

XAdES formátumok

- XAdES-BES – nem sok mindenre jó
- XAdES-T – igazolható az aláírás időpontja
- XAdES-C – bizonyos információk csatolva
- XAdES-X-L – minden visszavonási info csatolva és időbélyegezve
- XAdES-A – hosszú távú archiválás, archív időbélyegek
  - nem csak formátum, hanem eljárás
  - archív szolgáltató

Elektronikus aláírás ellenőrzése

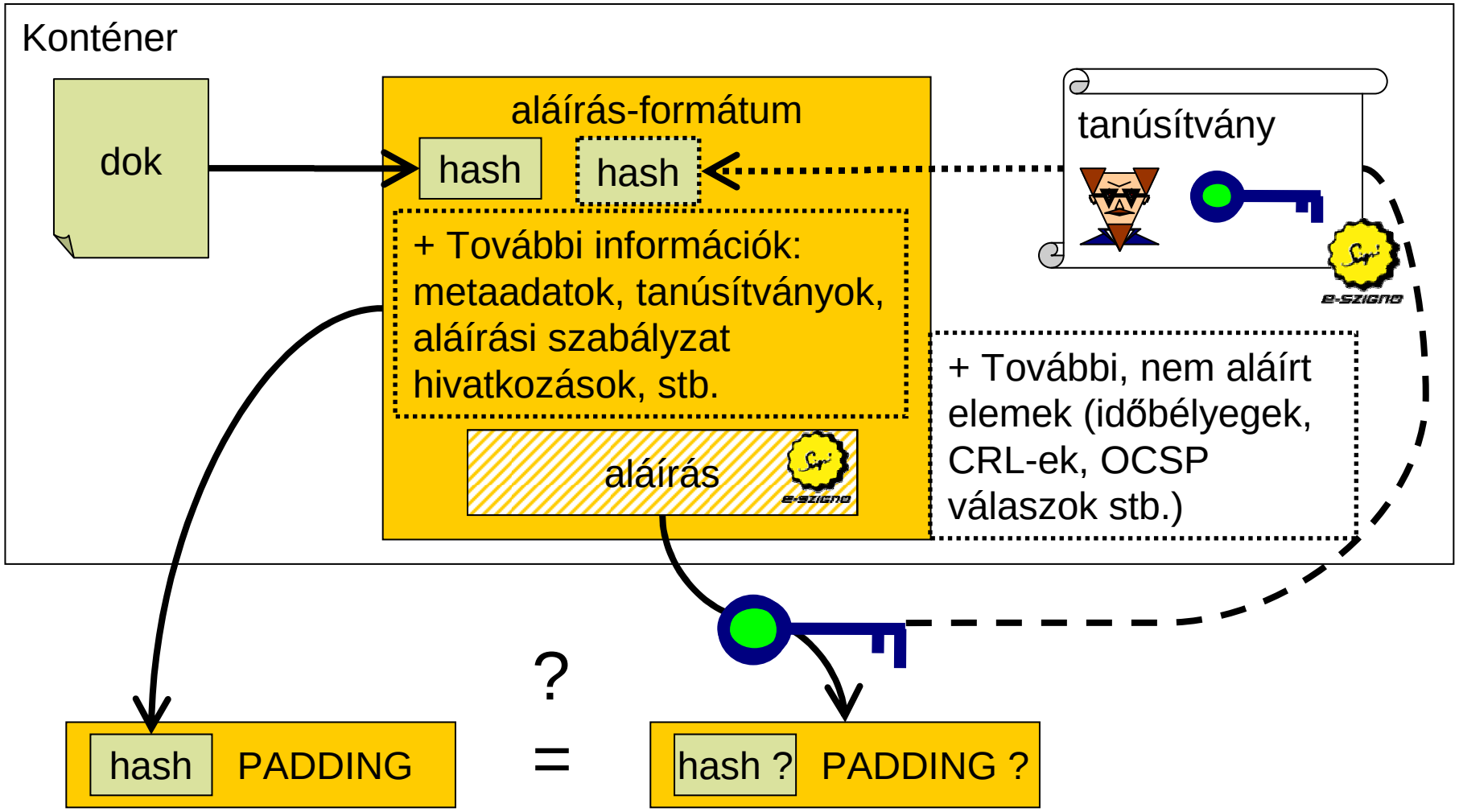
Aláírás ellenőrzése és befogadása

- Meg kell vizsgálni az aláírás műszaki érvényességét
- El kell dönteni, hogy az adott aláírás az adott környezetben elfogadható-e
  - aláírás biztonsági szintje
  - aláíró szerepe
  - aláírási szabályzat
  - mennyire lehetek biztos az aláírás érvényességében?
  - ...

