SZIGORÍTOTT aláírási szabályzat

és

EGYSZERŰSÍTETT aláírási szabályzat

	SZIGORÍTOTT	EGYSZERŰSÍTETT
Azonosító OID	1.3.6.1.4.1.21528.2.1.1.36	1.3.6.1.4.1.21528.2.1.1.37
Azonosító URI	http://e-szigno.hu/sigpol/scrict/1.0/	http://e-szigno.hu/sigpol/light/1.0/
Verzió	1.0	
Kibocsátás dátuma	2011. szeptember 8.	
Kibocsátó szervezet	Microsec Kft.	
Érvényességi idő	A kibocsátás időpontjától határozatlan ideig érvényes	
Alkalmazási terület	általános	

Változáskövetés

Verzió	A változás leírása	Kibocsátva	Készítette
1.0	Első változat	2011-09-08	Dr. Berta István Zsolt

Tartalom

1 Bevezetés

Aki elektronikusan aláírt okiratokat kíván befogadni vagy kibocsátani, annak célszerű meghatároznia az elektronikus aláírások típusát, mert minden létező műszaki megoldás támogatása nem lehet reális célkitűzés.

Az elektronikus aláírás típusának pontos meghatározása jelentős szakértelmet igényel, valamint szükség van hozzá az elérhető elektronikus aláírással kapcsolatos szolgáltatások alapos ismeretére is. Másrészt célszerű, ha a kibocsátott vagy befogadott aláírások típusa illeszkedik a mások által használt aláírásokhoz, különben olyan „szigetmegoldás" jöhet létre, amelyhez nem léteznek a szükséges eszközök, illetve nincsenek olyan felhasználók, akik ezekkel rendelkeznének.

Jelen dokumentumban elektronikus aláírási szabályzat formájában foglalja össze a Magyarországon elterjedt, a hazai hitelesítés-szolgáltatók, időbélyegzés-szolgáltatók, illetve alkalmazásfejlesztők által támogatott aláírás típusokat. Ugyanakkor bármely EU-s hitelesítés-szolgáltató technológiájával, valamint nemzetközileg elérhető, szabványos eszközökkel készíthetőek jelen szabályzatoknak megfelelő aláírások.

Javasoljuk, hogy **aki elektronikusan aláírt okiratokat kíván befogadni vagy kibocsátani**, az ne saját aláírás típust alkosson, hanem – az elektronikus aláírás technológia tekintetében – **jelen dokumentum valamelyik szabályzatát hivatkozza meg**. Ezáltal a rendszerében megjelenő aláírásokat más rendszerek is fel tudják majd használni, illetve a rendszeréhez csatlakozó felhasználók más rendszerekhez is könnyen csatlakozhatnak.

2 Általános rendelkezések

2.1 A szabályzat célja

Jelen dokumentum általános célú aláírási szabályzatokat tartalmaz, amelynek segítségével bármely fél könnyen meghatározhatja, hogy milyen típusú, azaz milyen műszaki feltételeknek megfelelő aláírásokat fogad el érvényes elektronikus aláírásnak.

Az aláírási szabályzat az elektronikus aláírás létrehozására és ellenőrzésére vonatkozó azon szabályok összessége, melyek alapján egy aláírás érvényesnek tekinthető egy adott jogi környezetben.

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény (Eat.) az aláíráshoz kapcsolódó joghatás szempontjából két biztonsági szintet nevesít[1]:

- minősített elektronikus aláírás – az Eat. és a polgári perrendtartásról szóló 1952. évi III. törvény (Pp.) szabályai szerint a minősített aláírással ellátott dokumentum teljes bizonyító erejű magánokiratnak minősül;
- fokozott biztonságú elektronikus aláírás – az Eat. értelmében a fokozott biztonságú aláírással ellátott dokumentum írásba foglaltnak minősül;

[1] Az Eat. szerint fokozott biztonságú aláírásnak nem minősülő elektronikus aláírás is létezik, de ezzel jelen dokumentumban nem foglalkozunk.

A jogilag azonos biztonsági szintnek megfelelő aláírások elvileg egyenértékűek, de a gyakorlatban nem reális, hogy egy alkalmazás minden lehetséges műszaki megoldást támogasson. Aki elektronikusan aláírt okiratokat fogad be, annak célszerű meghatároznia, hogy pontosan milyen típusú aláírásokat fogad el. Jelen dokumentum abban nyújt segítséget, hogy a befogadónak ne kelljen az elektronikus aláírások technikai részleteivel foglalkoznia, hanem jelen szabályzat meghivatkozásával egy számára megfelelő, általános célú szabályzatot fogadhasson el.

