eSign Day 2022

Visszaélés digitális aláírással és digitális aláírt irattal – hogyan védekezhetünk visszaélések ellen?

Dravecz Tibor Kálmán, INTEGRITY Kft.

2022. június 30. 15:15 - 15:35

Hagyományos aláírás (és pecsét)

Főbb biztonsági hátrányok:

- **Hitelesség** nehezen és bizonytalanul verifikálható, a verifikáció speciális szakértelmet és technikai felkészültséget, valamint az aláírt üzeneten (pl. dokumentumon) és az aláíráson felül **plusz információt** igényel
- **Integritás** nem biztosítható jól, valamint – **még plusz információk birtokában is** – nehezen verifikálható
  - Következésképpen könnyű visszaélési lehetőségek kínálkoznak
  - A visszaélési módszerekről több száz éve gyűlik már az ismeret

Biztonsági szempontból előnyös vagy előnyös lehet:

- Hosszú távú archiválást a technika részben segíti – részben pedig nehezíti (kockázat részben nagyobb, részben viszont kisebb)
- Bizonyos speciális esetekben vagy bizonyos digitális aláíró megoldásokkal szemben bizonyos helyzetekben még mindig előnyös vagy célszerű lehet az alkalmazása
- Mondják, hogy azt, hogy az aláíróhoz biológiailag kötődik az aláírás, és ez előnyös – azonban a digitális aláírás tanúsítványa is kötődhet biológiailag a tanúsított személyhez
- Sok esetben aláírás-másolattal (pl. aláírás képével) helyettesítik a hagyományos aláírást, mely megoldás a biztonság szintjét extrém mértékben csökkenti

Biztonsági követelmények

1. Authentication
2. Integrity
3. Non-repudation
4. Proof of existence for long-term archiving

---

5. Sending verifiability
6. Delivery verifiability

   \+ non-repudation of sending or delivery

There are 9 types of qualified trust services, as defined in the Regulation n°910/2014 (the 'eIDAS' Regulation). These types are:

- Qualified certificate for electronic signatures
- Qualified certificate for electronic seals
- Qualified certificate for web site authentication
- Qualified validation of qualified electronic signatures
- Qualified validation of qualified electronic seals
- Qualified preservation of qualified electronic signatures
- Qualified preservation of qualified electronic seals
- Qualified electronic time stamps
- Qualified electronic registered delivery

Digitális aláírás

1990-es évek végéig lényegében: **digitális aláírás = elektronikus aláírás**.

Számítástechnikai szemszögből a digitális aláírás nem csak az eIDAS szerinti digitális aláírást[1] jelenti,
valamint a természetes személy vagy nem természetes személy aláírása, illetve bélyegzője/pecsétje között jelen előadásban nem teszünk különbséget; jelen előadásban nem foglalkozunk a nem kriptográfiai alapon képzett 'elektronikus aláírásokkal' sem.

Digital signiture (DSIG)

The result of a cryptographic transformation of data which, when properly implemented, provides the services of:
1. origin authentication, 2. data integrity, and 3. signer non-repudiation.
Source(s): NIST SP 800-12 Rev. 1 under Digital Signature from FIPS 140-2

An asymmetric key operation where the private key is used to digitally sign data and the public key is used to verify the signature. Digital signatures provide authenticity protection, integrity protection, and non-repudiation, but not confidentiality protection.
Source(s): NIST SP 800-63-3 under Digital Signature; NISTIR 8011 Vol. 3 under Digital Signature from NIST SP 800-63-3

Mi nem tekintjük követelménynek, hogy PKI alapú legyen.

