ELEKTRONIKUS BÉLYEGZÉSI SZABÁLYZAT

Elektronikus bélyegző elhelyezése bizalmi szolgáltatás

MobilSign

Besorolás: Hatálybalépés:	Publikus 2018.06.26.	Verzió: OID:	1.1 1.3.6.1.4.1.46750.1.1.1.4.1.2.2
Készítésért felelős: Dátum:	Dohányos Péter, IBF 2018.06.05.	Jóváhagyta: Dátum:	Csik Balázs, Inf.Rendszer Fel.Vez. 2018.06.11.
Figyelem! Jelen dokumentumnak a https://www.mobilsign.com oldalon publikált, illetve bélyegzővel ellátott példányai tekinthetők hitelesnek.			

VERZIÓ KONTROLL

Verzió	Kiadva	Módosította	Jóváhagyta	Leírás
1.0	2017.11.20.	Dohányos Péter	Csik Balázs	Első kiadás
1.1	2018.06.26.	Dohányos Péter	Csik Balázs	Elektronikus bélyegzési szabályzat kiadás

TARTALOMJEGYZÉK

FOGALMAK ÉS RÖVIDÍTÉSEK

Fogalmak

- **„Bizalmi lista”**: Valamennyi (EU) tagállam bizalmi listákat állít össze, tart fenn és tesz közzé, amelyeken szerepelnek a felelőssége alá tartozó minősített bizalmi szolgáltatókra vonatkozó információk, valamint az e szolgáltatók által nyújtott minősített bizalmi szolgáltatásokra vonatkozó információk. A tagállamok biztonságos módon, automatizált feldolgozásra alkalmas formában állítják össze, tartják fenn és teszik közzé az elektronikus aláírással vagy bélyegzővel ellátott bizalmi listákat.
- „**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;
- „**Elektronikus bélyegző**”: olyan elektronikus adatok, amelyeket más elektronikus adatokhoz csatolnak, illetve logikailag hozzárendelnek, hogy biztosítsák a kapcsolt adatok eredetét és sértetlenségét;
- „**Fokozott biztonságú elektronikus bélyegző**”: olyan elektronikus bélyegző, amely megfelel az (eIDAS) 36. cikkben meghatározott követelményeknek:
    a) kizárólag a bélyegző létrehozójához kötött;
    b) alkalmas a bélyegző létrehozójának azonosítására;
    c) olyan, elektronikus bélyegző létrehozásához használt adatok felhasználásával hozzák létre, amelyeket a bélyegző létrehozója nagy megbízhatósággal kizárólag saját maga elektronikus bélyegző létrehozására használhat;
    d) olyan módon kapcsolódik azokhoz az adatokhoz, amelyekre vonatkozik, hogy az adatok minden későbbi változása nyomon követhető;
- „**Nonce**”: egyszer használatos véletlen szám egy kérés üzenet azonosítására
- „**Tanúsítvány**”: az elektronikus aláírás tanúsítvány, az elektronikus bélyegző tanúsítvány és a weboldal-hitelesítő tanúsítvány, valamint mindazon, a bizalmi szolgáltatás keretében a szolgáltató által kibocsátott elektronikus igazolás, amely tartalmazza a tanúsítványra vonatkozó érvényesítési adatot és a tanúsítvány használatához szükséges kapcsolódó adatokat, és amely elektronikus dokumentum megbízhatóan védve van a kibocsátáskor és az érvényességi ideje alatt rendelkezésre álló technológiákkal elkövetett hamisítás ellen;
- **Tanúsítványkibocsátó bizalmi szolgáltató**: aláíró- és bélyegzőtanúsítványok kibocsátását bizalmi szolgáltatásként nyújtó bizalmi szolgáltató

Rövidítések

- **CRL**: Certificate Revocation List (tanúsítvány-visszavonási lista)
- **EBSZ**: Elektronikus Bélyegzési Szabályzat (jelen dokumentum)
- **HSM**: Hardware Security Module (Kriptográfiai Hardver Modul)
- **OCSP**: Online Certificate Status Protocol (valós idejű tanúsítvány-állapot protokoll)
- **OID**: Object IDentifier (Objektum azonosító): az ITU és ISO/IEC által közösen kidolgozott hierarchikus szerkezetű azonosító, tetszőleges objektum globálisan egyedi, egyértelmű azonosítására.

