MICROSEC
Számítástechnikai Fejlesztő Kft.

# Azt írom alá, amit a képernyőn látok?

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

Microsec Kft.

# Miről fogok beszélni?

- Ökölszabály: Először mindig olvassuk el, amit aláírunk.
- Elektronikus aláírás esetén ez miért nem ilyen egyszerű?
  - Pontosan mire kerül az aláírás?
  - Hiteles megjelenítés kérdése
- Hogyan kezelhetjük ezt a gyakorlatban?

# Ökölszabály

- Aláírás: Értelmes tartalom elfogadása, tudomásul vétele, vagy kötelezettségvállalás ezen értelmes tartalom iránt.
- Ha aláírunk valamit, annak következménye lehet.
- Erősen ajánlott először elolvasni, amit aláírunk.

- Mindez egyaránt igaz a papír alapú és az elektronikus aláírásra

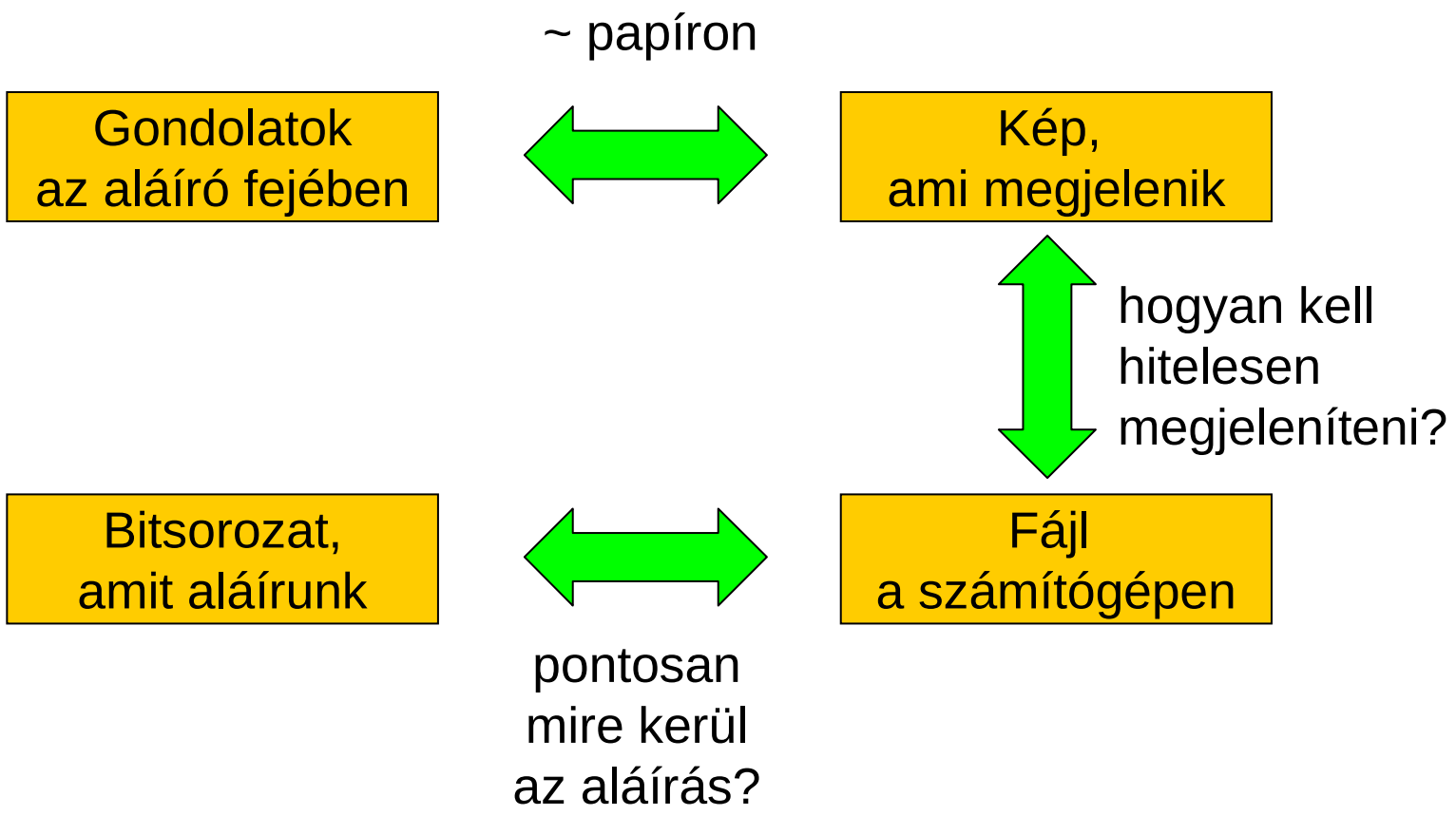
# „What you see is what you sign”