[1] bár a digitális aláírás az eIDAS által nem is használt fogalom

Digital Signature Standard (DSS) FIPS PUB 186-4 (July 2013)

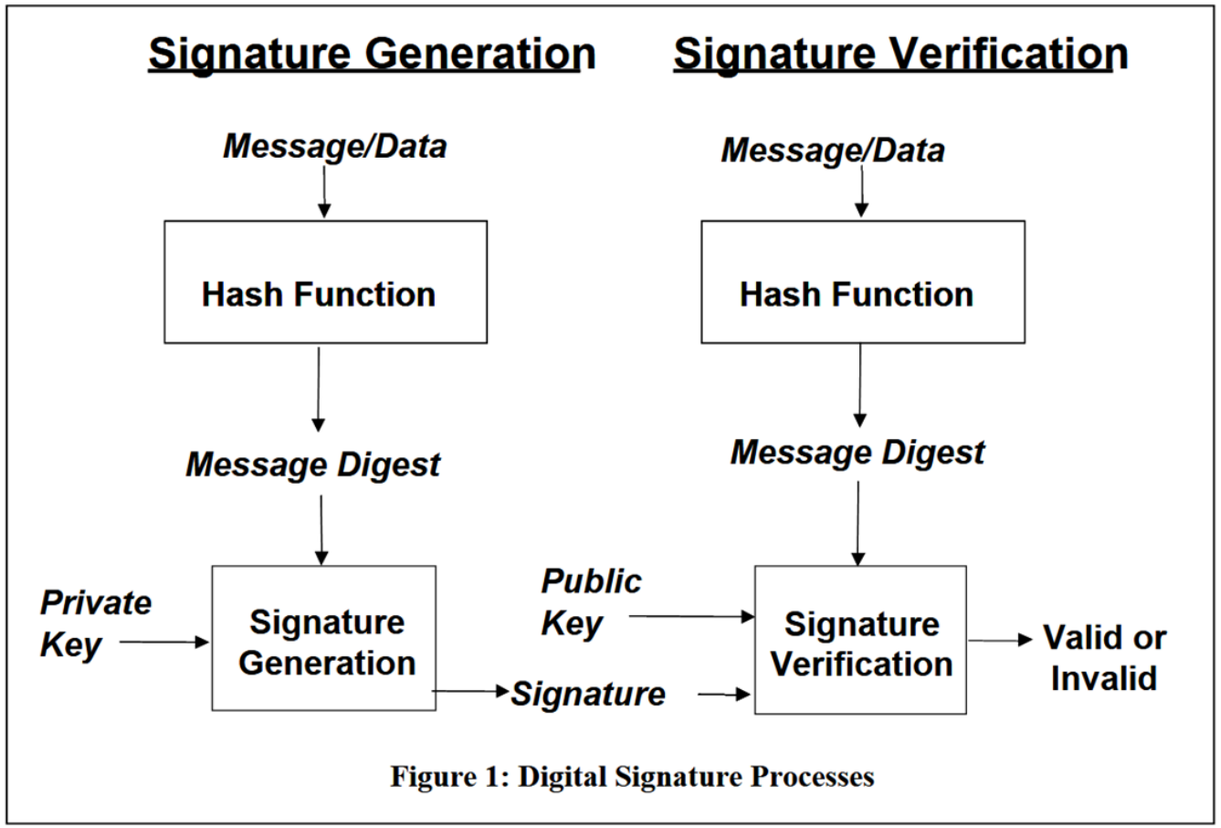

Figure 1: Digital Signature Processes

Digital Signature Standard (DSS) FIPS PUB 186-4
July 2013
https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.186-4.pdf

Digital Signature Standard (DSS),FIBS-186-1
Date Published: December 15, 1998
https://csrc.nist.gov/publications/detail/fips/186/1/archive/1998-12-15

Nem digitális, de elektronikus aláírás

"10. „**elektronikus aláírás**”: olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, és amelyet az aláíró aláírásra használ; *[mint látható ez csak egy pongyola, értéktelen megfogalmazás, meghatározásnak ezt nem mondhatjuk!]*

11. „**fokozott biztonságú elektronikus aláírás**”: olyan elektronikus aláírás, amely megfelel az a 26. cikkben meghatározott követelményeknek;

