MICROSEC
Számítástechnikai Fejlesztő zrt.

Algoritmusváltás a magyar elektronikus aláírás rendszerekben

Dr. Berta István Zsolt

e-SZIGNO

Miről fogok beszélni?

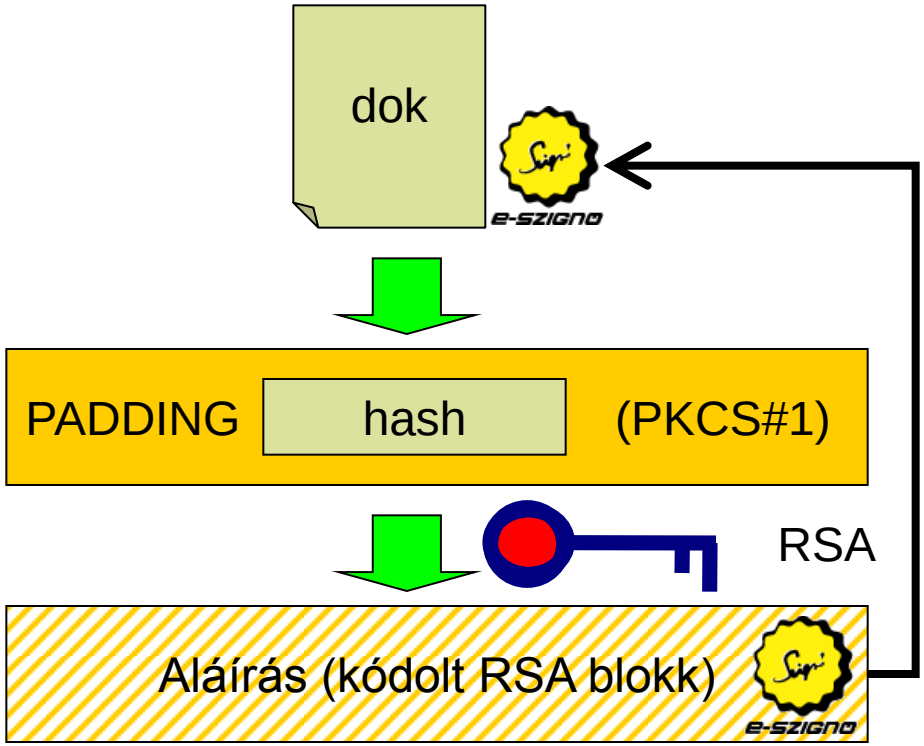
- Az elektronikus aláírások biztonsága kriptográfiai algoritmusok erejére épül
- A közelmúltban megváltozott az elektronikus aláíráshoz használható kripto algoritmusok köre
- Ez nemcsak a hitelesítés-szolgáltatóknál eredményezett változásokat, hanem az e-aláírást készítő és ellenőrző feleknél is
- Eddig „élesben” még nem történt ilyen
- Előadásomban az ezzel kapcsolatos eseményekről, illetve a belőlük levonható tanulságról, tapasztalatokról fogok beszélni

Milyen algoritmusokat kellett cserélni és miért?