1 ÁLTALÁNOS RENDELKEZÉSEK

1.1 A szabályzat célja

Jelen Elektronikus Bélyegzési Szabályzat (a továbbiakban: EBSZ) célja a MobilSign Kft. mint bizalmi szolgáltató (a továbbiakban: Szolgáltató) nem minősített Elektronikus Bélyegző Elhelyezése bizalmi szolgáltatás (a továbbiakban BSZ) nyújtása során alkalmazott minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegző képzési, ellenőrzési szabályainak meghatározása és összefoglalása.

1.2 A szabályzat hatálya és érvényessége

1.2.1 Fizikai hatálya

Kiterjed a Szolgáltató valamennyi:

- a bizalmi szolgáltatást biztosító IT infrastruktúrára, IT rendszerekre, IT berendezésekre és IT eszközökre (továbbiakban: BSZ Rendszerkörnyezet);
- a bizalmi szolgáltatás üzemeltetési tevékenységeire, illetve folyamataira;

1.2.2 Személyi hatálya

Kiterjed a Szolgáltató valamennyi:

- a bizalmi szolgáltatást biztosító IT környezeteket üzemeltetésében résztvevő és a támogató IT környezeteket használó munkatársakra és alvállalkozókra, valamint azok munkatársaira;
- a bizalmi szolgáltatást biztosító IT infrastruktúrához, IT rendszerekhez, IT berendezésekhez és IT eszközökhöz hozzáférési jogosultságot kapott harmadik felekre (pl.: szolgáltatók, tanácsadók, auditorok stb.).
- a külső megbízottak, alvállalkozók, harmadik felek szerződéseiben a jelen szabályzat vonatkozó rendelkezéseinek megismerését és alkalmazását érvényesíteni kell.

1.2.3 Időbeli hatálya

A szabályozás a címlapon feltüntetett időpontban lép hatályba és a visszavonásig érvényes.

Jelen EBSZ hatályba lépésével minden korábbi verzió (OID: 1.3.6.1.4.1.46750.1.1.1.4.1.2.x) hatályát veszti.

1.3 Kötelező felülvizsgálat

A szabályzatot tervezetten évente felül kell vizsgálni.

A szabályzatot bizalmi szolgáltatás jelentős technikai / technológiai változása esetén soron kívül felül kell vizsgálni.

A szabályzatot a törvényi előírások, illetve a kapcsolódó szabványok változása esetén soron kívül felül kell vizsgálni.

1.4 Irányadó jogszabályok és műszaki követelmények

- 32014R910 - eIDAS - AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről
- ETSI TS 101 733: „Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)”
- ETSI TS 102 176-1 v 2.1.1 (2011-07) - „Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms
- ETSI TS 119 101 v1.1.1 (2016-03) - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation
- ETSI EN 319 102-1 V1.1.1 (2016-05) Electronic Signatures and Infrastructures (ESI); Procedures for Creation and Validation of AdES Digital Signatures; Part 1: Creation and Validation
- ETSI EN 319 142-2 V1.1.1 (2016-04): Electronic Signatures and Infrastructures (ESI); PAdES digital signatures; Part 2: Additional PAdES signatures profiles
- RFC2986 - [PKCS #10] PKCS #10 Certification Request Syntax Specification Version 1.7
- RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)
- RFC 5208 - [PKCS #8] Public-Key Cryptography Standards (PKCS) #8 Private-Key Information Syntax Specification Version 1.2
- RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 5816: ESSCertIDv2 Update for RFC 3161
- RFC 5958 - Asymmetric Key Packages
- RFC 6818 - Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile
- RFC 6960: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP
- RFC 8017 - [PKCS #1] PKCS #1 RSA Cryptography Specifications Version 2.2
- Nemzeti Média- és Hírközlési Hatóság biztonságos kriptográfiai algoritmusok használatára vonatkozó határozata
- Federal Information Processing Standards Publication 140-2 (May 25, 2001) with CHANGE NOTICES (12-03-2002) - SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES

