

Elektronikus Bélyegző Bizalmi Szolgáltatási Rend

Hatályba lépés dátuma: 2018.03.27.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.
<i>Figyelem! Jelen dokumentumnak a https://www.mobilsign.com oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.</i>	

Dokumentum verziókövetés			
Verzió száma	Módosítás rövid leírása	Módosította	Hatálybalépés dátuma
v0.6	Első munkaváltozat	Benkó Tamás	
v0.7	Módosítások átvezetése	Benkó Tamás	
v1.0	Kiadott verzió	Benkó Tamás, Dohányos Péter	2017.11.30.
v1.1	Audit során felmerült észrevételek átvezetése	Benkó Tamás, Dohányos Péter	2018.02.07.
v1.2	NMHH észrevételei alapján módosított változat	Dohányos Péter	2018.03.27.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.
Figyelem! Jelen dokumentumnak a https://www.mobilsign.com oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.	

Tartalom

Tartalom.....	3
1 Bevezetés	9
1.1 Áttekintés	9
1.1.1 A Szolgáltató	9
1.2 A dokumentum neve és azonosítója	10
1.3 PKI közösség	10
1.3.1 Szolgáltató	10
1.3.2 Szerződött partner.....	10
1.3.3 Aláírást kezdeményező.....	10
1.3.4 Aláíró	10
1.3.5 Éritett felek.....	10
1.4 Tanúsítványok alkalmazhatósága.....	11
1.5 A Bizalmi Szolgáltatási Rend adminisztrációja.....	11
1.6 Fogalmak és rövidítések	11
1.6.1 Fogalmak	11
1.6.2 Rövidítések	12
2 Közzétételek	13
2.1 A nyilvános szabályzatok elérhetősége	13
2.2 Közzététel gyakorisága	13
3 Azonosítás és hitelesítés	13
4 A Szolgáltatás és életciklusa	13
4.1 A Szolgáltatás felhasználásának áttekintése	13
4.2 Szolgáltatás igénylése, üzembe állítása.....	13
4.3 Dokumentum fogadása	13
4.4 Elektronikus bélyegző létrehozása	14

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

4.5	Bélyegzett dokumentum átadása.....	14
4.6	Az előfizetés megszűnése.....	14
4.7	Magánkulcs letétbe helyezése és visszaállítása	14
5	Fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések.....	14
5.1	Fizikai óvintézkedések	15
5.1.1	Felépítés	15
5.1.2	Fizikai hozzáférésvédelem.....	15
5.1.3	Áramellátás, légkondicionálás.....	15
5.1.4	Beázás és elárasztódás veszélyeztetettsége.....	15
5.1.5	Tűz megelőzés és tűzvédelem	15
5.1.6	Adathordozók kezelése	15
5.1.7	Selejt kezelése	16
5.1.8	Szeperált mentés	16
5.1.9	Mobil eszközök használata	16
5.2	Eljárásrend intézkedések.....	16
5.2.1	Bizalmi munkakörök	16
5.2.2	Az egyes feladatokhoz szükséges személyzeti létszám	16
5.2.3	Az egyes szerepkörökhöz tartozó azonosítás és hitelesítés	16
5.2.4	Egyes szerepkörök összeférhetetlensége.....	16
5.3	Személyzetre vonatkozó előírások	16
5.3.1	Képzettségre, gyakorlatra és megbízhatóságra vonatkozó követelmények	17
5.3.2	Előélet vizsgálatára vonatkozó eljárások.....	17
5.3.3	Képzési követelmények	17
5.3.4	Továbbképzési gyakoriságok és követelmények	18
5.3.5	Munkabeosztás körforgásának sorrendje és gyakorisága.....	18
5.3.6	Felhatalmazás nélküli tevékenységek szankcionálása.....	18
5.3.7	Szerződéses közreműködőkre vonatkozó követelmények.....	18
5.3.8	A személyzet számára biztosított dokumentációk	18
5.4	Naplózási eljárások	18

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

5.4.1	A tárolt események típusai	18
5.4.2	A napló állomány feldolgozásának gyakorisága	18
5.4.3	A napló-állomány megőrzési időtartama	19
5.4.4	A napló állomány védelme	19
5.4.5	A napló állomány mentési folyamatai	19
5.4.6	A napló gyűjtési rendszere	19
5.4.7	Az eseményeket kiváltó alanyok értesítése	19
5.4.8	Sebezhetőség felmérése	19
5.5	Adatok archiválása	19
5.5.1	Az archivált adatok típusai	19
5.5.2	Az archivált adatok megőrzési ideje	19
5.5.3	Archív adatok védelme	19
5.5.4	Az archívum mentési folyamatai	19
5.5.5	Az adatok időbélyegzésére vonatkozó követelmények	20
5.5.6	Az archívum gyűjtési rendszere	20
5.5.7	Archív információk hozzáférését és ellenőrzését végző eljárások	20
5.6	Kulcscsere	20
5.7	Kompromittálódást és katasztrófát követő helyreállítás	20
5.7.1	Rendkívüli események és kompromittálódás kezelésének eljárásai	20
5.7.2	Informatikai erőforrások, szoftverek és adatok meghibásodása	20
5.7.3	Magánkulcs kompromittálódása	21
5.7.4	Működés helyreállítása katasztrófa esemény után	21
5.8	A szolgáltatási tevékenység megszüntetése	21
6	Műszaki, biztonsági óvintézkedések	22
6.1	Kulcspár generálás és telepítés	22
6.1.1	Kulcspár előállítása	22
6.1.2	Magánkulcs eljuttatása a Szerződött Partnerhez	22
6.1.3	Nyilvános kulcs eljuttatása tanúsítvány kibocsátóhoz	22
6.1.4	A szolgáltatói nyilvános kulcs közzététele	22