Aláírás készítésekor…

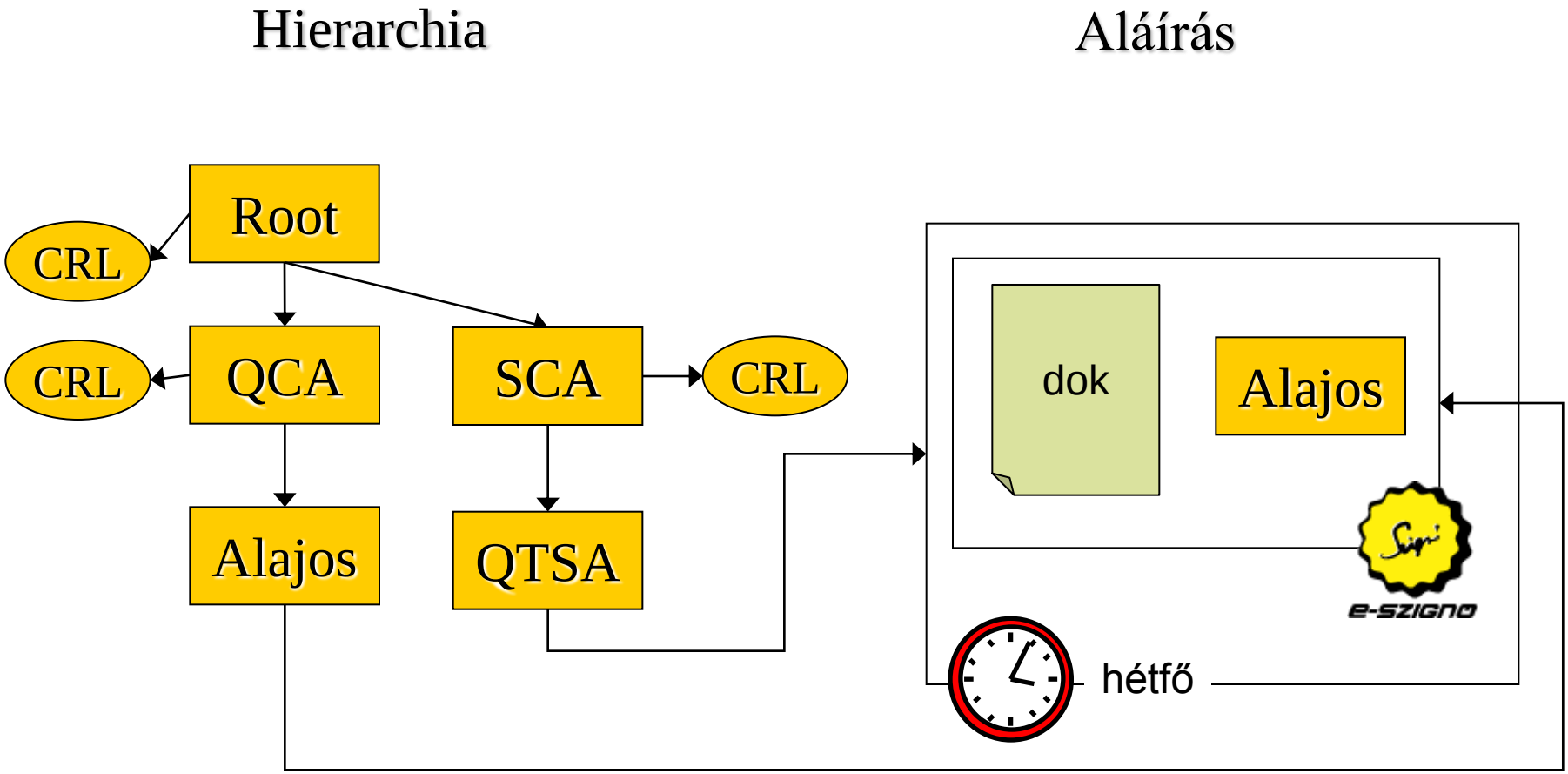
- Lenyomatot képzünk az aláírandó dokumentumból, általában több lépésben
- A lenyomatot kódoljuk a saját magánkulcsunkkal, ez a kripto aláírás
- Az aláírás a tanúsítványunkban lévő nyilvános kulcsunkkal ellenőrizhető
- A tanúsítvány egy tanúsítványlánc alapján ellenőrizhető
- Az aláíráson időbélyeget szokás elhelyezni, ahhoz is tartozik tanúsítvány és lánc is

Kriptográfiai értelemben vett aláírás



RSA blokkméret pl: 2048 bit

Az aláíráshoz szükséges infrastruktúra



Nemzetközi szabványok változása

- Európa: ETSI TS 102 176-1 (ALGO paper):
  - 2007: az SHA-1 és az 1024 bites RSA legfeljebb 1-3 évig javasolt
  - 2011: az SHA-1 és az 1024 bites RSA tiltott
- USA: NIST SP 800-57:
  - az 1024 bites RSA fokozatosan kivezetésre kerül
  - a CA-k 2012-től nem bocsáthatnak ki ilyen tanúsítványt, az érvényben lévőknek le kell járnia 2013 végéig
  - véletlen bitek kötelező szerepeltetése a tanúsítványokban
  - Microsoft, Mozilla, stb.

Hazai előírások változása

- A Nemzeti Média- és Hírközlési Hatóság határozza meg a szolgáltatók által használható kriptográfiai algoritmusok körét (Eat. 18. §)
- Az ETSI ALGO papert veszi alapul
- 2008-as algoritmus-határozat (HL-21917-13/2008)
  - az SHA-1 és 1024 bites RSA „nem ajánlott”
- 2011-es algoritmus-határozat (EF/26838-10/2011)
  - az SHA-1 tiltott,
  - 1024 bites RSA: ???? → „nem ajánlott”
  - Kelt: 2011. szeptember 27-én
  - Tiltás: 2012. január 1-től (!!)

A hazai e-aláírás rendszerekről

- Fő felhasználási területek:
  - igazságszolgáltatás (e-cégeljárás, ügyvédek, közjegyzők, bírósági végrehajtók)
  - e-számlázás, hiteles digitalizálás és megőrzés
  - bankok, pénzintézetek, egyes hatóságok
- Aláírók:
  - ~ 10-20 ezer emberi felhasználó
  - néhány automata → sok okirat
- ~ 300 millió meglévő e-aláírt okirat
- Gyorsan növekvő piac

Az algoritmusok cseréje

Algoritmuskészletek cseréje

- Az RSA kulcsméret megnövelése:
  1024 bit → 2048 bit
- Lenyomatképző algoritmus cseréje:
  SHA-1 → SHA-2 (SHA-256)

- A változások egy része jogszabályi előírás volt, egy másik részét a „józan ész” diktálta

Szempontok

- Határidőre át kellett térni az új algoritmusokra
- A működő elektronikus aláírás rendszerek nem állhattak le
- Sok különböző helyen kell változtatni, ez nem tud egyszerre történni
- A meglévő aláírások érvényessége és ellenőrizhetősége ne kerüljön veszélybe

Mit csináltunk?