12. „**minősített elektronikus aláírás**”: olyan, fokozott biztonságú elektronikus aláírás, amelyet minősített elektronikus aláírást létrehozó eszközzel állítottak elő, és amely elektronikus aláírás minősített tanúsítványán alapul;"

eIDAS 3. cikk (Fogalommeghatározások) 10.

eIDAS 26. cikk - A fokozott biztonságú elektronikus aláírásra vonatkozó követelmények
"A fokozott biztonságú elektronikus aláírásnak az alábbi követelményeknek kell megfelelnie:
a) kizárólag az aláíróhoz köthető *[a fogadó jellemzően ezt nemigen tudhatja, de vélelmezheti, és szokás ezt vélelmezni]*;
b) alkalmas az aláíró azonosítására *[ez nem jelenti azt, hogy a fogadó tudja is azonosítani, vagy erősen valószínűsíteni az aláírót]*;
c) olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat;
d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető."

A digitális aláírási folyamatok sérülékenysége

<table>
<tr>
<td rowspan="2">Tanúsítvány-igénylés/Tanúsító-szervezet
->
Tanúsítványkezelés (Tanúsító-szervezet)
->
Privát kulcs kezelése
1. az aláíró saját eszközén
2. szolgáltató eszközén
->
Aláírandó üzenet/dokumentum és előállítása
->
Aláírás
->
Továbbítás
->
Fogadás és tárolás a fogadó számítógépén
->
Aláírás-ellenőrzés
->
Megjelenítés</td>
<td></td>
<td>Hamis névre, hamis adatokkal vagy nem is létező személy nevére kiállított tanúsítvány

Kulcs feletti hatalom megszerzése

A privát kulcs és aláíró folyamat extrém nehezen hamisítható</td>
</tr>
<tr>
<td>Aláírást követő esetleges módosítás(ok)</td>
<td>A digitális aláírás maga nemigen hamisítható

Továbbítás során a digitális aláírás nemigen hamisítható, bár bizonyos szinten manipulálható az üzenet tartalma

Ellenőrzés és megjelenítés sérülékeny lehet</td>
</tr>
</table>

Emberi hibalehetőségek

A teljesség igénye nélkül:

- Privát kulcs gondatlan kezelése
- Ellenőrzés hiánya, vagy az ellenőrzés eredményének téves vagy hanyag interpretációja (hozzá nem értés vagy hanyagság)
- Eszközünk vagy eszközeink (beleértve a minket kiszolgáló eszközöket is) felett illetéktelen kontrollt szerez vagy nem ártó személynek engedjük azt át
- Trükkös támadások
- Nemigen látjuk át egészében a folyamatokat, a működést, azt, hogy honnan leselkedhet veszély - senki sem becsaphatatlan.

Váratlan helyről is érkezhet támadás, példa: a Domain Name System (DNS) meghackelése

EU Trust List

EU Trust Services Dashboard, Trusted List Browser (1.8.0 - 08/06/2022)
https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home

Root tanúsítvány listák

Visszavonási (revocation) listák

Validációs szervizek

...

Egy egész extrém lehetőség: Mimikált tanúsítványkiadó

Védekezési lehetőségek

- **Privát kulcsunk erős védelme**
- **Eszközeink és hálózatunk védelme**
- **Gondos és szakszerű aláírás-ellenőrzés**
- **További ellenőrzések végzése**
  például:
  - a fogadott üzenet DKIM aláírásának ellenőrzés,
  - az üzenet/dokumentum tartalma összhangban van-e a várttal, valaki számára ártó lehet-e,
  - visszaellenőrzések (visszakérdezések).

Szervezeti szintű lehetőségek

Amiről nem beszéltünk: a digitálisan aláírt üzenetek/dokumentumok és hitelességük tartóssága

Tartalom

Copyright

Free Cultural Works
https://freedomdefined.org/Definition
except for quotes and quoted images