Elektronikus Bélyegző Elhelyezése Szolgáltatás Bizalmi Szolgáltatási Szabályzat

Hatályba lépés dátuma: 2021.04.08.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2021.03.18.	Jóváhagyás dátuma: 2021.03.23.
Figyelem! Jelen dokumentumnak a https://www.mobilsign.com oldalon publikált, illetve bélyegzővel ellátott példányai tekinthetők hitelesnek.	

Dokumentum verziókövetés			
Verzió	**Módosítás rövid leírása**	**Módosította**	**Hatályba lépés**
0.1	Első munkaváltozat	Benkó Tamás	
0.2	Bejelentéshez kiegészítések	Benkó Tamás	
1.0	Kiadott verzió	Dohányos Péter	2017.11.30.
1.1	Auditori észrevételek átvezetése	Dohányos Péter	2018.02.07.
1.2	Auditori észrevételek átvezetése	Dohányos Péter	2018.02.26.
1.3	NMHH észrevételei alapján módosított változat	Dohányos Péter	2018.03.27.
1.4	NMHH észrevételei alapján módosított változat	Dohányos Péter	2018.04.21.
1.5	Szabvány- és dokumentum hivatkozások frissítése, adatok aktualizálása	Dohányos Péter	2021.04.08.

Tartalom

1 Bevezetés

Jelen dokumentum a MobilSign Kft. (továbbiakban Szolgáltató) Elektronikus Bélyegző Elhelyezése Szolgáltatás Bizalmi Szolgáltatási Szabályzata (továbbiakban Szolgáltatási Szabályzat, vagy Szabályzat), mely a nem minősített elektronikus bélyegző elhelyezése szolgáltatására vonatkozik.

A Szolgáltató jelen dokumentumban szabályozott bizalmi szolgáltatását az eIDAS rendelet 36. cikke szerinti, fokozott biztonságú elektronikus bélyegzőket létrehozó szolgáltatásként kell értelmezni (továbbiakban Szolgáltatás).

A Szolgáltató a Szolgáltatást a vele szerződéses viszonyban lévő Szerződött Partnerek részére nyújtja.

1.1 Áttekintés

Jelen Szabályzat célja annak ismertetése, hogy a Szolgáltató az elektronikus bélyegző elhelyezése bizalmi szolgáltatásával kapcsolatban milyen módon teljesíti az Elektronikus Bélyegző Elhelyezése Szolgáltatás Bizalmi Szolgáltatási Rendben meghatározott követelményeket és elvárásokat. A Szabályzat a nyújtott szolgáltatások feltételeit más, a Szolgáltató által kiadott dokumentumokkal –mint az ÁSZF, a Szerződött Partnerrel kötött Szolgáltatási Szerződés és egyéb szerződések – együtt, együttesen szabályozzák.

Jelen dokumentum megfelel az RFC 3647 nemzetközi ajánlás követelményeinek, követi az abban meghatározott dokumentum szerkezetet, ám annak nem minden fejezete értelmezhető a Szolgáltatásra vonatkozólag, illetve nem az ajánlásban meghatározott pontos fejezetnév használható a Szolgáltatás eltérő jellege miatt. Az érintett fejezetekben ez feltüntetésre kerül.

1.1.1 A Szolgáltató

A Szolgáltató adatai:

Név	MobilSign Korlátolt Felelősségű Társaság
Rövid név	MobilSign Kft.
Székhely	1126 Budapest, Királyhágó tér 8-9.
Telephely	1126 Budapest, Királyhágó tér 8-9.
Cégjegyzék szám	01-09-194592
Adószám	25010714-2-43
Telefon	+36 20 383 9236
Weboldal	https://www.mobilsign.com
Ügyfélkapcsolat elérhetősége és nyitva tartása	support@mobilsign.com H-P: 9-16
Szolgáltatás bizalmi felügyeletnek való bejelentése	2018.02.09.

A Bizalmi Felügyelet bizalmi szolgáltatásokat tartalmazó nyilvántartásának elérhetősége: http://webpub-ext.nmhh.hu/esign2016/

1.2 A dokumentum neve és azonosítója

A dokumentum teljes neve Elektronikus Bélyegző Elhelyezése Szolgáltatás Bizalmi Szolgáltatási Szabályzat. A dokumentum neve, verziószáma és OID azonosítója megtalálható a dokumentum minden oldalán látható fejlécben.

1.3 PKI közösség

A Szolgáltatás PKI közössége a következő csoportokból áll: a Szolgáltató, a vele szerződéses kapcsolatban álló Szerződött Partner, az Bélyegző elhelyezését kezdeményező, a Dokumentum közreműködő, és az Érintett felek

1.3.1 Szolgáltató

A Szolgáltató a bizalmi szolgáltatása keretében elektronikus bélyegzők létrehozását biztosítja.

1.3.2 Szerződött partner

A Szerződött Partner szerződéses viszonyban áll a Szolgáltatóval a vonatkozó Szolgáltatói Szerződésben, Általános Szerződési Feltételekben és a Szolgáltatási Szabályzatban foglaltak szerint.
A Szerződött Partner a Szolgáltatás 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.

1.3.3 Bélyegző elhelyezését kezdeményező

A Szerződött Partner alkalmazottja, vagy arra feljogosított személye, aki manuális interakcióval aktiválja a Szolgáltatás által megvalósított elektronikus bélyegző létrehozást.

1.3.4 Dokumentum közreműködő

A Szerződött Partner -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 Szolgáltatás használatával kezdeményezett elektronikus bélyegző létrehozását kell, hogy maga után vonja.

1.3.5 Éritett felek

Az Érintett fél a Szolgáltatóval és a Szerződött Partnerrel szerződéses viszonyban nem álló harmadik személy. Tevékenységére vonatkozó ajánlásokat a szabályzat és az abban megnevezett egyéb szabályzatok tartalmazzák.

1.4 Tanúsítványok alkalmazhatósága

Az elektronikus bélyegző elhelyezése szolgáltatásra az RFC 3647 ezen pontja nem értelmezett, így jelen dokumentum e ponthoz nem fogalmaz meg követelményt.

1.5 A Szabályzat adminisztrációja

Jelen Szabályzat adminisztrációját a Szolgáltató végzi, melynek adatai megtalálhatóak a 1.1.1 A Szolgáltató fejezetben.

A Szolgáltató legalább évente egyszer megvizsgálja a bizalmi szolgáltatási szabályzat releváns jogszabályi- és technológiai szabványok előírásainak megfelelőségét és szükség esetén a bizalmi szolgáltatási szabályzatból módosított, új verziót bocsát ki és léptet hatályba.

1.5.1 Szolgáltatási Szabályzat és Szolgáltatási rend kiadásának eljárása

A beérkezett, illetve felülvizsgálat során megállapított, indokolt és elfogadott módosítási igények teljesítésére új dokumentum verzió kerül kidolgozásra, melyet a szolgáltatásért felelős informatikai vezető jogosult jóváhagyni. Az új dokumentum verzió hatályba lépésének feltétele a jóváhagyás, valamint megnövelt verziószám és egyedi azonosítószám (OID) hozzárendelése.

A jóváhagyott, hatályba lépő szabályzat- illetve szolgáltatási rend dokumentum verziót a Szolgáltató honlapján publikálja: https://www.mobilsign.com

A hatályba lépő új verzió kötelező érvényű a Szolgáltatóval szerződéses viszonyban álló Szerződött Partnerekre.

1.6 Fogalmak ás rövidítések

1.6.1 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;
- **„Bizalmi szolgáltatási rend”**: olyan szabálygyűjtemény, amelyben egy bizalmi szolgáltató, igénybe vevő vagy más személy valamely bizalmi szolgáltatás használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára;
- **„Bizalmi szolgáltató”**: egy vagy több bizalmi szolgáltatást nyújtó természetes vagy jogi személy; a bizalmi szolgáltató lehet minősített vagy nem minősített bizalmi szolgáltató;
- **„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;

- **„HSM Security World”**: a kriptográfiai magánkulcsokat –és opcionálisan a hozzá tartozó nyilvános kulcsot és tanúsítványt– tároló, csak a HSM eszköz által feloldható titkosítással védett adategység
- **„Szerződött Partner”**: a Szolgáltatóval a Szolgáltatás igénybevételére szerződéses viszonyban álló ügyfél
- **„Szolgáltatás”**: a Szolgáltató által nyújtott, Elektronikus bélyegző elhelyezése –nem minősített– bizalmi szolgáltatás
- **„Szolgáltatási szabályzat”**: a bizalmi szolgáltató nyilatkozata az egyes bizalmi szolgáltatások nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről;
- **„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;

1.6.2 Rövidítések

- **ÁSZF**: Általános Szerződési Feltételek
- **eIDAS**: Az Európai Parlament és a Tanács 910/2014/EU rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről
- **Eüt**: 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól
- **HSM**: Hardware Security Module (Kriptográfiai Hardver Modul)
- **NMHH**: Nemzeti Média- és Hírközlési Hatóság, Bizalmi Felügyelet
- **OCSP**: Online Certificate Status Protocol (valós idejű tanúsítvány-állapot protokoll)
- **OID**: Object IDentifier
- **PKI**: Public Key Infrastructure (nyilvános kulcsú infrastruktúra)

2 Közzétételek

2.1 A nyilvános szabályzatok elérhetősége

A Szolgáltató a Szolgáltatással kapcsolatos nyilvános szabályzatok hatályos- és hatályát vesztett korábbi verzióit a honlapján teszi közzé, melynek elérhetősége 1.1.1 A Szolgáltató fejezetben található.

2.2 Közzététel gyakorisága, korlátozásai

A Szolgáltató a Szolgáltatással kapcsolatos szabályzatok változása esetén azokat a lehető leghamarabb, de mindenképpen azok hatálybalépése előtt a folyamatosan elérhető honlapján publikálja. A Szolgáltató az ilyen módon publikált információk tekintetében honlapján kizárólag olvasási jogosultságot biztosít, a publikált információk jogosulatlan módosítása, illetve annak kísérlete is tilos.

3 Azonosítás és hitelesítés

A Szolgáltató a Szerződött Partner (jelöttel) kötendő szerződésbe kerülő adatok ellenőrzésére közhiteles és egyéb nyilvántartásokat használ fel.

A Szerződött Partnerek és a nevükben eljáró személyek azonosítása a Szerződéskötéskor, valamint a Szolgáltató közreműködésével megvalósuló kulcsgeneráláskor történik meg.

A Szolgáltató a Szerződött Partner által megadott és az elektronikus bélyegző tanúsítványba kerülő adatokat közhiteles nyilvántartásban (cégnyilvántartás) ellenőrízheti.

A Bélyegző elhelyezését kezdeményező személyek azonosítása felhasználónév és jelszó alapján történik.

3.1 Azonosítás és hitelesítés kulcscsere kérelem esetén

Bélyegző kulcs (és tanúsítvány) cseréjét normál eljárásrend szerint a Szolgáltató kezdeményezi. Ha a Szerződött Partner valamilyen okból még ezt megelőzően szeretné kezdeményezni a bélyegző tanúsítvány lecserélését, ezt megteheti hivatalos – lehetőleg cégszerű aláírással, de minimum a felek közötti szerződésben a kapcsolattartásra, valamint e téren eljárásra kijelölt/felhatalmazott személy aláírásával ellátott és lebélyegzett – dokumentum formájában, vagy a Szerződött Partner elektronikus bélyegzőjével (illetve azzal egyenértékű elektronikus aláírással) ellátott elektronikus dokumentum formájában.