Aláírás műszaki érvényessége

- Összetartozik-e az aláírás és az aláíró nyilvános kulcsa?
- Az aláírás időpontjában érvényes volt-e az aláíró tanúsítványa (amely az adott nyilvános kulcsot tartalmazza)?

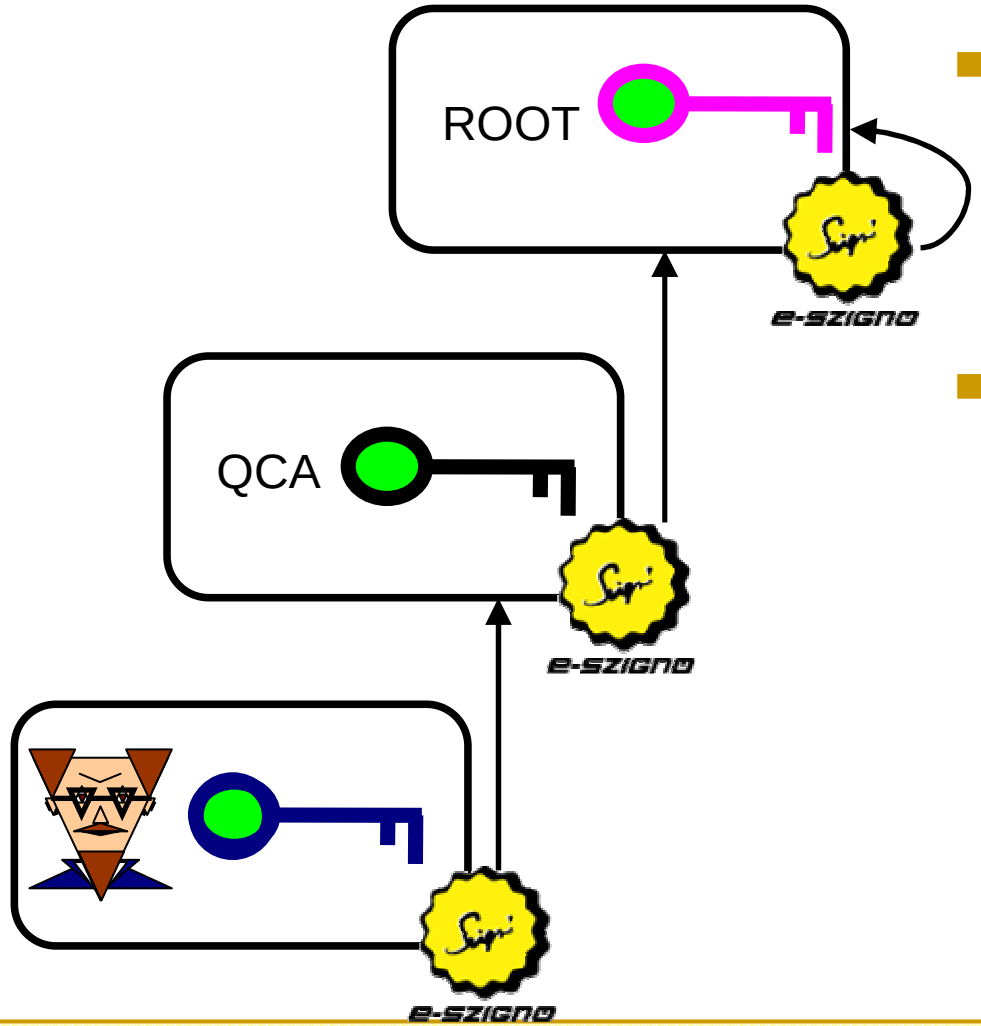
Aláírás és nyilvános kulcs összetartozása



Aláíráskor érvényes volt-e az aláíró tanúsítványa?