A jelen szabályzatban meghatározott, ún. SZIGORÍTOTT (STRICT) aláírási szabályzat olyan elektronikus aláírásokat határoz meg, amelyek érvényességéről gyorsan (jellemzően néhány másodperc alatt), nagy biztonsággal meggyőződhetünk. A SZIGORÍTOTT aláírással ellátott okirat írásba foglaltnak minősül, és az aláíró tanúsítványának lejártát vagy visszavonását követően is bizonyítható marad az aláírás érvényessége. Ha az aláírás alapján egy folyamatban lényeges döntést kell hozni, célszerű megkövetelni a SZIGORÍTOTT elektronikus aláírást.

A jelen szabályzatban meghatározott, ún. EGYSZERŰSTETT (LIGHT) aláírási szabályzat olyan elektronikus aláírásokat határoz meg, amelyek esetén az aláírt okirat írásba foglaltnak minősül, és az aláíró tanúsítványának lejártát vagy visszavonását követően is bizonyítható marad az aláírás érvényessége. EGYSZERŰSÍTETT aláírások esetén nem szempont, hogy az aláírást gyorsan, nagy biztonsággal ellenőrizni lehessen. Akkor célszerű EGSZERŰSÍTETT elektronikus aláírást használni, ha az aláírás célja valamely jogszabályi követelmény kielégítése, és nem kell lényeges döntést hozni az aláírás alapján.

> *Megjegyzés: A SZIGORÍTOTT aláírások egyúttal az EGYSZERŰSÍTETT aláírásokra vonatkozó követelményeknek is megfelelnek.*

A SZIGORÍTOTT, illetve EGYSZERŰSÍTETT aláírási szabályzatok szerint egyaránt készíthető fokozott biztonságú és minősített elektronikus aláírás. A jelen dokumentumban meghatározott aláírási szabályzatok az aláírás ellenőrizhetőségének műszaki követelményeit írják le.

> *Megjegyzés: Az Eat. által meghatározott joghatások és a jelen szabályzatban leírt technikai követelmények alapján a következő aláírás-fajták különíthetőek el:*
>
> 1. ***SZIGORÍTOTT minősített*** *aláírást akkor célszerű használni, ha teljes bizonyító erejű magánokiratra van szükség, amely alapján lényeges, érdemi döntést kell hozni.*
> 2. ***SZIGORÍTOTT fokozott biztonságú*** *aláírást akkor célszerű használni, ha lényeges, érdemi döntést kell hozni az aláírás alapján, de a minősített aláírás nem használható (akár azért, mert automatizmus hoz létre nagy tömegű elektronikus aláírást, akár azért, mert az aláíró nem természetes személy).*
> 3. ***EGYSZERŰSÍTETT fokozott biztonságú*** *aláírást akkor célszerű használni, ha nincs szükség teljes bizonyító erejű magánokiratra, és az aláírás elsősorban egy jogszabályi követelmény kielégítését szolgálja, érdemi döntést nem kell hozni az aláírás alapján.*
> 4. *EGYSZERŰSÍTETT minősített aláírást nem célszerű használni; ha minősített aláírást hozunk létre, célszerű inkább a SZIGORÍTOTT követelményrendszert használni.*
>
> *Az elektronikus cégeljárásban, a közjegyzői, illetve az önálló bírósági végrehajtói ügyvitelben használt elektronikus aláírások a SZIGORÍTOTT aláírási szabályzat*

követelményeinek felelnek meg. Az elektronikus számlázás során használt aláírások az EGYSZERŰSÍTETT aláírási szabályzat követelményeinek felelnek meg.

2.2 Jelölések

A narancssárga szöveg kizárólag a SZIGORÍTOTT aláírási szabályzatra vonatkozó követelményt jelent.

A zölddel írt szöveg kizárólag az EGYSZERŰSÍTETT aláírási szabályzatra vonatkozó követelményt jelent.

A fekete szövegben általános követelmények szerepelnek, amelyek mindkét aláírási szabályzatra érvényesek.

