NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
H-1081 Budapest, Csokonai utca 3.

Bizalmi Szolgáltatási Szabályzat tárolt kulcsos elektronikus aláírás és elektronikus bélyegző elhelyezés szolgáltatáshoz (BSZ-NISZ-TKASZ)

Verziószám	1.1
OID	0.2.216.1.200.1100.100.42.3.8.30.1.1
Hatályba lépés dátuma	2020.10.11.
Dokumentum besorolása	nyilvános

Dátum:
2020.10.01
06:33:38 +02'00'

NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
H-1081 Budapest, Csokonai utca 3.

Változáskövetés

verzió	dátum	a változás leírása	készítette	ellenőrizte	jóváhagyta
0.9	2018.08.01	Kiinduló változat	Polysys Kft.		
0.92	2019.06.03	Egyeztetett KDÜ változat	Polysys Kft.	Kővári Ferenc	
0.93	2020.07.09	KEASZ-WS-el bővített változat	Polysys Kft.		
0.94	2020.07.22	Termékfejlesztés által módosított és belső egyeztetésre megküldött változat	Németh Ágota	Kővári Ferenc	
1.0	2020.07.31	Első induló változat	Németh Ágota	Kővári Ferenc	Adorján István
1.1	2020.09.10	NMHH észrevételei alapján módosított változat	Polysys Kft.	Kővári Ferenc	Adorján István

Tartalomjegyzék

1 BEVEZETÉS

Jelen dokumentum a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt. Bizalmi Szolgáltatási Szabályzata, mely a tárolt kulcsos elektronikus aláírás és elektronikus bélyegző elhelyezés szolgáltatására vonatkozik (továbbiakban: BSZ-NISZ-TKASZ).

A {J7} 84/2012. (IV. 21.) Korm. rendelet 4. § több olyan, elektronikus dokumentumok hitelesítésére irányuló, a Kormány által kötelezően biztosított szabályozott elektronikus ügyintézési szolgáltatást (továbbiakban: SZEÜSZ) és központi elektronikus ügyintézési szolgáltatást (továbbiakban: KEÜSZ) határoz meg, melyeknél az elektronikus aláírások és bélyegzők létrehozásához szükséges kriptográfiai műveletek elvégzése bizalmi szolgáltatásban tárolt magánkulcsok felhasználásával is történhet:

h) központi dokumentumhitelesítési ügynök (továbbiakban: KDÜ);
k) Kormányzati Elektronikus Aláíró WEB-szolgáltatás (továbbiakban: KEASZ-WS).

A NISZ-TKASZ szolgáltatást (továbbiakban: Szolgáltatás) a NISZ Nemzeti Infokommunikációs Szolgáltató Zrt., mint a jogszabályban kijelölt kormányzati hitelesítés-szolgáltató (továbbiakban: Szolgáltató), az előző bekezdésben meghatározott SZEÜSZ/KEÜSZ-ökhöz (továbbiakban együttesen: TK-EÜSZ) kapcsolódóan nyújtja a vele szerződéses viszonyban levő Előfizetők számára.

A Szolgáltatást a {J2} E-ügyintési tv. 1. § 17. pontjában megnevezett, elektronikus ügyintézést biztosító szervek, továbbá költségvetési szervek, vagy egyéb, állami közfeladatot ellátó szervek vehetik igénybe. A Szolgáltatásban használt, elektronikus aláírás/bélyegző létrehozásához használt adatokat (magánkulcsokat) Szolgáltató az erre a célra szolgáló, elkülönített HSM komponensben (továbbiakban: TKASZ-HSM) tárolja. A Szolgáltatást az Előfizető egy adott informatikai rendszerében (továbbiakban: Szakrendszer), az adott TK-EÜSZ interfész specifikációja (továbbiakban: Interfész Specifikáció) szerint megvalósított gépi interfészen keresztül veheti igénybe. A Szolgáltatás igénybevétele során a Felhasználó (Aláíró vagy Bélyegző Létrehozó) a hozzá rendelt magánkulcsát távolról tudja aktiválni, így a Szakrendszeren keresztül képes az elektronikus aláírás/bélyegző létrehozásához szükséges, a vonatkozó nemzetközi szabvány[1] által meghatározott kriptográfiai művelet (továbbiakban: Kriptográfiai Művelet) távolból történő végrehajtására, a magánkulcshoz kapcsolódó minősített tanúsítvány felhasználásával.

A Kriptográfiai Művelet eredményének (a hitelesítendő dokumentum(ok) lenyomatának a magánkulccsal történő titkosításával előállított digitális jelsorozat) és a TK-EÜSZ felhasználásával, a Felhasználó a {J9} 137/2016. (VI. 13.) Korm. rendeletben (illetve a {J10} 1506/2015/EU rendelet mellékletében) meghatározott technikai specifikációknak megfelelő, minősített tanúsítványon alapuló, fokozott biztonságú elektronikus aláírásokat, illetve bélyegzőket hoz létre a távolból.

A NISZ-TKASZ szolgáltatásban tárolt magánkulcsok hitelesítéséhez minősített tanúsítványt kell igényelni a NISZ Zrt.-től, mely nem része a NISZ-TKASZ szolgáltatásnak. A minősített tanúsítványok igénylésére és kibocsátására a {D8} „Bizalmi Szolgáltatási Rend minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BR-MTT) és a {D9} „Bizalmi Szolgáltatási Szabályzat minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BSZ-MTT) dokumentum vonatkozik.

A Szolgáltatás csak azt követően használható, hogy a NISZ-TKASZ szolgáltatás keretében tárolt magánkulcsok hitelesítésére kibocsátott minősített tanúsítványok kiadása, illetve a Szolgáltatásban történő nyilvántartásba vétele megtörtént.

Szolgáltató a NISZ-TKASZ szolgáltatást nem minősített bizalmi szolgáltatásként valósítja meg és nyújtja az Előfizetők számára.

[1] {Sz11} RFC 8017

Jelen szolgáltatási szabályzat a Szolgáltatásra vonatkozó eljárási és működtetési szabályokat tartalmazza.

1.1 Áttekintés

Jelen szolgáltatási szabályzat a „Bizalmi Szolgáltatási Rend tárolt kulcsos elektronikus aláírás és elektronikus bélyegzés elhelyezés szolgáltatáshoz” (BR-NISZ-TKASZ) hatálya alá tartozó Szolgáltatásra vonatkozik.

A szolgáltatási szabályzat célja, hogy összefoglalja mindazokat az információkat, amelyeket a NISZ-TKASZ szolgáltatással kapcsolatba kerülő feleknek ismerni szükséges vagy érdemes. Biztosítja a Szolgáltató működésének átláthatóságát és annak megítélését az igénybe vevők számára, hogy az ismertetetett szolgáltatási gyakorlat mennyiben felel meg az elvárásaiknak.

Jelen dokumentum, valamint az 1.6.3 fejezetben hivatkozott jogszabályok, szabványok és műszaki specifikációk, továbbá a Szolgáltató 1.6.3.3 fejezetben felsorolt nyilvános dokumentumainak megismerése után a Szolgáltatás használói és a Szolgáltatásban létrehozott elektronikus aláírások/bélyegzők elfogadói egyértelműen meg tudják állapítani azok kezelésének módját, az általuk garantált biztonság mértékét, valamint a rájuk vonatkozó technikai, üzleti és pénzügyi garanciákat és jogi felelősségvállalásokat.

Jelen szolgáltatási szabályzat az {Sz1} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában követi annak előírásait. Az ott meghatározott felépítés szigorú megtartása érdekében azok a fejezetek is szerepelnek, melyeknél nincs követelmény előírva; ezekben a fejezetekben a „Nincs kikötés” vagy „Nem értelmezhető” szöveg szerepel.

Szolgáltató a jelen szolgáltatási szabályzat alapján nyújtott Szolgáltatást a Bizalmi Felügyeletnek 2020.07.31. napján jelentette be. A Bizalmi Felügyelet erre vonatkozó nyilvántartásának elérhetősége: http://webpub-ext.nmhh.hu/esign2016/index.jsp

1.2 Dokumentum neve és azonosítása

Jelen bizalmi szolgáltatási szabályzat teljes neve NISZ Zrt, „Bizalmi Szolgáltatási Szabályzat tárolt kulcsos elektronikus aláírás és elektronikus bélyegző elhelyezés szolgáltatáshoz”.

A szolgáltatási szabályzat rövid neve: BSZ-NISZ-TKASZ.

A szolgáltatási szabályzat objektum azonosítója és verziószáma a címlapon található.

Jelen BSZ-NISZ-TKASZ tartalmazza a BR-NISZ-TKASZ bizalmi szolgáltatási rend hatálya alatt létrehozott elektronikus aláírások/bélyegzők felhasználására vonatkozó részletes szabályokat. A szolgáltatási szabályzat hatályba lépését és hatályának megszűnését a 9.10 fejezet tartalmazza.

Jelen BSZ-NISZ-TKASZ-nak csak a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásokért felelős vezető elektronikus aláírásával ellátott változata tekinthető hitelesnek.

1.2.1 Bizalmi rendek

A BR-NISZ-TKASZ bizalmi szolgáltatási rend megfelel az {Sz3} TS 119 431-1 szabvány 4.3.2 és 5.2 fejezetében meghatározott alábbi hitelesítési rendnek:

```
LSCP: Lightweight SSASC Policy
itu-t(0) identified-organization(4) etsi(0) SIGNATURE CREATION SERVICE
-policies(19431) ops (1) policy-identifiers(1) lightweight (1)
```

1.3 PKI közösség

1.3.1 Hitelesítő szervezet

A hitelesítő szervezet a Szolgáltató központi szervezete, amely a szolgáltatás-támogató informatikai rendszer központi erőforrásaiból, az ezt körülvevő biztonságos fizikai környezetből, valamint az üzemeltető és szolgáltatást ellátó személyzetből áll.

1.3.2 SZEÜSZ Ügyfélszolgálat

A Szolgáltató – saját szervezetén belül – SZEÜSZ Ügyfélszolgálatot működtet.

A SZEÜSZ Ügyfélszolgálat végzi az ügyfelekkel való kapcsolattartást, a szerződéskötés előkészítését és közreműködik annak megkötésében, valamint gondoskodik a {D2} TKASZ Szolgáltatási Szerződésben foglaltak teljesítéséről.