- Az aláírás-létrehozó alkalmazásnak először meg kell jelenítenie a dokumentumot, amit aláírunk.
- „A biztonságos aláírás-létrehozó eszköz[ök] [...] nem akadályozhatják meg azt, hogy az aláíró a dokumentumot az aláírási eljárás előtt megjelenítse.”
  (Eat. 1. melléklet, 2.)
- „The SDP shall ensure that the SD presented to the signer by the SDP is the same as the one that will be signed in the signature process, and is the same as that selected by the signer for signing.”
  CWA 14170, 8.3. fejezet, 4. pont

# Miért nem ilyen egyszerű?

- Az aláíró egy értelmes tartalmat szeretne aláírni (gondolatok)
- A képernyőn egy kép jelenik meg (kép, pixelek)
- A tartalmat a számítógép egy fájlban tárolja el (fájl, bitsorozat)
- A magánkulccsal az e fájlból bonyolult számításokkal kapott, és különféle további információkkal kiegészített blokkot írjuk alá (bitsorozat, amit aláírunk)

# Mi a kapcsolat közöttük?

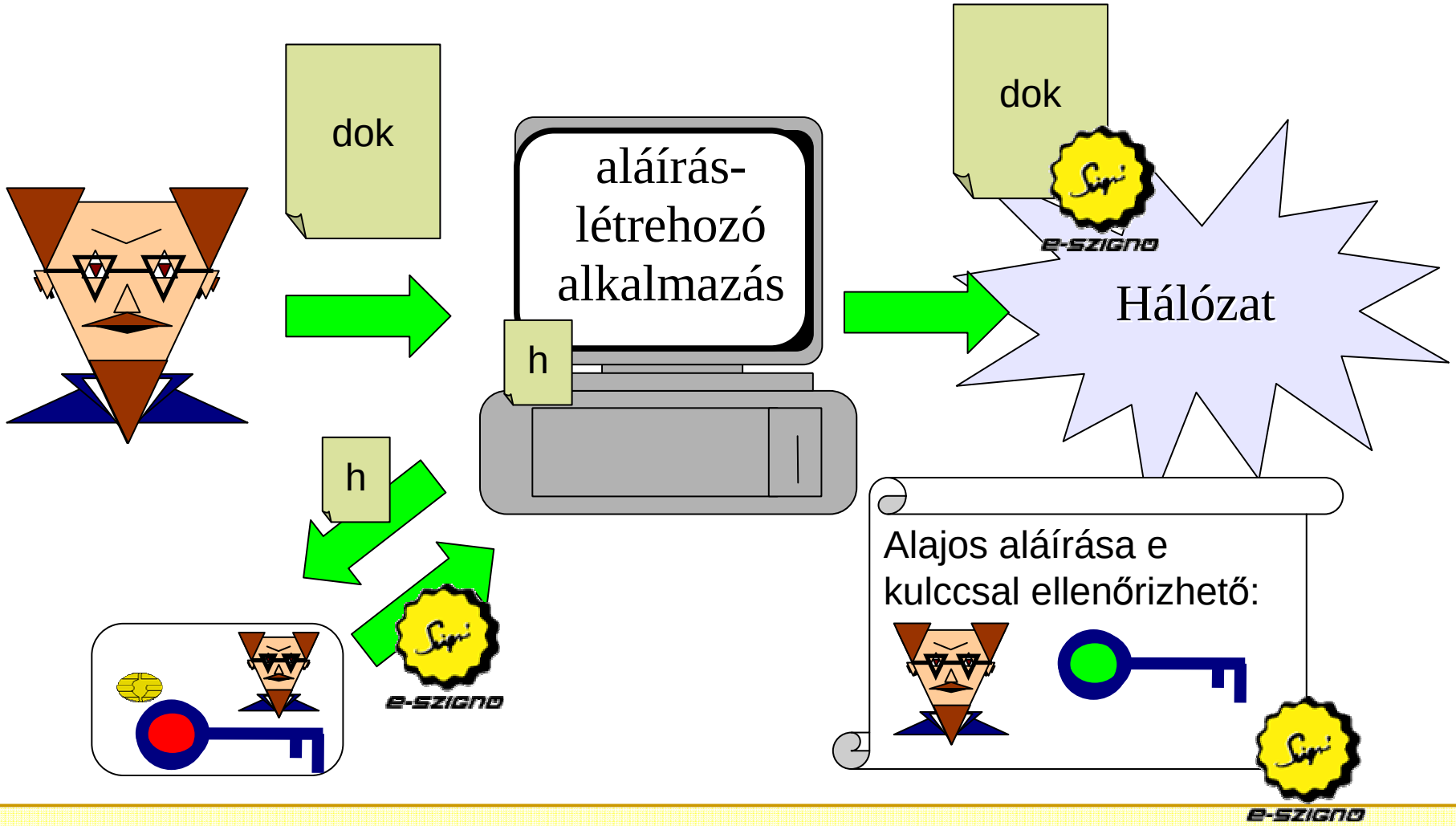


# Pontosan mire kerül az aláírás?

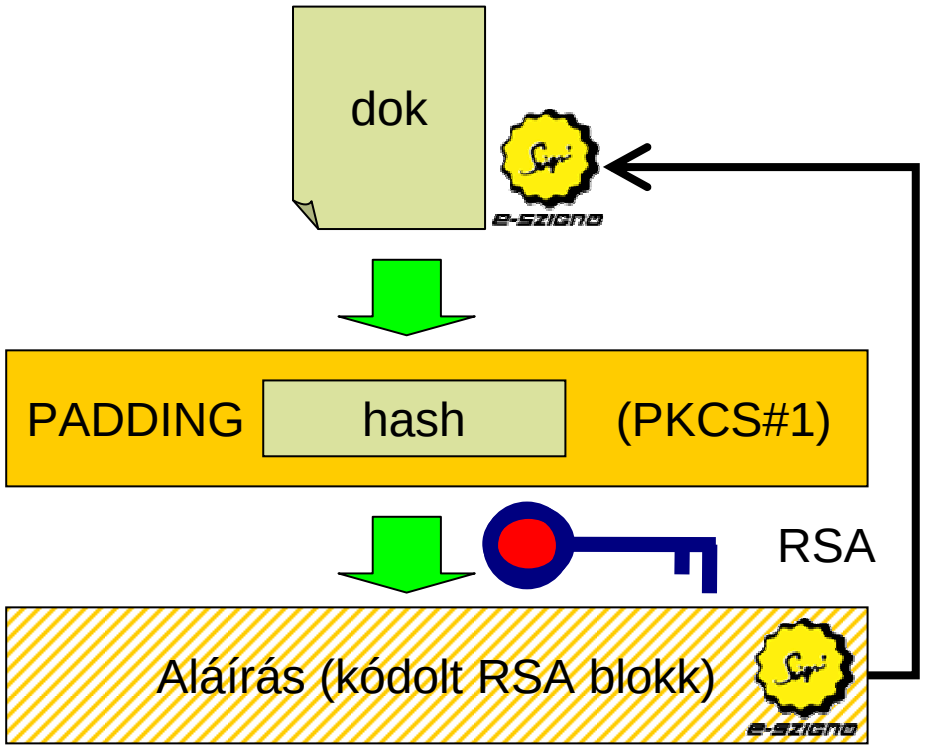
# Aláírás készítése

1. Az aláíró megtekint egy dokumentumot, majd úgy dönt, aláírja. Átadja az aláírás-létrehozó alkalmazásának.
2. Kriptográfiai lenyomat (hash) képzése a dokumentumból.
3. A hash eljuttatása az aláírás-létrehozó eszköznek (chipkártya/HSM/számítógép).
4. Az aláírás-létrehozó eszköz az aláíró magánkulcsával kódolja a hash-t, és az eredményt – az aláírást – visszaküldi az aláírás-létrehozó alkalmazásnak.