A Szolgáltató nem támogatja a tanúsítvány megújítási funkciót.

4 A Szolgáltatás és életciklusa

Jelen fejezet az RFC ajánlás által (eredetileg tanúsítvány kiadás szolgáltatáshoz) meghatározott fejezetstruktúrának a Szolgáltató elektronikus bélyegző elhelyezése szolgáltatására igazított leképezését tartalmazza, annak adattartalmával együtt.

4.1 Szolgáltatás igénylése, üzembe állítása

A Szolgáltatást szolgáltatási szerződés megkötése után lehetséges igénybe venni.

A Szolgáltató a Szerződött Partner számára a Szolgáltatási infrastruktúrában dedikált kiszolgáló példányt hoz létre, mely kizárólag a Szerződött Partner által küldött kéréseket szolgálja ki. Ennek pontos menetét nem nyilvános belső dokumentumok rögzítik.

A Szolgáltatás használatához kapcsolat létrehozása szükséges a Szolgáltatás technikai interfésze és a Szerződött Partner informatikai rendszere között. Ennek során a Műszaki dokumentáció ügyfél

csatlakozásához (nem nyilvános, a Szerződött Partner részére tartós adathordozón vagy védett csatornán átadásra kerülő) dokumentumok előírásait szükséges követni. A Szolgáltatás a Szerződött Partner részéről a biztosított technikai interfészek használatával kétféle módon érhető el és aktiválható: egyrészt a releváns üzleti folyamatait megvalósító informatikai rendszerei által kezdeményezve, másrészt feljogosított *Bélyegző elhelyezését kezdeményező* képviselői által dedikált kliens alkalmazás használatával manuálisan kezdeményezve.

A Szerződött Partner bélyegző kulcspárja a Szolgáltató közreműködésével, jegyzőkönyvezett módon kerül generálásra nagybiztonságú Kriptográfiai hardver modulban (HSM). A bélyegző kulcspár nyilvános kulcsához elkészített tanúsítvány kiállítási kérés adatelem (PKCS#11 CSR - Certificate Signing Request) segítségével a Szerződött Partner feladata minősített bélyegző tanúsítvány beszerzése egy EU nyilvántartásban szereplő bizalmi szolgáltatótól.

A bélyegző tanúsítvánnyal szemben támasztott technikai elvárások:

- minősített tanúsítvány
- nonRepudiation és/vagy digitalSignature kulcshasználati (key usage) beállítás
- tartalmaznia kell OCSP elérési információkat
- tanúsítvány lánca EU bizalmi listára (TL) visszavezethető legyen

A Szerződött Partner kiállított bélyegző tanúsítványát a Szolgáltató betölti az elektronikus bélyegző létrehozására használt HSM eszközbe. Ennek során a Szolgáltató ellenőrzi a tanúsítvány technikai megfelelőségét, valamint az abban szereplő adatokat, és jogosult a tanúsítvány alkalmazásának elutasítására, amennyiben az technikailag nem megfelelő (például nem minősített tanúsítvány) vagy adattartalmát tekintve nem elfogadható (például nem a Szerződött Partner részére került kiállításra).

4.2 Dokumentum fogadása

A Szolgáltató a Szerződött Partnertől elektronikus bélyegző létrehozásához dokumentumot a kialakított biztonságos kapcsolaton keresztül a dokumentum fogadó interfészen fogad. A Szolgáltatás kizárólag PDF dokumentumokat fogad be elektronikus bélyegzésre.

Ennek során a Szolgáltató a dokumentumot és a mellékelt metaadatokat ellenőrzésnek veti alá, és csak akkor fogadhatja be azokat, amennyiben azok technikailag és információ biztonsági szempontból is megfelelnek a Szolgáltatás által feldolgozáshoz szükséges követelményeknek. E követelmények és ellenőrzések a Műszaki dokumentáció ügyfél csatlakozásához (nem nyilvános, a Szerződött Partner részére tartós adathordozón vagy védett csatornán átadásra kerülő) dokumentumokban kerülnek ismertetésre, de különösen:

- A beérkező dokumentum valid (struktúrájú) PDF dokumentum
- A PDF dokumentum nem tartalmazhat kártékony aktív kódot, vagy a megjelenítést befolyásoló aktív kódot
- A dokumentumon esetlegesen már szereplő elektronikus aláírásoknak, elektronikus bélyegzőknek és időbélyegzőknek érvényesnek kell lenniük (CRL- illetve OCSP alapú online visszavonási ellenőrzés ezen a ponton nem történik)

Az ellenőrzési műveletek által nem megfelelőnek talált dokumentum befogadása elutasításra kerül az elutasítás okának megjelölésével (automatizált válaszüzenet formájában).

Befogadható dokumentum esetén a Szerződött Partner (dokumentumot az interfészen beküldő informatikai rendszere) pozitív válaszüzenetet kap és a dokumentum a feldolgozási folyamat időtartamára eltárolásra kerül a Szerződött Partner számára dedikált, védett tárolási helyen.

4.3 Elektronikus bélyegző létrehozása

A Szerződött Partner a Szolgáltatás 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.

Az első esetben a Szerződött Partner a dokumentum interfészen való beküldésekor –megfelelő paraméterezés útján– aktiválja elektronikus bélyegző befogadott dokumentumon való elhelyezését.

A második esetben a beküldéskor megfelelő vezérlési információval ellátott, befogadott dokumentum a Szerződött Partner feljogosított *Bélyegző elhelyezését kezdeményező* képviselői a Szerződött Partner IDM rendszerében (felhasználói név és jelszó alapon) azonosított és felhatalmazott módon használt dedikált kliens alkalmazásába továbbítódik titkosított, védett csatornán. A kliens alkalmazásban a *Bélyegző elhelyezését kezdeményező* és –a *Bélyegző elhelyezését kezdeményező* kontrollja alatt az általa beazonosított– *Dokumentum közreműködő* személy a dokumentumot elolvashatja és hozzá csatolandó információkat (metaadatokat, kézi aláírásokat) rögzíthet. Ezután a *Bélyegző elhelyezését kezdeményező* a kliens alkalmazásból sajátkezűleg (azonosítás utáni interfész hívással) aktiválja a Szolgáltatást és a metaadatokkal kiegészített dokumentumon létrehozza a paraméterezésnek megfelelő számú elektronikus bélyegzőt.

A Szolgáltatás aktiválásakor a Szerződött Partner magánkulcsát és bélyegző tanúsítványát tároló Kriptográfiai hardver modul használatával a dokumentumon (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 Szolgáltatás *Bélyegző elhelyezését kezdeményező* általi aktiválásakor egyszerre egynél több elektronikus bélyegző létrehozását, csak az egymásra épülő bélyegző-sorozat kezdő (első) és záró (utolsó) bélyegzője kerül ellátásra időbélyeggel

4.4 Bélyegzett dokumentum átadása

A Szolgáltatás az elektronikus bélyegzővel ellátott dokumentumot automatikusan továbbítja a Szerződött Partner részére a szolgáltatás üzembe állításakor kialakított elektronikus interfészen keresztül. Amennyiben a bélyegzővel ellátott dokumentum automatikus továbbítása kapcsolati vagy egyéb probléma miatt nem sikeres, a dokumentum továbbítása tetszőleges számban újraindítható a Szolgáltatás üzemeltetői oldaláról.

4.5 Az előfizetés megszűnése

Előfizetés megszűnésekor a Szerződött Partner bélyegző magánkulcsa visszaállíthatatlan módon törlésre kerül. Emellett a Szerződött Partner ajánlottan kezdeményezi a bélyegző tanúsítvány visszavonását az azt eredetileg kiállító bizalmi szolgáltatónál.

A Szolgáltató a megszűnt szerződéshez kapcsolódóan tárolt munkaadatokat egy évig megőrzi, melynek letelte után jogosult azokat törölni. A munkaadatok (bizonyítékrekordok, bélyegzők hosszú távú hitelességi bizonyítékai stb.) Szolgáltató általi esetleges további megőrzéséről és hitelességük fenntartásáról a felek egyedi megállapodás formájában dönthetnek.

A Szolgáltató a megszűnt szerződéshez kapcsolódó naplófájlokat 10,5 évig őrzi meg.

4.6 Magánkulcs letétbe helyezése és visszaállítása

A Szolgáltató a Szolgáltatás fenntartásához szükséges mentések keretében – a kulcsok biztonságát nem veszélyeztetve – a HSM Security Worldről biztonsági másolatot készít.

Előfizetési szerződés megszűnése esetén a Szerződött Partner bélyegző magánkulcsa törlésre kerül a Szolgáltató Kriptográfiai hardver moduljából, valamint biztonságos törlésre kerül minden olyan biztonsági mentés, melyben az azt kezelő HSM Security World előfordulhat.

5 Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések

A Szolgáltató gondoskodik arról, hogy kellő, az elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra.

Szolgáltató nem nyilvános Információbiztonsági Szabályzata tartalmazza az információbiztonsági szabályozással kapcsolatos előírásokat.

5.1 Fizikai óvintézkedések

A Szolgáltató gondoskodik arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen, és a kritikus szolgáltatások eszközeinek fizikai kockázatát minimalizálja. A fizikai óvintézkedések célja a Szolgáltató információjára és fizikai körleteire irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása. A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken valósítják meg a Szolgáltató rendszerében. A biztosított védelem arányban áll a Szolgáltató által végzett kockázat elemzésben megállapított kockázatokkal.

5.1.1 Felépítés

Bizalmi szolgáltatás nyújtásához használt Informatikai infrastruktúra a T-System Cloud and Data Center-ben (továbbiakban hosting szolgáltató - 1087 Budapest, Asztalos Sándor út 13.) került kialakításra. Az ottani környezetet egy biztonsági zónának tekintjük, mert a szolgáltatást biztosító infrastruktúra és alkalmazás komponensek mindegyike elengedhetetlen a szolgáltatás biztosításához.

A Szolgáltató telephelyén megfelelő védelmi zónák (Z0 – általános munkakörnyezet és Z1 - szerverhelyiség) kerültek kialakításra a Szolgáltatás kellő biztonságú üzemeltetése és támogatása érdekében.

5.1.2 Fizikai hozzáférésvédelem

A hosting szolgáltató területére való belépéshez az üzemeltetésért felelős szolgáltató képviselőjének van joga. A belépési jog 7/24 órában élő, a belépéseket a hosting szolgáltató rendszere naplózza, megőrzi.

A Szolgáltató telephelyén a Z0 – általános munkakörnyezet – zónába való bejutást kulccsal és kártyával nyíló ajtó védi. A bejutás a jogosultak számára 7/24 órában lehetséges. A belépés saját jogon jogosultsággal nem rendelkező látogató (beszállító, alvállalkozó, partner, hatóság, ügyfél stb.) számára csak beengedéssel lehetséges. Saját jogon ott tartózkodásra nem jogosult látogató, csak megfelelő jogosultsággal rendelkező kolléga kíséretében tartózkodhat a helyiségekben. A látogatókat a jelenlétük során végig kísérni szükséges. Belépésre jogosultak a cég munkavállalói, illetve az Ügyvezető által engedélyezett alvállalkozók.