Megjegyzés: A kékkel írt szöveg csupán megjegyzés, amely magyarázza a leírtakat, és nem tartalmaz szabályzó követelményt. A színek csupán segítik a szabályzatok értelmezését, szövegesen is jelöljük, ha egy követelmény csak az egyik szabályzatra vonatkozik.

2.3 Szereplők

- *Befogadó*: Az a fél, aki elektronikus aláírással ellátott aláírt okiratot fogad be. A Befogadó – vagy a Befogadóra vonatkozó valamely szabályozás – meghatározza, hogy mely *felhasználási területeken* fogadja el a jelen szabályzatnak megfelelő elektronikus aláírásokat. A Befogadó a jelen szabályzatban meghatározottakon kívül más típusú elektronikus aláírásokat is elfogadhat.
- *Aláíró*: Az a fél, aki elektronikus aláírással lát el egy okiratot.
- *Benyújtó*: Az a fél, aki az Aláíró által elektronikus aláírással ellátott okiratot eljuttatja a befogadónak, azaz felhasználja az aláírást a Befogadó által meghatározott felhasználási területen.

  Megjegyzés: A Benyújtó és az Aláíró sok esetben ugyanaz a személy.

2.4 A szabályzat hatálya

2.4.1 Személyi hatály

A szabályzat a Befogadóra, Benyújtóra és az Aláíróra terjed ki.

2.4.2 Tárgyi hatály

A szabályzat a Befogadó által meghatározott felhasználási területekre terjed ki.

2.4.3 Időbeli hatály

A szabályzat a kibocsátását követően lép hatályba, és határozatlan ideig érvényes. A kibocsátás időpontja a szabályzat címlapján szerepel.

2.5 Irányadó jogszabályok

- Az Európai Parlament és a Tanács 1999/93/EK irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről
- 2001. évi XXXV. törvény az elektronikus aláírásról
- 1952. évi III. törvény a polgári perrendtartásról.

- Európai Közösségek Bizottsága, Határozat az eljárásoknak a belső piaci szolgáltatásokról szóló 2006/123/EK európai parlamenti és tanácsi irányelv szerinti egyablakos ügyintézési pontokon keresztül elektronikus eszközökkel történő teljesítését lehetővé tevő rendelkezések meghatározásáról, C(2009)7806, 2009. 10. 16.
- 78/2010. (III. 25.) Korm. rendelet az elektronikus aláírás közigazgatási használatához kapcsolódó követelményekről és az elektronikus kapcsolattartás egyes szabályairól
- 13/2005. (X. 27.) IHM rendelet a papíralapú dokumentumról elektronikus úton történő másolat készítésének szabályairól
- 114/2007. (XII. 29.) GKM rendelet a digitális archiválás szabályairól
- 2007. évi CXXVII. törvény az általános forgalmi adóról
- 2000. évi C. törvény a számvitelről

2.6 Mértékadó szabványok, műszaki specifikációk

Aláírás-formátum és konténer-formátum specifikációk:

- ETSI TS 101 903: XML Advanced Electronic Signatures (XAdES)
- ETSI TS 101 733: CMS Advanced Electronic Signatures (CAdES)
- ETSI TS 102 778: PDF Advanced Electronic Signatures (PAdES)
- Az e-akta formátum specifikációja
  http://www.e-szigno.hu/?lap=eakta
- ISO 32000: Document management – Portable Document Format – Part 1: PDF 1.7
- PKCS#7: Cryptographic message syntax standard
- Egységes Melasz formátum elektronikus aláírásokra verzió: 2.0. Melasz Munkacsoport Megállapodás, MMM

Általános PKI specifikációk:

- Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 2560: Online Certificate Status Protocol – OCSP
  http://www.ietf.org/rfc/rfc2560.txt
- RFC 3161: Time-Stamp Protocol (TSP)
  http://www.ietf.org/rfc/rfc3161.txt
- ETSI TS 102 231: Provision of harmonized Trust-service status information

Aláírási szabályzatokról szóló specifikációk:

- ETSI TR 102 038: XML format for signature policies
- ETSI TR 102 272: ASN.1 format for signature policies
- Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírási szabályzatok készítésére

3 Az elektronikus aláírás létrehozása

Nincs megkötés.

Megjegyzés: Jelen szabályzat az ellenőrzés követelményeit írja el, azt határozza meg, mikor tekinthető egy aláírás érvényesnek. Az aláírás készítésének módja érdektelen, amíg jelen szabályzatok szerint ellenőrizhető aláírást kapunk. Ennek megfelelően a szabályzat nem fogalmaz meg előírást például az aláírás készítésének fizikai környezetére vagy az aláírás-létrehozó alkalmazásra.