1.3.3 Előfizetők és Felhasználók

Előfizető a Szolgáltatóval szerződéses viszonyban álló jogi személy vagy közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezet, amely – mint a {J2} E-ügyintézési tv. 1. § 17. pontja szerinti elektronikus ügyintézést biztosító szerv, vagy egyéb (költségvetési illetve állami közfeladatot ellátó) szerv - megrendeli a Szolgáltatótól a Szolgáltatást, jellemzően a tárolt magánkulccsal a Kriptográfiai Műveletek elvégzését - a TK-EÜSZ elektronikus aláírások vagy bélyegzők létrehozása során - az általa megnevezett Aláírók vagy Bélyegző Létrehozók (Felhasználók) számára:

a) Aláíró: az Előfizetővel kapcsolatban álló természetes személy, aki egy erre a célra kiadott tanúsítvány és a kapcsolódó elektronikus aláírás létrehozásához használt adat (a TKASZ-HSM-ben tárolt magánkulcs) felhasználásával távolról elektronikus aláírásokat hoz létre;

b) Bélyegző Létrehozó: az Előfizető szervezete, illetve annak valamely szervezeti egysége, amely az Előfizető által vagy nevében működtetett informatikai eszköz révén, egy erre a célra kiadott tanúsítvány és a kapcsolódó elektronikus bélyegző létrehozásához használt adat (TKASZ-HSM-ben tárolt magánkulcs) felhasználásával távolról elektronikus bélyegzőket hoz létre.

A Bélyegző Létrehozó kifejezés alatt - különösen a felelősségek és kötelezettségek vonatkozásában - Előfizető szervezetét, mint jogi személyt vagy közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezetet is érteni kell.

1.3.3.1 Előfizető Kapcsolattartója

A {D2} TKASZ Szolgáltatási Szerződés megkötése során az Előfizető kapcsolattartó személyt jelölhet meg, akit a képviseleti joggal rendelkező személy (pl. cégjegyzésre jogosult) felhatalmaz, illetve feljogosít a Szolgáltatással kapcsolatos ügyekben Előfizető szervezete nevében eljárni, akár meghatározott esetekre kiterjedő aláírási joggal is. Szolgáltató a későbbiekben ezen személy aláírását fogadja el a Szolgáltatással kapcsolatos ügyekben. Kapcsolattartó kijelölésének hiányában Szolgáltató csak a képviseleti joggal rendelkező személy (pl. cégjegyzésre jogosult) aláírását fogadja el a Szolgáltatással kapcsolatos ügyekben.

Jelen dokumentumban a továbbiakban az Előfizető Kapcsolattartója kifejezés a fentiek szerint kijelölt személyt, illetve kijelölés hiányában a képviseleti joggal rendelkező (pl. cégjegyzésre jogosult) személyt jelenti.

1.3.4 Érintett felek

Érintett Fél: a TK-EÜSZ elektronikus aláírással vagy bélyegzővel ellátott elektronikus dokumentumot – melyben a Szolgáltatásban elvégzett Kriptográfiai Művelet eredménye került elhelyezésre - fogadó természetes vagy jogi személy, aki/amely az elektronikus aláírásra vagy bélyegzőre hagyatkozva jár el a dokumentum hitelességének ellenőrzésekor.

1.3.5 Egyéb felek

Bizalmi Felügyelet

A Bizalmi Felügyelet ellátja a Szolgáltató és az általa nyújtott bizalmi szolgáltatások felügyeletét, ellenőrzi a szolgáltatások jogszabályi megfelelőségét. Többek között, figyelemmel kíséri a bizalmi szolgáltatásokkal kapcsolatos technológia és kriptográfiai algoritmusok fejlődését és határozatba foglalja a bizalmi szolgáltatók által a szolgáltatásaik nyújtása során használható biztonságos kriptográfiai algoritmusokat, és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket, továbbá jogerős és végrehajtható határozatában elrendelheti a Szolgáltatás felfüggesztését.

1.4 A Szolgáltatás alkalmazhatósága

A Szolgáltatás célja azon műszaki környezet és feltételek megvalósítása, amellyel a Felhasználó (Aláíró vagy Bélyegző Létrehozó) a magánkulcsát távolról aktiválja és hajtja végre az elektronikus aláírás/bélyegző létrehozásához szükséges, az {Sz11} RFC 8017 szerinti kriptográfiai műveleteket, melynek eredményeképpen minősített tanúsítványon alapuló, fokozott biztonságú elektronikus aláírásokat, illetve bélyegzőket hoz létre.

A Szolgáltatás önállóan nem, csak a TK-EÜSZ-höz integrált módon vehető igénybe.

Az elektronikus aláírás/bélyegző létrehozásának folyamata során a Felhasználó a Szolgáltatást távoli elektronikus aláírás/bélyegző létrehozó eszközként használja az Aláírás Értéknek (a hitelesítendő dokumentum(ok) lenyomatának a magánkulccsal történő titkosításával előállított digitális jelsorozatnak) a kiszámítására, valamint a TK-EÜSZ-t használja a kiszámított Aláírás Értéknek az elektronikus aláírás vagy bélyegző formátumban való elhelyezésére.

Így a Szolgáltatásban tárolt kulcsaik és a Szakrendszerük felhasználásával a Felhasználók a {J9} 137/2016. (VI. 13.) Korm. rendeletben (illetve a {J10} 1506/2015/EU rendelet mellékletében) meghatározott, alábbi technikai specifikációknak megfelelő elektronikus bélyegzőket, illetve aláírásokat hozhatnak létre:

- XAdES alapprofil: {Sz5} ETSI TS 103 171 v.2.1.1
- PAdES alapprofil: {Sz6} ETSI TS 103 172 v.2.2.2
- Aláírás-, illetve bélyegzőkonténer alapprofil: {Sz7} ETSI TS 103 174 v.2.2.1

Teszt szolgáltatás

A Szolgáltató - egyrészt saját rendszerének tesztelése céljából, másrészt azért, hogy Előfizetők a Szolgáltatást kipróbálhassák és az Interfész Specifikációnak megfelelően kialakított gépi interfészt tesztelhessék - teszt rendszert is fenntart és üzemeltet. A Szolgáltató semmilyen felelősséget nem vállal a teszt rendszer felhasználásáért, a hozzájuk kapcsolódó szolgáltatások rendelkezésre állásáért.

1.4.1 Engedélyezett használat

Felhasználók a Szolgáltatás keretében tárolt kulcsukat csak és kizárólag Előfizető elektronikus ügyintézést biztosító, vagy egyéb közfeladatot ellátó szervként végzett tevékenységével összefüggésben, a TK-EÜSZ-höz kapcsolódó Szakrendszerükkel használhatják elektronikus aláírás, illetve elektronikus bélyegző létrehozására.

A fentieken túl, a tárolt magánkulcsok csak a {D1} Általános Szerződési Feltételekben, illetve a {D2} TKASZ Szolgáltatási Szerződésben rögzített feltételekkel használhatók fel.

1.4.2 Tiltott használat

Tilos a tárolt kulcsot, illetve a hozzá kapcsolódó tanúsítványt felhasználni titkosításra vagy visszafejtésre, azonosításra, más tanúsítványok aláírására vagy bármilyen – Szolgáltatóval nem egyeztetett - bizalmi szolgáltatás nyújtásához.

Felhasználók a tárolt kulcsukat csak Előfizető elektronikus ügyintézést biztosító, vagy egyéb közfeladatot ellátó szervként végzett tevékenységéhez kapcsolódóan használhatják fel; a tárolt kulcsok bármilyen egyéb célra történő felhasználása tilos.

1.5 Szabályzat adminisztráció

1.5.1 Szabályzatot karbantartó szervezet

A Szolgáltató szervezetén belül Hitelesítési Rend és Szabályozási Csoportot működtet, amely többek között jelen bizalmi szolgáltatási szabályzat karbantartásáért is felelős.

1.5.2 Kapcsolat

Szolgáltató adatai

Szolgáltató neve:	NISZ Nemzeti Infokommunikációs Szolgáltató Zrt.
Cégjegyzék szám:	01-10-041633
Székhely:	1081 Budapest, Csokonai u.3.
Levélcím:	1389 Budapest, Pf.: 133.
Telefon:	+36 1 459-4200
Fax:	+36 1 303-1000
Internetes honlap címe:	www.nisz.hu

SZEÜSZ Ügyfélszolgálat

Az ügyfelekkel való kapcsolattartás érdekében a Szolgáltató SZEÜSZ Ügyfélszolgálatot tart fenn, amellyel az ügyfelek postai úton, valamint telefonon és emailen keresztül léphetnek kapcsolatba, nyitvatartási időben. A mindenkori nyitvatartási időket a Szolgáltató a Szolgáltatás alábbi internetes honlapján megtalálható {D1} Általános Szerződési Feltételekben teszi közé.

Telefon:	+36-1-550-3200
Email:	szeusztamogatas@1818.hu

Szolgáltatás internetes honlapja	https://nisz.hu/hu/nisz-tkasz
Postacím:	NISZ Zrt., SZEÜSZ Ügyfélszolgálat, 1389 Budapest, Pf. 133

Illetékes fogyasztóvédelmi felügyelőség

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

Illetékes békéltető testület

Budapesti Békéltető Testület

Cím:	1016 Budapest, Krisztina krt. 99. III, em.310.
Levelezési cím:	1253 Budapest, Pf.:20.
Telefon:	+36 1 488 2131
Email:	bekelteto.testulet@bkik.hu

1.5.3 Szabályzat alkalmasságának meghatározása

A Szolgáltató legalább évente egyszer megvizsgálja a bizalmi szolgáltatási rend, illetve a szolgáltatási szabályzat tartalmi és formai megfelelőségét a vonatkozó jogszabályok, előírások és műszaki szabványok tekintetében, és ennek eredményeit változtatási igényként figyelembe veszi.

A változtatási igényeket a Hitelesítési Rend és Szabályozási Csoport gyűjti, a módosításokat legalább évente egyszer elvégzi, majd ellenőrzésre és jóváhagyásra előterjeszti.

1.5.4 Szabályzat jóváhagyásának eljárása

Az ellenőrzésre, illetve jóváhagyásra a Szolgáltató belső szervezete, illetve a Szolgáltatásért felelős vezetője rendelkezik hatáskörrel és felelősséggel.

A jóváhagyás előtt a Szolgáltató megvizsgálja a szolgáltatási szabályzat bizalmi szolgáltatási rendnek való megfelelését.

A szolgáltatási szabályzat jogszabályoknak való megfelelőségét a Bizalmi Felügyelet is ellenőrzi.

A jóváhagyott szolgáltatási szabályzat a Szolgáltató elektronikus bélyegzőjével vagy a Szolgáltatásokért felelős vezető elektronikus aláírásával kerül hitelesítésre.

A jóváhagyott szolgáltatási szabályzatot Szolgáltató vezetése lépteti hatályba. A hatályba lépés napját a dokumentum címlapja tartalmazza.