A Szolgáltató telephelyén a Z1 – szerverhelyiség – hozzáférésvédett zónába való bejutás a jogosultak számára 7/24 órában lehetséges. A belépés saját jogon jogosultsággal nem rendelkező látogató (beszállító, alvállalkozó, partner, hatóság, ügyfél stb.) számára csak beengedéssel lehetséges. Saját jogon ott tartózkodásra nem jogosult látogató, csak megfelelő jogosultsággal rendelkező kolléga kíséretében tartózkodhat a helyiségben. A látogatókat a jelenlétük során végig kísérni szükséges. A szerverhelyiségbe való belépések és kilépések elektronikusan nyomon követésre kerülnek.

5.1.3 Áramellátás, légkondicionálás

A hosting szolgáltató rendszerkörnyezetre vonatkozóan e szolgáltatásokat a hosting szolgáltatás üzemeltetője szolgáltatja:

- duplikált, georedundáns áram betáplálás;
- szünetmentes áramellátás;
- aggregátorok biztosítása;
- duplikált klímarendszer;

A telekommunikációs hálózat védelmét a beléptetés szigorú kontrollja és a kiépített georendundáns csatlakozások támogatják.

A Szolgáltató telephelyén a Z1-es zónában az áramkimaradás elleni védelmet szünetmentes tápegységek biztosítják a szerverszobában.

A Szolgáltató telephelyére vonatkozóan a Z0-ás zónában a szolgáltatások (áram, víz, gáz, klíma rendszer) felügyeletét az irodaház működtetőjének a feladata.

5.1.4 Beázás és elárasztódás veszélyeztetettsége

A Szolgáltató szolgáltatási helyszínei védettek a beázástól és az elárasztódástól. A védett számítógépteremben a biztonságot növeli az álpadló alkalmazása.

5.1.5 Tűzmegelőzés és tűzvédelem

A hosting rendszerkörnyezetre vonatkozóan a tűzvédelmi rendszer (füstérzékelés és riasztás, valamint oltás) működtetését a hosting szolgáltatás üzemeltetője szolgáltatja.

A Szolgáltató telephelyére vonatkozóan (Z0 és Z1-es zóna) a tűzvédelmi rendszer (füstérzékelés és riasztás) működtetése az irodaház működtetőjének feladata.

5.1.6 Adathordozók kezelése

A szolgáltató a tárolandó adathordozókat, így különösen az Offsite backup mentés és újrainstallálási „how-to" leírásokat, jelszó borítékokban őrzött felhasználói információkat, védett adatokat tároló páncélkazettákat, adminisztrátori és operátori kártyákat páncélszekrényben őrzi.

A páncélszekrényekhez való hozzáférés, az azokhoz dokumentált jogosultsággal rendelkező tisztviselők közreműködésével lehetséges a szabályzatoknak megfelelően. A páncélszekrényekből bármely tételt kivenni legalább egy jogosult tisztviselő engedélyével és jelenlétében lehetséges. A kivételről feljegyzést kell készíteni, melyet megőrizni szükséges.

5.1.7 Selejt kezelése

A használhatatlan leselejtezett adathordozók (pl.: USB drive, PC, laptop stb.) fizikai megsemmisítéséről gondoskodni kell. A megsemmisítés előtt az adathordozókon található adatokat a helyreállíthatatlanságot biztosító törlési technikákkal és eljárásokkal a rendszergazda törli.

Ennek érdekében:

- a törlésnél olyan szoftvert kell alkalmazni, amely legalább 3x felülírja az adatot a törlés során, melyek közül legalább 1 felülírás véletlenszerű értékekkel történik (titkosított adathordozó esetén csak a kulcs megsemmisítése szükséges). Amennyiben ez nem lehetséges, akkor az adathordozót kötelező elzárt helyen, dokumentáltan tárolni/biztonságos és környezettudatos módon, dokumentáltan megsemmisíteni,
- a törlést az ügyvezető hagyja jóvá,
- garanciális eszközök esetén, ha az eszköz hibája miatt az adatok törlésére nincs mód, az ügyvezető dönt az eszköz cserére történő kiadhatóságáról:
    - a bélyegző HSM technológiai megoldásából fakadóan perzisztens módon nem tárolja a bélyegző magánkulcsokat, így meghibásodás esetén nem áll fenn magánkulcs kiadásával járó kockázat
    - egyéb adathordozó esetében meghibásodás esetén nincs mérlegelési lehetőség, az adathordozó kötelezően megsemmisítésre kerül

Az adatok megfelelő módon történő eltávolításáért az IT biztonsági vezető a felelős. Az adatok eltávolítását a rendszergazda végzi.

Biztonsági tisztviselőnek kell ellenőriznie a selejtezett adathordozók biztonságos, ellenőrzött és dokumentált megsemmisítését, melyet az Infrastruktúra üzemeltető végez. A selejtezésről jegyzőkönyvet szükséges készíteni, illetve a vonatkozó dokumentációkat (leltár, konfigurációs dokumentáció) frissíteni szükséges.

5.1.8 Szeparált mentés

A mentés elsődleges fizikai helyszíne a T-System Cloud and Data Center, kizárólag a Szolgáltató által nyitható és felügyelt, zárt rack szekrényében lokalizált dedikált mentő szervere.

Ezen felül a Szolgáltatásban offsite mentések is megvalósításra kerültek, melyek folyamatait belső szabályzatok rögzítik.

5.1.9 Mobil eszközök használata

A bizalmi szolgáltatás nyújtásához használt Informatikai infrastruktúrához mobil eszközzel kapcsolódni (mobiltelefon, tablet, laptop stb.) nem engedélyezett (kivéve a MobilSign SaaS kliens alkalmazásokat futtató mobil eszközök számára a bizalmi szolgáltatás kliens interfészein keresztül). Távoli elérésű üzemeltetői/adminisztrációs VPN kapcsolat felépítése csak a MobilSign irodai infrastruktúrában kialakított, fizikailag elzárt helyen (szerverszoba) elhelyezett ugrógépről engedélyezett. Ettől eltérni kizárólag az ITBV kifejezett engedélyével lehet.

5.2 Eljárásrend intézkedések

5.2.1 Bizalmi munkakörök

A Szolgáltató a jelen szabályzatban nyújtott szolgáltatás keretében a következő bizalmi szerepköröket alkalmazza:

- a Szolgáltató informatikai rendszeréért általánosan felelős vezető;
- IT biztonsági vezető (ITBV): feladata a biztonsági beállítások és policy módosítások jóváhagyása és ellenőrzése, a Szolgáltatással kapcsolatos biztonsági vonatkozású egyéb módosítások engedélyezése, elzárt kripto eszközök kiadása
- Security Officer (Biztonsági tisztviselő): feladata biztonsági vonatkozású műveletek elvégzése, valamint az Admin Portálon elérhető biztonsági rendszerbeállítások módosítása
- System Administrator (Rendszeradminisztrátor): feladata a telepítések és konfigurációs feladatok elvégzése, biztonsági mentések lefolytatása, valamint az Admin Portálon elérhető nem biztonsági rendszerbeállítások módosítása
- System Operator (Rendszerüzemeltető): feladata a Szolgáltatással kapcsolatos üzemeltetési feladatok ellátása
- Független rendszervizsgáló: A szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy

A Szolgáltató a bizalmi munkakörökről folyamatosan karbantartott, naprakész nyilvántartást vezet.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszám

Szolgáltató az alábbi tevékenységeket legalább kettő arra kijelölt és közvetlen felhatalmazással rendelkező bizalmi munkatárs együttes fizikai jelenlétével, egy fizikailag védett környezetben végzi (melynek részletes szabályozása a Szolgáltató nem publikus belső szabályzataiban található):

- Szerződött Partner bélyegző kulcspárok és CSR (PKCS#10) generálása
- Szerződött Partner elektronikus bélyegző- és kibocsátói tanúsítvány lánc visszatöltés

- A bélyegző HSM Security Worldhöz kapcsolódó karbantartási és üzemeltetési műveletek
- Szerződött Partner bélyegző kulcspárok és bélyegzők törlése

5.2.3 Az egyes szerepkörökhöz tartozó azonosítás és hitelesítés

Az informatikai rendszer minden felhasználója és az adminisztratív folyamatok minden szereplője személy szerint kerül azonosításra. Sikeres hitelesítés előtt egyetlen biztonság kritikus tevékenységet sem lehet végrehajtani. A Szolgáltató munkatársai számára megadott hozzáférési jogosultságok engedélyezési folyamaton mennek át, a feleslegessé vált hozzáférések felülvizsgálatra kerülnek és már nem indokolt esetben visszavonásra kerülnek.

A Szolgáltatás szempontjából kritikus rendszerek fizikai megközelítése is hozzáféréshez, azonosításhoz kötött.

5.2.4 Egyes szerepkörök összeférhetetlensége

A Szolgáltatás nyújtása közben a szerepkörök estében a következő kizáró szabályok érvényesek.

Minden Szolgáltatói és Szerződött partneri szerepkör kizárja egymást.

A Szolgáltatónál meglévő szerepkörök kizárását az alábbi táblázat szemlélteti:

	Inf.Rsz.Ált. Felelős Vezető	ITBV	Biztonsági tisztviselő	Rendszer adminisztrátor	Rendszer üzemeltető	Független rendszervizsgáló
Inf.Rsz.Ált. Felelős Vezető		X	X			X
ITBV	X			X	X	X
Biztonsági tisztviselő	X			X	X	X
Rendszer adminisztrátor		X	X		X	X
Rendszer üzemeltető		X	X	X		X
Független rendszervizsgáló	X	X	X	X	X	

ahol X (piros) az összeférhetetlen szerepköröket jelöli

5.3 Személyzetre vonatkozó előírások

A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a visszaélések kockázatának csökkentése. Ezek megelőzésére a Szolgáltató már a munkatársak felvételének folyamán törekszik, és az alkalmazás során folyamatosan folyamatos ellenőrzésekkel biztosítja az ezek csökkentésére irányuló kontrollok működését.

Minden bizalmi szerepkört betöltő munkatársnak és külső félnek – aki a Szolgáltató Szolgáltatásaival kapcsolatba kerül – titoktartási nyilatkozatot kell aláírnia.

5.3.1 Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények

A Szolgáltató a Szolgáltatás nyújtásához csak az adott munkakörhöz megfelelő tudással és képzettségekkel rendelkező dolgozót alkalmaz. Amennyiben alvállalkozót vesz igénybe, ezt az alvállalkozóktól is megköveteli.

A Szolgáltató a megfelelő képzettségeket felvételkor ellenőrzi. A megfelelő tudásszint fenntartására a Szolgáltató a dolgozók részére éves tervet készít. Amennyiben a Szolgáltató rendszereiben vagy folyamataiban történő változások ezt indokolják, a Szolgáltató a dolgozók részére soron kívüli oktatást biztosít.

A bizalmi munkakört a munkatársak a megfelelő gyakorlati tapasztalat megszerzését követően tölthetnek be.

5.3.2 Előélet vizsgálatára vonatkozó eljárások

A Szolgáltató vezető munkakörben illetve bizalmi szerepkörben csak olyan alkalmazottakat foglalkoztat, akik:

- büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, amely a büntetlenséget befolyásolhatja;
- nem állnak a bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkozástól eltiltás hatálya alatt.

Kinevezéskor a Szolgáltató vezető munkakört betöltő alkalmazottjának nyilatkozatával, bizalmi szerepkört betöltő alkalmazottjának 3 hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolnia büntetlen előéletét.