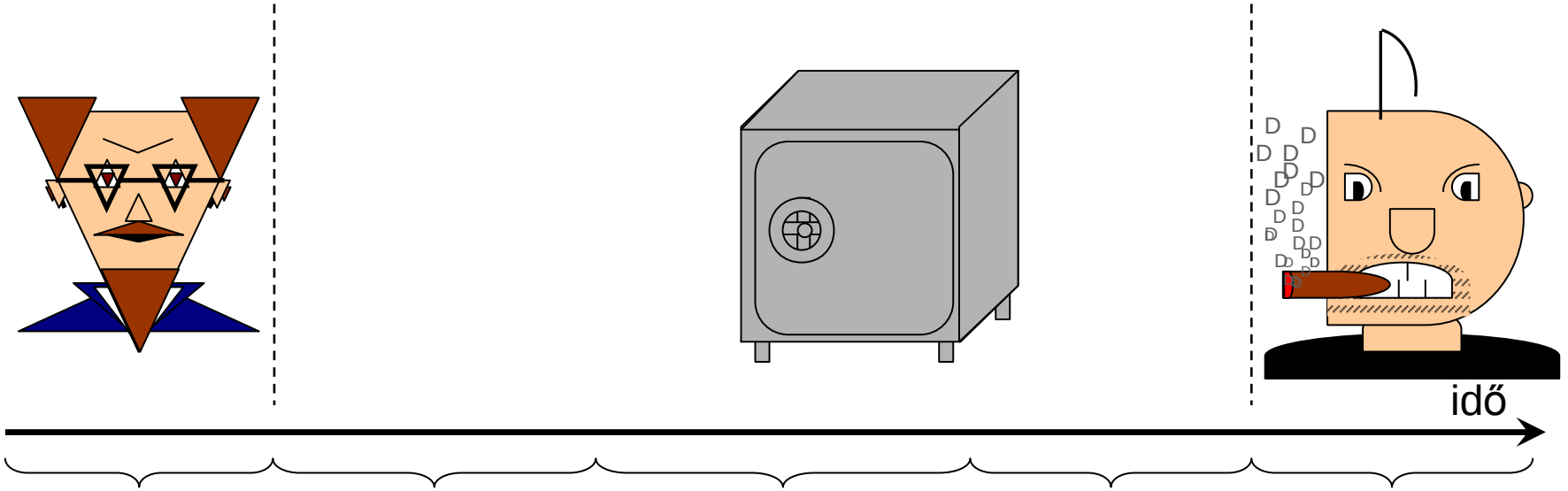
- Mikor készült az aláírás?
  - van rajta időbélyeg? ☺
  - van rá más bizonyíték, amiben megbízunk?
- Visszavezethető-e az aláíró tanúsítványa egy megbízható gyökértanúsítványra?
  - több gyökér is lehet
  - több elfogadható lánc is lehet
- Érvényes volt-e a tanúsítványlánc minden eleme az aláírás pillanatában?
  - érvényességi időn belül történt-e?
  - nem volt-e valamelyik elem visszavonva?

Tanúsítványlánc ellenőrzése



- Az aláírás pillanata a lánc minden elemének érvényességi idején belül van-e?
- Meg kell vizsgálni a lánc elemeinek visszavonási állapotát.

Felfüggesztési kérelem feldolgozása



felfüggesztés / visszavonás bejelentése

a HSZ megállapítja a kérelem jogosságát

a HSZ átvezeti nyilvántartásában a kérelmet

a HSZ közzéteszi a megváltozott visszavonási állapotot

az érintett felek értesülnek az új visszavonási állapotról

Időpontok a CRL-ben / OCSP válaszban

- thisUpdate – erre az időpontra vonatkozik, a szolgáltató nyilvántartásából ekkor frissítették
- producedAt – ekkor készült (csak OCSP)
- nextUpdate – ekkor már biztosan lesz újabb CRL / OCSP válasz (eddig érvényes??)

- revocationDate – az adott tanúsítványt ekkor vonták vissza (<thisUpdate)
- invalidityDate – kulcskompromittálódás feltételezett időpontja (lehet <revocationDate, lehet <thisUpdate !)

