MELASZ

Minősített aláírás és az emailek

Erdősi Péter Máté, CISA

2020. november 19.

Tartalom

MELASZ

- Mi az az elektronikus aláírás?
- Miért nem digitális az, ami elektronikus?
- Az európai (eIDAS) és a magyar szabályozás
- Minősített aláírások létrehozása a gyakorlatban
- Message User Agent (MUA) és a minősített elektronikus aláírások

MELASZ

- eIDAS (910/2014 EU rendelet)
- Eübszt. (2015. évi CCXXII törvény)
  - és végrehajtási rendeleteik…

eIDAS (910/2014 EU rendelet)

25. cikk - Az elektronikus aláírás joghatása

(1) Az elektronikus aláírás joghatása és bírósági eljárásokban bizonyítékként való elfogadhatósága nem tagadható meg kizárólag amiatt, hogy az elektronikus formátumú, illetve nem felel meg a minősített elektronikus aláírásra vonatkozó követelményeknek.

(2) A minősített elektronikus aláírás a saját kezű aláírással azonos joghatású.

(3) A valamely tagállamban kibocsátott minősített tanúsítványon alapuló minősített elektronikus aláírást az összes többi tagállamban el kell ismerni minősített elektronikus aláírásként.

Mi van az EU-n kívül?

Electronic Signature Law of the People's Republic of China

Article 2

For the purposes of this Law, electronic signature means the data in electronic form contained in and

attached to a data message to be used for identifying the identity of the signatory and for showing that

the signatory recognizes what is in the message.

The data message as mentioned in this Law means the information generated, dispatched, received or

stored by electronic, optical, magnetic or similar means.

(nincs „qualified electronic signature" definiálva)

The Federal Law of the Russian Federation On Electronic Signature - Article 5. Types of electronic signatures

1. The types of electronic signatures, the relationship in the field of use which are regulated by this Federal Law, They are

- simple electronic signature and
- enhanced electronic signature.

Differ reinforced unskilled electronic signature (hereinafter - non-qualified electronic signature) and Reinforced qualified electronic signature (hereinafter - qualified electronic signature).

(van „qualified electronic signature” definiálva)

MELASZ

- 19. „**bizalmi szolgáltató**”: egy vagy több bizalmi szolgáltatást nyújtó természetes vagy jogi személy; a bizalmi szolgáltató lehet minősített vagy nem minősített bizalmi szolgáltató;

- 20. „**minősített bizalmi szolgáltató**”: olyan bizalmi szolgáltató, amely egy vagy több minősített bizalmi szolgáltatást nyújt, és amelynek minősített státusát a felügyeleti szerv jóváhagyta;

16. „**bizalmi szolgáltatás**”: rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások:

a) elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy

b) weboldal-hitelesítő tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy

c) elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése;

17. „minősített bizalmi szolgáltatás”: olyan bizalmi szolgáltatás, amely megfelel az e rendeletben foglalt alkalmazandó követelményeknek;

MELASZ

- 9. „aláíró”: elektronikus aláírást létrehozó természetes személy;
- 10. „elektronikus aláírás”: olyan elektronikus adat, amelyet más elektronikus adatokhoz csatolnak, illetve logikailag hozzá-rendelnek, és amelyet az aláíró aláírásra használ; (bármi)
- 25. „elektronikus bélyegző”: olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét; (bármi)
- 24. „bélyegző létrehozója”: elektronikus bélyegzőt létrehozó jogi személy;

MELASZ

– NIST FIPS PUB 186-4 „2.1 Digital signature: The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation.”

azaz „digitális aláírás: kriptográfiai művelet eredményeként előálló adat, amely módszert biztosít a forrás hitelességének és az adatok sértet-lenségének ellenőrzésére, valamint az aláírás letagadhatatlanságára – ha helyesen valósítják meg”.