A Szolgáltató a felvételi eljárás során ellenőrzi a jelentkező önéletrajzában megadott releváns információk valódiságát.

5.3.3 Képzési követelmények

A bizalmi munkakört betöltő munkatársaknak rendelkezniük kell a feladataik ellátásához szükséges tudással. Az ennek való megfelelést megfelelő szakképzetséggel és munkatapasztalattal is igazolni kell. Ezek hiányában a Szolgáltató rendszereihez nem adható ki hozzáférési jogosultság.

5.3.4 Továbbképzési gyakoriságok és követelmények

A Szolgáltató folyamatos képzésekkel gondoskodik a Szolgáltatás nyújtásában közreműködők megfelelő szintű tudásáról. Amennyiben a Szolgáltatás informatikai környezetben ezt igénylő jelentős változás következik be, a Szolgáltató gondoskodik a munkatársak megfelelő szintű képzéséről.

5.3.5 Munkabeosztás körforgásának sorrendje és gyakorisága

A Szolgáltató nem alkalmaz kötelező jellegű körforgást az egyes munkabeosztások között.

5.3.6 Felhatalmazás nélküli tevékenységek szankcionálása

A Szolgáltató a szabályzatait megszegő dolgozók esetében a munkaszerződésben, munkaköri leírásban, valamint a magatartási kódexben meghatározott intézkedéseket hozza.

5.3.7 Szerződéses közreműködőkre vonatkozó követelmények

A Szolgáltató nem munkaviszonyban dolgozó szerződéses közreműködőire ugyanazok a biztonsági szabályok vonatkoznak, mint a munkaviszonyban dolgozókra.

5.3.8 A személyzet számára biztosított dokumentációk

A Szolgáltató folyamatosan biztosítja a szolgáltatásnyújtásban közreműködő személyek részére a szerepkörük ellátásához szükséges aktuális szabályzatokat és dokumentációkat.

5.4 Naplózási eljárások

Szolgáltató rendszere széleskörű naplózási tevékenységet folytat a Szolgáltatásra vonatkozó műveletek és az ezek során felhasznált adatok megőrzése érdekében. A naplózáshoz szükséges pontos időt a kiszolgáló szerverek központi időszinkronizációja garantálja, mely legfeljebb 1 másodperces eltérést engedélyez a valódi időhöz képest. A naplóesemények központi naplószerveren biztonságosan tárolásra – és rendszeresen mentésre – kerülnek, a beavatkozást igénylő eseményekről a naplóeseményeket automatikusan elemző logika értesítést küld az érintett üzemeltetőknek. E naplózások tulajdonságai az adott alkalmazások függvényei.

Minden naplóesemény tartalmazza a következőket, amennyiben releváns és értelmezhető:

- napló esemény dátuma és ideje
- esemény típusa
- a tevékenységért felelős entitás (pl. felhasználó, rendszergazda, processz) azonosítója (de hitelesítési információit nem tartalmazhatja!)
- naplózott esemény sikeres vagy sikertelen volt-e
- az eseménnyel kapcsolatos kulcsinformáció (pl. belépés vagy kilépés);
- eszköz azonosító (és helye amennyiben lehetséges) rendszer azonosító;
- használt jogosultsági információk;
- használt rendszer kiszolgáló alkalmazások és service-ek;
- file hozzáférések és a felhasznált jogosultság;
- hálózati címek és protokollok;
- figyelmeztetések - amennyiben a rendszer küldött;
- védelmi rendszerek aktivációja vagy kikapcsolása (antivírus, IPD, IDS)

5.4.1 A tárolt események típusai

A naplózás kiterjed kiemelten a következőkre:

- kulcs menedzsment események
- napló generáló funkcionalitás elindulása és leállása
- naplózási paraméterek megváltozása
- hozzáférési kísérletek (rendszer és adat- illetve más erőforrás hozzáférési kísérletek)
- kulcs irányítási tevékenységek
- rendszer konfigurációs változások
- bélyegző létrehozási események
- rendszeradminisztrátori és rendszeroperátori tevékenységek.

5.4.2 A napló állomány feldolgozásának gyakorisága

A Szolgáltató központi naplógyűjtő és elemző rendszert alkalmaz, melyben az események feldolgozása és átvizsgálása valós időben megtörténi. A rendszerben alkalmazott szabályok által generált riasztások késedelem nélkül besorolásra kerülnek, és kivizsgálásuk a besorolás függvényében a belső szabályzatok szerint megtörténik a megfelelő szaktudással rendelkező munkatárs által. A kivizsgálások dokumentálása a Szolgáltató jegykezelő rendszerében történik.

5.4.3 A napló-állomány megőrzési időtartama

Az üzemeltetési napló-állományokat a Szolgáltató 10,5 évig tárolja a központi naplógyűjtő szerveren, illetve archiválva. A Szolgáltató a naplókat és archivált naplóállományokat a Független rendszervizsgáló számára igény esetén hozzáférhetővé teszi.

5.4.4 A napló állomány védelme

Szolgáltató rendszerének naplóbejegyzései a törlések és beszúrások észrevétlen végrehajtását kizáró módon kerülnek tárolásra, integritásukat időbélyegzés védi, mely esetében biztosított az ellenőrzés lehetősége is. A napló állományt a véletlen és szándékos rongálások ellen biztonsági mentések védik. Az esetlegesen személyes adatokat tartalmazó naplóbejegyzések esetében Szolgáltató gondoskodik az adatok bizalmas tárolásáról. A napló állományokhoz való hozzáférésre csak azok jogosultak, akiknek erre munkakörük folytán szükségük van. Szolgáltató a hozzáféréseket biztonságos módon ellenőrzi.

5.4.5 A napló állomány mentési folyamatai

A rendszer naplóállományai a központi naplózó szerveren redundánsan kerülnek tárolásra. A naplókról rendszeres offsite mentés is készül. A részletes folyamatot a Szolgáltató Mentési Eljárásrendje tartalmazza.

5.4.6 A napló gyűjtési rendszere

Minden szerver függetlenül a funkcionalitásától napló állományt készít, amelyek a naplóvizsgáló alrendszerbe és a központi napló szerverre érkeznek meg. A naplók ez utóbbiról kerülnek mentésre és archiválásra.

5.4.7 Az eseményeket kiváltó alanyok értesítése

A riasztást kiváltó személyeket, szervezeteket és alkalmazásokat a Szolgáltató nem feltétlenül értesíti, ugyanakkor szükség esetén bevonhatja őket az esemény kivizsgálásába. Az esemény kiváltásában érintett feleknek ilyen esetben kötelességük a Szolgáltatóval való együttműködés a riasztást kiváltó események feltárása érdekében.

5.4.8 Sebezhetőség felmérése

A Szolgáltató évente, vagy amennyiben a kontroll környezet, illetve egyéb változások indokolják, sebezhetőség felmérést és kockázatértékelést végez, amely segítségével azonosítja, értékeli és kockázati osztályba sorolja az olyan előrelátható külső és belső fenyegetettségeket, amelyek lehetővé tehetik a Szolgáltatás működésének, vagy annak bizalmasságának sérülését. A kockázatelemzés a fentiek mellett tartalmazza a fenyegetettségek elhárítására a Szolgáltató által alkalmazott folyamatok, védelmi intézkedések leírását is.

5.5 Adatok megőrzése

5.5.1 Az archivált adatok típusai

A Szolgáltatás keretében létrejövő, elektronikus bélyegzővel ellátott dokumentumok fizikai tárolása a Szerződött Partnerek feladata.

A Szolgáltató megőrzi minden Szolgáltatási Rend, Szolgáltatási Szabályzat, Általános Szerződési Feltételek és Szolgáltatási Szerződés korábbi verzióját, melyek a Szolgáltatás nyújtásának és igénybevételének adott időpontbeli feltételeinek visszakövethetőségét biztosítják.

A Szolgáltatás során létrejött és begyűjtött minden naplóbejegyzés archiválásra kerül.

5.5.2 Az archivált adatok megőrzési ideje

A Szolgáltatónak biztosítja a Szolgáltatás működési naplóinak megőrzését 10,5 évig, a Szolgáltatás biztosításának és igénybevételének feltételeit rögzítő szabályzatok megőrzését pedig hatályon kívül helyezésüktől számított 10 évig.

5.5.3 Archív adatok védelme

Az archívumokra a Szolgáltató az 5.4.4 pontban leírt védelmet biztosítja.

5.5.4 Az archívum mentési folyamatai

A Szolgáltató az archívum mentésére az 5.4.5 pont megfelelő intézkedései alkalmazza.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi elektronikus naplóbejegyzés tartalmaz idő adatot, amelyen legalább másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont. A Szolgáltató biztosítja, hogy a szolgáltatást nyújtó rendszerein a gépidő maximum 1 másodpercre tér el a referenciaidőtől. Az időjel előállításához használt gépidőt naponta legalább négy alkalommal szinkronizálja az UTC időhöz.

5.5.6 Az archívum gyűjtési rendszere

A Szolgáltató a naplóinformációk gyűjtésére rendszeresen mentett, védett központi naplógyűjtő rendszert tart fenn.

5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások

A Szolgáltatónak az archivált dokumentumokat és adatokat védett környezetben tárolja, melyhez való hozzáférés csak jogosultság ellenőrzés után lehetséges. A hozzáférések naplózásra kerülnek.

5.6 Szolgáltatói kulcscsere

A Szerződött Partner –a Szolgáltatásban alkalmazott– bélyegző tanúsítványa érvényességének lejárta előtt 3 hónappal a Szolgáltató kezdeményezi a Szerződött Partner felé új bélyegző tanúsítvány kiállításának folyamatát, mely során az új kulcs generálása után átadja az új bélyegző tanúsítvány kiállításához szükséges tanúsítvány kérést és kulcsgenerálási jegyzőkönyvet. A Szolgáltató csak úgy tudja vállalni az elektronikus bélyegzési szolgáltatás folyamatosságát, ha a Szerződött Partner az elkészült új bélyegző tanúsítványt legkésőbb a lejáró tanúsítvány érvényességének vége előtt legalább két héttel eljuttatja a Szolgáltató részére.

Amennyiben a Szolgáltatás által az elektronikus bélyegző létrehozásához használt algoritmusok tekintetében olyan hirtelen elavulás következik be, mely nem teszi lehetővé a Szerződött Partner bélyegző tanúsítványának normál életciklus szerinti cseréjének bevárását, a Szolgáltató szintén a

Szerződött Partner felé új bélyegző tanúsítvány kiállításának folyamatát, új biztonságosnak számító algoritmusok használatával. A Szolgáltató ebben az esetben is csak úgy tudja vállalni az elektronikus bélyegzési szolgáltatás folyamatosságát, ha a Szerződött Partner az elkészült új bélyegző tanúsítványt legkésőbb a lejáró tanúsítvány érvényességének vége előtt legalább két héttel eljuttatja a Szolgáltató részére.

Az egyéb, a Szolgáltatás működéséhez használt kriptográfiai kulcsok cseréjére vonatkozó eljárásokat nem nyilvános belső szabályzatok tartalmazzák.

5.7 Kompromittálódást és katasztrófát követő helyreállítás

A Szolgáltató a rendkívüli helyzetek kezelésére Katasztrófa Elhárítási tervvel rendelkezik. Az észlelt incidens fajtásától és kiterjedtségétől függően ezen terv szerinti lépéseket kell végrehajtani a bekövetkezett esemény hatásainak csökkentése érdekében.