A szolgáltatási szabályzat új verziója mindig új verziószámmal kerül nyilvánosságra és közzétételre a Szolgáltatás internetes honlapján.

Az új verzió kötelező érvényű az összes Előfizetőre, továbbá az abban foglalt változásokat javasolt figyelembe vennie az összes, a bizalmi szolgáltatási rend előző verzióinak hatálya alatt létrehozott elektronikus aláírásokat és bélyegzőket felhasználó Érintett Félnek.

1.6 Fogalmak, rövidítések és hivatkozások

1.6.1 Fogalmak

A jelen szabályzatban használt fogalmak értelmezése megegyezik a Szolgáltatásra vonatkozó jogszabályokban (1.6.3.1 fejezet) szereplő meghatározásokkal.

Az ezen felül alkalmazott fogalmak meghatározását a BR-NISZ-TKASZ bizalmi szolgáltatási rend 1.6.1 fejezete tartalmazza.

1.6.2 Rövidítések

AdES	Advanced Electronic Signature / Seal	fokozott biztonságú elektronikus aláírás vagy bélyegző, formátuma lehet PAdES (PDF aláírási formátum) vagy XAdES (XML aláírási formátum)
CHSM	Cloud HSM	felhő HSM
EIAD	az Egységes Infrastruktúra Active Directory szolgáltatása	
eDirectory	X.500-kompatibilis könyvtárszolgáltatási szoftver	
HSM	Hardware Security Module	hardver biztonsági modul, kriptográfiai eszköz
HTTPS	HyperText Transfer Protocol Secure	biztonságos hipertext átviteli protokoll
KDÜ	a {J7} 84/2012. (IV. 21.) Korm. rendelet 4. § h) pontjában meghatározott központi dokumentumhitelesítési ügynök	
KEASZ-WS	a {J7} 84/2012. (IV. 21.) Korm. rendelet 4. § k) pontjában meghatározott a Kormányzati Elektronikus Aláíró WEB-szolgáltatást megvalósító részszolgáltatás	
LSCP	Lightweight SSASC Policy	„könnyűsúlyú”, szerver oldali aláírási szolgáltatást megvalósító összetevőre vonatkozó szabályzat
NETHSM	Network HSM	hálózati HSM
PAdES	PDF Advanced Electronic Signature	PDF aláírási formátum
QSCD	Qualified Signature/Seal Creation Device	az eIDAS II. mellékletének megfelelő, minősített aláírást/bélyegzőt létrehozó eszköz
SCAL	Sole Control Assurance Level	kizárólagos irányítás biztosítási szintje
SCAL1	Sole Control Assurance Level 1	kizárólagos irányítás 1-es biztosítási szintje
SSA	Server Signing Application	szerver oldali aláírás létrehozó alkalmazás
SSASC	Server Signing Application Service Component	szerver oldali aláírási szolgáltatást megvalósító összetevő, amellyel az Aláíró

		vagy Bélyegző Létrehozó a TKASZ-HSM-ben tárolt magánkulcsa felhasználásával kiszámíttatja az Aláírás Értéket
SSASP	Server Signing Application Service Provider	a szerver oldali aláírási szolgáltatást megvalósító összetevőt működtető bizalmi szolgáltató
SIC	Signer's Interaction Component	aláíró közreműködését kiváltó összetevő
SZEÜSZ	szabályozott elektronikus ügyintézési szolgáltatás	
TKASZ	tárolt kulcsos aláírás szolgáltatás	
UTC	Coordinated Universal Time	koordinált univerzális idő
XAdES	XML Advanced Electronic Signature	XML aláírási formátum

1.6.3 Hivatkozások

1.6.3.1 Alkalmazandó jogszabályok

{J1} 910/2014/EU Európai Parlament és a Tanács rendelete a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről (továbbiakban: eIDAS)

{J2} 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól (továbbiakban: E-ügyintézési tv.)

{J3} A BIZOTTSÁG (EU) 2015/1502 végrehajtási rendelete (2018. szeptember 8.) az elektronikus azonosító eszközök biztonsági szintjeire vonatkozó minimális technikai specifikációknak és eljárásoknak a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 8. cikkének (3) bekezdése szerint történő megállapításáról (továbbiakban: 2015/1502/EU)

{J4} 2016. évi CXXX. törvény a polgári perrendtartásról (továbbiakban: Pp.)

{J5} 2013. évi V. törvény a Polgári Törvénykönyvről (továbbiakban: Ptk.)

{J6} 451/2016. (XII. 16.) Korm. rendelet az elektronikus ügyintézés részletszabályairól

{J7} 84/2012. (IV. 21.) Korm. rendelet egyes, az elektronikus ügyintézéshez kapcsolódó szervezetek kijelöléséről

{J8} 24/2016 (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

{J9}	137/2016 (VI. 13.) Korm. rendelet az elektronikus ügyintézés céljára felhasználható elektronikus aláíráshoz és bélyegzőhöz kapcsolódó követelményekről
{J10}	1506/2015/EU végrehajtási határozat a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról szóló 910/2014/EU európai parlamenti és tanácsi rendelet 27. cikkének (5) bekezdése és 37. cikkének (5) bekezdése szerint a közigazgatási szervek által elismert fokozott biztonságú elektronikus aláírások és bélyegzők formátumára vonatkozó műszaki specifikációk meghatározásáról
{J11}	679/2016/EU Európai Parlament és Tanács rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (továbbiakban: GDPR)

1.6.3.2 Szabványok és műszaki-technikai specifikációk

{Sz1}	RFC 3647	Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework
{Sz2}	EN 319 401	General policy requirements for Trust Service Providers
{Sz3}	TS 119 431-1	Policy and security requirements for Trust Service Providers; Part 1: TSP service components operating a remote QSCD/SCDev
{Sz4}	EN 419 241-1	Trustworthy Systems Supporting Server Signing; Part1: General System Security Requirements
{Sz5}	TS 103 171	XAdES Baseline Profile, v.2.1.1 (2012-03)
{Sz6}	TS 103 172	PAdES Baseline Profile, v.2.2.2 (2013-04)
{Sz7}	TS 103 174	ASiC Baseline Profile, v.2.2.1 (2013-06)
{Sz8}	MSZ/ISO/IEC 15408	ISO/IEC 15408 (parts 1 to 3): Information technology – Security techniques – Evaluation criteria for IT security
{Sz9}	ISO/IEC 19790	ISO/IEC 19790:2012: Information technology – Security techniques – Security requirements for cryptographic modules
{Sz10}	FIPS 140-2	FIPS PUB 140-2 (2001): Security Requirements for Cryptographic Modules
{Sz11}	RFC 8017	PKCS #1: RSA Cryptography Specification Version 2.2

1.6.3.3 Hivatkozott dokumentumok

{D1}	ÁSZF-TKASZ	Általános Szerződési Feltételek a NISZ Zrt. NISZ-TKASZ szolgáltatásához
{D2}	SZSZ-TKASZ	TKASZ Szolgáltatási Szerződés
{D3}		NISZ Zrt. Szervezeti és Működési Szabályzata

{D4}		NISZ Zrt. Adatvédelmi és adatbiztonsági előírásai
{D5}		NISZ Zrt. Informatikai biztonsági szabályzata
{D6}		NISZ Zrt. Üzletmenet-folytonossági terve
{D7}		NISZ-TKASZ kulcsgenerálási űrlap
{D8}	BR-MTT	Bizalmi Szolgáltatási Rend minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz
{D9}	BSZ-MTT	Bizalmi Szolgáltatási Szabályzat minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz
{D10}	ISPEC-TK-EÜSZ	NISZ-TKASZ szolgáltatást kiközvetítő TK-EÜSZ-re vonatkozó interfész specifikáció (Interfész Specifikáció)
{D11}	KDA-TKASZ	NISZ-TKASZ külső félre delegált autentikációs folyamatra vonatkozó követelmények
{D12}		NISZ Zrt. Személy-, objektum- és vagyonvédelmi szabályzata
{D13}	CSK-TK-EÜSZ	TK-EÜSZ Csatlakozási Kérelem

2 KÖZZÉTÉTEL

2.1 Szabályzatok elérhetősége

A Szolgáltató gondoskodik arról, hogy a Szolgáltatással kapcsolatos szabályzatok, valamint az egyéb közérdekű szolgáltatói információk az Előfizetők és Érintett Felek részére folyamatosan rendelkezésre álljanak. Szolgáltató az információk elérhetőségét az év minden napján, napi 24 órában, 99 %-os rendelkezésre állással biztosítja, úgy, hogy a kiesés nem lépheti túl esetenként a 24 órás időtartamot.

A Szolgáltató nem hozza nyilvánosságra azokat az érzékeny és/vagy bizalmas információkat tartalmazó dokumentációkat, melyek biztonsági intézkedéseket, eljárási szabályokat és belső biztonsági szabályzatokat tartalmaznak.

2.2 A szolgáltatói információ közzététele

A Szolgáltató a Szolgáltatással kapcsolatos szabályzatokat és az egyéb közérdekű szolgáltatói információkat a Szolgáltatás internetes honlapján teszi közzé.

2.3 A közzététel gyakorisága

Szolgáltató a Szolgáltatással kapcsolatos szabályzatokat azok változása esetén közzé teszi legalább 30 nappal a változás hatályba lépését megelőzően.

2.4 Hozzáférés-ellenőrzések

Szolgáltató olvasás céljára korlátozás nélküli hozzáférést biztosít a Szolgáltatással kapcsolatos szabályzatokhoz.

Szolgáltató biztonsági intézkedésekkel és eljárási szabályokkal gondoskodik az információk jogosulatlan megváltoztatása, törlése, sérülése és megsemmisülése elleni védelemről.

A Szolgáltatással kapcsolatos szabályzatoknak csak az elektronikus, aláírással vagy bélyegzővel ellátott formája tekinthető hitelesnek, a dokumentumok nyomtatott változatai semmilyen formában nem tekinthetők hivatalos példánynak vagy hiteles másolatnak.

3 AZONOSÍTÁS ÉS HITELESÍTÉS

3.1 Azonosítás és hitelesítés biztonsági szintje

Szolgáltató a NISZ-TKASZ szolgáltatást a TK-EÜSZ-höz kapcsolódó, nem minősített bizalmi szolgáltatásként nyújtja, melynek felhasználásával a Bélyegző Létrehozók, illetve az Aláírók olyan, minősített tanúsítványon alapuló fokozott biztonságú elektronikus bélyegzőket, illetve elektronikus aláírásokat hozhatnak létre a távolból, melyekben a Szolgáltatásban tárolt magánkulcsukkal elvégzett Kriptográfiai Művelet eredménye került elhelyezésre.