MELASZ

– ISO 7498-2:1989(en) szabvány definícióját: „3.3.26: digital signature: Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient”,

azaz „digitális aláírás: olyan adat, amely hozzákapcsolódik egy másik adategységhez, vagy kriptográfiai művelettel transzformálja azt, és amely lehetővé teszi az adategység fogadójának a forrás és a sértetlenség bizonyítását, valamint védelmet nyújt a (fogadó általi) hamisítás ellen”.

MELASZ

– ETSI EN 319 411-1, 3.1 fejezetében a digitális aláírás definícióját: „Definitions: digital signature: data appended to, or a cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient”.

A definíció teljes mértékben megegyezik az ISO 7498-2 definíciójával.

MELASZ

- 11. „fokozott biztonságú elektronikus aláírás”: olyan elektronikus aláírás, amely megfelel a 26. cikkben meghatározott követelményeknek;
- 26. „fokozott biztonságú elektronikus bélyegző”: olyan elektronikus bélyegző, amely megfelel a 36. cikkben meghatározott követelményeknek;

MELASZ

A fokozott biztonságú elektronikus aláírásnak az alábbi követelményeknek kell megfelelnie (26. cikk):

- 1. kizárólag az aláíróhoz köthető,
- 2. alkalmas az aláíró azonosítására,
- 3. olyan, elektronikus aláírás létrehozásához használt adatok felhasználásával hozzák létre, amelyeket az aláíró nagy megbízhatósággal kizárólag saját maga használhat,
- 4. olyan módon kapcsolódik azokhoz az adatokhoz, amelyeket aláírtak vele, hogy az adatok minden későbbi változása nyomon követhető.

MELASZ

A fokozott biztonságú elektronikus bélyegzőnek az alábbi követelményeknek kell megfelelnie (36. cikk):

- 1. kizárólag a bélyegző létrehozójához kötött,
- 2. alkalmas a bélyegző létrehozójának azonosítására;
- 3. olyan, elektronikus bélyegző létrehozásához használt adatok felhasználásával hozzák létre, amelyeket a bélyegző létrehozója nagy megbízhatósággal kizárólag saját maga elektronikus bélyegző létrehozására használhat;
- 4. olyan módon kapcsolódik azokhoz az adatokhoz, amelyekre vonatkozik, hogy az adatok minden későbbi változása nyomon követhető.

MELASZ

- 12. „minősített elektronikus aláírás”: olyan, fokozott biztonságú elektronikus aláírás, amelyet minősített elektronikus aláírást létrehozó eszközzel állítottak elő, és amely elektronikus aláírás minősített tanúsítványán alapul;
- 27. „elektronikus aláírás minősített tanúsítványa”: olyan, elektronikus aláírás céljára használt tanúsítvány, amelyet minősített bizalmi szolgáltató bocsát ki; és amely megfelel az I. mellékletben megállapított követelményeknek;

MELASZ

I. mellékletben megállapított követelmények:

Az elektronikus aláírások minősített tanúsítványainak a következőket kell tartalmazniuk:

a) legalább automatizált feldolgozásra alkalmas formában utalnia kell arra, hogy a tanúsítványt elektronikus aláírás minősített tanúsítványaként bocsátották ki;

b) a minősített tanúsítványt kibocsátó minősített bizalmi szolgáltatót egyértelműen azonosító adatok, beleértve legalább azt a tagállamot, amelyben az érintett szolgáltató letelepedett, valamint jogi személy esetében a hivatalos nyilvántartásban szereplő megnevezést és adott esetben nyilvántartási számot, természetes személy esetében a személy nevét;

MELASZ

I. mellékletben megállapított követelmények (folyt.):

c) legalább az aláíró neve vagy pedig egy álnév;. álnév használata esetén ezt egyértelműen jelezni kell;

d) az elektronikus aláírás érvényesítéséhez használt adat, amely megfelel az elektronikus aláírás létrehozásához használt adatnak;

e) a tanúsítvány érvényességi idejének kezdete és vége;

f) a tanúsítvány azonosító kódja, amelynek a minősített bizalmi szolgáltatóhoz tartozó egyedi kódnak kell lennie;

g) a minősített bizalmi szolgáltató fokozott biztonságú elektronikus aláírása vagy fokozott biztonságú elektronikus bélyegzője;