Visszavonási állapot vizsgálata

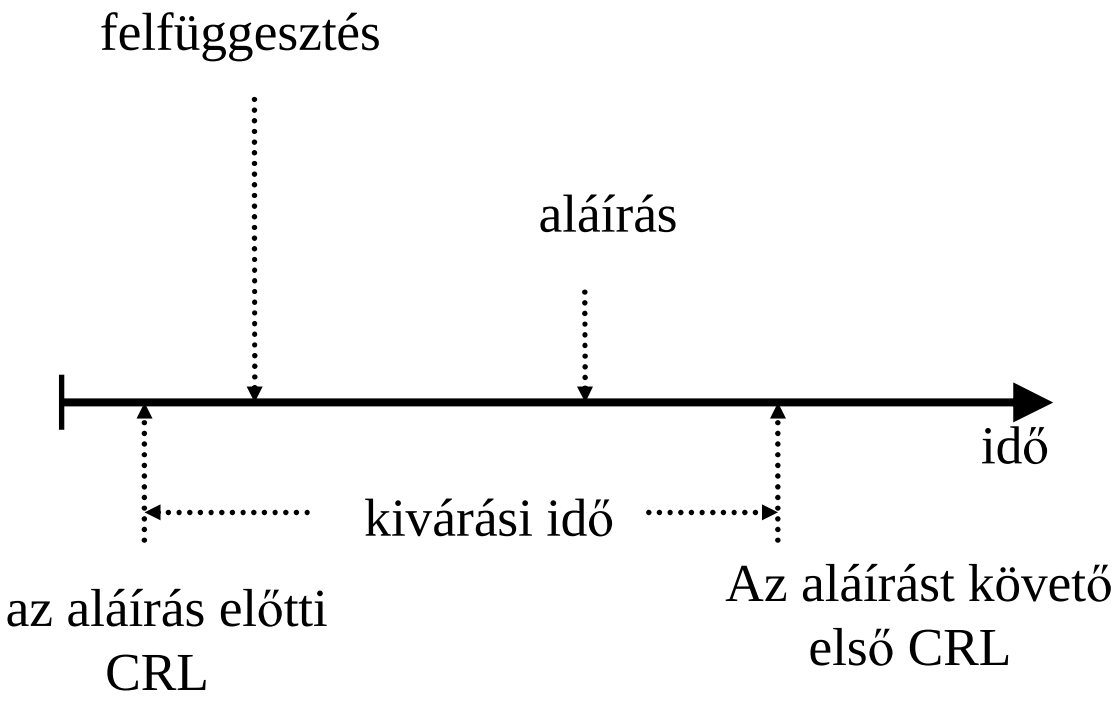
Lehetséges hozzáállások:

- A tanúsítvány „jó”, amíg le nem jár.
  (Nem vizsgálunk visszavonási állapotot.)
- A tanúsítvány „jó”, kivéve, ha tudunk róla, hogy visszavonták.
  - bármilyen régi visszavonási információt elfogadunk (☹)
  - csak a még nem lejárt visszavonási információt fogadjuk el (CRL.nextUpdate>controlTime)
- Meg akarunk győződni róla, hogy a tanúsítvány az aláírást követően is jó volt. (Már meg kellett volna jelennie az új CRL-nek, de nem jelent meg. Biztos?)
  (controlTime+ΔT időpontban nincs negatív CRL)
- Arra keresünk bizonyítékot, hogy a tanúsítvány az aláírást követően is „jó” volt (CRL.thisUpdate>controlTime)
- Még tovább várakozunk.
  (CRL.thisUpdate>controlTime+ΔT)
  De mire várunk?