4 Az elektronikus aláírás ellenőrzése

4.1 Formátum

4.1.1 Az aláírás formátuma

A Befogadó eltérő rendelkezése hiányában az aláírás a következő formátumok valamelyikével kell, hogy rendelkezzen. A Befogadó jogosult elutasítani a más formátumú aláírásokat:

- Elektronikus akta (e-akta) formátum, amely egy ETSI TS 101 903 (XAdES[2]) formátumú aláírásokat tartalmazó XML „konténer” fájl. Az e-akta kiterjesztése `.es3` vagy `.dosszie`.
- PDF aláírás, amely egy PDF fájlban elhelyezett PKCS#7 aláírás vagy ETSI TS 101 733 (CAdES[3]) formátumú aláírás, illetve ETSI TS 101 788 (PAdES[4]) aláírás lehet. A PDF kiterjesztése `.pdf`.

Az automatizált feldolgozhatóság érdekében a Befogadó a fentiektől eltérő, automatizált feldolgozásra alkalmas formátumot – például adott XML sémának megfelelő XML formátumot – is meghatározhat, és megteheti, hogy jelen szabályzat keretében kizárólag e formátumnak megfelelő aláírt dokumentumokat fogad el. XML formátum esetén XAdES aláírást kell használni.

Amennyiben a Befogadó nem rendelkezik speciális formátumról, a fenti két formátumot (e-akta és PDF aláírás) kell használni.

4.1.2 Az aláírt dokumentum formátuma

- E-akta használata esetén – amennyiben a Befogadó másképp nem rendelkezik – az e-akta PDF fájlokat és további e-aktákat tartalmazhat.
- PDF aláírás használata esetén az aláírt fájl formátuma PDF.
- Amennyiben a Befogadó speciális aláírás-formátumot határozott meg, a Befogadó az aláírt dokumentum formátumát is meghatározza.

[2] XAdES v1.2.2, vagy frissebb.

[3] CAdES v1.8.1, vagy frissebb.

[4] PAdES Part 2, vagy fejlettebb.

4.1.3 Aláírási szabályzat meghivatkozása az aláírásban

A XAdES, CAdES és PAdES aláírásokban feltüntethető, hogy az adott aláírás pontosan mely aláírási szabályzat szerint készült. Jelen szabályzat nem javasolja, de megengedi ezen hivatkozás használatát.

> *Megjegyzés: Ezen hivatkozások interoperabilitási problémákat okozhatnak például ha a szabályzat változik, problémássá teheti a más szabályzatok szerint készült aláírások felhasználását, illetve problémássá válik a Befogadó által nem ismert szabályzatok szerint készült aláírások elfogadása.*

Amennyiben mégis az aláírási szabályzatot hivatkozó, ún. –EPES alapú aláírás készül, jelen szabályzat a SignaturePolicyImplied[5] opció használatát javasolja.

4.2 Elfogadott kriptográfiai algoritmusok köre

Jelen szabályzat értelmében az Eat. 18. §-a szerinti mindenkori hatósági határozat értelmében biztonságos kriptográfiai algoritmusok használhatóak. Ezen határozatok a Nemzeti Média- és Hírközlési Hatóság honlapján[6] érhetőek el.

A korábban kibocsátott tanúsítványok és időbélyegek, illetve a korábban készült aláírások tekintetében a korábbi határozatok szerinti algoritmusokat is el kell fogadni.

4.3 Elfogadott hitelesítés-szolgáltatók

Jelen szabályzat értelmében minden olyan hitelesítés-szolgáltató elfogadott, amely az Európai Unió tagállamai által kibocsátott ún. bizalmi listákon[7] (trust services list) hitelesítés-szolgáltatóként szerepel. A listákon szereplő szolgáltatói tanúsítványok e tekintetben megbízható gyökérként (trust anchor) kezelendőek akkor is, ha maguk nem önhitelesített gyökértanúsítványok.

A tagállamok által kibocsátott bizalmi listák elérhetőségét tartalmazó „listák listája” (list of lists) aláírásához használt tanúsítvány lenyomatát az Európai Unió Hivatalos Lapjában[8] publikálták. E lenyomat alapján a Befogadó meggyőződhet a listák listájának hitelességéről. A listák listája tartalmazza a tagállamokban kibocsátott listák elérhetőségét, és a listákon lévő aláírások ellenőrzéséhez szükséges tanúsítványt.