Szolgáltató a Szolgáltatás nyújtása során teljesíti az {Sz4} EN 419 241-1 szabvány 5.4 fejezete szerinti - a minősített elektronikus aláírásra és bélyegzőre vonatkozó biztonsági szintnél alacsonyabb - SCAL1 (Sole Control Assurance Level 1) biztonsági szinthez előírt valamennyi követelményt a Bélyegző Létrehozók, illetve az Aláírók azonosítása, jogosultságuk ellenőrzése, valamint a Kriptográfiai Művelet aktiválása során.

Szolgáltató a Bélyegző Létrehozók, illetve az Aláírók azonosítására, jogosultságuk ellenőrzésére, a Kriptográfiai Művelet aktiválására (továbbiakban: Autentikációs Folyamat) külső felet is igénybe vesz. Szolgáltató teljes körűen felel a külső fél tevékenységéért, és biztosítja, hogy a külső fél a jelen szabályzatban előírt, vonatkozó biztonsági követelményeket maradéktalanul teljesítse.

3.2 Bélyegző Létrehozók azonosítása és jogosultság ellenőrzése

Az elektronikus bélyegző létrehozására irányuló kérés fogadásakor Szolgáltató az Előfizető Autentikációs Tanúsítványának felhasználásával, a HTTPS protokoll szerinti PKI autentikációval azonosítja és hitelesíti a Bélyegző Létrehozót, mielőtt a TKASZ-HSM-ben tárolt kulcsát használhatná.

3.3 Aláírók azonosítása és jogosultság ellenőrzése

A NISZ-TKASZ szolgáltatás esetében az Aláírók csak olyan természetes személyek lehetnek, akik Előfizető szervezetével valamilyen kapcsolatban állnak, azaz például Előfizető szervezete által foglalkoztatott személyek, illetve képviseleti joggal rendelkező vagy cégjegyzésre jogosult személyek.

Szolgáltató a {D2} TKASZ Szolgáltatási Szerződés megkötését megelőzően ellenőrzi, hogy az adott Előfizető (illetve az általa használt Szakrendszer) által a természetes személyek azonosítására használt Autentikációs Folyamat megfelel a {D11} KDA-TKASZ külső félre delegált autentikációs folyamatra vonatkozó követelményrendszernek, valamint a Szakrendszer az Autentikációs Folyamatot megfelelően, az Interfész Specifikációban előírt műszaki és biztonsági követelmények betartásával használja. Előfizetővel a {D2} TKASZ Szolgáltatási Szerződés megkötésére csak azt követően kerül sor, hogy a fenti ellenőrzés maradéktalanul és sikeresen megtörtént, és erről bizonyítékok kerültek rögzítésre.

Az Autentikációs Folyamatot biztosító külső fél Delegált Autentikáció keretében azonosítja és hitelesíti az Aláírókat, mielőtt a Szakrendszer az elektronikus aláírás létrehozására irányuló kérést összeállítaná. A kérés Szolgáltatónak való megküldésekor a HTTPS kapcsolat felépítéséhez az Előfizető Autentikációs Tanúsítványát kell használni, Szolgáltató ellenőrzi, hogy az azonosított személy valóban Előfizető szervezetével kapcsolatban álló személy-e.

4 A SZOLGÁLTATÁS ÉS ÉLETCIKLUSA

4.1 Szolgáltatás igénylése

A Szolgáltatás igénylésének lépései a következők:

- A SZEÜSZ Ügyfélszolgálat tájékoztatja leendő Előfizetőt a Szolgáltatás igénylésével és használatával kapcsolatos információkról.
- Előfizető szervezet a {D13} TK-EÜSZ Csatlakozási Kérelem kitöltésével jelzi csatlakozási szándékát.
- Szolgáltató kialakítja és elérhetővé teszi Előfizető teszt rendszerhez való kapcsolódását, ennek során Előfizető számára teszt autentikációs, teszt aláíró és teszt bélyegző tanúsítványt bocsát ki.
- Előfizető a Szakrendszerében implementálja az Interfész Specifikációnak megfelelő, a Szolgáltatás igénybe vételéhez szükséges interfészt, elvégzi és jegyzőkönyvezi az integrációs teszteket.
- A sikeres integrációs tesztelést követően Szolgáltató ellenőrzi az integrációs tesztről készített jegyzőkönyveket, valamint ellenőrzi, hogy az adott Előfizető (illetve az általa használt Szakrendszer) által a természetes személyek azonosítására használt Autentikációs Folyamat megfelel a {D11} KDA-TKASZ külső félre delegált autentikációs folyamatra vonatkozó követelményrendszernek, valamint a Szakrendszer az Autentikációs Folyamatot megfelelően, az Interfész Specifikációban előírt műszaki és biztonsági követelmények betartásával használja.
- A SZEÜSZ Ügyfélszolgálat előkészíti és kiküldi Előfizetőnek a {D2} TKASZ Szolgáltatási Szerződést, valamint a minősített aláírás vagy bélyegzés célú tanúsítványszolgáltatásra vonatkozó {D9} BSZ-MTT szerinti Szolgáltatási Szerződést, melyekben Előfizető kapcsolattartót jelöl ki.
- Előfizető Kapcsolattartója kitölti a Szakrendszer autentikációs tanúsítványához szükséges tanúsítvány megrendelő és regisztrációs űrlapot, valamint a {D7} NISZ-TKASZ kulcsgenerálási űrlapot a végfelhasználók számára igényelt tárolt kulcsokra vonatkozóan. A {D7} űrlapok a {D2} TKASZ Szolgáltatási Szerződés mellékleteit képezik.
- Szolgáltató és Előfizető írásbeli szerződést kötnek egymással mindkét szerződés vonatkozásában. A {D13} TK-EÜSZ Csatlakozási Kérelem benyújtását és Szolgáltató általi befogadását követően, a {D2} TKASZ Szolgáltatási Szerződés megkötésekor vagy azt megelőzően Előfizető számára kibocsátásra kerül az Előfizető Autentikációs Tanúsítványa.
- A 6.1.1.2 fejezetben leírtak szerint történik meg az igényelt kulcspárok generálása Szolgáltató által, a TKASZ-HSM modulban, valamint megtörténik a PKCS#10 formátumnak megfelelő tanúsítványkérelmek előállítása, és a kérelmek megküldése Előfizető Kapcsolattartója részére.
- Előfizető Kapcsolattartója, illetve az Aláírók minden egyes igényelt tárolt kulcshoz kitöltenek egy {D9} BSZ-MTT szerinti tanúsítvány megrendelő és regisztrációs űrlapot, és ezeket, valamint a PKCS#10 tanúsítványkérelmeket benyújtják a NISZ Zrt. minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokat kibocsátó szolgáltatásának. A tanúsítvány kibocsátása nem része a NISZ-TKASZ szolgáltatásnak, a minősített tanúsítványok kibocsátását NISZ Zrt. különálló, minősített bizalmi szolgáltatásában végzi, melyre a {D8} „Bizalmi Szolgáltatási Rend minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BR-MTT) és a {D9} „Bizalmi Szolgáltatási Szabályzat minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BSZ-MTT) vonatkozik.

4.2 Szolgáltatás üzembe állítása

Felhasználók a Szolgáltatást csak azt követően használhatják, hogy a TKASZ-HSM modulban tárolt kulcspárjukhoz kapcsolódó, minősített tanúsítvány kibocsátása és nyilvántartásba vétele rendben megtörtént.

Ennek lépései a következők:

- az Előfizető részéről megigényelt minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványok kibocsátásra kerülnek a vonatkozó {D8} és {D9} szabályzatok szerint;
- a minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokat Előfizető regisztrálja a Szakrendszerben, illetve az Autentikációs Folyamatban;
- Előfizető beállítja, hogy a Szakrendszer a Szolgáltatás igénybe vétele során az Előfizető Autentikációs Tanúsítványát használja a HTTPS protokoll szerinti PKI autentikációra;
- ezzel párhuzamosan Szolgáltató is regisztrálja a minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokat a TKASZ-HSM modulba, és erről a SZEÜSZ Ügyfélszolgálat értesítést küld Előfizető részére;
- Szolgáltató a Szolgáltatás nyújtásához használt informatikai rendszerében regisztrálja Előfizető Autentikációs tanúsítványát, valamint megvalósítja a Kriptográfiai Műveletet aktivizáló adatok és a Felhasználók tárolt kulcsai közötti összekapcsolást.

Szolgáltató a Szolgáltatás teljes életciklusában biztosítja a tárolt kulcs és az ahhoz tartozó minősített tanúsítvány közötti összerendelés sértetlenségét.

4.3 Szolgáltatás elérhetősége és rendelkezésre állása

A Szolgáltatás az Interfész Specifikációban meghatározott web címen érhető el.

Szolgáltató a Szolgáltatás elérhetőségét az év minden napján, napi 24 órában, 99 %-os rendelkezésre állással biztosítja, úgy, hogy a kiesés nem lépheti túl esetenként a 48 órás időtartamot.

4.4 Szolgáltatás használata

A Szolgáltatás használatának előfeltétele a Felhasználó (Aláíró vagy Bélyegző Létrehozó) sikeres azonosítása és jogosultságának ellenőrzése. Az Aláíró azonosítása és jogosultságának ellenőrzése a 3.3 fejezetben, a Bélyegző Létrehozó azonosítása és jogosultságának ellenőrzése a 3.2 fejezetben leírt módon történik meg.

Felhasználók a Szolgáltatást úgy használhatják, hogy az Interfész Specifikációnak megfelelően összeállított kérést a Szakrendszerrel (a kérés összeállítása során a TKASZ-HSM-ben tárolt magánkulcsukat távolról aktiválják) beküldik a 4.3 fejezetben meghatározott web címre, majd erről a címről válaszként megkapják az általuk aktivált magánkulccsal létrehozott, elektronikus aláírással vagy elektronikus bélyegzővel hitelesített dokumentumot tartalmazó választ, melynek előállításához:

1) a TK-EÜSZ összeállítja a kért AdES formátumot;
2) a TK-EÜSZ a Szolgáltatást hívja meg, hogy a Felhasználó az aktivált magánkulcsával történő Kriptográfiai Művelet elvégeztesse, majd elhelyezi az így kapott Aláírás Értéket az AdES formátumban.

Az Interfész Specifikáció alapján a Szakrendszer azonosítását Szolgáltató a Szakrendszer számára kiadott autentikációs tanúsítvánnyal biztosítja. A kérés tartalmazza a Felhasználó aláírás vagy bélyegzés célú tanúsítványát is, a TKASZ-HSM modulban a megfelelő tárolt kulcs ez alapján

kerül kiválasztásra, a Kriptográfiai Műveletet aktivizáló adatok, valamint az aktivizáló adatok és a tárolt kulcs összerendelésének ellenőrzése után.