2 SZEREPKÖRÖK

Az elektronikus bélyegző létrehozása és felhasználása kapcsán az alábbi szerepköröket kell megkülönböztetni:

2.1 Bélyegző létrehozója

A *Bélyegző létrehozója* jogi személy, mely szerződéses viszonyban áll a Szolgáltatóval a vonatkozó Szolgáltatói Szerződésben, Általános Szerződési Feltételekben és a Szolgáltatási Szabályzatban foglaltak szerint.

A *Bélyegző létrehozója* a BSZ használatával elektronikus dokumentumait elektronikus bélyegzővel látja el egyrészt a releváns üzleti folyamatait megvalósító informatikai rendszerei által kezdeményezve, másrészt feljogosított *Bélyegző elhelyezését kezdeményező* képviselői által manuálisan kezdeményezve.

2.2 Bélyegző elhelyezését kezdeményező

A *Bélyegző létrehozója* jogi személy alkalmazottja, vagy arra feljogosított személye, aki manuális interakcióval aktiválja a BSZ által megvalósított elektronikus bélyegző létrehozást a megfelelő azonosítás és jogosultság ellenőrzés után.

2.3 Dokumentum közreműködő

A *Bélyegző létrehozója* jogi személy -egy nevesített képviselőjének felelőssége alá tartozó- üzleti folyamatában (ügyfélként vagy egyéb minőségben) résztvevő személy, aki a képviselő kontrollja és koordinálása alatt az üzleti folyamat keretében számára bemutatott elektronikus dokumentumon olyan műveletet hajt végre, mely az üzleti folyamat metaadataként, megfelelő felülhitelesítés érdekében a képviselő által a BSZ használatával kezdeményezett elektronikus bélyegző létrehozását kell, hogy maga után vonja.

2.4 Bélyegző elfogadója/ellenőrzője

A *Bélyegző elfogadója/ellenőrzője* fél az a személy, vagy felügyelt automatizmus, aki/amely az elektronikus bélyegzővel ellátott elektronikus üzenetek aláíráskori, illetve ellenőrzéskori tartalmát összeveti, továbbá a bélyegzőt létrehozó személyét azonosítja az üzenet, illetve a Tanúsítvány kibocsátó bizalmi szolgáltató által közzétett ellenőrző adat, tanúsítvány visszavonási információk, valamint a tanúsítvány felhasználásával.

2.5 Tanúsítványkibocsátó bizalmi szolgáltató

A *Tanúsítványkibocsátó bizalmi szolgáltató* az elektronikus bélyegző tanúsítvánnyal kapcsolatos szolgáltatást nyújtó jogi személy vagy jogi személyiség nélküli szervezet.

2.6 BSZ Kapcsolattartó

A *BSZ Kapcsolattartó* a Szolgáltató által kijelölt természetes személy, aki eljárhat a szolgáltató részéről a BSZ szolgáltatásokkal kapcsolatos ügyintézés során.

2.7 Szakértői támogatás / help desk

Szolgáltató a BSZ használata során felmerülő technikai kérdések kezelésére szakértőn keresztül támogatást nyújt. Ezen szakértőket a BSZ help desk szolgáltatásán keresztül lehet elérni.

2.8 BSZ Operátor

A BSZ Operátor a szolgáltatói oldalon támogatja az elektronikus bélyegző elhelyezéséhez szükséges hardveres és szoftveres kriptográfiai környezet megfelelő működését.