A Befogadó nem köteles elfogadni az olyan szolgáltatót, amely:

- egyik EU tagállam bizalmi listáján sem szerepel hitelesítés-szolgáltatóként,
- olyan EU tagállamban működik, amely nem bocsátott ki ETSI TS 102 231 szerinti, géppel értelmezhető, XML formátumú bizalmi listát,

---

[5] ETSI TS 101 903 (XAdES), 7.2.3. fejezet, illetve ETSI TS 101 733 (CAdES), 5.8.1. fejezet.

[6] http://www.nmhh.hu/?id=dokumentumtar&mid=1085&lang=hu

[7] Az Európai Unió tagállamai – az Európai Bizottság C(2009)7806 határozatának megfelelően – bizalmi listákat bocsátnak ki, amelyen felsorolják a tagállamban működő felügyelt, illetve akkreditált szolgáltatókat. A listák kötelezően tartalmazzák a minősített hitelesítés-szolgáltatók tanúsítványait, de egyéb szolgáltatói tanúsítványokat is tartalmazhatnak. A géppel is feldolgozható listák javasolt formátuma az ETSI TS 102 231 által meghatározott XML formátum. A tagállamok által kibocsátott bizalmi listák elérhetőségét tartalmazó „listák listája” az alábbi címen érhető el:
https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

[8] Official Journal of the European Union, C 45 of 23.02.2010, 16. oldal.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2010:045:0016:01:HU:HTML

- olyan bizalmi listán szerepel, amely nincsen aláírva,
- olyan bizalmi listán szerepel, amely nem ellenőrizhető a listák listáján publikált tanúsítványok alapján.

Tekintve, hogy a bizalmi listák történeti adatokat is tartalmaznak, a már nem működő, illetve már nem felügyelt hitelesítés-szolgáltatók tanúsítványait szintén el kell fogadni, amennyiben egy aláírást olyan múltbeli időpontra nézve ellenőriz a Befogadó, amely időpontban a kérdéses szolgáltató még működött, illetve felügyelet alatt állt.

> *Megjegyzés: A bizalmi listákon a tagállamok kizárólag a minősített hitelesítés-szolgáltatókat kötelesek feltüntetni, így előfordulhat, hogy egy hitelesítés-szolgáltató nem minősített hitelesítés-szolgáltatóként működik, és mégsem szerepel bizalmi listán. Az ilyen szolgáltatókat a Befogadó nem köteles elfogadni.*

Amennyiben a Befogadó kizárólag minősített aláírásokat fogad el, akkor a bizalmi listákról csak azon hitelesítés-szolgáltatók tanúsítványait tekinti megbízható gyökérnek, amelyek szerint minősített tanúsítványok kibocsátása történik. Amennyiben a Befogadó nem kizárólag minősített aláírásokat fogad el, akkor a bizalmi listán lévő összes hitelesítés-szolgáltatói tanúsítvány elfogadja.

A Befogadó elfogadhat további, a bizalmi listákon nem szereplő hitelesítés-szolgáltatókat is.

A Befogadó kizárólag indokolt esetben tagadhatja meg a bizalmi listákon szereplő hitelesítés szolgáltatók elfogadását. Ilyen esetet jelent, ha a tudomására jut, hogy egy adott hitelesítés-szolgáltató magánkulcsa kompromittálódott.

4.4 Elfogadott időbélyegzés-szolgáltatók

Minden olyan időbélyegzés-szolgáltató elfogadott, amely az Európai Unió tagállamai által kibocsátott bizalmi listán (trust services list) minősített időbélyegzés-szolgáltatóként szerepel. A listákon szereplő szolgáltatói tanúsítványok e tekintetben megbízható gyökérként (trust anchor) kezelendőek akkor is, ha maguk nem önhitelesített gyökértanúsítványok.

A hitelesítés-szolgáltatók esetén leírt szabályok itt is érvényesek.