4.4.1 Kérés elfogadása vagy visszautasítása

Szolgáltató ellenőrzi a kapott kérés formai és tartalmi megfelelőségét.

Szolgáltató visszautasítja a kérést, ha:

- Előfizető (illetve az általa használt Szakrendszer) azonosítása és/vagy jogosultságának ellenőrzése sikertelen;
- a kérés nem felel meg az Interfész Specifikációban megjelölt műszaki- és biztonsági előírásoknak;
- a tárolt kulcshoz kapcsolódó tanúsítvány lejárt, visszavont vagy felfüggesztett;
- a kérésben a Kriptográfiai Művelet végrehajtásához megadott aláírási algoritmus a nemzetközi mértékadó szakmai dokumentumok szerint nem kellően erős a tárolt kulcshoz kapcsolódó tanúsítvány teljes érvényességi időszakában.

Szolgáltató elfogadja és kiszolgálja a kérést, ha a fenti ellenőrzések mindegyike sikeresen megtörtént.

4.5 Visszavonás és felfüggesztés

A Szolgáltatás igénybe vételét megszüntetni illetve szüneteltetni az egyes, a tárolt kulcshoz tartozó tanúsítványok visszavonásával, illetve felfüggesztésével lehetséges.

4.6 Előfizetés vége

Az előfizetés a {D2} TKASZ Szolgáltatási Szerződésben, illetve a {D1} Általános Szerződési Feltételek meghatározott esetekben és módon szűnik meg.

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

Szolgáltató a Szolgáltatás nyújtása során a kellő, az irányadó szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket és az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmazza.

Szolgáltató a rendszer kialakításakor kockázat elemzést végzett üzleti kockázatainak felmérésére, valamint a szükséges biztonsági követelmények és működési eljárások meghatározására; a kockázatok felülvizsgálatáról évente rendszeresen, valamint szükség esetén eseti jelleggel gondoskodik. Szolgáltató a szervezetén belüli biztonságkezeléshez szükséges informatikai biztonsági infrastruktúrát folyamatosan fenntartja. A biztonság szintjére hatást gyakorló bárminemű változtatást a Szolgáltató vezetősége hagy jóvá.

A biztonságkezelési szabályokat a Szolgáltató belső társasági dokumentumai - így különösen a {D5} A NISZ Zrt. Informatikai biztonsági szabályzata, valamint a {D12} NISZ Zrt. Személy-, objektum- és vagyonvédelmi szabályzata - tartalmazza. Ezek a szabályzatok biztonsági okokból nem nyilvánosak.

Szolgáltató megvalósította és folyamatosan fenntartja a Szolgáltatást nyújtó eszközök, rendszerek biztonsági ellenőrzéseit és üzemeltetési eljárásait. A Szolgáltató rendszeres belső ellenőrzései és külső auditjai révén ezen eljárásokat, a vonatkozó dokumentumokat és a Szolgáltatásra vonatkozó előírások teljesülését rendszeres időközönként vizsgálja.

A fenti eljárásokat a Szolgáltatóval munkaviszonyban álló, megbízható és szakértő üzemeltető személyzet biztosítja.

Szolgáltató gondoskodik arról, hogy eszközei és információi a megfelelő szintű védelemben részesüljenek. Szolgáltató valamennyi informatikai értékéről leltárt vezet, ezek védelmi követelményeit az elvégzett kockázatelemzéssel összhangban osztályokba sorolja és minősíti. A Szolgáltató az informatikai értékekről vezetett leltárt jelentős változás esetén a változáskor, egyébként legalább évente egyszer felülvizsgálja.

Szolgáltató a Szolgáltatás nyújtásában közreműködő informatikai rendszereit, berendezéseit és eszközeit a legmagasabb védelmi szintet képező központi géptermeiben, illetve helyszínein helyezi el.

5.1 Fizikai óvintézkedések

5.1.1 Telephely elhelyezése és szerkezeti felépítése

A Szolgáltató a Szolgáltatás nyújtásában közreműködő informatikai rendszereit fizikai és logikai védelemmel ellátott, legmagasabb védelmi szintet képező objektumaiban helyezte el és üzemelteti. Az objektumok elhelyezése és kialakítása során olyan egymásra épülő és egymást támogató védelmi megoldásokat alkalmaz, melyek képesek megakadályozni az illetéktelen hozzáférést és alkalmasak az informatikai rendszerek és Szolgáltató által tárolt bizalmas adatok megóvására.

5.1.2 Fizikai hozzáférés

A Szolgáltató megvédi a Szolgáltatás nyújtásában közreműködő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében.

Ehhez biztosítja az alábbiakat:

- a gépterembe történő minden belépés naplózásra kerül;
- a gépterembe csak a bizalmi szerepkört betöltő, erre feljogosított munkatárs léphet be, azonosítást követően;
- önálló jogosultsággal nem rendelkező személy csak indokolt és engedélyezett esetben, a szükséges időtartamig tartózkodhat a gépteremben, megfelelő jogosultságú kísérő személy állandó felügyelete mellett;
- az eszközök aktivizáló adatai (jelszavak, PIN kódok, stb.) a géptermen belül sem tárolhatók nyílt formában;
- jogosulatlan személy jelenlétében:
    - a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva tartják;
    - a bejelentkezett terminálok nem maradnak felügyelet nélkül;
    - nem végeznek olyan munkafolyamatot, amely során bizalmas adat felfedésre kerülhet;
- a gépterem elhagyásakor ellenőrzésre kerül:
    - minden eszköz és berendezés megfelelően biztonságos üzemállapotban van;
    - minden terminálon megtörtént a kijelentkezés;
    - a fizikai tároló eszközök megfelelően elzárásra kerültek;
    - a fizikai védelmet biztosító rendszerek és berendezések megfelelően működnek.

5.1.3 Áramellátás és légkondicionálás

A Szolgáltató a gépteremben olyan szünetmentes áramellátó rendszert alkalmaz, amely:

- megfelelő teljesítménnyel rendelkezik a gépterem informatikai és kisegítő létesítményi berendezései áramellátásának biztosítására;
- megvédi az informatikai berendezéseket a külső hálózat feszültség ingadozásai, feszültség kimaradásai és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramellátó berendezés biztosítja - üzemanyag utántöltéssel - tetszőlegesen hosszú időtartamig az áramellátást.

Szolgáltató a gépteremben olyan légkondicionáló berendezést alkalmaz, mely biztosítja az alábbiakat:

- az operátorok biztonságos munkavégzéséhez szükséges mennyiségű oxigén biztosított;
- a levegő nedvességtartalma nem haladja meg az informatikai rendszerek által megkívánt szintet;
- hűtés történik a szükséges üzemi hőmérséklet biztosítására, az eszközök és berendezések túlhevülésének megakadályozására

5.1.4 Beázás és elárasztás veszélyeztetettség

Szolgáltató megvédi a géptermet a beázástól, víz betöréstől és elárasztástól nedvességérzékelő és riasztó rendszer alkalmazásával.

5.1.5 Tűzmegelőzés és tűzvédelem

Szolgáltató a géptermet füst- és tűzérzékelőkkel szerelte fel, melyek automatikusan riasztják az illetékes személyzetet. Minden helyiségben jól látható helyen van elhelyezve a vonatkozó előírásoknak megfelelő típusú és mennyiségű tűzoltó készülék. A gépteremben automatikus

tűzoltó rendszer került kialakításra, amely emberi egészségre nem veszélyes és nem károsítja az informatikai eszközöket.

5.1.6 Adathordozók tárolása

Szolgáltató megvédi valamennyi adathordozóját a jogosulatlan hozzáféréstől, a megsemmisüléstől vagy véletlen rongálódástól, jellemzően páncélszekrénybe történő elzárással.

5.1.7 Selejt kezelése és megsemmisítése

Szolgáltató a környezetvédelmi előírások betartásával gondoskodik feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről. A felesleges eszközök és adathordozók az erre kijelölt munkatárs személyes felügyelete mellett, széleskörűen elfogadott módszerekkel kerülnek használhatatlanná tételre vagy visszaállíthatatlan módon törlésre.

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

Szolgáltató azt az adatmentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható, olyan külső helyszínen tárolja, mely megfelelő fizikai és működési védelemmel rendelkezik. Biztosítja helyszínek között a mentett adatok biztonságos továbbítását.

Az adatmentést, vagy abból a helyreállítást rendszerüzemeltető bizalmi munkakört betöltő személy végzi el.

5.2 Eljárásbeli előírások

A Szolgáltató gondoskodik arról, hogy informatikai rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltessék. Szolgáltató személyzete a feladatokat olyan eljárásbeli előírások alapján végzi, melyek szinkronban vannak a jogszabályi, szabványi és belső biztonsági előírásokkal.

Az eljárásbeli szabályokat a következő szabályzatok tartalmazzák:

- {D3} a Szolgáltató Szervezeti és Működési szabályzata, mely meghatározza a Szolgáltató szervezeti felépítését, azon belül az egyes szervezetekhez kapcsolt feladat-, felelősség- és hatásköröket;
- jelen szolgáltatási szabályzat, mely a Szolgáltató és a PKI közösség (Előfizetők, Felhasználók, Érintett Felek, stb.) viszonyát szabályozza.

5.2.1 Bizalmi munkakörök

Szolgáltató az alábbi bizalmi munkaköröket azonosította, melyektől a Szolgáltatás biztonsága függ:

a) a Szolgáltató informatikai rendszeréért általánosan felelős vezető;

b) biztonsági tisztviselő: a szolgáltatás biztonságáért általánosan felelős személy;

c) rendszeradminisztrátor: az informatikai rendszer telepítését, konfigurálását, karbantartását végző személy;

d) rendszerüzemeltető: az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy;

e) 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 bizalmi munkakörökhöz tartozó feladatkörök és felelősségek leírását a Szolgáltató belső, nem nyilvános biztonsági szabályzata tartalmazza. A bizalmi munkakört betöltő személy munkaviszonyban áll a Szolgáltatóval. Bizalmi munkakörbe Szolgáltató felső vezetősége nevezi ki a munkatársakat. Minden bizalmi munkakört legalább két személy tölt be.

A bizalmi munkakörökön kívül Szolgáltató bizalmi szerepköröket is alkalmaz a Szolgáltatás nyújtásához szükséges feladatok hatékony ellátása céljából. A bizalmi szerepkört betöltő személyek munkaviszonyban állnak a Szolgáltatóval.