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

6.1.5	Használt kriptográfiai algoritmusok	22
6.1.6	A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése	23
6.1.7	A kulcshasználat célja	23
6.2	A magánkulcsok védelme és kriptográfiai modulra vonatkozó szabályok	23
6.2.1	Kriptográfiai modulra vonatkozó szabványok	23
6.2.2	A több-szereplős ("n-ből m") ellenőrzés	23
6.2.3	Magánkulcs letét	23
6.2.4	Magánkulcs mentése.....	23
6.2.5	Magánkulcs archiválása.....	23
6.2.6	Magánkulcs bejuttatása a kriptográfiai modulba, vagy onnan történő exportja.....	24
6.2.7	Magánkulcs tárolása kriptográfiai modulban.....	24
6.2.8	A magánkulcs aktivizálásának módja	24
6.2.9	A magánkulcs deaktiválásának módja.....	24
6.2.10	A magánkulcs megsemmisítésének módja.....	24
6.2.11	Kritográfiai modulok értékelése	24
6.3	A kulcspár kezelés egyéb szempontjai	24
6.4	Aktiváló adat.....	24
6.4.1	Aktivizáló adatok előállítása és telepítése.....	24
6.4.2	Az aktivizáló adatok védelme	24
6.4.3	Aktivizáló adatok egyéb szempontjai	25
6.5	Informatikai biztonsági előírások	25
6.5.1	Informatikai biztonsági műszaki követelmények meghatározása.....	25
6.5.2	Informatikai biztonság értékelése	25
6.6	Életciklusra vonatkozó biztonsági előírások	25
6.6.1	Rendszerfejlesztési előírások.....	26
6.6.2	Biztonságkezelési előírások	26
6.6.3	Életciklusra vonatkozó biztonsági előírások	26
6.7	hálózatbiztonsági előírások	26
6.8	Időbélyegzés	26

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

7	Tanúsítvány és CRL profilok.....	26
7.1	Tanúsítvány profil	26
7.2	CRL profil	26
7.3	OCSP profil.....	26
8	A megfelelés vizsgálatát	27
8.1	Az ellenőrzések körülményei és gyakorisága	27
8.2	A külső auditor képesítése	27
8.3	Auditor függetlensége	27
8.4	A hiányosságok kezelése	27
8.5	Az eredmények kommunikálása.....	27
9	Egyéb üzleti és jogi kérdések	27
9.1	Díjak.....	27
9.2	Anyagi felelősségvállalás	27
9.3	Üzleti információk bizalmassága	28
9.3.1	Bizalmasan kezelendő információk köre	28
9.3.2	Nem bizalmasnak tekintett információk köre	28
9.3.3	Bizalmas információ védelme.....	28
9.4	Személyes adatok védelme	28
9.4.1	Adatkezelési szabályzat	28
9.4.2	Bizalmasan kezelendő személyes adatok.....	28
9.4.3	Személyes adatnak nem minősülő adatok	28
9.4.4	Személyes adatok védelme	28
9.4.5	Személyes adatok felhasználása.....	28
9.4.6	Felfedés bírósági vagy polgári peres eljárás keretében	29
9.5	Szellemi tulajdonjogok	29
9.6	Tevékenységért viselt felelősség és helytállás	29
9.6.1	A Szolgáltató felelőssége és helytállása	29
9.6.2	A Szerződött Partner felelőssége és helytállása	30

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

9.6.3	Az aláírást kezdeményező felelőssége és helytállása.....	32
9.6.4	Az Aláíró felelőssége és helytállása	32
9.6.5	Az Érintett felek kezdeményező felelőssége és helytállása	32
9.7	Helytállás érvénytelenségi köre	32
9.8	Felelősség korlátozása	32
9.9	Kártérítési kötelezettség	32
9.10	Hatályosság és megszűnés	33
9.10.1	Érvényesség.....	33
9.10.2	Megszűnés.....	33
9.10.3	A megszűnés következményei.....	33
9.11	A résztvevők közötti kommunikáció	33
9.12	Módosítások	33
9.12.1	Módosítási eljárás.....	33
9.12.2	Az értesítések módja és határideje	34
9.12.3	A dokumentum azonosító (OID) változása	34
9.13	Vitás kérdések rendezése.....	34
9.14	Irányadó Jog	34
9.15	Megfelelés a hatályos jogszabályoknak	34
9.16	Vegyes rendelkezések	34
9.16.1	Teljességi záradék.....	34
9.16.2	Átruházás.....	34
9.16.3	Részleges érvénytelenség.....	34
9.16.4	Igényérvényesítés.....	34
9.16.5	Vis maior.....	35
9.17	Egyéb rendelkezések	35

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

1 Bevezetés

Jelen dokumentum a MobilSign Kft. (továbbiakban Szolgáltató) Bizalmi Szolgáltatási rendje, mely a nem minősített elektronikus bélyegző szolgáltatására vonatkozik (továbbiakban Szolgáltatási Rend, vagy Rend). Jelen dokumentum egy szabálygyűjtemény, mely azon minimum követelményeket foglalja össze, melyek a Szolgáltató a Szolgáltató szolgáltatására, illetve annak igénybevételére vonatkoznak.

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 dokumentum a Szolgáltató elektronikus bélyegző bizalmi szolgáltatására vonatkozó elvárásokat tartalmazza.

A meghatározott követelmények és elvárások teljesítésének módját és leírását a MobilSign Elektronikus Bélyegző Bizalmi Szolgáltatási Szabályzat dokumentum tartalmazza.

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 1 6120817
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.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

A Bizalmi Felügyelet elektronikus aláírással kapcsolatos szolgáltatásokat tartalmazó nyilvántartásának elérhetősége: <http://webpub-ext.nmhh.hu/esign/>

1.2 A dokumentum neve és azonosítója

A dokumentum teljes neve MobilSign Elektronikus Bélyegző Bizalmi Szolgáltatási Rend. 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 Aláírást kezdeményező, az Aláíró 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 Aláírást kezdeményező képviselői által manuálisan kezdeményezve.