3 ELEKTRONIKUS ALÁÍRÁSHOZ / BÉLYEGZŐHÖZ KAPCSOLÓDÓ KÖVETELMÉNYEK

3.1 Az elektronikus bélyegző létrehozása

A *Bélyegző létrehozója* a BSZ használatával elektronikus dokumentumait elektronikus bélyegzővel látja el egyrészt a releváns üzleti folyamatait megvalósító informatikai rendszerei által kezdeményezve, másrészt feljogosított *Bélyegző elhelyezését kezdeményező* képviselői által manuálisan kezdeményezve - ezek részletes menete a Szolgáltatási Szabályzatban kerül kifejtésre.

A BSZ aktiválásakor a Szerződött Partner magánkulcsát és bélyegző tanúsítványát tároló Kriptográfiai hardver modul használatával a dokumentumon időbélyeggel és jelen szabályzatra hivatkozással a (ETSI EN 319 142-1 és ETSI EN 319 142-2 európai szabványok szerinti) PAdES elektronikus bélyegző készül, mely teljesíti PAdES-B-T és időbélyeggel ellátott PAdES-E-EPES feltételeit, valamint megfelel az eIDAS által a fokozott biztonságú elektronikus bélyegzőkkel szemben támasztott követelményeknek. Az időbélyegek elkészítésére a Szolgáltató bizalmi listában szereplő külső időbélyegző szolgáltatást vesz igénybe a következő módon:

- alapértelmezetten minden elektronikus bélyegző időbélyeggel kerül létrehozásra
- amennyiben a BSZ Bélyegző elhelyezését kezdeményező általi aktiválása által egyszerre egynél több elektronikus bélyegzőt hoz létre, akkor csak az egymásra épülő bélyegző-sorozat kezdő (első) és záró (utolsó) bélyegzője kerül ellátásra időbélyeggel

3.2 Az elektronikus bélyegző ellenőrzése

Az elektronikus bélyegzővel ellátott dokumentum hitelességének ellenőrzése az alábbi elemek ellenőrzését foglalja magában:

- a dokumentum sértetlenségének ellenőrzése
- a bélyegző tanúsítvány(lánc) megfelelőségének ellenőrzése
- az időbélyeg ellenőrzése

Az elektronikus bélyegző és az ahhoz tartozó tanúsítvány ellenőrzése az alábbiakra terjed ki:

- az elektronikus bélyegzőhöz tartozó tanúsítvány segítségével azonosítani kell az bélyegző tanúsítványt kibocsátó bizalmi szolgáltatót;
- a bélyegző tanúsítványt kibocsátó bizalmi szolgáltató tanúsítványának segítségével meg kell győződni a bélyegző tanúsítvány integritásáról;
- a bélyegző tanúsítvány és az azt kibocsátó bizalmi szolgáltató tanúsítványának állapotát (érvényességét) ellenőrizni kell a tanúsítvány visszavonási listák vagy egyéb hiteles érvényességi információforrások alapján;

- A gyökér tanúsítvány kibocsátó bizalmi szolgáltató tanúsítványának visszavonási állapota az NMHH által karbantartott Bizalmi listában (Trusted list) ellenőrizhető
- meg kell vizsgálni a bélyegző tanúsítvány összes attribútumát

Nem fogadható el az elektronikus bélyegző, ha az elektronikus bélyegző, a bélyegző tanúsítvány vagy az érvényességi lánc valamely tanúsítványának valamely adata a bélyegző érvénytelenségére utal.

Az elektronikus bélyegző állapotára vonatkozó ellenőrzést és az elektronikus bélyegzővel kapcsolatos egyéb érvényességi feltételek megfelelőségének igazolását a bélyegzőt ellenőrző fél szoftveres és webes eszközök alkalmazásával is elvégezheti.

3.2.1 Megbízható időpont meghatározása

A bélyegzőt időbélyeggel kell ellátni. Az időbélyeget olyan módon kell csatolni a bélyegzőhöz, hogy a kapott bélyegző legalább PAdES-B-T bélyegző legyen.