A bizalmi munkaköröket és szerepköröket betöltő személyekről Szolgáltató nyilvántartást vezet. A bizalmi munkaköröket tartalmazó nyilvántartásban bekövetkező minden változást a változtatás bevezetése előtt a Bizalmi Felügyeletnek bejelenti.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Szolgáltató {D5} biztonsági szabályzata előírja, hogy csak védett környezetben, legalább kettő, bizalmi munkakört betöltő munkatárs egyidejű jelenléte mellett, illetéktelen személy jelenlétét kizárva végezhetők el az alábbi műveletek:

- az előfizetői kulcspár előállítására szolgáló TKASZ-HSM modul üzembe helyezése;
- a Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok előállítása és egyéb kulcsgondozási funkciói.

5.2.3 Bizalmi munkakörökben elvárt azonosítás és hitelesítés

A bizalmi munkaköröket betöltő személyek azonosítása és hitelesítése erős PKI eljárásokkal, pl. tokenen tárolt tanúsítványok és az azt aktivizáló PIN kód megadásával történik meg, mielőtt a Szolgáltatás nyújtásában érintett kritikus informatikai rendszerekhez hozzáférhetnének.

5.2.4 Egymást kizáró munkakörök

Szolgáltató biztosítja, hogy a bizalmi munkakörök vonatkozásában:

a) biztonsági tisztviselő nem láthatja el a független rendszervizsgáló, a rendszeradminisztrátor, és az informatikai rendszerért általánosan felelős vezető feladatait;
b) a független rendszervizsgáló nem láthatja el az informatikai rendszerért általánosan felelős vezető, és a rendszeradminisztrátor feladatait;
c) megvalósítja a bizalmi munkakörök teljes személyi szétválasztását.

5.3 Személyzetre vonatkozó előírások

Szolgáltató gondoskodik arról, hogy a személyzeti előírásai, a munkatársak alkalmazására vonatkozó gyakorlatai fokozzák és támogassák a Szolgáltató működésének megbízhatóságát.

Szolgáltató kellő számú, a Szolgáltatás nyújtásához szükséges feladatok jellegének, terjedelmének és mennyiségének megfelelő végzettséggel, képzettséggel, szakmai tudással és tapasztalattal rendelkező személyzetet alkalmaz.

Szolgáltató valamennyi bizalmi munkakört betöltő munkatársa mentes minden olyan ütköző érdektől, ami hátrányosan érinthetné a Szolgáltatás megbízhatóságát és biztonságát.

A munkatársak a feladatok szétválasztása és a legkisebb meghatalmazás szempontjai alapján meghatározott munkaköri leírásokkal rendelkeznek.

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

Szolgáltató biztosítja, hogy bizalmi munkakört csak olyan személyek töltsenek be, akiknek a bizalmi munkakör betöltéséhez szükséges befolyásmentességét és szakértelmét erkölcsi bizonyítvánnyal, szakmai gyakorlattal, végzettséggel és szakképesítéssel igazolni tudja.

A Szolgáltató informatikai rendszeréért általánosan felelős vezető kinevezéséhez szakirányú felsőfokú végzettséggel és legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal rendelkezik. Szakirányú felsőfokú végzettség a matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség.

A biztonsági tisztviselők és rendszervizsgálók esetén szakirányú közép- vagy felsőfokú végzettség, középfokú végzettség esetén legalább három, felsőfokú végzettség esetén legalább egy év informatikai biztonsággal összefüggésben szerzett szakmai gyakorlat szükséges.

A rendszerüzemeltető és rendszeradminisztrátor esetén középfokú szakirányú végzettség és legalább egy év, hasonló munkakörben szerzett szakmai gyakorlat szükséges.

Az egyes bizalmi munkakörök betöltéséhez elvárt szakirányú végzettségek meghatározását a Szolgáltató belső, nem nyilvános szabályzata tartalmazza.

5.3.2 Biztonsági háttér ellenőrzés eljárásai

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

- büntetlen előélettel rendelkeznek és nincs ellenük folyamatban olyan eljárás, ami a büntetlenséget befolyásolhatja (a büntetlen előéletet három hónapnál nem régebbi erkölcsi bizonyítvánnyal kell igazolni);
- nem állnak a bizalmi szolgáltatási tevékenység gyakorlását kizáró foglalkoztatástól eltiltás hatálya alatt.

Szolgáltató ellenőrzi a felvételi eljárásban benyújtott önéletrajzban megadott, releváns információkat.

Az 5.2.1 fejezetben meghatározott bizalmi munkakör betöltését a legmagasabb szintű biztonsági ellenőrzés (a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényben meghatározott nemzetbiztonsági ellenőrzés) előzi meg. A többi, a Szolgáltatás nyújtásával kapcsolatos munkakörben, a munkakör betöltését fokozott szintű, a Szolgáltató által végzett biztonsági ellenőrzés előzi meg. Mind a legmagasabb, mind a fokozott biztonsági ellenőrzés lefolytatásához szükséges az érintett személy hozzájárulása. Nem tölthet be bizalmi munkakört az a személy, akinél a biztonsági ellenőrzés kockázatot tár fel.

A bizalmi munkakörhöz történő hozzárendeléskor az érintett személy:

- pontos és írásos munkakör leírást vesz át a fölérendelt vezetőtől vagy a Szolgáltató humán szervezetétől;

- titoktartási nyilatkozatot kell aláírnia, melyben három év titoktartási kötelezettség szerepel a kilépés időpontjától számítva;
- szükséges mértékű oktatásban részesül, annak érdekében, hogy a feladat-, felelősség és hatáskörét pontosan megismerje és gyakorolni tudja.

Kilépéskor:

- A kilépésről szóló döntés meghozatalakor a kilépő fizikai és logikai belépési és hozzáférési jogosultságai megszüntetésre kerülnek. Ezt követően, a kilépő személy csak biztonsági tisztviselő kíséretében léphet be a Szolgáltatással kapcsolatos körletekbe.
- vissza kell venni az azonosításhoz és hitelesítéshez használt eszközét, és dokumentáltan meg kell semmisíteni azt. A kapcsolódó tanúsítványokat vissza kell vonni.

5.3.3 Képzési követelmények

A bizalmi munkakörökben Szolgáltató olyan személyeket foglalkoztat, akik az adott munkakör vagy szerepkör ellátásához szükséges mértékben elsajátították:

- a PKI elméletet;
- Szolgáltató informatikai rendszerének sajátosságait és kezelésének módját;
- a szerepkör ellátáshoz szükséges speciális ismereteket;
- Szolgáltató nyilvános és belső szabályzataiban meghatározott folyamatokat és eljárásokat;
- az egyes tevékenységek jogi következményeit;
- az alkalmazandó biztonsági szabályokat.

A Szolgáltató éles informatikai rendszereihez csak a képzést elvégző alkalmazottak kaphatnak hozzáférési jogosultságot.

5.3.4 Továbbképzési gyakoriságok és követelmények

Szolgáltató gondoskodik arról, hogy a munkatársak folyamatosan a megfelelő tudással rendelkezzenek, szükség esetén továbbképzést vagy ismétlő jellegű képzést tart.

Szolgáltató minden lényeges változás esetén megismétli az érintett személyek részére a képzést vagy annak elemeit.

Jelentős változás, azaz a szervezeti biztonságpolitika módosulása, a szoftver vagy hardver változása (upgrade), valamint a kulcs kezelés és biztonság kezelési óvintézkedések változása esetén, valamennyi munkatárs, az őt érintő mélységben továbbképzésben részesül, illetve megkapja a szükséges dokumentációkat.

Kisebb változások esetén a munkatársak a változás bekövetkezte előtt írásos tájékoztatást kapnak.

Szolgáltató rendszeresen (pl. évente egyszer) továbbképzést biztosít az újonnan ismertté vált sebezhetőségekről, az IT biztonság aktuális gyakorlatáról, a munkatársak saját szakterületét érintően.

5.3.5 Felhatalmazás nélküli tevékenységek büntető következményei

Szolgáltató a dolgozóval kötött munkaszerződésben szabályozza a dolgozó felelősségre vonásának lehetőségét a dolgozó által elkövetett mulasztások, vétlen vagy szándékos károkozás esetére.

5.3.6 Szerződéses munkavállalókra vonatkozó követelmények

Szolgáltató bizalmi munkakörben csak munkaviszonyban álló személyt foglalkoztat.

Az egyéb feladatok ellátására, vállalkozási vagy megbízásos szerződés keretében a beszállítóval Szolgáltató írásos megállapodást köt. A szerződő fél titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a szerződés teljesítésében közreműködő személyek a munkavégzés során birtokukba kerülő üzleti titkokat és bizalmas információkat illetéktelen személynek fel nem fedik, más módon sem hasznosítják, és amely tartalmazza a megszegése esetén alkalmazott szankciókat.

5.3.7 A személyzet számára biztosított dokumentációk

Szolgáltató folyamatosan biztosítja a személyzet részére a munkakörük ellátásához szükséges dokumentációk és szabályzatok rendelkezésre állását.

Minden bizalmi munkakört betöltő munkatárs megkapja írásban:

- egyéni munkaköri leírást;
- a Szolgáltató szervezeti és biztonsági szabályzatait;
- rendszeres és rendkívüli továbbképzések alkalmával az adott oktatási formához tartozó oktatási segédanyagokat.

5.4 A biztonsági naplózás folyamatai

5.4.1 Naplózott esemény típusok

Szolgáltató naplóz minden, az informatikai rendszerével és Szolgáltatás nyújtásával kapcsolatos eseményt. A naplózott adatállomány átfogja a szolgáltatás nyújtásának teljes folyamatát, és lehetővé teszi, hogy a valós helyzetek megítéléséhez a szükséges mértékben minden, a Szolgáltatással kapcsolatos eseményt rekonstruálni lehessen.

Az informatikai rendszerrel kapcsolatos események különösen a rendszer indítás és leállítás, biztonsági profil változása, rendszer összeomlás és hardver hibák, tűzfal aktivitás, hozzáférési kísérletek, szolgáltatói kulcs kezelés eseményei, óraszinkronizációs események, naplózási funkció elindítása és leállítása, naplózási paraméterek megváltoztatása, naplóadatok tárolásával kapcsolatos hibák, napló adatok integritásának sérülése eseményei.

A Szolgáltatás nyújtásával kapcsolatos események különösen az alábbiak:

- a Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok életciklusával kapcsolatos minden esemény;
- Előfizető tárolt kulcspárja életciklusával kapcsolatos minden esemény;
- a Szolgáltatásban kapott kérések és válaszok;
- Előfizető tárolt kulcspárja használatának eseményei.

A naplózott adatállomány tartalmazza a naplózott esemény bekövetkeztének dátumát és pontos időpontját, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az esemény kiváltásában közreműködő felhasználó vagy más személy nevét vagy azonosítóját.