A Szolgáltató Katasztrófa Elhárítási Terve a következő jelentősebb eseményekre terjed ki:

- Informatikai erőforrás meghibásodása
- Belső szabotázs, szándékos károkozás
- Külső IT biztonsági támadás
- Hálózati hiba
- Üzemeltetési hiba

A Szolgáltató indokolatlan késedelem nélkül, de minden esetben az esetről való értesüléstől számított 24 órán belül értesítik a felügyeleti szervet a biztonság megsértéséről vagy az adatok sértetlenségének megszűnéséről, amennyiben az jelentős hatást gyakorol a bizalmi szolgáltatásra vagy az annak keretében tárolt személyes adatokra.

5.7.1 Rendkívüli események és kompromittálódás kezelésének eljárásai

A Szolgáltató rendelkezik –nem nyilvános– Katasztrófa Elhárítási tervvel. A kialakított eljárások biztosítják a bekövetkezett esemény hatásának korlátozását és a Szolgáltatás esetleges megszakadásának mielőbbi elhárítását. A Szolgáltató a rendszer mentései az elsődlegestől elkülönült– de azzal azonos biztonságú – helyszínen is tárolja, ezzel is biztosítva, hogy a bekövetkezett esemény utáni helyreállás biztosítható legyen.

A Szolgáltató belső szabályzataiban rendelkezik kidolgozott, dokumentált incidenskezelési eljárásokkal.

5.7.2 Informatikai erőforrások, szoftverek és adatok meghibásodása

A Szolgáltató informatikai rendszereit megbízható hardver és szoftver komponensekből építette fel. A Szolgáltató a rendszereiről a belső mentési szabályzatnak megfelelően rendszeres, a rendszer helyreállíthatóságát biztosító mentést készít. E mellett a hivatkozott Katasztrófa Elhárítási terv rendelkezik a meghibásodások esetén követendő eljárásokról.

5.7.3 Magánkulcs kompromittálódása

Szerződött Partner bélyegző magánkulcsának kompromittálódása esetén a Szolgáltató következő lépéseket teszi meg:

- az érintett bélyegző magánkulcs használatát haladéktalanul megszünteti, és erről értesíti a Szerződött Partnert
- amennyiben a bélyegző magánkulcs kompromittálódása jelentős hatással van a bizalmi szolgáltatás nyújtására is, a Szolgáltató értesíti a Bizalmi Felügyeletet
- a Szerződött Partner értesítése a kompromittálódásáról és a tanúsítvány visszavonatásának kezdeményezése
- Közzétenni a kompromittálódás által esetlegesen érintett elektronikus bélyegzők körét, vagy olyan információkat, melyek alapján az érintett elektronikus bélyegzők köre beazonosítható

A Szolgáltató belső szabályzataiban a Szolgáltatás keretében használt egyéb magánkulcsok kompromittálódásának esetére kidolgozott eljárásokkal rendelkezik.

5.7.4 Működés helyreállítása katasztrófa esemény után

A Szolgálató Katasztrófa Elhárítási terve részletezi a bekövetkezett esemény után követelendő lepéseket a Szolgáltatás mielőbbi helyreállításához.

5.8 A szolgáltatási tevékenység megszüntetése

A Szolgáltatónak a szolgáltatási tevékenység megszűntetése esetén követni a jogszabályokban ez esetre meghatározott eljárást:

- Legkésőbb a tevékenység megszüntetésekor értesíti a bizalmi felügyeletet, valamint a bizalmi szolgáltatási ügyfeleket. Az értesítés időpontjától kezdve a Szolgáltató nem hozhat létre az adott bizalmi szolgáltatás kapcsán új elektronikus bélyegzőt.
- Ha a bizalmi szolgáltató más bizalmi szolgáltatás nyújtását továbbra is folytatja, akkor köteles gondoskodni a megszüntetni kívánt bizalmi szolgáltatással összefüggő, a nyilvánosság számára elérhető nyilvántartásainak folyamatos elérhetőségéről.
- Ha a bizalmi szolgáltató a továbbiakban nem nyújt bizalmi szolgáltatást, a bizalmi felügyeletnek, valamint a bizalmi szolgáltatási ügyfeleknek küldöttértesítésben megjelöli azt a bizalmi szolgáltatót (a továbbiakban: átvevő bizalmi szolgáltató), aki a bizalmi szolgáltatási tevékenység megszűnését követően biztosítja a megszüntetett bizalmi szolgáltatással összefüggő, a nyilvánosság számára elérhető nyilvántartásokhoz való hozzáférést
- A Szolgáltató tevékenysége befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, időbélyegzővel ellátott mentést készít. A szolgáltató a mentett adatállományokat védi a jogosulatlan módosítástól, és biztosítja, hogy az adatállomány tartalmához jogosulatlan személy nem férhet hozzá. A szolgáltató biztosítja, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.
- A Szolgáltató köteles az átvevő bizalmi szolgáltatónak a hozzáférési kötelezettség alá eső nyilvántartási adatokat átadni

A Szolgáltató – annak érdekében, hogy adatait átadhassa egy másik szolgáltatónak – az adatokat az új szolgáltató által fogadóképes médián és formátumban helyezi el vagy biztosítja az új szolgáltató számára az adatok eredeti formátumban történő feldolgozásának lehetőségét, amelyekhez átadja a megfelelő eszközöket, dokumentációkat és ismereteket.

6 Műszaki, biztonsági óvintézkedések

A Szolgáltató megbízható, biztonságtechnikailag értékelt és ellenőrzött termékekből álló informatikai rendszert használ Szolgáltatásai nyújtásához.

6.1 Kulcspár generálás és telepítés

6.1.1 Kulcspár előállítása

A Szolgáltató gondoskodik valamennyi általa (saját maga-, illetve Szerződött Partnerei számára) generált magánkulcs biztonságos és az ipari szabványoknak megfelelő generálásáról kidolgozott, dokumentált -nem nyilvános- eljárásrenddel rendelkezik. A kulcsgenerálás során alkalmazott kriptográfiai algoritmusok és algoritmus paraméterek megfelelnek a Nemzeti Média- és Hírközlési Hatóság biztonságos kriptográfiai algoritmusok használatára vonatkozó határozatában foglaltaknak.

Egy Szerződött Partner szerződésenként (rendszerpéldányonként) egy-, vagy több aktív bélyegző kulcspárral rendelkezhet.

A Szerződött Partnerek bélyegző kulcspárjai semmilyen körülmények között nem kerülhetnek ki a Kriptográfiai hardver modul védelme alól.

6.1.2 Magánkulcs eljuttatása a Szerződött Partnerhez

A Szerződött Partnerek bélyegző magánkulcsai a Szolgáltatónál üzemelő Kriptográfiai hardver modulban generálódnak, tárolódnak és aktiválódnak a Szolgáltatás részeként, azok továbbítása nem szükséges és nem is megengedett.

6.1.3 Nyilvános kulcs eljuttatása tanúsítvány kibocsátóhoz

A Szerződött Partner bélyegző kulcspárjához tanúsítvány kérés kerül kiállításra, mely személyesen a Szerződött Partner jogosult képviselője számára kerül átadásra, vagy elektronikus úton közösen elfogadott védett csatornán, vagy egyéb elektronikus úton a Szolgáltató elektronikus bélyegzőjével hitelesítve. Utóbbi esetben a Szerződött Partner felé elvárás az elektronikus bélyegző hitelességének ellenőrzése a tanúsítvány kérés felhasználása előtt.

A tanúsítvány kérés alapján a tanúsítvány igénylése és kiállíttatása a Szerződött Partner feladata. A tanúsítvány kérés alapján a tanúsítvány kiállítását bármely, EU bizalmi listában szereplő bizalmi-szolgáltatónál kérheti.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

A Szolgáltató a Szerződött Partnerek felé nyújtott Szolgáltatás keretében a Szerződött Partner saját bélyegző kulcspárjának (és bélyegző tanúsítványának) segítségével hoz létre elektronikus bélyegzőket, nem pedig szolgáltatói kulcspár használatával. A Szerződött Partnerek bélyegző kulcspárjainak nyilvános kulcsait (tanúsítványait) a Szolgáltató saját nyilvános felületein (weboldal stb.) nem teszi közzé, de a Szerződött Partner a bélyegző tanúsítványának közzétételét korlátozás nélkül megteheti.

6.1.5 Használt kriptográfiai algoritmusok

A Szolgáltató elektronikus bélyegző létrehozásakor minden esetben a Nemzeti Média- és Hírközlési Hatóság biztonságos kriptográfiai algoritmusok használatára vonatkozó határozata alapján

megfelelőnek tekinthető algoritmust alkalmaz, valamint a használt algoritmusok megfelelnek az ETSI TS 119 312 ajánlásnak.

6.1.6 A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

Nincs külön megkötés

6.1.7 A kulcshasználat célja

A Szerződött Partner bélyegző magánkulcsa kizárólag a Szerződött Partner által aktivált elektronikus bélyegző készítéshez kerül felhasználásra.

A Szolgáltató által a Szolgáltatásban használt egyéb kriptográfiai kulcsokról és azok használatának céljáról karbantartott dokumentációval rendelkezik.

6.2 A magánkulcsok védelme és kriptográfiai modulra vonatkozó szabályok

6.2.1 Kriptográfiai modulra vonatkozó szabványok

Szolgáltató Szerződött Partnerek bélyegző kulcsainak generálására, biztonságos tárolására, és használatára kizárólag olyan Kriptográfiai hardver modult alkalmazhat, mely megfelelő minősítésekkel rendelkezik a biztonságos kulcskezelés garantálására:

- megfelel a FIPS 140-2 követelményeknek 3-as vagy annál magasabb szinten, vagy
- megfelel az ISO/IEC 19790 követelményeinek

A Szerződött Partnerek bélyegző kulcsainak generálása, használata és tárolása Thales nC4433E-500 nShield F3 500+ hardver eszközzel történik, amely FIPS 140-2 szabvány szerint 3. szinten bevizsgált HSM.

A Szolgáltatás keretében alkalmazott egyéb kriptográfiai kulcsok védelmére és kezelésére vonatkozólag a Szolgáltató rendelkezik kidolgozott és dokumentált szabályzatokkal.

6.2.2 A több-szereplős (“n-ből m”) magánkulcs visszaállítás ellenőrzése

A Szolgáltató a Szerződött Partnerek bélyegző kulcsait tároló Kriptográfiai hardver modul adminisztrátori- és kulcskezelési funkcióiban is alkalmazza az n-ből m ellenőrzést.

6.2.3 Magánkulcs letét

A Szolgáltató nem nyújt magánkulcs letétbe helyezési szolgáltatást, és a Szolgáltatás működéséhez használt kulcsokat nem helyezi letétbe.

6.2.4 Magánkulcs mentése

A Szerződött Partnerek bélyegző magánkulcsait tartalmazó bélyegző HSM Security Worldről a Szolgáltató biztonsági mentést készít. A Security World biztonsági mentését és visszaállítási szükségességét eredményező rendkívüli üzemi helyzetek esetében a Security World mentésből való visszaállítását fizikailag védett környezetben, legalább kettő bizalmi munkakört betöltő személy együttes munkájával megvalósítja meg. A Security World biztonsági mentésére és visszaállítására a Szolgáltató rendelkezik kidolgozott, dokumentált szabályozással.