1.3.3 Aláírást kezdeményező

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

1.3.4 Aláíró

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 (kézi aláírás), mely az üzleti folyamat metaadatoként, megfelelő felülhitelesítés érdekében a képviselő által a Szolgáltatás használatával kezdeményezett elektronikus bélyegző létrehozását kell, hogy maga után vonja.

1.3.5 Érintett 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.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

1.4 Tanúsítványok alkalmazhatósága

A Szerződött Partner elektronikus bélyegző tanúsítványa kizárólag a Szerződött Partner elektronikus bélyegzőinek –Szerződött Partner és Aláírás kezdeményező személyei által kezdeményezett– létrehozására használható.

1.5 A Bizalmi Szolgáltatási Rend adminisztrációja

Jelen Bizalmi Szolgáltatási Rend adminisztrációját a Szolgáltató végzi, melynek adatai megtalálhatóak a 1.1.1 A Szolgáltató fejezetben.

A Szolgáltató legalább évente egyszer megvizsgálja a bizalmi szolgáltatási rend releváns jogszabályi- és technológiai szabványok előírásainak megfelelőségét és szükség esetén a bizalmi szolgáltatási rendből módosított, új verziót bocsát ki és léptet hatályba, melynek eljárásrendjét a szolgáltatási szabályzatban meghatározni szükséges.

1.6 Fogalmak és 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
 - b) szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy
 - c) weboldal-hitelesítő tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy
 - d) 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;

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

- **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
- **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)

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

2 Közzétételek

2.1 A nyilvános szabályzatok elérhetősége

A Szolgáltató köteles megoldani a Szolgáltatással kapcsolatos nyilvános szabályzatok publikálását folyamatosan elérhető, nyilvános módon.

2.2 Közzététel gyakorisága

A Szolgáltatónak meg kell határoznia a nyilvános szabályzatok publikálásának gyakoriságát az elérhetőséggel kapcsolatos esetleges korlátozások

3 Azonosítás és hitelesítés

A Szolgáltatási Szabályzatban ismertetni kell a Szolgáltatást igénybe vevő Szerződött Partner / Szerződött Partner jelöltek azonosításának módszerét.

4 A Szolgáltatás és életciklusa

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

A Szolgáltatás igénybevétele során az elektronikus bélyegző létrehozásának folyamata röviden a következő:

-

4.1 A Szolgáltatás felhasználásának áttekintése

4.2 Szolgáltatás igénylése, üzembe állítása

A Szolgáltatást szolgáltatási szerződés megkötése után lehetséges igénybe venni.

A Szolgáltatás használatához szükséges a Szerződött Partner számára dedikált kiszolgáló példány – Szolgáltató általi– üzembe állítása, valamint kapcsolat létrehozása a Szolgáltatás technikai interfésze és a Szerződött Partner informatikai rendszere között.

A Szerződött Partner számára szükséges aláíró kulcsot generálni, ahhoz aláíró tanúsítványt kiállítani, majd az elkészült aláíró tanúsítványt visszatölteni. Ennek módja a Szabályzatban kerül ismertetésre.

4.3 Dokumentum fogadása

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.
Figyelem! Jelen dokumentumnak a https://www.mobilsign.com oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.	

A Szolgáltató a Szerződött Partnertől elektronikus bélyegző létrehozásához dokumentumot a kialakított biztonságos kapcsolaton keresztül a dokumentum fogadó interfészen fogad. Ennek során a Szolgáltató a dokumentumot és a mellékelt metaadatokat ellenőrzésnek veti alá, és csak akkor fogadhatja be azokat, amennyiben azok technikailag és biztonságilag megfelelnek a Szolgáltatás általi feldolgozáshoz szükséges követelményeknek.

4.4 Elektronikus bélyegző létrehozása

A Szerződött Partnertől beérkezett elektronikus dokumentumokon az elektronikus bélyegzőt a Szerződött Partner hozza létre a Szolgáltatás aktiválásával. Ennek módját a Szabályzatban ismertetni szükséges.

4.5 Bélyegzett dokumentum átadása

A Szolgáltatás az elektronikus bélyegzővel ellátott dokumentumot automatikusan továbbítja a Szerződött Partner részére.

4.6 Az előfizetés megszűnése

A Szolgáltató a megszűnt szerződéshez kapcsolódóan tárolt munkaadatokat egy évig megőrzi, melynek letelte után jogosult azokat törölni.

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

4.7 Magánkulcs letétbe helyezése és visszaállítása

A Szolgáltató a Szolgáltatás fenntartásához szükséges mentések keretében – a kulcsok biztonságát nem veszélyeztetve – a kulcsokat tároló, csak a HSM eszköz által feloldható titkosítású adategységről (HSM Security World) biztonsági másolatot készít.

A Szolgáltatási Szabályzatban rendelkezésnek kell szerepelnie a Szerződött Partner aláíró kulcsának kezeléséről az előfizetés megszűnése esetére.

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.

Szolgáltatónak rendelkeznie kell információbiztonsági szabállyal, mely részletesen szabályozza a Szolgáltató Szolgáltatással kapcsolatos informatikai rendszereinek és az ehhez kapcsolódó belső folyamatainak biztonsági kontroljait.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

5.1 Fizikai óvintézkedések

A hitelesítés-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 megfelelő fizikai és logikai védelemmel (pl. tűz-, víz-, lopás-, fizikai és logikai hozzáférésvédelem) van ellátva. A kialakításnak támogatnia kell a rendszerek használatuknak és besorolásuknak megfelelő logikai és fizikai szeparációt.