- Új CA hierarchiát hoztunk létre, új gyökérrel
- Az e-Szignó programot felkészítettük az új algoritmusok fogadására
- Az időbélyegzés szolgáltatásunkat átállítottuk az új algoritmusokra
- Át kellett térni új algoritmusokat támogató ún. „BALE” tanúsítású intelligens kártyákra
- Ügyfeleknél:
  - frissíteni kellett az aláírás-létrehozó alkalmazást
  - minden ügyfélnél le kellett cserélni a kártyákat
  - meglévő aláírások felülidőbélyegzése → …

Időzítés – fokozatos átállás

- 2009: Új algoritmusokat támogató „rendszerek” kiépítése, létrehozása
- 2010-től: Új algoritmusokat elfogadó rendszerek és szoftverek terjesztése
- 2011 kezdetétől:
  Átváltás, azaz alapértelmezetten új típusú aláírások/tanúsítványok létrehozása
- 2012 ???: Régi aláírások/rendszerek elutasítása

- A webszerver tanúsítványok kivételt jelentenek.
- További info:
  http://berta.hu/publications/Berta2011efpe.pdf

Problémák… ☹

A néhány legsúlyosabb probléma

1. Szabályozási zavarok, logisztikai kérdések…
2. Pontosan kire/mire vonatkozik az algoritmus-határozat?
3. Mi lesz a korábban létrehozott, régi algoritmusokra épülő aláírásokkal?
4. Hogyan történik a régi algoritmusok letiltása?

1. Szabályozási zavarok, logisztikai kérdések

- Egy ilyen áttérés **hosszú** időbe telik
- Elsősorban azért, mert nemcsak a szolgáltatókat érinti, hanem az ügyfeleket is
- Nem voltak tiszták és világosak a határidők, hogy mit mikorra kell végrehajtani
- Az éles követelmény megjelenésétől a végrehajtásig alig 3 hónap állt rendelkezésre
- Korábban kellett volna kihirdetni az áttérés határidejét

2. NMHH határozat – kire/mire vonatkozik?

- ***Eat. 18. §*** *„A Hatóság figyelemmel kíséri az elektronikus aláírással kapcsolatos technológia és kriptográfiai algoritmusok fejlődését és határozatba foglalja* ***a szolgáltatók által szolgáltatásaik nyújtása során*** *használható biztonságos kriptográfiai algoritmusokat és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket. […]”*

2. NMHH határozat – kire/mire vonatkozik?

- A határozat a szolgáltatókra vonatkozhat
- Nem vonatkozik az aláíró által használt hash függvényre
- Nem vonatkozik az időbélyeget lekérő által használt hash függvényre
- Pedig ezek talán a legfontosabb, legérzékenyebb lenyomatok
- Ezeken a helyeken akár MD5 vagy MD2 is szerepelhet
- Így a lényeg veszett el… ☹

3. Régi aláírások érvényessége

- Ha a régi aláírásokat felülidőbélyegzik, igazolhatók, hogy akkor készültek, amikor még erősek volt az SHA-1 és az 1024 bites RSA
- A felülidőbélyegzés az archív szolgáltatónál elhelyezett okiratokon megtörtént
- De az okiratok legalább 90%-án szinte biztosan nem

- Érvényesek azok az aláírások???
  - jogilag: valószínűleg igen
  - műszakilag: hogy állapítom meg?

4. Régi algoritmusok letiltása

- Az aláírás befogadónak akkor hasznos az algoritmusváltás, ha kitilthatja rendszeréből a régi algoritmusokat
- Egyes pontokon még mindig szabad használni ezeket régi algoritmusokat
- Egyes szolgáltatók még használják őket, illetve nem vezették ki őket az ügyfeleiknél

- Nem tudjuk kitiltani őket az ügyfeleink rendszereiből! ☹

Összefoglalás

- Egy algoritmusváltás ügyfeleket is érint, **sok időt** vesz igénybe
- A lebonyolításához világos, értelmes szabályokra, előre ismert határidőkre, és erős szabályozásra lenne szükség
- A szolgáltatók és az ügyfeleik számra országosan százmillió forintos nagyságrendű költséget okozott a váltás
- De a dolog értelme valahol elveszett…

Köszönöm a figyelmet!