MELASZ

I. mellékletben megállapított követelmények (folyt.):

h) az a helyszín, ahol a g) pontban említett, a fokozott biztonságú elektronikus aláírásra vagy fokozott biztonságú elektronikus bélyegzőre vonatkozó tanúsítvány ingyenesen hozzáférhető;

i) azoknak a szolgáltatásoknak a helye, amelyek segítségével felvilágosítás kérhető a minősített tanúsítvány érvényességi állapotáról;

j) amennyiben az elektronikus aláírás érvényesítéséhez használt adathoz kapcsolódó, elektronikus aláírás létrehozásához használt adat minősített elektronikus aláírást létrehozó eszközön található, ennek megfelelő feltüntetése, legalább automatizált feldolgozásra alkalmas formában

MELASZ

- 23. „minősített elektronikus aláírást létrehozó eszköz”: olyan, elektronikus aláírást létrehozó eszköz, amely megfelel a II. mellékletben megállapított követelményeknek;
- 32. „minősített elektronikus bélyegzőt létrehozó eszköz”: olyan, elektronikus bélyegzőt létrehozó eszköz, amely értelemszerűen megfelel a II. mellékletben megállapított követelményeknek;

MELASZ

A II. mellékletben megállapított követelmények:

A minősített elektronikus aláírást létrehozó eszközöknek megfelelő technikai és eljárási megoldások segítségével garantálniuk kell legalább azt, hogy:

a) az elektronikus aláírás létrehozásához használt adat bizalmassága ésszerű mértékben biztosítva legyen;

b) az elektronikus aláírás létrehozásához használt adat gyakorlatilag csak egyszer jöhessen létre;

c) az elektronikus aláírás létrehozásához használt adatok kikövetkeztethetősége ésszerű mértékig kizárható legyen, az elektronikus aláírás pedig megbízhatóan védve legyen a jelenleg rendelkezésre álló technológiákkal elkövetett hamisítás ellen;

MELASZ

A II. mellékletben megállapított követelmények (folyt.):

A minősített elektronikus aláírást létrehozó eszközöknek megfelelő technikai és eljárási megoldások segítségével garantálniuk kell legalább azt, hogy:

d) az elektronikus aláírás létrehozásához használt adatot a jogszerűen aláíró személy megbízható védelemmel tudja ellátni a mások általi felhasználás ellen.

2. A minősített elektronikus aláírást létrehozó eszközök nem módosíthatják az aláírással ellátandó adatokat, és nem akadályozhatják meg, hogy az adatokat az aláíró az aláírás előtt megtekintse.

MELASZ

3. Az elektronikus aláírás létrehozásához használt adatnak az aláíró nevében történő előállítását és kezelését csak minősített bizalmi szolgáltató végezheti.

4. Az 1. pont d) alpontjának sérelme nélkül, az elektronikus aláírás létrehozásához használt adat kezelését az aláíró nevében végző minősített bizalmi szolgáltatók kizárólag adatmentési célból biztonsági másolatot készíthetnek az elektronikus aláírás létrehozásához használt adatról, amennyiben teljesülnek a következő követelmények:

a) a biztonsági adatállomány ugyanolyan biztonságos, mint az eredeti adatállomány;

b) a biztonsági adatállományok száma nem haladhatja meg a szolgáltatás folytonosságának biztosításához minimálisan szükséges mennyiséget.

MELASZ

- MUA-k
  - MS Outlook
  - Evolution
  - Thunderbird
  - stb.
- Honnan jön az aláírás-létrehozó adat (titkos kulcs)?
  - Zsebemben van (csipkártya, SIM kártya, USB token)
  - Szolgáltatónál van (tárolt kulcsos szolgáltatás) – én írok alá, nem a szolgáltató

Köszönöm a megtisztelő figyelmet!

Erdősi Péter Máté
elnokseg@melasz.hu

https://www.melasz.hu