A Szerződött Partnerek bélyegző magánkulcsai soha nem hagyják el a generálásukra használt Kriptográfiai hardver modul védett környezetét (Security World).

Szerződött Partner bélyegző tanúsítványa érvényességének megszűnésekor (lejárat, visszavonás stb.) a Szolgáltató jegyzőkönyvezés mellett, visszaállíthatatlan módon törli a bélyegző HSM Security Worldjének minden biztonsági mentését, mely tartalmazza az érvényét vesztett tanúsítványhoz tartozó bélyegző kulcspárt.

6.2.5 Magánkulcs archiválása

A Szolgáltató nem archiválja a Szerződött Partnerek bélyegző magánkulcsait, sem az azokat tartalmazó bélyegző HSM Security Worldöt.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba, vagy onnan történő exportja

A Szerződött Partnerek bélyegző magánkulcsai nem hagyják el a generálásukra használt Kriptográfiai hardver modul védett környezetét.

A Szolgáltató a Szolgáltatással kapcsolatban alkalmazott egyéb kriptográfiai kulcsok magánkulcsainak kezelésére kidolgozott szabályozással rendelkezik.

6.2.7 Magánkulcs tárolása kriptográfiai modulban

A Szerződött Partnerek bélyegző magánkulcsai a bélyegző Kriptográfiai hardver modul védett Security Worldjében tárolódnak, a HSM által kezel erős titkosítással kódolva.

6.2.8 A magánkulcs aktivizálásának módja

A Szolgáltató a magánkulcs aktiválását a Kriptográfiai hardver modul gyártója által megadott biztonságos eljárások szerint végzi.

6.2.9 A magánkulcs deaktiválásának módja

A Thales nShield HSM kriptográfiai hardver modul magánkulcsa akkor deaktiválódik, ha a modul (szabályos vagy szabálytalan módon) kikerül az aktív állapotból. Ez az alábbi esetben következik be:

- a felhasználó deaktiválja a kulcsot,
- a modul áramellátása megszakad (kikapcsolás vagy tápellátási probléma),
- a modul hibaállapotba kerül.

Az így deaktivált magánkulcs mindaddig nem használható, amíg a modul ismét aktív állapotba nem kerül.

6.2.10 A magánkulcs megsemmisítésének módja

A Szolgáltató a Szerződött Partnerek bélyegző magánkulcsához tartozó tanúsítványának lejáratakor, visszavonásakor, vagy a bélyegző kulcs használatának egyéb befejeződésekor a kulcsot a Kriptográfiai hardver modulból törli, valamint visszaállíthatatlan módon törli az arról készült biztonsági mentéseket is.

6.2.11 Kritográfiai modulok értékelése

A Szolgáltató a 6.2.1 fejezetben meghatározott eszközöket használja.

6.3 A kulcspár kezelés egyéb szempontjai

A Szerződött partnerek bélyegző kulcspárja és a hozzá tartozó tanúsítvány érvényességi idejét a választott bizalmi szolgáltató határozza meg, azzal a megkötéssel, hogy a Szolgáltató nem támogatja a tanúsítvány megújítást, azaz a tanúsítvány lejáratakor új kulcspár és tanúsítvány előállítás szükséges.

6.4 Aktiváló adat

6.4.1 Aktivizáló adatok előállítása és telepítése

A Szolgáltató a felhasznált Hardver kriptográfiai eszközök felhasználói útmutatójában és az eszköz tanúsítványban megfogalmazott eljárásoknak, követelményeknek megfelelő aktiváló módszereket alkalmaz szolgáltatói és szerződött partneri magánkulcsainak védelmére.

6.4.2 Az aktivizáló adatok védelme

A Szolgáltató a Szerződött Partneri bélyegző magánkulcsok aktiváló adataihoz a Szerződött Partner írásos felhatalmazásával fér hozzá szabályozott, jegyzőkönyvezett módon. A magánkulcsot kizárólagosan használó elektronikus bélyegző elhelyezése szolgáltatást kizárólag a Szerződött Partner aktiválhatja.

6.4.3 Aktivizáló adatok egyéb szempontjai

Nincs kikötés.

6.5 Informatikai biztonsági előírások

6.5.1 Informatikai biztonsági műszaki követelmények meghatározása

A Szolgáltató a Szolgáltatás nyújtásához a következő szabványokat és előírásokat vette figyelembe:

- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről
- 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 119 312 v1.3.1 (2019-02) - „Electronic Signatures and Infrastructures (ESI); Cryptographic Suites
- ETSI EN 319 401 v2.2.1 (2018-02) - „Elektronikus aláírások és infrastruktúrák (ESI). A bizalmi szolgáltatókra vonatkozó általános politika-követelmények.” által meghatározott követelmények
- CEN/EN 419 241-1:2018 – „Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements”
- 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 TS 101 533-1 V1.3.1 (2012-04) Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management

- ETSI TS 119 101 V1.1.1 “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation” által meghatározott követelmények
- MSZ ISO/IEC 27001:2014 Informatika. Biztonságtechnika. Információbiztonság-irányítási rendszerek. Követelmények

6.5.2 Informatikai biztonság értékelése

Az ide vonatkozó rendelkezéseket a Szolgáltató belső használatú Kockázatkezelési Szabályzata tartalmazza.

6.6 Életciklusra vonatkozó biztonsági előírások

6.6.1 Rendszerfejlesztési előírások

Az ide vonatkozó szabályokat a Szolgáltató „A bizalmi szolgáltatást támogató alkalmazás fejlesztését biztosító IT környezetekre vonatkozó biztonsági intézkedéseket tartalmazó Információbiztonsági Szabályzata” tartalmazza.

A Szolgáltató a Szolgáltatás nyújtásához csak megbízható, tesztelt, követelményeknek megfelelő eszközöket és alkalmazásokat használ. Az egyedi fejlesztésű alkalmazások estében megköveteli, hogy a biztonsági követelmények már a fejlesztés korai fázisában megfogalmazásra kerüljenek, valamint a fejlesztés teljes életciklusa alatt érvényre jussanak.

6.6.2 Biztonságkezelési előírások

A Szolgáltató olyan eszközöket, alkalmazásokat és eljárásokat alkalmaz, melyek biztosítják a rendszerek megfelelő biztonsági konfigurációs beállításait. Ezeket a Szolgáltató Információbiztonsági szabályzatai és egyéb belső biztonsági szabályzatai tartalmazzák.

6.6.3 Életciklusra vonatkozó biztonsági előírások

A Szolgáltató a Szolgáltatás nyújtásához eszközök és alkalmazások teljes életciklusa alatt figyelembe veszi és biztosítja a megfelelő kontrollok működését.

6.7 Hálózatbiztonsági előírások

A Szolgáltató a Szolgáltatáshoz nyújtott eszközöket azok funkcionalitása és rendeltetése szerint külön biztonsági zónákba sorolja. A zónák közötti kommunikáció csak biztonságos, felügyelt csatornákon keresztül történhet. A zónák közötti kommunikációs beállítások módosítása engedélyezéshez kötött, végrehajtásuk dokumentált.

A Szolgáltató a saját rendszereit, valamint a Szerződött Partnerek rendszereit logikailag szétválasztja, azok között csak az engedélyezett, felügyelt csatornákon történhet kommunikáció.

6.8 Időbélyegzés

A Szolgáltatás során használt időbélyegek külső bizalmi szolgáltatótól kerülnek beszerzésre (Microsec és Netlock időbélyegzők).

A Szolgáltató a rendszereinek óráit egymással és külső UTC időforráshoz (idő szerver) szinkronizálja.

7 Tanúsítvány és CRL profilok

7.1 Tanúsítvány profil

A Szolgáltató által a Szerződött Partnerek bélyegző tanúsítványaival szemben elvárt megkötések a következők:

- minősített tanúsítvány
- nonRepudiation és/vagy digitalSignature kulcshasználati (key usage) beállítás
- tartalmaznia kell OCSP elérési információkat
- tanúsítvány lánca EU bizalmi listára (TL) visszavezethető legyen

7.2 CRL profil

Nincs megkötés

7.3 OCSP profil

A tanúsítványnak tartalmaznia kell OCSP elérési információkat.

8 A megfelelőség vizsgálata

A Szolgáltató a rendszerét rendszeres időközönként külső független auditorral felülvizsgáltatja, hogy megfelel-e a Szolgáltatás nyújtásához szükséges követelményeknek, de különösen az:

- ISO/IEC 27001:2013 "A" mellékete által meghatározott követelmények
- CEN/EN 419241-1:2018 „Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements” által meghatározott első szintű (Level 1) követelmények
- ETSI EN 319 401 v2.2.1 „Elektronikus aláírások és infrastruktúrák (ESI).A bizalmi szolgáltatókra vonatkozó általános politika-követelmények.” által meghatározott követelmények
- ETSI TS 101 533 v1.3.1 “Electronic Signatures and Infrastructures (ESI); Data Preservation Systems Security; Part 1: Requirements for Implementation and Management” 6. fejezete által meghatározott követelmények
- ETSI TS 119 101 v1.1.1 “Electronic Signatures and Infrastructures (ESI); Policy and security requirements for applications for signature creation and signature validation” által meghatározott követelmények

elvárásainak.

8.1 Az ellenőrzések körülményei és gyakorisága

A Szolgáltató a Szolgáltatás indulásakor elvégeztette a szükséges külső független auditokat, és az ezek által biztosított minősítéseket felülvizsgálati- és megújító auditok segítségével fenntartja.

8.2 A külső auditor képesítése

A külső auditokat Szolgáltató olyan szakértővel vagy szervezettel végezteti el, aki rendelkezik egy EU tagállam nemzeti akkreditációs szervezetétől megfelelő felhatalmazással.

8.3 Auditor függetlensége

A külső vizsgálatokat végző szervezet, annak munkatársai, valamint a külső rendszervizsgáló teljes mértékben függetlenek Szolgáltatótól.

8.4 A hiányosságok kezelése

A feltárt hiányosságok kezelésére a Szolgáltató intézkedési tervet készít, mely tartalmazza az elvégzendő intézkedéseket, azok felelőseit és határidejét, valamint gondoskodik az intézkedések megfelelő végrehajtásának ellenőrzéséről.

8.5 Az eredmények kommunikálása

A független auditori jelentés a Szolgáltató üzleti titka, azt csak az arra feljogosítottak ismerhetik meg.

9 Egyéb üzleti és jogi kérdések

9.1 Díjak

A Szolgáltató a Szolgáltatás nyújtásán belül a Szolgáltatási Szerződésben meghatározott díjakat használja. A Szolgáltató fenntartja magának a jogot, hogy egyedi megállapodás keretében különböző Szerződött Partnerek esetén eltérő díjazást használjon.

9.2 Anyagi felelősségvállalás

A Szolgáltató a megbízhatóság biztosítása érdekében a jogszabályi előírásoknak megfelelő felelősségbiztosítással is rendelkezik.

9.3 Üzleti információk bizalmassága

9.3.1 Bizalmasan kezelendő információk köre

Szolgáltató minden, a rendszer által kezelt adatot és információt bizalmasnak tekint, kivéve a 9.3.2 fejezetben megadott adatokat és információkat.

9.3.2 Nem bizalmasnak tekintett információk köre

A Szolgáltató a következő információkat nem tekinti bizalmasnak:

- Szolgáltatói tanúsítványok
- A Szolgáltató honlapján közzétett szabályzatok és dokumentumok
- Olyan adatok és információk, melyek más forrásból jogszerűen, nyilvánosan elérhetők

9.3.3 Bizalmas információ védelme

A Szolgáltató adatvédelmi szabályzata részletezi a védelem érdekében hozott intézkedéseket.