# Aláírás készítése

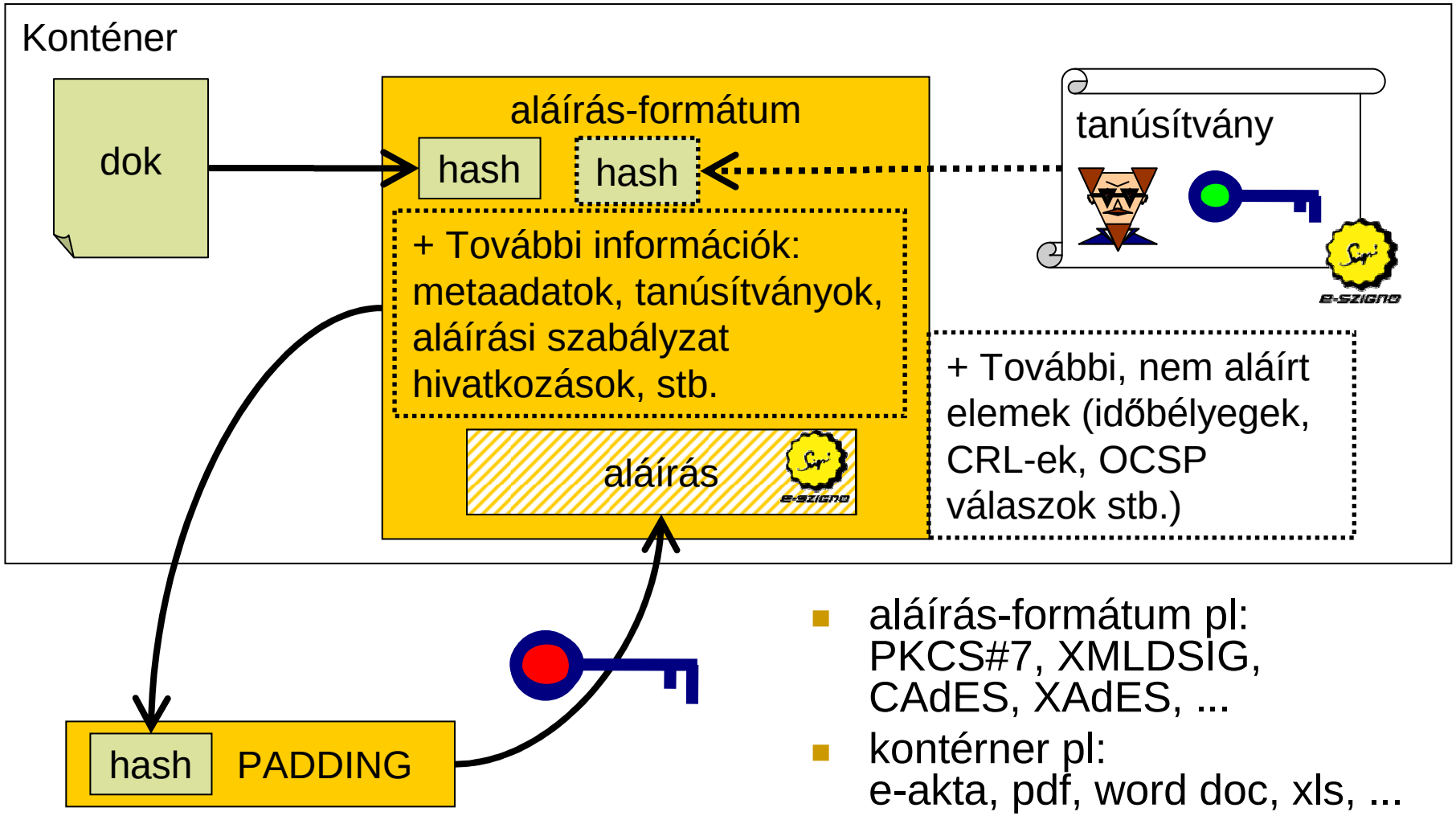


# Hogyan készül az aláírás (egyszerű ábra)?




RSA blokkméret pl: 2048 bit

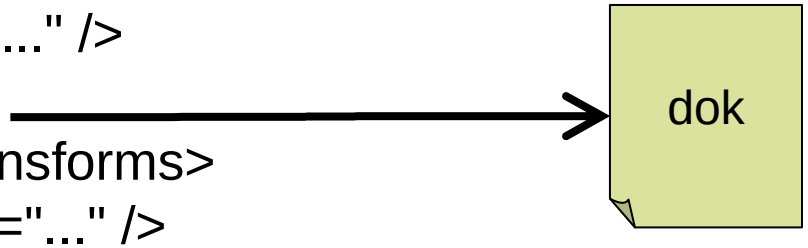
# Hogyan készül az aláírás (valójában)?




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

# XMLDSIG aláírás

```
<ds:Signature>
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="..." />
    <ds:SignatureMethod Algorithm="..." />
    <ds:Reference Id="..." URI="...">
          <ds:Transforms> ... </ds:Transforms>
          <ds:DigestMethod Algorithm="..." />
          <ds:DigestValue>...</ds:DigestValue>
     </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue ...> ... </ds:SignatureValue>
  <ds:KeyInfo ...> ... pl. aláírói tanúsítvány ... <ds:KeyInfo>
    ...
</ds:Signature>
```



# XAdES aláírás

```
<ds:Signature>
  <ds:SignedInfo>
    <ds:CanonicalizationMethod Algorithm="..." />
    <ds:SignatureMethod Algorithm="..." />
    <ds:Reference Id="..." URI="..."> ... </ds:Reference>
  </ds:SignedInfo>
  <ds:SignatureValue ...> ... </ds:SignatureValue>
  <ds:KeyInfo ...> ... <ds:KeyInfo>
  <ds:Object><xades:QualifyingProperties>
          <xades:SignedProperties> aláírási szabályzat ref., aláírás  helye,
          ideje, aláíró szerepe stb. </xades:SignedProperties>
          <xades:UnsignedProperties> időbélyeg, visszavonási
          információk,archiváláshoz szükséges információk
    </xades:UnsignedProperties>
    </xades:QualifyingProperties></ds:Object>