A bélyegzőt a rajta lévő időbélyegen szereplő megbízható időpontra nézve kell ellenőrizni.

3.2.2 Tanúsítványlánc felépítése

A bélyegző tanúsítványát vissza kell vezetni egy elfogadott bizalmi szolgáltató tanúsítványára. A bélyegzőhöz csatolni kell az így kapott tanúsítványláncot, amely a bélyegző tanúsítványától egy elfogadott megbízható gyökérig (lásd: 4.3. fejezet) vezet. A megbízható gyökér nem része a tanúsítványláncnak, így nem kötelező csatolni. A bélyegzőhöz további szolgáltatói tanúsítványok is csatolhatók.

3.2.3 Visszavonási információk beszerzése

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

3.3 Elfogadott kriptográfiai algoritmusok köre

Jelen szabályzat értelmében a „*2015. évi CCXXII. Törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól” 92. § (1)* szerinti mindenkori hatósági határozat értelmében biztonságos kriptográfiai algoritmusok használhatók.

Jelenleg az NMHH EF/26838/2011[1] határozata az irányadó.

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

1 http://webpub-ext.nmhh.hu/esign2016/showPdfAction.do?tipus=kozlemeny&id=38

Irányadó szabvány:

- European Telecommunications Standards Institute (ETSI) ETSI TS 102 176-1 v 2.1.1 (2011-07 „Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures; Part 1: Hash functions and asymmetric algorithms”

3.4 Elfogadott bizalmi szolgáltatók

Jelen szabályzat értelmében minden olyan tanúsítvány kibocsátó bizalmi szolgáltató elfogadott, amely az Európai Unió tagállamai által kibocsátott ún. bizalmi listák valamelyikén (trusted list) bizalmi szolgáltatóként szerepel. A listákon szereplő szolgáltatói tanúsítványok e tekintetben megbízható gyökérként (trust anchor) kezelendők akkor is, ha maguk nem önhitelesített gyökértanúsítványok.

A Szolgáltató nem köteles elfogadni az olyan szolgáltatót, amely:

- egyik EU tagállam bizalmi listáján sem szerepel bizalmi szolgáltatóként,
- olyan EU tagállamban működik, amely nem bocsátott ki ETSI TS 102 231 szerinti, géppel értelmezhető, XML formátumú bizalmi listát,
- olyan bizalmi listán szerepel, amely nincsen aláírva,
- olyan bizalmi listán szerepel, amely nem ellenőrizhető az EU tagállamok bizalmi listáit összefoglaló listák listáján publikált tanúsítványok alapján.

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

Amennyiben a Befogadó kizárólag minősített bélyegzőket fogad el, akkor a bizalmi listákról csak azon bizalmi szolgáltatók tanúsítványait tekinti megbízható gyökérnek, amelyek szerint minősített tanúsítványok kibocsátása történik.

Amennyiben a Befogadó nem kizárólag minősített bélyegzőket fogad el, akkor a bizalmi listán lévő összes bizalmi szolgáltatói tanúsítványt elfogadja.

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

3.5 Elfogadott tanúsítványok

A Szolgáltató az aláírások és bélyegzők ellenőrzése során az alábbi tanúsítványtípusokat fogadja el:

- fokozott biztonságú (nem minősített) bizalmi szolgáltatótól származó tanúsítvány, és
- minősített bizalmi szolgáltatótól származó tanúsítvány,

amennyiben a szolgáltatók megfelelnek a Bizalmi szolgáltatók pontban meghatározott követelményeknek.

A Szolgáltató a Szolgáltatás általi elektronikus bélyegző elhelyezésére kizárólag minősített bélyegző tanúsítványt fogad el.