5.1.2 Fizikai hozzáférésvédelem

A fizikai hozzáférésvédelmet úgy kell kialakítani, hogy a rendszerhez való hozzáférés csak ellenőrzött pontokon legyen lehetséges. A fizikai hozzáférési jogosultságokat jóvá kell hagyni és a belépéseket naplózni kell.

5.1.3 Áramellátás, légkondicionálás

Az áramellátást úgy kell kialakítani, hogy megfeleljen az alábbi követelményeknek:

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

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

5.1.4 Beázás és elárasztódás veszélyeztetettsége

A Szolgáltató szolgáltatási helyszíneinek kialakítása során figyelembe kell venni a beázásból és elárasztódásból adódó kockázatok minimalizálását.

5.1.5 Tűz megelőzés és tűzvédelem

A rendszer tűzvédelmét legalább füstérzékelés és riasztás kialakításával kell biztosítani. Ezen felül a rendelkezésre állás szempontjából kritikus infrastruktúra esetén az automata tűzfolytás kialakítása is szükséges.

5.1.6 Adathordozók kezelése

A Szabályzatban ki kell térni a Szolgáltató által tárolt adathordozókkal kapcsolatban alkalmazott intézkedésekre, melyeknek biztosítaniuk kell azok megfelelő védelmét.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

5.1.7 Selejt kezelése

A Szolgáltatónak eljárásokat kell kidolgoznia az adathordozók selejtezésével és használatból való kivonásával kapcsolatban, különösen az érzékeny adatokat tartalmazó adathordozók esetén.

5.1.8 Szeparált mentés

A szervezetnek rendelkeznie kell az elsődleges telephelytől elkülönített másodlagos mentéssel. A mentések elkészültéről jegyzőkönyvet kell készíteni.

5.1.9 Mobil eszközök használata

A Szabályzatnak rendelkeznie kell arról, hogy ha bizonyos keretek között megengedhető, mobil eszközöket milyen korlátozásokat és védelmi intézkedéseket betartva lehet bizalmi szolgáltatáshoz kapcsolódó műveletvégzésekhez használni.

5.2 Eljárásrend intézkedések

5.2.1 Bizalmi munkakörök

A Szolgáltatónak meg kell határoznia azokat a bizalmi munkaköröket, melyek a Szolgáltatás megfelelő, biztonságos működtetése érdekében létrehozásra és betöltésre kerülnek. A munkakörök kialakításánál figyelembe kell venni a jogszabályi előírásokat.

A bizalmi munkakörökről a Szolgáltatónak naprakész nyilvántartást kell vezetnie.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszám

A Szabályzatban szükséges meghatározni azokat a tevékenységeket és műveleteket, melyekhez kötelezően egyénél több, bizalmi munkakört betöltő személy jelenléte elvárt.

5.2.3 Az egyes szerepkörökhöz tartozó azonosítás és hitelesítés

A Szolgáltató informatikai rendszereinek minden felhasználója és az adminisztratív folyamatok minden szereplője esetén személy szerinti azonosítás szükséges. Sikeres hitelesítés előtt egyetlen biztonság kritikus tevékenységet sem lehet végrehajtani. Törekedni kell arra, hogy a Szolgáltató minden munkatársa csak annyi hozzáférési jogosultsággal rendelkezzen, amennyi a feladatköre ellátásához szükséges.

5.2.4 Egyes szerepkörök összeférhetetlensége

A Szabályzatnak tartalmaznia kell az egyes bizalmi munkakörök egymással való kizárásának meghatározását.

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

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

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 tölthetik 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 valóságát.

5.3.3 Képzési követelmények

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

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

5.3.4 Továbbképzési gyakoriságok és követelmények

A Szolgáltatónak gondoskodnia kell a Szolgáltatás nyújtásában közreműködők megfelelő szintű tudásáról és az ehhez szükséges képzésekről.

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 Szolgáltatónak folyamatosan biztosítania kell a szolgáltatásnyújtásban közreműködő személyek részére a szerepük ellátásához szükséges aktuális szabályzatokat és dokumentációkat.

5.4 Naplózási eljárások

Szolgáltatónak a Szolgáltatással kapcsolatos informatikai rendszerével és támogató rendszereivel összefüggő eseményeket naplózni kell. A naplók alapján vissza kell tudni követni a Szolgáltatás működése során történt események életútját és útvonalát.

5.4.1 A tárolt események típusai

A megvalósított naplózásnak ki kell terjednie kiemelten a következő eseménytípusokra:

- kulcs menedzsment események
- napló generáló funkcionális elindulása és leállása
- naplózási paraméterek megváltozása
- hozzáférési kísérletek (rendszer és adat- illetve más erőforrás hozzáférési kísérletek)
- kulcs irányítási tevékenységek
- rendszer konfigurációs változások
- aláírás események, kiemelten: aláíráskészítés és aláírás-hitelesítés
- rendszeradminisztrátori és rendszeroperátori tevékenységek.

5.4.2 A napló állomány feldolgozásának gyakorisága

Szolgáltatónak biztosítania kell a naplóállományok rendszeres ellenőrzését és kiértékelését.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

5.4.3 A napló-állomány megőrzési időtartama

Az üzemeltetési napló-állományokat legalább 10,5 évig tárolni szükséges a naplógyűjtő rendszerben, vagy archivált állapotban. A naplókat és archivált naplóállományokat a Független rendszervizsgáló számára elérhetővé kell tudni tenni.

5.4.4 A napló állomány védelme

A naplóállományokat védeni kell az utólagos módosításoktól és az egyes naplóbejegyzések utólagos törlésétől. Biztosítani kell a naplóállományok integritását és annak ellenőrizhetőségét.

5.4.5 A napló állomány mentési folyamatai

A Szolgáltatónak kidolgozott eljárásokkal kell rendelkeznie a naplóállományok tárolására és mentésére.