</ds:Signature>
```

# Az aláírás-formátum blokk szerepe

- Meghivatkozza, hogy mire vonatkozik az aláírás
- Leírja, hogy milyen algoritmusok szerint készült az aláírás
- Meghivatkozhatja az aláírói tanúsítványt (XAdES esetén kötelező)
- Meghivatkozhatja az aláírási szabályzatot
- Tartalmazhat segítséget az aláírás ellenőrzéséhez (pl. tanúsítványláncot)
- Tartalmazhat időbélyeget és az archiváláshoz szükséges információkat

# Mi az, amit aláírunk?

- Az értelmes dokumentum tartalma?
- A kép, ahogy a dokumentum megjelenik?
- A fájl, amely a dokumentumot tartalmazza?
- A fájl a különféle transzformációkat követően?
- A transzformációkon átesett fájl lenyomata?
- Az aláírás-formátum blokk?
- Az aláírás-formátum blokk lenyomata?
- Az előbbi lenyomat paddinggel ellátva?

# Mit jelenítsen meg az aláíró program?

- Az értelmes dokumentumot?
  - amire az aláíró gondolt???
- A fájlt
  - hogyan kell hitelesen megjeleníteni?
- Az aláírás-formátum blokkot?
  - az aláíró nem érti / nem kontrollálja
- Valamelyik lenyomatot?
  - annak mi értelme van? honnan tudjuk, hogy az minek a lenyomata?
- …

# Hiteles megjelenítés kérdése

# Mi a probléma?

- Komplex dokumentum-formátumokat használunk
- Ezek hiteles, egyértelmű megjelenítése nem egyszerű feladat
- Egy dokumentum megjelenítése az informatikai környezet nagyon sok elemétől függ

- Mi biztosítja, hogy az aláírást befogadó fél ugyanazt a dokumentumot látja, amit az aláíró aláírt?
- A két dokumentum tartalma ugyanaz?