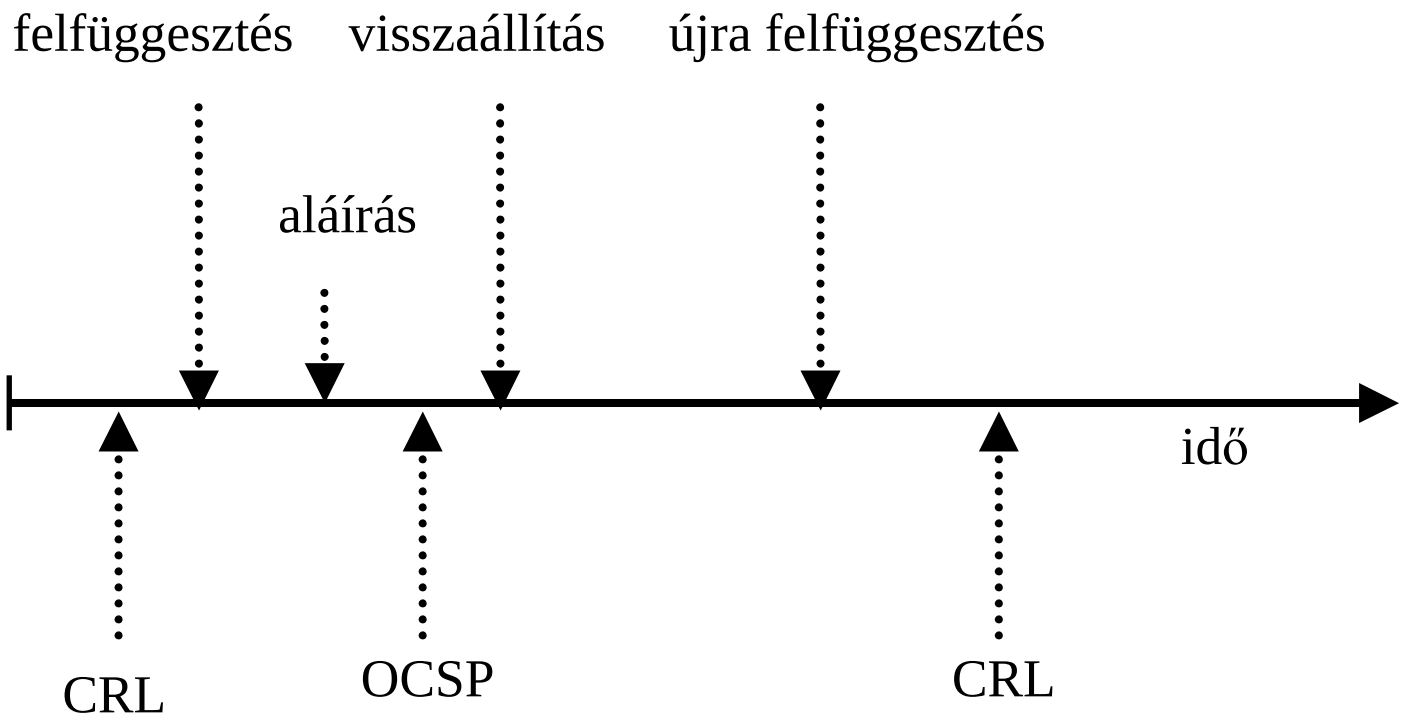
Kivárási idő (grace period)

- Az aláírás időpontjában elérhető legfrissebb CRL-ek nem mindig alkalmasak az aláírás ellenőrzésére, mert
  - a kulcs kompromittálódást csak későn veszi észre az ügyfél (ez nem tartozik ide, PKI alapon nemigen kezelhető)
  - a felfüggesztési/visszavonási kérelem benyújtása és feldolgozása időt vesz igénybe
    → szolgáltató
  - a visszavonási állapot közzététele időt vesz igénybe
    → szolgáltató
  - az érintett fél csak adott idő után értesül a közzétett visszavonási állapotról (pl. nextUpdate előtt nem)
    → érintett fél ?, szolgáltató ?
  - az érintett fél csak adott idő után tudja igazolni, hogy begyűjtötte a visszavonási információt (XAdES-A)
    → szolgáltató ?

Kivárási idő, példa



Visszavonás időpontja



Aláírás ellenőrzésekor

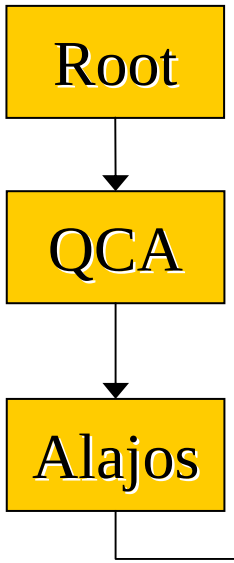
- Az aláírás érvényességét próbáljuk bebizonyítani valamilyen aláírás ellenőrzési szabályzat alapján
- Az aláírás érvényességét egy trust anchor-ra, egy megbízható gyökértanúsítványra vezetjük vissza
- Ennek során aláírt bizonyítékokat is felhasználunk, amelyek lehetnek
  - tanúsítványok,
  - időbélyegek,
  - visszavonási listák,
  - OCSP válaszok,
  - stb.