A bélyegző tanúsítvány érvénytelennek tekintendő és az elektronikusan bélyegzett dokumentum visszautasítható, ha:

- a tanúsítvány érvényességi lánca nem építhető fel egy megbízható bizalmi szolgáltatóig, illetve a bizalmi szolgáltató tanúsítványa kompromittálódott;
- a bélyegző létrehozásához használt adat kompromittálódott;
- a bélyegzőhöz, illetve az időbélyeghez tartozó tanúsítvány a bizalmi szolgáltató visszavonási listáján szerepel;
- a bélyegzőt ellenőrző személy tudomására jut, hogy az bélyegző-létrehozó adat bizalmassága sérült, vagy azzal visszaélés történt;
- az elektronikus bélyegző alkalmazásakor használt algoritmusok nem megfelelőek vagy nem biztonságosak;
- a bélyegzésre használt tanúsítvány nem használható elektronikus aláírás céljára;
- a bélyegzés egy olyan időpontban készült, amikor a bélyegzőhöz, illetve időbélyeghez tartozó tanúsítvány érvényessége lejárt, illetve a tanúsítvány még nem volt érvényes;
- a tanúsítványban szereplő adatok nem felelnek meg a valóságnak, vagy hiányosak.

3.5.1 A tanúsítványok érvényessége

A szolgáltató az alábbi esetekben tekinti a tanúsítványokat érvénytelennek:

- kompromittált, amikor a tanúsítványhoz kapcsolódó érvényességi lánc bármely eleméhez adat bizalmassága sérült,
- az alkalmazott aláírási/bélyegzési algoritmusok nem megfelelőek, vagy nem biztonságosak (a bélyegző-ellenőrző adatból származtatható az bélyegző-létrehozó adat, vagy egy előre meghatározott lenyomathoz utólag elkészíthető egy e-üzenet)
- a tanúsítványban feltüntetett adatok nem a valóságnak megfelelően szerepelnek,
- a tanúsítvány lejárt („notAfter” szerinti érvényességi idő elmúlt) vagy ha a tanúsítvány még nem érvényes („notBefore” szerinti érvényességi idő meg nem kezdődött el)
- a tanúsítvány a bizalmi szolgáltató visszavonási listáján szerepel;
- a tanúsítványhoz kapcsolódó érvényességi lánc bármely elemére a fenti pontok bármelyike teljesül

A tanúsítványok kezelésére vonatkozó részletszabályok a nem nyilvános Kriptográfiai szabályzatban találhatóak.

3.6 Elfogadott időbélyegzés-szolgáltatók

Minden olyan időbélyegzés-szolgáltató elfogadott, amely az Európai Unió tagállamai által kibocsátott bizalmi listák valamelyikén (trusted list) minősített időbélyegzés-szolgáltatóként szerepel vagy a szolgáltatás saját tanúsítványaival, vagy a szolgáltatás tanúsítványait kibocsátó tanúsítványkibocsátó tanúsítványával. A szolgáltatás tanúsítványának teljesítenie kell az RFC 3161 2.3 pontjában megfogalmazott feltételeket. A listákon szereplő szolgáltatói tanúsítványok e tekintetben megbízható gyökérként (trust anchor) kezelendők akkor is, ha maguk nem önhitelesített gyökértanúsítványok.

A hitelesítés-szolgáltatók esetén leírt szabályok itt is érvényesek.

3.7 Bélyegző-létrehozó termékek és alkalmazás szolgáltatók igénybe vétele

A BSZ rendszereiben a bélyegző automatizmusoknál, a HSM eszközökben, valamint a védett kommunikációs csatornák esetében a kriptográfiai kulcsok védelme megoldott, az alkalmazott eszközök és eljárások a (nem nyilvános) technikai dokumentumokban szerepelnek.

A BSZ FIPS PUB 140-2 szerint (Overall) Security Level 3 minősítésű, megfelelően biztonságos bélyegző létrehozó eszközt (HSM – Kriptográfiai hardver modult) alkalmaz.