5.4.2 Naplóállomány feldolgozásának gyakorisága

Szolgáltató biztosítja a naplóállományok rendszeres ellenőrzését és kiértékelését.

A Szolgáltatás nyújtásával kapcsolatos események naplóállományait naponta feldolgozzák a rendszervizsgálók.

Az informatikai rendszer eseményeinek naplóállományait a rendszervizsgálók rendszeres időközönként, a biztonsági szabályzatban meghatározott sűrűséggel végzik el.

5.4.3 Naplóállomány megőrzési időtartama

Szolgáltató a naplóállományokat archiválja és gondoskodik azok biztonságos megőrzéséről az 5.5.2 fejezetben előírt időtartamig. Ezen időtartamig Szolgáltató biztosítja az archivált állományok olvashatóságát, megőrzi az ehhez szükséges hardver és szoftver eszközöket.

5.4.4 Naplóállomány védelme

Szolgáltató a naplóállományokat és azok mentéseit biztonságos, fizikailag is védett környezetben tárolja. A naplóállományokat időbélyegzővel, a naplóállományok archív mentéseit időbélyegzőt is tartalmazó elektronikus aláírással vagy bélyegzővel látja el.

Szolgáltató gondoskodik arról, hogy a naplóállományokhoz és azok mentéseihez csak az arra feljogosított személyek férhessenek hozzá.

5.4.5 Naplóállomány mentési folyamatai

A naplóállományokról Szolgáltató rendszeres mentést készít. A mentéssel kapcsolatos eljárásokat és szabályokat a Szolgáltató belső szabályzata tartalmazza.

5.4.6 Naplózás gyűjtési rendszere

A naplóbejegyzések gyűjtését belső komponens oldja meg. A naplóbejegyzések gyűjtése megkezdődik rendszer indításkor és rendszer leállításig folyamatosan működik, és közben biztosítja a gyűjtött bejegyzések integritását és rendelkezésre állását, szükség esetén a bizalmasságát is.

A naplóbejegyzések gyűjtési rendszerének működési rendellenessége esetén Szolgáltató felfüggeszti az érintett területek működését az üzemzavar elhárításáig.

5.4.7 Rendellenes eseményeket kiváltó alanyok értesítése

A rendellenes eseményeket kiváltó alanyokat (személyeket, szervezeteket) Szolgáltató nem feltétlenül értesíti minden esetben. Szolgáltató szükség esetén bevonhatja az eseményt kiváltó alanyt az esemény kivizsgálásába. Ilyen esetben az érintett Előfizető, Aláíró vagy Bélyegző Létrehozó kötelessége a Szolgáltatóval való együttműködés az esemény feltárása érdekében.

5.4.8 Sebezhetőség értékelések

Szolgáltató a vonatkozó szabványok által meghatározott rendszeres időközönként, a naplóállományok és egyéb információk kiértékelésén alapuló sebezhetőség vizsgálatot és behatolás tesztet végez, mely segítségével feltérképezi a potenciális belső és külső fenyegetéseket, melyek jogosulatlan hozzáférést eredményezhetnek vagy a Szolgáltatásban kezelt adatok megmásítását, módosítását, sérülését vagy megsemmisülését eredményezhetik.

A sebezhetőség vizsgálathoz kapcsolódóan Szolgáltató kockázatelemzésben értékeli az egyes fenyegetések bekövetkeztének valószínűségét és a bekövetkezés esetén várható kárt. Értékeli az alkalmazott folyamatokat, informatikai rendszereket, védelmi intézkedéseket, hogy azok megfelelően képesek-e ellenállni a fenyegetésnek.

A kiértékelést követően Szolgáltató megteszi a megfelelő intézkedéseket annak érdekében, hogy a feltárt sebezhetőség kihasználhatósága ne következzen be.

Szolgáltató folyamatosan figyelemmel kíséri az újonnan ismertté vált, kritikus sebezhetőségeket, és a szükséges ellenintézkedéseket lehetőség szerint 48 órán belül megteszi. Bármely olyan sebezhetőség esetén, melynek kihatása lehet a Szolgáltatás nyújtására, Szolgáltató vagy cselekvési tervet készít és hajt végre annak érdekében, hogy a sebezhetőség ne legyen kihasználható, illetve annak hatása elhanyagolható legyen, vagy dokumentálja annak ténybeli alapját, hogy az adott sebezhetőség nem igényel intézkedést.

5.5 Adatok archiválása

5.5.1 A tárolt adatok típusai

Szolgáltató gondoskodik arról, hogy megőrzésre kerüljön minden olyan információ, amely a Szolgáltató és a rendszereinek megfelelő működését alátámasztja.

Ehhez legalább az alábbi információkat tárolja papír alapon vagy elektronikusan:

- a Szolgáltatás igénylésével kapcsolatos minden adat vagy irat, különösen a {D2} TKASZ Szolgáltatási Szerződés, Előfizető által aláírt nyilatkozatok és átvételi elismervények;
- Előfizető tárolt kulcsával kapcsolatos valamennyi információ a teljes életciklusra vonatkozóan;
- a bizalmi szolgáltatási rend és szolgáltatási szabályzat valamennyi kibocsátott verziója;
- a {D1} Általános Szerződési Feltételek valamennyi kibocsátott verziója;
- a Szolgáltató működésével kapcsolatos alvállalkozói szerződések;
- valamennyi naplóállomány.

5.5.2 Archívum megőrzési időtartama

Szolgáltató az 5.5.1 fejezetben meghatározott archivált adatokat, az Előfizető tárolt kulcsához kapcsolódó tanúsítvány érvényességének lejáratáról számított 7 évig, illetve a tanúsítvánnyal előállított elektronikus aláírással vagy bélyegzővel kapcsolatos jogvita jogerős lezárásáig, szabályzatok, szerződések esetében a hatályon kívül helyezés vagy megszűnés utáni 7 évig őrzi meg.

5.5.3 Archívum védelme

Szolgáltató olyan fizikai védelmet biztosít és biztonsági óvintézkedéseket alkalmaz, melyek fenntartják az archivált adatok sértetlenségét, hitelességét, rendelkezésre állását és a bizalmasságát. Az elektronikus formában archivált adatokat Szolgáltató legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel, valamint minősített időbélyegzővel látja el.

5.5.4 Archívum mentési eljárásai

Szolgáltató a papír alapú iratokat, dokumentumokat a dokumentumtárban, az elektronikus állományokat pedig több példányban, fizikailag elkülönített helyszíneken őrzi meg, illetve tárolja.

Szolgáltató biztosítja az elektronikus formában archivált állományok adathordozóinak elavulás elleni védelmét a megőrzési időn belül.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi naplóbejegyzésben olyan időjel szerepel, amely a 6.8 fejezetben ismertetett időforrásokkal szinkronizált rendszeridőt tartalmazza, melynek pontossága egy másodpercen belüli.

Az elektronikus formában archivált adatokon elhelyezett elektronikus bélyegző minősített időbélyeget tartalmaz.

Szolgáltató az archivált adatok megőrzése során szükség esetén (pl. algoritmus váltás) gondoskodik az elektronikus aláírások vagy bélyegzők, valamint az időbélyegzők hitelességnek fenntartásáról.

5.5.6 Archívum gyűjtési rendszere

A naplóállományok és az egyéb elektronikusan keletkezett adatokat a Szolgáltató védett informatikai rendszerén belül gyűjti. A védett informatikai rendszerből történő kimozgatás során az adatok minősített időbélyeget tartalmazó elektronikus aláírással vagy bélyegzővel kerülnek hitelesítésre.

A papíralapú iratokat Szolgáltató elhelyezi a saját dokumentumtárában tárolás és megőrzés céljából.

5.5.7 Archívum hozzáférés és ellenőrzés eljárásai

Szolgáltató az archivált adatokat megvédi a jogosulatlan hozzáféréstől. Szolgáltató a jogosultságot ellenőrzi, és a hozzáféréseket naplózza.

Szolgáltató a SZEÜSZ Ügyfélszolgálat közreműködésével biztosítja az Aláírók számára a róluk tárolt személyes adatokra vonatkozó tájékoztatást.

Szolgáltató a 9.4.6 fejezetben ismertetett hatósági vagy jogi eljárásokban a szükséges mértékben a biztosítja a hozzáférést az archívumban tárolt adatokhoz.

5.6 Kulcs átállás

Amennyiben az előfizetői tárolt kulcsok algoritmusa, paraméterei vagy kulcshossza tekintetében olyan hirtelen elavulás következik be, amely miatt a tárolt kulcshoz tartozó tanúsítvány érvényességének lejárata előtt visszavonásra került, Előfizető új kulcspárt kell igényeljen.

5.7 Helyreállítás rendkívüli üzemi helyzetek esetén

Szolgáltató minden szükséges intézkedést meghoz annak érdekében, hogy rendkívüli üzemeltetési helyzet, katasztrófa esetén a szolgáltatás kiesésből származó károkat minimalizálja

és a Szolgáltatást a lehető legrövidebb időn belül helyreállítsa. A rendkívüli üzemeltetési helyzet bekövetkezése esetén a Szolgáltatással kapcsolatos szabályzatok és egyéb közérdekű szolgáltatói információk közzétételének helyreállítása minden más szolgáltatás vagy tevékenység helyreállítását megelőzi.

Incidens esetén - amennyiben az jelentős hatást gyakorol a szolgáltatásra vagy az annak keretében tárolt személyes adatokra -, Szolgáltató az esetről való értesüléstől számított 24 órán belül értesíti az Érintett Feleket, valamint jelenti az incidenst a Bizalmi Felügyeletnek.

A bekövetkezett incidens kiértékelése alapján Szolgáltató meghozza a szükséges módosító, javító intézkedéseket, hogy az incidens jövőbeli előfordulását megakadályozza.

5.7.1 Rendkívüli események és kompromittálódás kezelésének eljárásai

Szolgáltató rendelkezik {D6} üzletmenet folytonossági tervvel. Ez a dokumentum biztonsági okokból kifolyólag nem nyilvános.

A rendkívüli üzemeltetési helyzetben a Szolgáltató dokumentálja az eseményeket, azok körülményeit, az elhárításukra megtett intézkedéseket.

Rendkívüli üzemeltetési helyzetben Szolgáltató életbe lépteti az üzletmenet folytonossági tervében megtervezett eljárásait annak érdekében, hogy az üzemeltetés helyreálljon az üzletmenet folytonossági tervben megjelölt időn belül.

A helyreállítás időtartamát az esemény súlyossága, azaz az üzletmenet folytonossági terv szerint értelmezett osztályba sorolása határozza meg.