# Miért jelenhet meg másképp?

- Ha nem tudjuk, hogy mivel, és hogyan kell megjeleníteni
- Megjelenítő eszköz típusa, verziószáma
- Megjelenítő eszköz beállításai
  - pl: rejtett szöveg megjelenítése
- Plugin-ek a megjelenítő eszközben
- A megjelenítéshez használt egyéb könyvtárak
  - típusa, verziószáma stb.
- Operációs rendszer beállítása
  - pl: betűkészlet, papírméret, regionális és nyelvi beállítások
- Aktív tartalom a dokumentumban
  - pl: makrók
- „Vírus” a dokumentumban
- A dokumentum tartalma, szövegezése félreérthető
- Ha nem egyértelmű, hogy mit jelent az aláírás
- …

# Hogyan jelenthet biztonsági problémát?

- A támadó olyan dokumentumot készít elő az aláíró számára, amelyben lényeges elemek másképp, más tartalommal jelennek meg, mint általában
- Az aláíró szándékosan készít többféleképpen értelmezhető dokumentumot/aláírást
- Az aláírást befogadó fél rájön, hogy a kapott aláírt dokumentum többféleképpen értelmezhető, és ezt kihasználja
- Nagyon sok idő telik el az aláírás óta, és már nem tudjuk, hogyan kell hitelesen megjeleníteni (pl. megszűnik a fájlformátum)

# Példák

- Nem rögzítjük, hogy pontosan milyen típusú fájlra kerül az aláírás
  - Buccafurri: A new Attack on Digital Signature, http://www.unirc.it/firma/en/attack_en.html
  - Rybár: http://elpi2.szm.com/priklad.htm
- „Hidden” betűtípus, word dokumentumban
- Word makró, a dokumentum másképp jelenik meg ma és holnap
- Betűkészlet megváltoztatása az aláíró számítógépén
  - Leitold: Vulnerabilities of the usage of digital signature, 15th EICAR Conf., Hamburg, 2006
- Más betűtípussal ugyanazon szöveg, más jelentés

# Többféleképpen értelmezhető szöveg

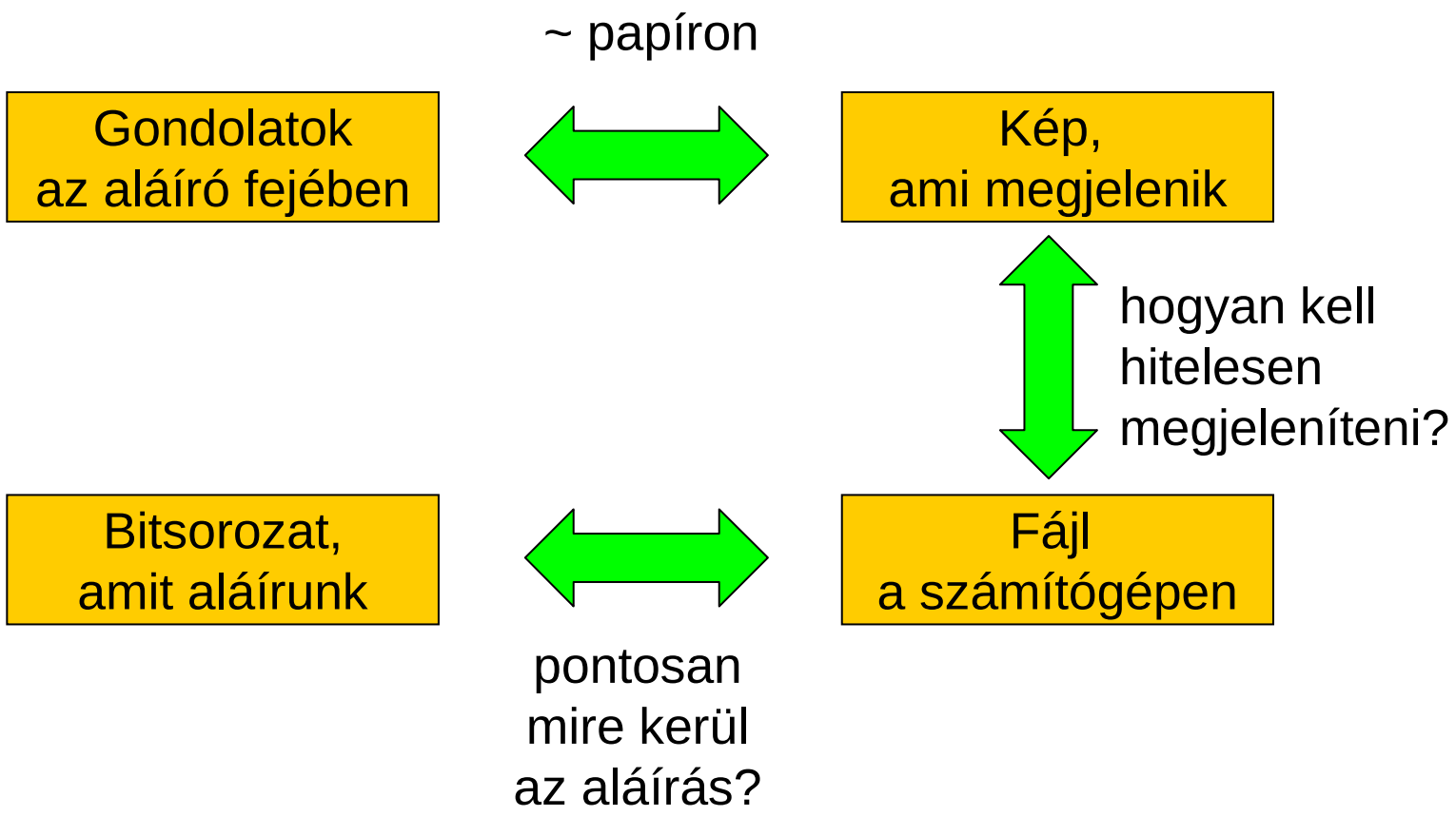
- A királynét megölni nem kell félnetek jó lesz ha mindenki beleegyezik én nem ellenzem.