A Szolgáltató és a Szolgáltatás nyújtásában közreműködő felek minden esetben titoktartási nyilatkozatot tettek a megismert adatok vonatkozásában.

9.4 Személyes adatok védelme

9.4.1 Adatkezelési szabályzat

A Szolgáltató belső adatvédelmi és adatbiztonsági szabályzata rögzíti a személyes adatkezelés szabályait. A személyes adatok védelme érdekében hozott intézkedéseket a releváns rendszerleírások és szabályzatok tartalmazzák, melyek megfelelnek a 2011. évi CXII törvénynek.

A Szolgáltató adatvédelmi elveinek nyilvános kivonatát tartalmazó Adatbiztonsági tájékoztató című dokumentum a Szolgáltató weboldalán elérhető a letölthető dokumentumok között.

9.4.2 Bizalmasként kezelendő személyes adatok

Szolgáltató csak a Szerződött Partnerrel való szerződéskötéshez, kapcsolattartáshoz, és jogosult képviselők rögzítéséhez szükséges adatokat gyűjti és a Szerződött Partner által a Szolgáltatás igénybevétele során a Szolgáltatóhoz esetlegesen továbbított személyes adatokat kezel olyan mértékben, ami szolgáltatás nyújtásához feltétlenül szükséges.

A Szolgáltató minden tudomására jutott személyes adatot véd.

9.4.3 Személyes adatnak nem minősülő adatok

A Szolgáltató nem kezel személyes adatként olyan adatot, mely nyilvános adatforrásból jogszerűen elérhető.

9.4.4 Személyes adatok védelme

A személyes adatok védelmére az Adatvédelmi és adatbiztonsági szabályzat rendelkezési az irányadóak.

9.4.5 Személyes adatok felhasználása

A Szolgáltató az általa kezelt személyes adatokat csak a 2011. évi CXII törvénynek megfelelően használja fel.

9.4.6 Felfedés bírósági vagy polgári peres eljárás keretében

A Szolgáltató bűncselekmények felderítése vagy megelőzése céljából, illetve nemzetbiztonsági érdekből - az adatigénylésre meghatározott jogszabályi feltételek teljesülése esetén - a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak haladéktalanul és egyéb feltételek nélkül feltárja a jogszabályban meghatározott bizalmas információkat. Szolgáltató rögzíti az adatátadás tényét, de arról nem tájékoztatja az érintett Szerződött Partnert és/vagy Dokumentum közreműködőt.

Szolgáltató az elektronikus bélyegző érvényességét érintő polgári peres, illetve nem peres eljárás során - az érintettség igazolása esetén - az ellenérdekű peres félnek vagy képviselőjének, valamint a megkereső bíróságnak feltárhatja a jogszabályban meghatározott bizalmas információkat. Szolgáltató rögzíti az adatátadás tényét, és arról tájékoztatja érintett Szerződött Partnert. A Szerződött Partner feladata a Dokumentum közreműködő értesítése.

9.5 Szellemi tulajdonjogok

A Szolgáltató a Szolgáltatás nyújtásához csak olyan eszközöket alkalmaz, melyek nem sértik harmadik fél szellemi tulajdonjogait.

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 A Szolgáltató felelőssége és helytállása

A Szolgáltató felelőssége

A Szolgáltató a Szolgáltatások nyújtásával összefüggésben okozott károkért legfeljebb a szolgáltatás havidíjának értékhatárig felel. A Szolgáltató kárfelelőssége nem terjed ki azokra a károkra, amelyek bekövetkezéséért más felelős, amelyek közvetlen ok-okozati viszonyban nem állnak a szolgáltatói tevékenységgel. A Szolgáltató csak a ténylegesen bekövetkezett károkért tehető felelőssé, így nem felel az elmaradt haszonért, üzletvesztésért, várt megtakarításért vagy egyéb közvetett, különleges, vagy következményes károkért, illetve sérelemdíjért. A Szolgáltató felelőssége nem terjed ki az esetleges kártérítési igények kielégítésére, ha a szolgáltatás elérése vagy használata jogszabály – a technológiát érintő - rendelkezése okán nem lehetséges vagy jogszabály alapján a szolgáltatás nyújtása megszüntetésre kerül.

A Szolgáltató a közvetlenül az Szerződött Partnernél kimutatott, az általa szándékosan vagy gondatlanul a Szerződött Partnernek okozott kárért felelős. A Szolgáltató nem tartozik felelősséggel azokért a károkért, amelyek abból erednek, hogy az Szerződött Partner veszélyezteti a Szolgáltatás biztonságát vagy a Műszaki Dokumentációban előírt műszaki követelményeknek nem tesz eleget.

A Szolgáltató a szolgáltatásaira – így mindenekelőtt az általa képzett elektronikus bélyegzők megfelelősségére, hitelességére– felelősségbiztosítással rendelkezik. Amennyiben a Szolgáltató által szolgáltatott elektronikus bélyegző hitelessége esetlegesen valamely bíróság vagy hatóság előtt nem minősül megfelelőnek, és ebből eredően a Szerződött Partnert kár éri, a Szolgáltató felelőssége kizárólag a felelősségbiztosítással maximum összeg erejéig terjedhet.

A Szolgáltató érzékeny adatokat tartalmazó információk (rendszernaplók, ügyfél adatokat tartalmazó dokumentumok, a Szolgáltatással kapcsolatos biztonsági vagy egyéb bizalmas adatok stb.) Szerződött Partnernek elektronikus formában (email stb.) való küldésekor köteles azt titkosítással védett módon tennie, hogy azok bizalmassága ne sérüljön. Az alkalmazható technológiákkal és megoldásokkal kapcsolatos információkat a Műszaki dokumentáció tartalmazza.

A Szolgáltató 24 órán belül értesíti a Szerződött Partnert minden olyan eseményről, mely biztonsági szabályszegéssel vagy az adatok sértetlenségének kompromittálódásával jár, és jelentős hatása lehet a Szolgáltató által nyújtott szolgáltatásokra, és a tárolt személyes adatokra.

A Szolgáltató kötelezettsége

A Szolgáltató köteles a Szolgáltatásokat a mindenkori Szolgáltatási Szabályzat, a Szolgáltatási Szerződés, az ÁSZF, és a vonatkozó jogszabályok szerint nyújtani. A Szolgáltató a hatályos jogszabályoknak való megfelelés miatt indokolt változásokat köteles bevezetni.

Bizalmi szolgáltatói státuszát köteles fenntartani, a jogszabályok által előírt feltételek teljesülését biztosítani, határidőben gondoskodni a tanúsítványainak a meghosszabbításáról.

A Szolgáltató köteles a Rendszer használatát, rendelkezésre állását (üzemképességét) a Szolgáltatási Szerződésben szavatolt időtartamban biztosítani.

A Szolgáltató a tanúsított rendszeren belül elektronikusan bélyegzett dokumentumot, időbélyegzővel ellátott PDF formájában köteles a Szerződött Partner rendelkezésére bocsátani.

A Szolgáltató szavatolja a nyers dokumentumok a Rendszer általi végleges törlését.

A Szolgáltató köteles a PDF formátumú dokumentumra —az azt a Rendszerbe továbbító, Szerződött Partner társrendszer kérése esetén– fokozott biztonságú elektronikus bélyegzőt elhelyezni, amely védi a dokumentum integritását.

A Szolgáltató a szolgáltatás nyújtásának – a Szolgáltató érdekkörében felmerült ok vagy jogszabály általi - megszüntetése előtt a szolgáltatás befejezését a Szerződött Partner részére bejelenti és azt az internetes honlapján keresztül közzéteszi.

A Szolgáltató a vele szerződéses jogviszonyban álló felekkel szemben az eIDAS 13. cikke szerint felelős minden olyan kárért, amelyet szándékosan vagy gondatlanul bármely természetes vagy jogi személynek okoz az eIDAS rendelet szerinti kötelezettségei megszegéséből eredően. Ennek biztosítása érdekében Szolgáltató felelősségbiztosítással rendelkezik. Amennyiben a Szolgáltató előzetesen megfelelően tájékoztatja az ügyfeleit az általa nyújtott szolgáltatások igénybevételére vonatkozó korlátozásokról, és amennyiben ezek a korlátozások harmadik felek számára felismerhetők, a Szolgáltató nem felelős a szolgáltatások igénybevételéből eredő, a jelzett korlátozásokat meghaladó károkért.

A Szolgáltató a kárt azt követően téríti meg, miután a kártérítési igény elbírálásához szükséges, valamint a Szolgáltató felelősségét, a kár időpontját és összegét bizonyító valamennyi dokumentum a rendelkezésre áll.

9.6.2 A Szerződött Partner felelőssége és helytállása

A Szerződött Partner köteles a szolgáltatási díjakat a Szolgáltatási Szerződésnek és az ÁSZF rendelkezéseinek megfelelően, határidőben megfizetni.

A Szerződött Partner köteles a Szolgáltató által kért, a Szolgáltatások igénybevételéhez szükséges adatokat hiánytalanul megadni, valamint köteles a valóságnak megfelelő adatokat szolgáltatni. A Szerződött Partner köteles minden olyan változást bejelenteni, mely érinti a Szerződést, vagy bármely a Szolgáltatással kapcsolatos információt. Amennyiben kiderül, hogy a benyújtott adatok nem felelnek meg a valóságnak, a Szolgáltatónak joga van felülbírálni a Szerződött Partner Szerződését, felszólíthat javításra, illetve azonnali hatállyal felbonthatja a Szerződést.

A Szerződött Partner köteles biztosítani, hogy a Szolgáltatások igénybevételéhez szükséges adatokhoz és eszközökhöz (jelszavakhoz) kizárólag az arra jogosult személyek férhessenek hozzá.

A Szerződött Partner köteles értesíteni a Szolgáltatót, amennyiben státuszában változás áll be, így különösen, ha jogutódlás mellett, vagy jogutód nélkül megszűnik, valamint ha átalakulás folytán a

Szerződésből eredő jogok és kötelezettségek valamely jogutódra szállnak át, továbbá ha vele szemben jogerős határozattal elrendelt csődeljárás, felszámolás vagy végelszámolási eljárás indult.

A Szerződött Partner a Műszaki Dokumentációban meghatározott módon köteles a műszaki követelményeknek eleget tenni, gondoskodni az előírt biztonsági intézkedések szigorú betartásáról. A Szerződés feltételeitől eltérő megoldást eredményezhet bármely műszaki előírás hiányos alkalmazása.

A Szerződött Partner köteles a Szolgáltatásokat kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a Szolgáltató szabályzataiban (Szolgáltatási Szabályzat, Bizalmi Szolgáltatási Rend), a Szolgáltatási Szerződésben és a vonatkozó magyar és Uniós jogszabályokban foglaltaknak megfelelően használni.

A Szerződött Partner kötelessége a Szolgáltató által megfogalmazott követelmények betartása és betartatása a Szolgáltatás igénybevétel során a Bélyegző elhelyezését kezdeményező féllel.