> *Megjegyzés: A bizalmi listákon a tagállamok kizárólag a minősített hitelesítés-szolgáltatókat kötelesek feltüntetni. Az időbélyegzés szolgáltatók nem minden tagállamban szerepelnek a bizalmi listán, és nem is minden tagállamban vannak felügyelt vagy akkreditált időbélyegzés szolgáltatók. A „minősített időbélyegzés” sem minden EU tagállamban ismert fogalom.*

4.5 Az aláírás ellenőrzésének módja

4.5.1 Megbízható időpont meghatározása

Az aláírást minősített időbélyeggel kell ellátni. Az időbélyeget olyan módon kell csatolni az aláíráshoz, hogy a kapott aláírás legalább XAdES-T, PAdES-T, CAdES-T, illetve időbélyeggel ellátott PKCS#7 aláírás legyen.

Az időbélyeg beszerzése és csatolása a Benyújtó feladata, az időbélyeg nélküli aláírásokat a Befogadó nem köteles elfogadni. Amennyiben a Befogadó úgy rendelkezik, hogy időbélyeg nélküli aláírásokat is befogad, akkor a Befogadó köteles biztosítani, hogy az aláírásokhoz a minősített időbélyegek csatolásra kerüljenek.

Az aláírást a rajta lévő minősített időbélyegen szereplő megbízható időpontra nézve kell ellenőrizni.

4.5.2 Tanúsítványlánc felépítése

Az aláíró tanúsítványát vissza kell vezetni egy elfogadott hitelesítés-szolgáltató tanúsítványára. Az aláíráshoz csatolni kell az így kapott tanúsítványláncot, amely az aláíró tanúsítványától egy elfogadott megbízható gyökérig (lásd: 4.3. fejezet) vezet. A megbízható gyökér nem része a tanúsítványláncnak, így nem kötelező csatolni.

Az aláíráshoz további szolgáltatói tanúsítványok is csatolhatóak.

A tanúsítványlánc csatolása a Benyújtó feladata.

A Befogadó köteles figyelembe venni az aláíráshoz csatolt tanúsítványláncot, de más tanúsítványláncokat is felhasználhat az aláírás ellenőrzése során.

A tanúsítványlánc minden eleme érvényes kell, hogy legyen azon időpontban, amelyre nézve az aláírást ellenőrizzük.

> *Megjegyzés: Sok szolgáltató többszintű tanúsítvány-hierarchiával rendelkezik, például a szolgáltató saját gyökere egy produktív hitelesítő egységet hitelesít, és az aláírók tanúsítványait e produktív hitelesítő egysége bocsátja ki. Ekkor előfordulhat, hogy a bizalmi listán nem a szolgáltató gyökere, hanem a produktív hitelesítő egysége szerepel. Jelen szabályzat tekintetében a bizalmi listán szereplő egység gyökérnek minősül, így elegendő az odáig vezető láncot (azaz csak az aláíró tanúsítványát) csatolni. A Befogadó akkor is köteles érvényesnek tekinteni egy aláírást, ha a Benyújtó az ennél hosszabb, a szolgáltató saját gyökeréig vezető láncot csatolta.*

Az időbélyegekre, illetve az esetleges visszavonási információkra vonatkozó tanúsítványláncokat is az itt leírtakhoz hasonlóan kell csatolni.

4.5.3 Visszavonási információk beszerzése

Meg kell vizsgálni, hogy a tanúsítványlánc egyes elemei nem voltak-e visszavont állapotban azon időpontban, amelyre nézve az aláírást ellenőrizzük. A visszavonási állapot ellenőrizhető visszavonási listák (CRL) vagy online tanúsítvány-állapot protokoll (OCSP) segítségével.

EGYSZERŰSÍTETT aláírás esetén az ellenőrzést elegendő valamely „kellően friss”, azaz még nem lejárt visszavonási információ alapján elvégezni. Ekkor követelmény, hogy a visszavonási információban szereplő `nextUpdate` időpont későbbi legyen, mint az az időpont, amelyre nézve az aláírást ellenőrizzük.

> *Megjegyzés: EGYSZERŰSÍTETT aláírás esetén nem szükséges mindig a legfrissebb visszavonási információt beszerezni, a visszavonási információ mindaddig használható, amíg nem garantált, hogy van nála frissebb. EGYSZERŰSÍTETT aláírás esetén előfordulhat, hogy az Aláíró tanúsítványa időközben visszavonásra került, és ekkor már van olyan visszavonási információ, amely szerint az Aláíró tanúsítványa már érvénytelen.*

SZIGORÍTOTT aláírás esetén olyan visszavonási információt kell használni, amely azon időpontra vonatkozik, amelyre nézve az aláírást ellenőrizzük. Ekkor követelmény, hogy a visszavonási információban szereplő `thisUpdate` későbbi legyen, mint az az időpont, amelyre nézve az aláírást ellenőrizzük. E követelményt a teljes tanúsítványláncra, így a láncban szereplő szolgáltatói tanúsítványokra is érvényesíteni kell.