5.4.6 A napló gyűjtési rendszere

A Szabályzatnak tartalmaznia kell a napló gyűjtési rendszerére vonatkozó előírásokat.

5.4.7 Az eseményeket kiváltó alanyok értesítése

Nincs kikötés.

5.4.8 Sebezhetőség felmérése

A Szolgáltatónak rendszeresen végeznie kell sebezhetőség felmérést a Szolgáltatással kapcsolatos újonnan adódó fenyegetések feltárására, melynek eredménye alapján indokolt esetben kockázatértékelést kell végeznie.

5.5 Adatok archiválása

5.5.1 Az archivált adatok típusai

A Szolgáltatónak szükséges megoldania minden olyan adat és információ megőrzését, mely lehetővé teszi a Szolgáltatás biztosításával és igénybevételével kapcsolatos feltételek korábbi időpontokra vonatkozó visszakövethetőségét.

Archiválandó a Szolgáltatás során létrejött és begyűjtött minden naplóbejegyzés.

5.5.2 Az archivált adatok megőrzési ideje

A Szolgáltatónak biztosítania kell 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

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

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

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi elektronikus naplóbejegyzés tartalmaznia kell idő adatot, amelyen legalább másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont. A Szolgáltatónak biztosítania kell, hogy a szolgáltatást nyújtó rendszerein a gépidő maximum 1 másodpercre tér el a referenciaidőtől.

5.5.6 Az archívum gyűjtési rendszere

Nincs megkötés

5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások

A Szolgáltatónak az archivált dokumentumokat és adatokat védett környezetben kell tárolnia és biztosítania kell a megfelelő hozzáférési védelmet.

5.6 Kulcscsere

A Szolgáltatónak eljárásokkal kell rendelkeznie a Szerződött Partnerek aláíró kulcsainak- és a Szolgáltatásban használt egyéb kriptográfiai kulcsok cseréjéről a tanúsítvány lejáratára- vagy a használt kriptográfiai algoritmusok váratlan elavulása miatt. Az aláíró kulcsok esetén meg kell oldani a cseréből adódó működési kiesés minimalizálását.

5.7 Kompromittálódást és katasztrófát követő helyreállítás

Szolgáltató intézkedéseket kell tennie annak érdekében, hogy rendkívüli üzemeltetési helyzet, vagy katasztrófa bekövetkezésekor a Szolgáltatás elérhetetlensége vagy a vállalt válaszidők sérülése miatt adódó károkat elkerülje vagy minimalizálja.

A Szolgáltató indokolatlan késedelem nélkül, de minden esetben az esetről való értesüléstől számított 24 órán belül értesíti 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 Szolgáltatónak incidens kezelési eljárásokat kell kidolgoznia és katasztrófa elhárítási tervet kell összeállítania és karbantartania a rendkívüli események és katasztrófa-helyzetek gyors reagálású kezelése érdekében.

5.7.2 Informatikai erőforrások, szoftverek és adatok meghibásodása

A Szolgáltató informatikai rendszereit, különösen a Szolgáltatásba bevont rendszerek esetén megbízható hardver és szoftver komponensekből kell összeállítania. A Szolgáltatónak a rendszereiről a belső mentési szabályzatnak megfelelően rendszeres, a rendszer helyreállíthatóságát biztosító mentést kell készítenie. E mellett a hivatkozott Katasztrófa Elhárítási tervnek rendelkeznie kell a meghibásodások esetén követendő eljárásokról.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

5.7.3 Magánkulcs kompromittálódása

Szerződött Partner aláíró magánkulcsainak kompromittálódása esetén legalább a következő lépések megtétele szükséges:

- az érintett aláíró magánkulcs használatát haladéktalanul megszünteti, és erről értesíti a Szerződött Partnert valamint a Bizalmi Felügyeletet
- a Szerződött Partner értesítése a kompromittálódásról és a tanúsítvány visszavonásának kezdeményezése
- a Bizalmi felügyelet értesítése a kompromittálódásról
- Közzétenni a kompromittálódás által esetlegesen érintett elektronikus bélyegzők körét, vagy olyan információkat, melyek alapján az érintett elektronikus bélyegzők köre beazonosítható

A Szolgáltatónak eljárásokat kell kidolgoznia a Szolgáltatás keretében használt egyéb magánkulcsok kompromittálódásának esetére is.

5.7.4 Működés helyreállítása katasztrófa esemény után

A Szolgáltató Katasztrófa Elhárítási terve részletezi a bekövetkezett esemény után követelendő lépéseket a Szolgáltatás mielőbbi helyreállításához.

5.8 A szolgáltatási tevékenység megszüntetése

A Szolgáltatónak a szolgáltatási tevékenység megszüntetése esetén követnie kell 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 küldött értesítésben 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.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

- A Szolgáltató köteles az átvevő bizalmi szolgáltatónak a hozzáférési kötelezettség alá eső nyilvántartási adatokat átadni

6 Műszaki, biztonsági óvintézkedések

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

6.1 Kulcspár generálás és telepítés

6.1.1 Kulcspár előállítás

A Szolgáltató gondoskodnia kell a Szerződött Partnerek aláíró kulcspárjának biztonságos és az ipari szabványoknak megfelelő generálásáról, és erről kidolgozott, dokumentált eljárásrenddel kell rendelkeznie. A Szerződött Partnerek aláíró kulcspárjának generálása fizikailag védett környezetben, egy biztonsági tisztviselő és legalább még egy bizalmi munkakört betöltő személy részvételével kell, hogy történjen, kizárólag a Szolgáltatás aláíró Kriptográfiai hardver moduljában (HSM).

A kulcsgenerálás során alkalmazott kriptográfiai algoritmusoknak és algoritmus paramétereknek meg kell felelnie a Nemzeti Média- és Hírközlési Hatóság Elektronikus aláírással kapcsolatos szolgáltatások nyújtásánál használható biztonságos kriptográfiai algoritmusok határozatának.