Aláírás ellenőrzésének menete

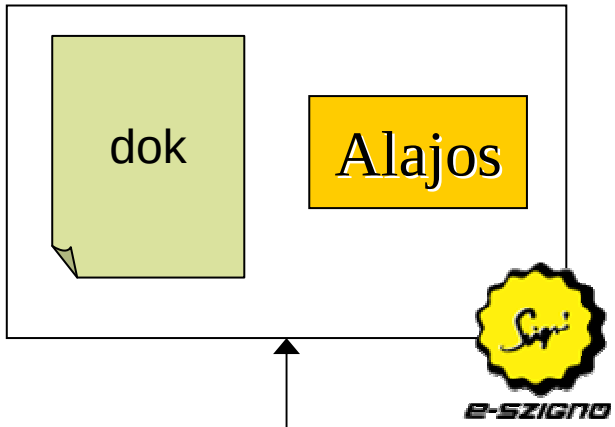
- Meghatározzuk, hogy milyen időpontra vonatkozóan kell ellenőrizni az aláírást
  - ha időbélyeg alapján, ekkor ellenőrizni kell az időbélyeget és a rajta lévő aláírást ($\rightarrow$)
  - biztonságos naplófájl vagy más bizonyíték alapján
  - ha ezek egyike sem létezik, akkor az aktuális időpontra nézve ellenőrizhetünk
- Az adott időpontra nézve
  - felépítjük a tanúsítványláncot,
  - ellenőrizzük a láncban lévő tanúsítványokon az aláírást ($\rightarrow$)
  - bizonyítékokat (CRL/OCSP) gyűjtünk a láncban lévő tanúsítványok visszavonási állapotára, és ellenőrizzük a rajtuk lévő aláírást ($\rightarrow$)
  - az egyes bizonyítékokon lévő aláírásokkal kapcsolatban kivárási időt érvényesíthetünk

Aláírás ellenőrzése, -BES

Hierarchia



Aláírás



Ellenőrzések

aláírás (most)

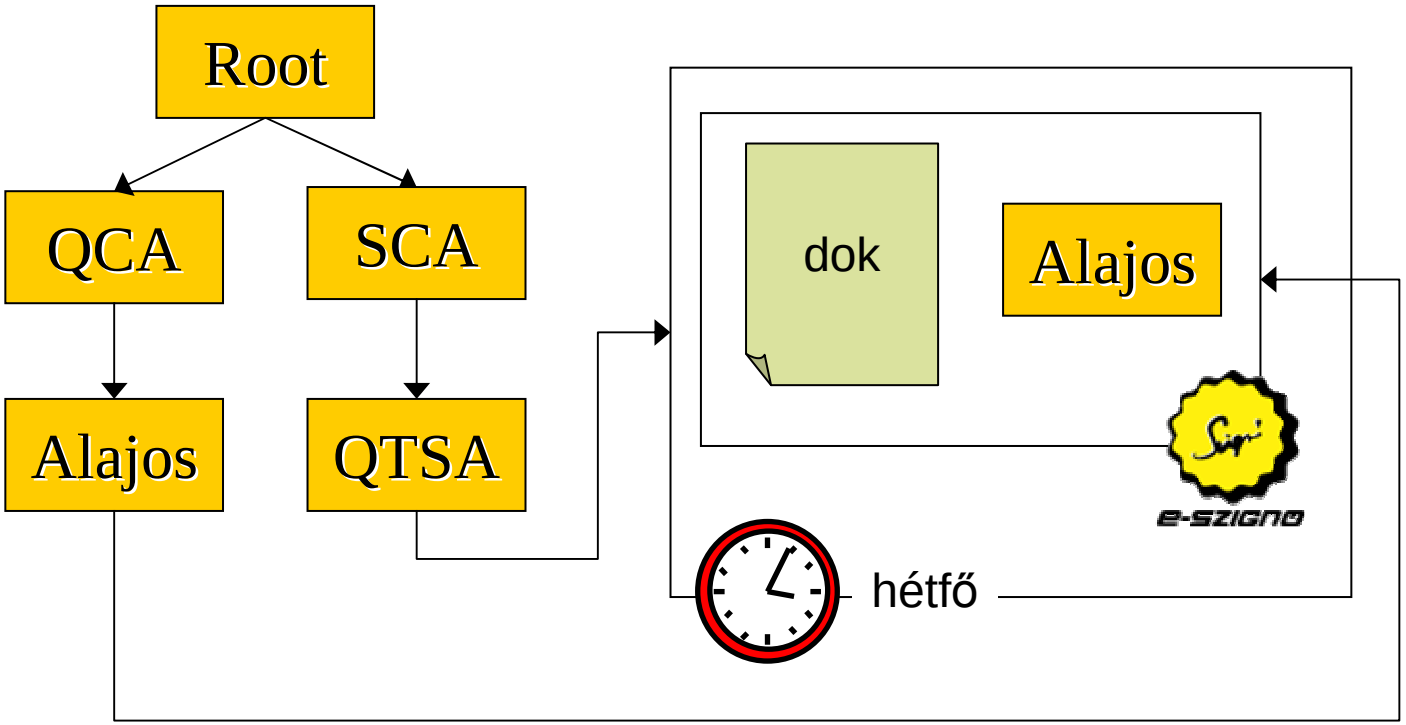
Alajos (most)
QCA-CRL (most)