A legkülső időbélyeg, valamint a hozzá kapcsolódó tanúsítványlánc tekintetében SZIGORÍTOTT aláírás esetén is elegendő a „kellően friss”, még nem lejárt visszavonási információ.

A Befogadó az alábbi forrásokból próbálja meg beszerezni a visszavonási információkat:

- a tanúsítványban meghivatkozott elérhetőségről (CRL esetén ez a `CRL distribution point`, OCSP esetén az `authority information access` mező);
- az aláíráshoz csatolt információk közül (*AdES-C, vagy magasabb szintű aláírások esetén);

A Befogadó megteheti, hogy más forrásokat is figyelembe vesz, de nem köteles erre. Amennyiben a fenti forrásokból se megfelelő CRL, se megfelelő OCSP válasz nem szerezhető be akkor a Befogadó érvénytelennek tekintheti az aláírást.

Megjegyzés:

1. *A visszavonási lista jellemzően periodikusan jelenik meg, így a CRL technológia segítségével általában időbe telik, amíg egy elektronikus aláírásból SZIGORÍTOTT elektronikus aláírás hozható létre, mert ekkor meg kell várni a következő visszavonási lista kibocsátását.*
2. *A SZIGORÍTOTT aláíráshoz nem követelmény az OCSP technológia használata, de a gyakorlatban leginkább OCSP segítségével képzelhető el, hogy valaki létrehoz egy elektronikus aláírást, majd rögtön fel is használja SZIGORÍTOTT aláírásként. Ez főként akkor képzelhető el, ha a kérdéses hitelesítés-szolgáltató gyorsan fel tudja dolgozni a beérkező visszavonási kérelmeket, és ha gyorsan közzé tudja tenni a megváltozott visszavonási állapotot.*
3. *Ha egy tanúsítványhoz tartozik OCSP szolgáltatás, de az OCSP elérhetősége nem szerepel a tanúsítványban, és nincsen csatolva OCSP válasz, akkor a Befogadó nem köteles OCSP alapú ellenőrzést végezni, így megtagadhatja egy aláírás SZIGORÍTOTT aláírásként való elfogadását.*

5 Az elektronikus aláírás archiválása

SZIGORÍTOTT aláírás esetén mindaddig, amíg az aláírt okiratokat hitelesen meg kell őrizni, a Befogadó rendszeresen új időbélyeggel látja el az aláírt okiratot, mielőtt:

- a korábbi, legkülső időbélyeghez kapcsolódó szolgáltatói tanúsítvány érvényessége lejár;
- a korábbi, legkülső időbélyeghez kapcsolódó szolgáltatói tanúsítvány visszavonásra kerül;
- a korábbi, legkülső időbélyeghez kapcsolódó kriptográfiai algoritmusok elavulnak (az Eat. 18. §-a szerinti határozata szerint).

A SZIGORÍTOTT aláírások archiválását a megőrzésre kötelezetett saját maga is elvégezheti vagy minősített archiválás szolgáltatót is megbízhat e feladattal.

Az EGYSZERŰSÍTETT aláírások archiválására jelen szabályzat nem határoz meg követelményeket. Amennyiben egy EGYSZERŰSÍTETT aláírás archiválása mégis szükségessé válik, célszerű átalakítani SZIGORÍTOTT aláírássá, és célszerű annak megfelelően archiválni.

6 Az aláírt okirat befogadásának menete

A Befogadó eljárásrendi követelményeket határozhat meg a befogadott aláírások, illetve okiratok feldolgozásával kapcsolatban.

Megjegyzés: Célszerű meghatározni, hogy hova és milyen módon kell benyújtani az aláírt okiratokat, hogyan és mi alapján ellenőrzik a benyújtó jogosultságát, milyen módon küldenek visszaigazolást a benyújtott okiratokról, mennyi időn belül dolgozzák fel a benyújtott okiratot stb. Jelen szabályzat az aláírt okiratok PKI vonatkozásaival foglalkozik, az eljárásrendi kérdéseket nem szabályozza.