6.1.2 Magánkulcs eljuttatása a Szerződött Partnerhez

A Szerződött Partnerek aláíró kulcsai 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 aláíró kulcsához tanúsítvány kérés kerül kiállításra, melyet manipulálástól védett módon kell a Szerződött Partner részére eljuttatni.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

A Szolgáltató a Szerződött Partnerek felé nyújtott Szolgáltatás keretében a Szerződött Partner saját aláíró kulcsával hoz létre elektronikus bélyegzőket, nem szolgáltatói kulcspár segítségével. A Szerződött Partnerek aláíró kulcspárjainak nyilvános kulcsait (tanúsítványait) csak a Szerződött partnerek számára teszi elérhetővé.

6.1.5 Használt kriptográfiai algoritmusok

A Szolgáltató digitális aláírásra minden esetben a Nemzeti Média- és Hírközlési Hatóság Elektronikus aláírással kapcsolatos szolgáltatások nyújtásánál használható biztonságos kriptográfiai algoritmusok határozata alapján megfelelőnek tekinthető algoritmust kell használnia, valamint a használt algoritmusoknak meg kell megfelelniük az ETSI TS 102 176 ajánlásnak.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.
Figyelem! Jelen dokumentumnak a https://www.mobilsign.com oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.	

6.1.6 A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

Nincs külön megkötés

6.1.7 A kulcshasználat célja

A Szerződött Partner aláíró magánkulcsa kizárólag a Szerződött Partner által aktivált elektronikus bélyegző készítéshez használható.

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

6.2 A magánkulcsok védelme és kriptográfiai modulra vonatkozó szabályok

6.2.1 Kriptográfiai modulra vonatkozó szabványok

Szolgáltató Szerződött Partnerek aláíró 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 Szolgáltatás keretében alkalmazott egyéb kriptográfiai kulcsok védelmére és kezelésére vonatkozólag a Szolgáltatónak rendelkeznie kell kidolgozott és dokumentált szabályzatokkal.

6.2.2 A több-szereplős ("n-ből m") ellenőrzés

A Szolgáltató a Szerződött Partnerek aláíró kulcsait tároló Kriptográfiai hardver modul adminisztrátori funkcióiban is és a magánkulcsok használatának engedélyezéséhez 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 aláíró magánkulcsairól a Szolgáltatónak biztonsági mentést kell készítenie. A kulcsok biztonsági mentését és kulcs visszaállítási szükségességét eredményező rendkívüli üzemi helyzetek esetében a kulcs mentésből való visszaállítást fizikailag védett környezetben, legalább kettő bizalmi munkakört betöltő személy együttes munkájával szükséges megvalósítani. A kulcs biztonsági mentésére és visszaállítására a Szolgáltatónak kidolgozott, dokumentált szabályozással kell rendelkeznie.

6.2.5 Magánkulcs archiválása

A Szolgáltató nem archiválhatja a Szerződött Partnerek aláíró magánkulcsait.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

6.2.6 Magánkulcs bejuttatása a kriptográfiai modulba, vagy onnan történő exportja

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

A Szolgáltató által a Szolgáltatással kapcsolatban alkalmazott egyéb kriptográfiai kulcsok magánkulcsainak kezelésére kidolgozott szabályozással kell rendelkeznie.

6.2.7 Magánkulcs tárolása kriptográfiai modulban

A Szerződött Partnerek aláíró magánkulcsai az aláíró 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 szükséges elvégezni.

6.2.9 A magánkulcs deaktiválásának módja

Nincs megkötés

6.2.10 A magánkulcs megsemmisítésének módja

A Szerződött Partnerek aláíró magánkulcsához tartozó tanúsítványának lejáratakor, visszavonásakor, vagy az aláíró kulcs használatának egyéb befejeződésekor a kulcsot a Kriptográfiai hardver modulból törölni szükséges, valamint az arról készült minden biztonsági mentést visszaállíthatatlan módon törölni kell.

6.2.11 Kriptográfiai modulok értékelése

A Szolgáltató a 6.2.1 fejezetben meghatározott eszközöket használja.

6.3 A kulcspár kezelés egyéb szempontjai

A Szerződött partnerek aláíró 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 Szolgáltatónak a felhasznált Hardver kriptográfiai eszközök felhasználói útmutatójában és az eszköz tanúsítványban megfogalmazott eljárásoknak, követelményeknek megfelelő aktiváló módszereket kell alkalmaznia a Szerződött Partneri magánkulcsok védelmére.

6.4.2 Az aktivizáló adatok védelme

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

A Szolgáltatónak a Szerződött Partneri aláíró magánkulcsok aktiváló adatait biztonságos módon kell tárolnia és hozzáférésükhöz legalább kettő, bizalmi munkakört betöltő munkatárs együttműködése legyen szükséges.

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 EN 319401 v2.1.1 (2016-02) „Elektronikus aláírások és infrastruktúrák (ESI). A bizalmi szolgáltatókra vonatkozó általános politika-követelmények.” által meghatározott követelmények
- CEN/TS 419 241:2014 Security Requirements for Trustworthy Systems Supporting Server Signing
- 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

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

6.6.1 Rendszerfejlesztési előírások

A Szolgáltatónak rendelkeznie kell kidolgozott szabályozással a Szolgáltatást megvalósító rendszer fejlesztésével, továbbfejlesztésével kapcsolatos elvárásokról.

6.6.2 Biztonságkezelési előírások

A Szolgáltatónak olyan eszközöket, alkalmazásokat és eljárásokat kell alkalmaznia, melyek biztosítják a rendszerek megfelelő biztonsági konfigurációs beállításait.