QCA (most)
Root-CRL (most)

Root (most)

Aláírás ellenőrzése, -T

Hierarchia



Aláírás

Ellenőrzés

aláírás (hétfő)

Alajos (hétfő)
QCA-CRL (hétfő)

QCA (hétfő)
Root-CRL (hétfő)

Root (hétfő)

időbélyeg (most)

QTSA (most)
SCA-CRL (most)

SCA (most)
Root-CRL (most)

Root (most)

Az ellenőrzés eredménye lehet

- ÉRVÉNYES: az aláírás érvényessége az ellenőrzési szabályzat szerint **levezethető**, bizonyítható
- BEFEJEZETLEN: az aláírás érvényessége az ellenőrzési szabályzat szerint csak további bizonyítékok alapján lenne levezethető, és ezen bizonyítékok (visszavonási információk) még nem jöttek létre; az ellenőrzést később meg kell ismételni
- ÉRVÉNYTELEN: az aláírás érvényessége az ellenőrzési szabályzat szerint nem vezethető le, vagy létezik olyan bizonyíték, amely értelmében az aláírás érvénytelen

Ha műszakilag érvényes az aláírás

- Nem biztos, hogy el is fogadhatjuk egy adott célra.
- Lehet, hogy
  - az aláíró hazudik
  - az aláíró nem volt jogosult aláírni a dokumentumot
  - nem tudjuk megállapítani az aláíró kilétét (bár ez nem mindig baj)
  - az aláíró tévedésből vagy kényszer alatt írta alá
  - az aláírót megtévesztették (pl. vírusos számítógép)
  - az aláíró elfelejtette vagy nem tudta bejelenteni a kulcskompromittálódást
- Ne feledjük, hogy aláírás érvényességéről csak valamilyen szabályzat kontextusában beszélhetünk!

Mitől válhat egy aláírás érvénytelenné?

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

Tanulság

- Az aláírás műszaki és jogi érvényessége két külön fogalom.
- A minősített aláírásra szigorú szabályok vonatkoznak
  - Könnyen megfeleltethető egy adott biztonsági szintnek.
  - Természetes személyhez kapcsolódik.
  - Teljes bizonyító erejű magánokirat hozható létre vele.
- A fokozott biztonságú aláírásra kevesebb szabály vonatkozik, rugalmasabban használható.
- Az aláírás érvényessége nem objektív fogalom, csak egy policy kontextusában tárgyalható.
- Az aláírások érvényessége időbélyegek érvényességére alapul, az aláírásnak az időbélyeggel együtt van értelme.
- Gondoskodni kell az aláírások hosszú távú hiteles archiválásáról.

Köszönöm a figyelmet