4 AZ ELEKTRONIKUS BÉLYEGZŐ ELHELYEZÉS ELJÁRÁSAI

4.1 A dokumentum érkeztetési folyamata

A BSZ a bélyegzésre kapott dokumentumokon befogadása előtt a következő kriptográfiai- és adatformátum ellenőrzéseket hajtja végre:

- A BSZ csak meghatározott dokumentumtípusokat fogad, melyek adatformátumát befogadás előtt ellenőrzi;
- Kiszűrésre és elutasításra kerülnek a dokumentum megjelenítésének manipulálására alkalmas aktív kódokat tartalmazó dokumentumok;
- Kiszűrésre és elutasításra kerülnek a jelszóval védett dokumentumok;
- A BSZ ellenőrzi a dokumentumon található összes elektronikus aláírást és bélyegzőt. Nem megfelelő (lejárt stb.) elektronikus aláírást vagy bélyegzőt tartalmazó dokumentumot a BSZ nem fogad be.

4.2 BSZ bélyegzési folyamata

A BSZ dokumentumon elektronikus bélyegző elhelyezésekor a következő ellenőrzéseket és lépéseket hajtja végre:

- A dokumentumon szereplő korábbi elektronikus aláírások és bélyegzők, valamint a hozzájuk tartozó tanúsítványláncok kriptográfiai ellenőrzése
- Az elektronikus bélyegző létrehozása a dokumentumon Kriptográfiai hardver modul (HSM) által az abban tárolt magánkulccsal
- Az elkészült aláírás azonnal visszaellenőrzésre kerül kriptográfiailag
- Az aláíráshoz időbélyeg kérés kerül feladásra az időbélyeg szolgáltató felé nonce alkalmazásával
- Az elkészült időbélyeg azonnal visszaellenőrzésre kerül (nonce-szal együtt) kriptográfiailag

A bélyegző tanúsítvány érvényessége fél óránként online ellenőrzésre kerül OCSP használatával. A bélyegző tanúsítvány láncának ellenőrzése a szolgáltatás induláskor történik meg bizalmi listák használatával.

A bizalmi listákban a tanúsítványkibocsátó tanúsítványával szereplő időbélyegző tanúsítványok érvényessége fél óránként online ellenőrzésre kerül OCSP használatával. A bizalmi listákban szereplő időbélyegző tanúsítványok ellenőrzése a szolgáltatás indulásakor történik meg.

4.3 A bélyegzőkhöz kapcsolódó kötelezettségek

A BSZ dokumentum partnertől (*Bélyegző létrehozója*) való befogadásakor – a mellékelt vezérlési információkban jelzett igény esetén – azt elektronikus szervezeti bélyegzővel látja

el. Az ehhez kapcsolódó kötelezettség (commitment type) a „Proof of origin”, azaz a dokumentumot olvasók számára biztosítékot nyújt a dokumentum származását tekintve.

A Bélyegző *létrehozója* üzleti folyamatainak keretében az elektronikus dokumentumon a *Dokumentum közreműködő* által végrehajtott műveletek (kézi aláírás stb.) és hozzáadott metaadatok elektronikus felülhitelesítésére a *Bélyegző elhelyezését kezdeményező* kezdeményezésére a BSZ által elhelyezett elektronikus bélyegzők kötelezettség típusa (commitment type) a „Proof of approval”, azaz a *Bélyegző elhelyezését kezdeményező* jóváhagyta a *Dokumentum közreműködő* által kiegészített/módosított dokumentumot és elektronikus bélyegzővel elláthatónak értékelte.

5 HELP DESK SZOLGÁLTATÁS NYÚJTÁSA

A felmerülő problémák megoldására a Szolgáltató help desk támogatást nyújt, amelynek elérhetőségét a szolgáltatási szerződésben rögzíti.

6 KAPCSOLÓDÓ DOKUMENTUMOK

Publikus dokumentumok

- Szolgáltatási Szabályzat (Elektronikus Bélyegző Elhelyezése Szolgáltatás Bizalmi Szolgáltatási Szabályzat)

Belső dokumentumok

- Kriptográfiai szabályzat (nem nyilvános)