6.6.3 Életciklusra vonatkozó biztonsági előírások

A Szolgáltatónak a Szolgáltatás nyújtásához használt eszközök és alkalmazások teljes életciklusa alatt figyelembe kell vennie és biztosítja a megfelelő kontrollok működését.

6.7 hálózatzbiztonsági előírások

A Szolgáltató a Szolgáltatáshoz nyújtott eszközöket azok funkcionalitása és rendeltetése szerint meghatározott biztonsági zónákba kell sorolni. A zónák közötti kommunikáció csak biztonságos, felügyelt csatornákon keresztül történhet.

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 időbélyegeket EU bizalmi listában szereplő szolgáltatótól szükséges beszerezni.

A Szolgáltató a rendszereinek óráit külső UTC időforráshoz (idő szerver) kell szinkronizálni.

7 Tanúsítvány és CRL profilok

7.1 Tanúsítvány profil

A Szolgáltató által a Szerződött Partnerek aláíró tanúsítványaival szemben elvárt megkötések a Szabályzat tartalmazza.

7.2 CRL profil

Nincs megkötés

7.3 OCSP profil

A Szolgáltató által a Szerződött Partnerek aláíró tanúsítványaival szemben elvárt megkötések a Szabályzat tartalmazza.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

8 A megfelelés vizsgálat

A Szolgáltató a rendszerét rendszeres időközönként külső független auditorral felül kell vizsgáltatnia, hogy megfelel-e a Szolgáltatás nyújtásához szükséges követelményeknek.

8.1 Az ellenőrzések körülményei és gyakorisága

A Szolgáltató évente, illetve a szolgáltatásban bekövetkező jelentős változások esetén elvégezteti a külső független auditot.

8.2 A külső auditor képesítése

A külső auditokat Szolgáltatónak olyan szakértővel vagy szervezettel kell elvégeztetnie, aki rendelkezik egy EU tagállam nemzeti akkreditációs szervezetétől megfelelő felhatalmazással.

8.3 Auditor függetlensége

A külső vizsgálatokat végző szervezetnek, annak munkatársainak, valamint a külső rendszervizsgálónak teljes mértékben függetleneknek kell lennie a Szolgáltatótól.

8.4 A hiányosságok kezelése

A belső és külső ellenőrzések, elvégzett auditok által feltárt hiányosságok kezelésére a Szolgáltatónak intézkedési tervet kell készítenie, mely tartalmazza az elvégzendő intézkedéseket, azok felelőseit és határidejét.

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 Szolgáltatónak nem kell határoznia és nyilvánosságra kell hozni a használt díjakat.

9.2 Anyagi felelősségvállalás

A szolgáltatónak a megbízhatóság biztosítása érdekében felelősségbiztosítással kell rendelkeznie, amelynek ki kell terjednie a szolgáltató által nyújtott bizalmi szolgáltatásokkal összefüggésben okozott alábbi károkra és költségekre:

- a bizalmi szolgáltatási ügyfélnek a bizalmi szolgáltatási szerződés megszegésével összefüggésben okozott károkra,
- a bizalmi szolgáltatási ügyfélnek és harmadik személynek szerződésen kívüli okozott károkra,
- az E-ügyintézési tv. 88. §-ában foglalt kötelezettségek nem teljesítése miatt a bizalmi felügyeletnél felmerült, az E-ügyintézési tv. 89. §-a szerinti költségekre, és

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

- az eIDAS Rendelet 17. cikk (4) bekezdés e) pontja alapján a bizalmi felügyelet által felkért megfelelőségértékelő szervek eljárásának költségeire, ha azt a bizalmi felügyelet eljárási költségként érvényesíti.
- A szolgáltatónak biztosítania kell, hogy a megkötött biztosítási szerződés kiterjedjen a fent felsorolt költségekre és károkra. A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként nem lehet alacsonyabb, mint 3 000 000 forint.

9.3 Üzleti információk bizalmassága

9.3.1 Bizalmasan kezelendő információk köre

A Szolgáltatónak meg kell határoznia azon adatok és információk körét, melyet bizalmasan kezelendőnek tekint.

9.3.2 Nem bizalmasnak tekintett információk köre

Nincs megkötés

9.3.3 Bizalmas információ védelme

A Szolgáltatónak védenie kell az általa bizalmasnak tekintett adatokat és információkat. Ennek módját a Szolgáltatási szabályzatban rögzíteni szükséges.

9.4 Személyes adatok védelme

9.4.1 Adatkezelési szabályzat

A Szolgáltatónak rendelkeznie kell adatvédelmi és adatbiztonsági szabályzattal, mely részletezi a személyes adatkezelés szabályait.

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 Szolgáltatónak minden tudomására jutott személyes adatot védenie szükséges.

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

Szolgáltatónak védenie szükséges a személyes adatokat.

9.4.5 Személyes adatok felhasználása

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

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 Szolgáltatónak a Szabályzatban meg kell határoznia a bírósági vagy polgári peres eljárások keretében kiadott információk körét és a kiadás módjával kapcsolatos feltételeket.

9.5 Szellemi tulajdonjogok

A Szolgáltató a Szolgáltatás nyújtásához csak olyan eszközöket alkalmazhat, csak olyan módon, 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 Ügyfélnél kimutatott, az általa szándékosan vagy gondatlanul az Ügyfélnél okozott kárért felelős. A Szolgáltató nem tartozik felelősséggel azokért a károkért, amelyek abból erednek, hogy az Ügyfél 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 megfelelőségére, hitelességére – felelősségbiztosítással rendelkezik. Amennyiben a Szolgáltató által szolgáltatott elektronikus bélyegző hitelessége esetlegesen valamely bíróság vagy hatóság előtt nem minősül megfelelőnek, és ebből eredően az Ügyfelet kár éri, a Szolgáltató felelőssége kizárólag a felelősségbiztosítással maximum összeg erejéig terjedhet.