A Szerződött Partner érzékeny adatokat tartalmazó információk (rendszernaplók, ügyfél adatokat tartalmazó dokumentumok, a Szolgáltatással kapcsolatos biztonsági vagy egyéb bizalmas adatok stb.) Szolgáltatónak elektronikus formában (email stb.) való küldésekor köteles azt titkosítással védett módon tennie, hogy azok bizalmassága ne sérüljön. Az illetéktelen hozzáférés ellen nem védett módon küldött információk befogadását a Szolgáltató jogosult megtagadni. Az alkalmazható technológiákkal és megoldásokkal kapcsolatos információkat a Műszaki dokumentáció tartalmazza.

9.6.3 A Bélyegző elhelyezését kezdeményező felelőssége és helytállása

A Bélyegző elhelyezését kezdeményező köteles a tevékenysége során a Szerződött Partner szabályzatainak betartására, a technológiai utasítások követésére. Ennek keretében figyelembe kell vennie a Szolgáltató kliens eszköz és szoftver használatára vonatkozó ajánlásainak releváns részeit.

A Bélyegző elhelyezését kezdeményező kötelessége az elektronikus bélyegző elhelyezésének kezdeményezésekor ellenőrizni, hogy az aktivált szolgáltatás keretében a megfelelő bélyegző kulcs aktiválódott-e.

9.6.4 Az Érintett felek kezdeményező felelőssége és helytállása

Az érintett felek az elektronikus bélyegzővel ellátott PDF-ek ellenőrzésekor kötelesek a Szerződött Partner által választott bizalmi szolgáltató szolgáltatási szabályzatának releváns részei szerint eljárni. E mellett kötelesek betartani a Szolgáltató Bélyegzési szabályzatának vonatkozó részeit is.

A Szolgáltató szolgáltatási beszállítóinak a Szolgáltató felé a következő tájékoztatási időtartamot szükséges betartaniuk: szervezeti változásról 15 nappal előtte, tervezett szolgáltatás kiesés esetén legalább 3 nappal előtte, változás szükségessége esetén legalább 30 nappal előtte.

9.7 Helytállás érvénytelenségi köre

Szolgáltató nem felelős az olyan károkért, amelyek abból adódtak, hogy a Szerződött Partner vagy harmadik fél a szolgáltatás igénybevétele, illetve annak felhasználása során nem a hatályos jogszabályoknak, illetve szolgáltatói szabályzatoknak megfelelően járt el, illetve nem tanúsította a tőle elvárható gondosságot.

Szolgáltató a szolgáltatásaival kapcsolatos szerződéses és szerződésen kívüli károkért harmadik személlyel szemben kizárólag a saját hibájából, kötelezettségeinek megszegéséből, valamint a neki felróható okokból bekövetkező, bizonyítható károkért tartozik helyt állni.

9.8 Felelősség korlátozása

A Szolgáltató felelősségének korlátozása a 9.6.1 fejezetben található. Ezek mellett a Szolgáltatási Szerződés és az Általános Szerződési Feltételek által meghatározott feltételek érvényesek.

9.9 Kártérítési kötelezettség

A Szolgáltató kártérítési kötelezettségének korlátozása a 9.6.1 fejezetben található. Ezek mellett a Szolgáltatási Szerződés és az Általános Szerződési Feltételek által meghatározott feltételek érvényesek.

9.10 Hatályosság és megszűnés

9.10.1 Érvényesség

Tárgyi hatálya

A Szabályzat az 1.1.4 pontban ismertetett szolgáltatások nyújtását és igénybevételét foglalja magában.

Időbeli hatálya

A Szabályzat jelen verziója a dokumentum címlapján feltüntetett hatálybalépési dátumtól határozatlan ideig hatályos. A hatályosság megszűnik a Szabályzat újabb verziójának hatályba lépésekor vagy a szolgáltatások beszüntetésekor.

Személyi hatálya

A szabályzat hatálya kiterjed a:

- 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 szolgáltatást igénybevevő ügyfelekre
- a szolgáltatásban érintett harmadik felekre

9.10.2 Megszűnés

A bizalmi szolgáltatási szabályzat a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

9.10.3 A megszűnés következményei

A Szolgáltató vállalja, hogy a Szolgáltatási Szabályzat visszavonása esetén is érvényben maradnak a mindenkor hatályos vonatkozó jogszabályokban meghatározott bizalmas adatok védelmére vonatkozó előírások.

9.11 A részvevők közöttikommunikáció

A Szerződött Partnerekkel való kommunikációs módokat a Szolgáltató és a Szerződött Partner közötti Szolgáltatási szerződés rendezi.

Ezen kívül a Szolgáltató érzékeny adatokat tartalmazó információk (rendszernaplók, ügyfél adatokat tartalmazó dokumentumok, a Szolgáltatással kapcsolatos biztonsági vagy egyéb bizalmas adatok stb.) Szerződött Partnernek elektronikus formában (email stb.) való küldésekor köteles azt titkosítással védett módon tennie, hogy azok bizalmassága ne sérüljön. Az alkalmazható technológiákkal és megoldásokkal kapcsolatos információkat a Műszaki dokumentáció tartalmazza.

Egyéb felekkel a Szolgáltató a 1.3.1 pontban megadott elérhetőségein keresztültart kapcsolatot.

9.12 Módosítások

9.12.1 Módosítási eljárás

A Szolgáltató szabályzatokért felelős munkatársai a szabályzatokat amennyiben új igény jelentkezik, de legalább évente felülvizsgálják. Az előkészített verziót a Szolgáltatásért felelős vezető helyezi hatályba. A jóváhagyott dokumentumokat a Szolgáltató internetes honlapján teszi közzé. A módosított Szabályzatot a Szolgáltató megküldi a Bizalmi Felügyelet részére is.

9.12.2 Az értesítések módja és határideje

Amennyiben a változás hordereje ezt megköveteli, a változás előtt a Szolgáltató értesíti a Szerződött Partnereket a szabályozások változásáról, elegendő időt hagyva nekik a változásra való felkészülésre.

9.12.3 A dokumentum azonosító (OID) változása

Jelen Szabályzat újabb verziói minden esetben új azonosítóval kerülnek kiadásra.

9.13 Vitás kérdések rendezése

A Szolgáltató törekszik a működése során felmerülő vitás kérdések békés, tárgyalásos rendezésére. A rendezés során a fokozatosság elvét követi.

A Szolgáltató tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat e-mailben, telefonon fogad. A Szolgáltató a telefonos csatornán fogadott panaszok esetében jegyzőkönyvet vesz fel a panasz fogadásáról.

Bármely vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra terelése előtt a Szerződött Partnereknek kötelessége, az Érintett Félnek vagy bármely harmadik félnek pedig ajánlott a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása az ügy minden vonatkozását érintően.

A benyújtott panaszokat a Szolgáltató 30 napon belül kivizsgálja. A Szolgáltató a vizsgálat eredményéről –felek eltérő megállapodását kivéve– emailben küldött, bélyegzővel ellátott pdf dokumentum útján tájékoztatja a panasz benyújtóját. Amennyiben a kivizsgálás 30 napon belül nem fejeződik be, a Szolgáltató ennek tényről – megjelölve az okot, és a várható kivizsgálási időt – tájékoztatja a panasz benyújtóját.

Amennyiben a választ a benyújtó nem fogadja el, egyeztetést kezdeményezhet a Szolgáltatóval. Amennyiben ez meghiúsul, vagy nem vezet eredményre 30 napon belül, a bejelentő jogosult a Budapesti Békéltető Testülethez fordulni egy esetleges bírósági eljárást megelőzően.

Jelen szabályzat hatálybalépésekor az illetékes szervezetek elérhetőségei a következők:

Budapesti Békéltető Testület:

Cím: 1016 Budapest, Krisztina krt. 99. I. em. 111.

Levelezési cím: 1253 Budapest, Pf.: 10.

Email cím: bekelteto.testulet@bkik.hu

Weboldal: https://bekeltet.bkik.hu

Budapest Főváros Kormányhivatala, Fogyasztóvédelmi Főosztály:

Cím: 1051 Budapest, Sas u. 19. III. em.

Telefon: +36 1 450-2598

Email: fogyved_kmf_budapest@bfkh.gov.hu

Amennyiben az eljárás nem vezet eredményre, a bejelentő jogosult az ügyet peres útra terelni. Ebben az esetben a felek kölcsönösen alávetik magukat a Budapesti II. és III. Kerületi Bíróság kizárólagos illetékességének.

9.14 Irányadó Jog

A Szolgáltató szerződéseire és Szolgáltatásaira a magyar jog az irányadó, azokat a magyar jog szerint kell értelmezni.

9.15 Megfelelés a hatályos jogszabályoknak

Szolgáltató tevékenységét a mindenkor hatályos Európai Uniós, illetve magyar jogszabályoknak megfelelően végzi.

9.16 Vegyes rendelkezések

9.16.1 Teljességi záradék

Nincs megkötés.

9.16.2 Átruházás

A szolgáltatások nyújtásába bevont Szolgáltatói partnerek csak a Szolgáltató előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és/vagy ruházhatják át kötelezettségeiket harmadik félnek.

9.16.3 Részleges érvénytelenség

A jelen szolgáltatási szabályzat egyes rendelkezéseinek tetszőleges okból történő érvénytelenné válása esetén a többi rendelkezés változatlan formában érvényben marad.

9.16.4 Igényérvényesítés

Szolgáltató kártérítésre, az ügyvédi díjak megfizetésére tarthat igényt a partnerei által okozott károk, veszteségek, költségek megtérítése érdekében. Amennyiben Szolgáltató egy konkrét esetben nem él kártérítési igényével, az nem jelenti azt, hogy a jövőben hasonló esetben a szolgáltatási szabályzat más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.5 Vis maior

A Vis Maior a Feleket mentesíti a Szerződés szerinti kötelezettségeik teljesítése alól olyan mértékben, amennyire a Vis Maior az érintett Felet gátolja a szerződéses kötelezettségeinek teljesítésében és addig az ideig, amíg a Vis Maior hatása fennáll. Vis maiornak minősül minden olyan rendkívüli, a Szerződés létrejötte után bekövetkező, annak teljesítését lehetetlenné tevő esemény, amelyet a Felek kellő körültekintés ellenére sem láthattak előre és nem háríthattak el, amely nem vezethető vissza egyikük saját hibájára vagy gondatlanságra sem.

Vis Maior eseménynek minősül különösen (i) rendkívüli állapot, szükségállapot, veszélyhelyzet, megelőző védelmi helyzet, váratlan támadás, árvíz, tűzvész vagy egyéb katasztrófahelyzetnek minősíthető helyzet; (ii) sztrájk vagy hasonló munkabeszüntetés, a Fél munkavállalói által végrehajtott sztrájk vagy munkabeszüntetés kivételével. A Vis Maior tényét, ha az nem köztudomású, igazoltatni kell az illetékes Gazdasági Kamara által.

Egyik Fél sem felelős a szerződés szerinti kötelezettségeinek nem-, hibás- vagy késedelmes teljesítésért, ha azt az előző pontban meghatározott Vis Maior esemény okozta. Vis Maior esemény bekövetkezte esetén az érintett Fél köteles a másik Felet írásban haladéktalanul értesíteni Vis Maior helyzetről és annak okáról. Ennek elmaradásából eredő károkért az értesítést elmulasztó Fél teljes felelősséggel tartozik.

A Szolgáltató katasztrófa esetén minden szükséges intézkedést meghoz annak érdekében, hogy a Szolgáltatásokat a lehető legrövidebb időn belül helyreállítsa.

9.17 Egyéb rendelkezések

Nincs megkötés.