7 A szabályzatok változtatásainak követése

A jövőben szükségessé válhat a jelen dokumentumban meghatározott aláírási szabályzatok változtatása. Ezt okozhatják jogszabályi változások, szabványokban bekövetkezett változások, vagy egyéb természetű változások is. A dokumentumban meghatározott aláírási szabályzatok változása esetén új verzió kerül kibocsátásra.

- Amennyiben a változás nem változtatja meg alapvetően a szabályzatok jelentését, az új verzió új verziószámmal és új kibocsátási dátummal rendelkezik, de a korábbi változatokkal megegyező azonosítókat (OID, URI) tartalmaz. A megadott URI-n elérhető információ lenyomata ekkor nem változik.

  Megjegyzés: Az aláírási szabályzat azonosítójának megváltozása zavart okozhat azon befogadók működésében, akik nem értesültek hiteles formában az új azonosítóról, illetve nem készültek fel annak befogadására. Az adott URI-n publikált információ változása zavart okozhat, mert aláírások tartalmazhatják a korábbi információ lenyomatát, és ez aláírások téves elutasítását eredményezheti.

- Alapvető változás esetén új szabályzatok kerülnek kibocsátásra, amelyek új azonosítókat tartalmaznak.

8 Megfelelés

Az EGYSZERŰSÍTETT aláírások (így egyúttal a SZIGORÍTOTT aláírások is) megfelelnek:

- az elektronikus számlákon elhelyezett elektronikus aláírásokra vonatkozó, az ÁFA törvényben, illetve a számviteli törvényben rögzített követelményeknek.
- a papír alapú számlák elektronikus másodpéldányain elhelyezett elektronikus aláírásokra vonatkozó, a 24/1995. PM rendeletben rögzített követelményeknek.
- a papír alapú iratokról készített hiteles elektronikus másolatokra vonatkozó, a 13/2005. IHM rendeletben rögzített követelményeknek.
- a digitális archiválás szabályairól szóló 114/2007. GKM rendeletben rögzített, az elektronikus aláírásokra vonatkozó követelményeknek, amennyiben a megőrzés időtartama kisebb, mint 11 év; a SZIGORÍTOTT aláírások a 11 évet meghaladó megőrzés követelményeinek is megfelelnek.

A jelen dokumentumban meghatározott aláírási szabályzatok megfelelnek „Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható elektronikus aláírási szabályzatok készítésére” című specifikáció követelményeinek.

9 Ajánlások a szabályzat használatára

Jelen szabályzat használatához arra van szükség, hogy a Befogadó a saját szabályzataiban:

1. Rögzítse, hogy milyen felhasználási területen fogad be elektronikusan aláírt okiratokat (azaz például milyen típusú kérelmeket fogad el elektronikusan aláírva).
2. Hivatkozza meg a kiválasztott (SZIGORÍTOTT vagy EGYSZERŰSÍTETT) aláírási szabályzatot. A hivatkozás tartalmazza a szabályzat elérhetőségét, verziószámát és azonosítóját.
3. Rögzítse, amennyiben kizárólag minősített elektronikus aláírásokat kíván elfogadni. (Célszerű tekintetbe venni, hogy a jelen szabályozás szerint automatizmussal csak fokozott biztonságú aláírás készíthető.)
4. Írja le, hogy milyen módon kell beküldeni az aláírt okiratokat. (Például: e-mailen kell elküldeni egy megadott e-mail címre, vagy weben keresztül kell feltölteni egy megadott weboldalon, vagy CD lemezre írva postán is elküldhetőek stb.)
5. Ha bármilyen további, speciális feltételt kíván alkalmazni, rögzítse ezeket. Speciális feltétel lehet például:
    a. Ha speciális fájlformátumot vagy aláírás-formátumot kíván használni, ekkor határozza meg ezeket.
    b. Ha nem követeli meg, hogy a benyújtott okiratokon időbélyeg legyen, hanem saját maga helyez el rajtuk időbélyeget.
    c. Ha további hitelesítés szolgáltatókat is elfogad.
    d. Ha az aláíró tulajdonságát, szerepkörét vagy jogosultságát kívánja ellenőrizni, rögzítse, hogy ez hogyan történik. E célra az elektronikus aláírt attribútum-tanúsítványokra épülő megoldás használatát javasoljuk.

Az aláírást befogadó fél tegye elérhetővé a fenti szabályokat az okiratokat benyújtó felek számára.