A Szolgáltató továbbá semmilyen körülmények között nem felel azért, ha az Ügyfelet abból eredően éri kár, hogy a saját ügyfelének, az Aláíró személyazonosítását nem, vagy nem kellő körültekintéssel végezte el. A jelen kárfelelősséget kizáró klauzula alól kivételt kizárólag a törvényben (Ptk.)

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

meghatározottak képeznek, így Szolgáltató nem zárhatja ki felelősségét a szándékosan okozott, továbbá az emberi életet, testi épséget vagy egészséget megkárosító károkozásért.

A Szolgáltató kötelezettsége

A Szolgáltató köteles a Szolgáltatásokat a mindenkor 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 aláírt dokumentumot, időbélyegzővel ellátott PDF formájában köteles az Ügyfél 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 az Ügyfél 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

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

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 az Ügyfél 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 a saját ügyfelét / a természetes vagy jogi személy Aláíró felet megfelelő módon azonosítani, amely szabályozott piaci tevékenység esetén a jogszabályoknak megfelelő személyazonosítást jelenti, egyéb esetekben pedig a személyazonosítás olyan módját, amely az általánosan alkalmazott gyakorlatnak megfelelően alkalmas a személyazonosításra (legalább egy személyazonosító okmány ellenőrzése, és legalább három személyazonosító adat felvétele, valamint az okmány típusának és sorszámaának rögzítése).

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 csőd eljárás, 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 Szerződésben és a vonatkozó magyar és Uniós jogszabályokban foglaltaknak megfelelően használni.

A Szerződött Partner kötelessége a Szolgáltató által megfogalmazott követelmények betartás és betartatása a Szolgáltatás igénybevétel során az Aláírást kezdeményező, valamint az Aláíró 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

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

küldött információk befogadását a Szolgáltató jogosult megtagadni. Az alkalmazható technológiákkal és megoldásokkal kapcsolatos információkat a Műszaki dokumentáció tartalmazza.

9.6.3 Az aláírást kezdeményező felelőssége és helytállása

Az Aláírást 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.

Az Aláírást kezdeményező kötelessége az aláírás kezdeményezésekor ellenőrizni, hogy az aktivált szolgáltatás keretében a megfelelő aláíró kulcs aktiválódott-e.

9.6.4 Az Aláíró felelőssége és helytállása

Az aláíró felelőssége, hogy aláírás előtt ellenőrizze az aláírandó dokumentum tartalmát.

Az aláíró kötelessége, hogy az Aláírás kezdeményező által ismertetett esetleges utasításokat kövesse.

9.6.5 Az Érintett felek kezdeményező felelőssége és helytállása

Az érintett felek az elektronikusan aláírt PDF-ek aláírás ellenőrzésekor kötelesek a Szerződött Partner által választott hitelesítés szolgáltató szolgáltatási szabályzatának releváns részei szerint eljárni. E mellett kötelesek betartani a Szolgáltató Aláírási szabályzatának vonatkozó részeit is.

Az elektronikus bélyegzőhöz csatolt metaadatok hitelességének ellenőrzése az 9.4.6 fejezetben foglaltak estén lehetséges. Ilyen esetekben a Szolgáltatóhoz kell fordulni a 1.3.1 pontban megadott elérhetőségeken. A megfelelő felhatalmazással rendelkező szakértő részére a Szolgáltató biztosít környezetet, ahol a Szerződött Partnerrel együttműködve lehetőséget biztosítanak az elektronikus bélyegzőhöz csatolt metaadatok történő hozzáférésnek.

9.7 Helytállás érvénytelenségi köre

Szolgáltató nem felelős az olyan károkért, amelyek abból adódtak, hogy az Igénybevevő vagy az 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.

9.9 Kártérítési kötelezettség

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

A Szolgáltatónak a kártérítésekről a szolgáltatási szabályzatban rendelkezni szükséges.

9.10 Hatályosság és megszűnés

9.10.1 Érvényesség

Tárgyi hatálya

A Szolgáltatási rend 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 Szolgáltatási rend 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 rend a Szolgáltató szolgáltatási tevékenységének befejezésével tekintendő megszűntnek.

9.10.3 A megszűnés következményei

A megszűnés következményeiről a Szabályzatban nyilatkozni szükséges.

9.11 A résztvevők közötti kommunikáció

A Szerződött Partnerekkel való kommunikációs módokat a Szolgáltatási szabályzat írja le.

Egyéb felekkel a Szolgáltató a 1.3.1 pontban megadott elérhetőségein keresztül tart kapcsolatot.

9.12 Módosítások

9.12.1 Módosítási eljárás

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

A módosítási eljárással kapcsolatos megkötések a Szabályzatban kerülnek kifejtésre.

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 Szolgáltatási Rend újabb verziói minden esetben új azonosítóval kerülnek kiadásra.

9.13 Vitás kérdések rendezése

A Szolgáltató törekszik a vitás kérdések tárgyalás útján történő rendezésére.

Amennyiben a tárgyalások – annak megkezdésétől számított - 30 (harminc) napon belül nem vezetnek eredményre, úgy a Felek a Polgári Perrendtartásról szóló 1952. évi III. törvény általános szabályai szerint illetékességgel és hatáskörrel rendelkező bírósághoz fordulnak.

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 Unió, 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 jogosultságukat 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

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.

Figyelem! Jelen dokumentumnak a <https://www.mobilsign.com> oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.

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 katasztrófa helyzetnek 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.

Készítésért felelős:	Jóváhagyta:
Dohányos Péter biztonsági tisztviselő	Csik Balázs Inf. Rendsz. Fel. Vez.
Készítés dátuma: 2018.03.20.	Jóváhagyás dátuma: 2018.03.26.
Figyelem! Jelen dokumentumnak a https://www.mobilsign.com oldalon publikált, illetve az aláírt példányai tekinthetők hitelesnek.	