- A királynét megölni nem kell félnetek, jó lesz, ha mindenki beleegyezik, én nem ellenzem.
- A királynét megölni nem kell, félnetek jó lesz, ha mindenki beleegyezik, én nem, ellenzem.

http://hu.wikipedia.org/wiki/Reginam_occidere

# Mit tehetünk a gyakorlatban?

# Visszatekintés



# Pontosan mire kerül az aláírás?

- Az értelmes tartalom a fontos az aláíró számára
- Az aláírandó fájl az egzakt, ezt lehet megjeleníteni
- A fájlt önmagában nem elég aláírni, ki kell egészíteni további adatokkal
- Egy bizonyos szinten túl nincs értelme élezni, hogy pontosan milyen transzformációkon mehet keresztül az aláírandó fájl, de ki kell, hogy lehessen deríteni, hogy mi történik
- Célszerű bevizsgált, tanúsított aláíró alkalmazást használni

# Hiteles megjelenítés kérdése

- Nem e-aláírás-specifikus probléma, de itt különösen élesen jelenik meg
- Célszerű kerülni az aktív tartalmat megengedő formátumokat
- Célszerű nyílt formátumot használni
- Spec. archiváló formátumok (pl: PDF/A)
- Archiválás szolgáltatás, olvashatóság, értelmezhetőség
- Bármilyen formátum esetén felmerül e kérdés!
- Egy bizonyos szinten túl már nem műszaki, hanem jogi problémáról van szó, ne műszaki megoldást keressünk rá
- E probléma papíron is felmerül, jogi eszközökkel gyakran nagyon egyszerűen kezelhető

# Összefoglalás

- Továbbra is erősen ajánlott először elolvasni, amit aláírunk
- Ha a „what you see is what you sign” elvet a végsőkig el akarjuk vinni, könnyen kaphatunk a gyakorlatban használhatatlan megoldást
- Az aláírandó értelmes tartalmat célszerű megjeleníteni, ez a fontos az aláíró számára
- Az aláírandó fájl egzakt, ez az, amit később is meg lehet jeleníteni
- Az „erre gondolt-e az aláíró” probléma papíron ugyanúgy felmerül, a jogászok már régóta kezelik

# Köszönöm a figyelmet!

MICROSEC
Számítástechnikai Fejlesztő Kft.

# Azt írom alá, amit a képernyőn látok?

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

Microsec Kft.