Szolgáltató kialakította és fenntartja azt a tartalék rendszert, mely a rendkívüli üzemeltetési helyzetben képes a nyilvános szabályzatok elérhetőségét közzétételét biztosítani.

A rendkívüli üzemeltetési helyzet határidőn túli fennállása esetén Szolgáltató haladéktalanul értesíti a Bizalmi Felügyeletet, az esemény bekövetkeztéről, annak hatásáról, várható időtartamáról, az elhárítás érdekében tett és tervezett intézkedésekről, továbbá a rendkívüli üzemeltetési helyzet megszűnéséről.

A rendkívüli üzemeltetési helyzetben Szolgáltató a lehető legrövidebb időn belül tájékoztatást tesz közzé internetes honlapján, valamint, lehetőség szerint, elektronikus levélben értesíti azokat a személyeket, akiket az esemény érint.

A biztonságot érintő vagy a sértetlenség megszűnését eredményező incidens esetén – amennyiben annak hátrányos kihatása van a Szolgáltatást igénybe vevő Előfizetőkre – Szolgáltató indokolatlan késedelem nélkül értesíti az érintett Előfizetőket.

5.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok

Szolgáltató olyan megbízható rendszert működtet, mely redundáns műszaki megoldásokkal, biztonsági mentésekkel és eljárásokkal a rendszerben bekövetkezett hiba esetén is biztosítja a Szolgáltatás működtetését és elérhetőségét. A pontos és részletes előírásokat és intézkedéseket az üzletmenet folytonossági terv, illetve a Szolgáltató belső szabályzatai tartalmazzák.

5.7.3 Előfizetői magánkulcsának kompromittálódása esetén követendő eljárás

Az előfizetői magánkulcsok kompromittálódása esetére akciótervvel rendelkezik, melyet az üzletmenet folytonossági tervében tervezett meg. E szerint megteszi az alábbi főbb lépéseket:

- megszünteti az érintett magánkulcsok használatát;
- értesíti Előfizető Kapcsolattartóját és kezdeményezi az érintett tanúsítványok visszavonatását;
- intézkedik valamennyi érintett fél értesítéséről.

5.7.4 Üzletmenet folytonosság helyreállás katasztrófát követően

Szolgáltató rendelkezik tartalék helyszínnel és informatikai rendszerrel, továbbá megtervezett eljárásokkal az áttelepülésre.

A súlyos üzemzavar és a katasztrófa eseteit - többek között - az különbözteti meg egymástól, hogy katasztrófa esetén nagy valószínűséggel nem csak az informatikai rendszer, hanem annak fizikai környezete is megsemmisül részben vagy egészben. Ez utóbbi esetben egy válságstáb az üzletmenet folytonossági tervben meghatározott módon intézkedik a tartalék helyszínre való áttelepülésről és ott az informatikai rendszer szükséges mértékű visszaállításáról a tartalék helyszínen korábban elhelyezett mentések segítségével.

5.8 A szolgáltatási tevékenység megszüntetése

Szolgáltató rendelkezik olyan bankgaranciával, mely fedezi a szolgáltatási tevékenység megszüntetésének költségeit abban az esetben, ha Szolgáltató csődeljárás alá kerül vagy más okból kifolyólag nem képes önmaga fedezni a költségeket. Ha Szolgáltató ellen felszámolási, végelszámolási vagy egyéb kényszertörlési eljárás indult, erről és a felszámolóról vagy végelszámolóról Szolgáltató haladéktalanul tájékoztatja a Felügyeleti Szervet.

Szolgáltató az alábbi, a szolgáltatási tevékenység megszüntetésére vonatkozó tervvel rendelkezik:

- A tervezett megszűnés előtt kellő időben tárgyalásokat kezdeményez más bizalmi szolgáltatókkal a Szolgáltatással járó kötelezettségek - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig - átadás-átvételéről.
- Szolgáltató gondoskodik a Szolgáltatás megszüntetéséből fakadó, a felhasználói közösséget érintő zavarok minimalizálásáról. Különösképpen gondoskodik a Szolgáltatással kapcsolatos nyilvános szabályzatok közzétételének folyamatos fenntartásáról.
- A megszüntetés előtt legalább 60 nappal korábban:
    - értesíti a Bizalmi Felügyeletet, és internetes honlapján tájékoztatja a felhasználói közösség tagjait;
    - megszünteti a nevében eljáró szerződött alvállalkozói összes felhatalmazását és jogosultságaikat megvonja, a velük kötött szerződéseket megszüntetni;
    - beszünteti az új Szolgáltatás igénylések fogadását;
    - egy másik bizalmi szolgáltatóval megállapodást köt a Szolgáltatással járó kötelezettségeknek átadás-átvételéről, és ennek másolatát megküldi a Bizalmi Felügyeletnek;
- A megszüntetés előtt legalább 20 nappal korábban:
    - Előfizető Kapcsolattartójának bevonásával kezdeményezi az összes tárolt kulcshoz kapcsolódó tanúsítvány visszavonatását;

- a Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsokat és azok mentéseit olyan módon semmisíti meg, hogy azok használata a továbbiakban már nem lehetséges;
- beszünteti a Szolgáltatással kapcsolatos nyilvános szabályzatok közzétételét és gondoskodik arról, hogy ezzel egyidejűleg azok az átvevő szolgáltatónál elérhetővé váljanak;

- A megszüntetés napjával:
  - Szolgáltató az informatikai rendszerében foglalt adatokról teljes körű, időbélyegzővel és elektronikus aláírással vagy bélyegzővel ellátott mentést készít. Szolgáltató a mentett adatállományokat védi a jogosulatlan módosítástól, és biztosítja, hogy az adatállomány tartalmához jogosulatlan személy nem férhet hozzá. Szolgáltató a megkötött szerződés révén biztosítja, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek.

6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

6.1.1.1 Szolgáltatói kulcsok előállítása

Szolgáltató a Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsokat fizikailag védett környezetben, az erre szolgáló HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, más személy jelenlétének kizárásával generálja. A kriptográfiai modul megfelel a 6.2.1 fejezet szerinti követelményeknek.

6.1.1.2 Előfizetői kulcspárok előállítása

Szolgáltató az előfizetői (felhasználói) kulcspárok előállítására szolgáló TKASZ-HSM modul üzembe helyezését szigorúan védett környezetben, legalább két bizalmi munkakört betöltő személy részvételével, illetéktelen személy jelenlétének kizárásával végzi, az előfizetői kulcspárok generálását megelőzően. A TKASZ-HSM modul megfelel a 6.2.1 fejezet szerinti követelményeknek.

Szolgáltató a 6.1.5 és 6.1.6 fejezetek szerinti algoritmusú és kulcshosszú előfizetői kulcspárt szigorúan védett környezetben, az erre szolgáló TKASZ-HSM modulban, szigorúan védett környezetben, kizárólag bizalmi munkakört betöltő személyek részvételével állítja elő.

[CHSM] A generálást követően az előfizető kulcspárok a Szolgáltató infrastrukturális kulcsain alapuló titkosított export állományban kerülnek tárolásra, majd a CHSM modulból törlésre kerülnek. A titkosításhoz használt szolgáltató infrastrukturális kulcs algoritmusa és hossza erősebb, mint az általa védett előfizetői kulcspárok algoritmusa, illetve hossza. A titkosított export állomány előállítása a CHSM modul erre szolgáló, tanúsítással rendelkező biztonsági funkciójával történik. A későbbiekben, az előfizetői magánkulcs aktiválása során, a kulcspárok CHSM modulba való visszatöltése (importálása) a CHSM modul erre szolgáló biztonsági funkciójával történik, az előfizetői kulcspárok használata a CHSM modulból történik.

[NETHSM] Az előfizetői kulcspárok teljes életciklusuk alatt a NETHSM modulban maradnak.

6.1.2 Magánkulcs eljuttatása a tulajdonoshoz

Az előfizetői kulcspárok a Szolgáltatás keretében a TKASZ-HSM modulban kerülnek előállításra, és abból kerülnek felhasználásra, a magánkulcs eljuttatása a tulajdonoshoz nem szükséges és nem megengedett.

6.1.3 Nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

Szolgáltató az előfizetői nyilvános kulcsokat PKCS#10 formátumnak megfelelő, a nyilvános kulcshoz tartozó magánkulccsal létrehozott digitális aláírással hitelesített tanúsítványkérelmekben juttatja el Előfizetőnek, aki benyújtja a tanúsítványkérelmeket a NISZ Zrt. számára, annak minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokat kibocsátó szolgáltatása keretében. A tanúsítvány kibocsátása nem része a NISZ-TKASZ szolgáltatásnak, a minősített tanúsítványok kibocsátását a NISZ Zrt. különálló, minősített bizalmi szolgáltatásában

végzi, melyre a {D8} „Bizalmi Szolgáltatási Rend minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BR-MTT) és a {D9} „Bizalmi Szolgáltatási Szabályzat minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BSZ-MTT) vonatkozik.

6.1.4 A szolgáltatói nyilvános kulcs közzététele

Szolgáltató nem teszi közzé a Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális vagy vezérlő kulcspárokból a nyilvános kulcsot.

6.1.5 Kulcs méretek

Szolgáltató a Szolgáltatás nyújtása során – mind a szolgáltatói, mind az előfizetői kulcsok tekintetében - a Bizalmi Felügyelet vonatkozó határozatának megfelelő olyan szabványos algoritmusokat, paramétereket és kulcshosszokat használ, melyek a kulcs generálását követő legalább két év időtartamra megfelelően erősnek tekinthetők.

Az előfizetői kulcspárok algoritmusa és mérete: SHA256withRSA, 2048 bit.

A Szolgáltató folyamatosan figyelemmel kíséri a technikai fejlődést és ennek függvényében szükség esetén, megfelelő időben gondoskodik az algoritmus váltásról vagy a kulcshosszak növeléséről.

6.1.6 A nyilvános kulcs paraméterek előállítása és megfelelőségének ellenőrzése

A szolgáltatói kulcsok előállítása a 6.1.1.1 fejezet szerint védett környezetben és tanúsított HSM modulban, legalább két bizalmi munkakört betöltő személy együttes részvételével, illetéktelen személy jelenlétét kizárva történik. A szolgáltatói kulcsok generálása során Szolgáltató betartja a HSM modul tanúsítási jelentésében foglalt előírásokat is.

Az előfizető kulcspárok előállítása a 6.1.1.2 fejezet szerint, szigorúan védett környezetben és tanúsított TKASZ-HSM modulban, kizárólag bizalmi munkakört betöltő személyek jelenlétében történik. Az előfizetői kulcspárok generálása során Szolgáltató betartja a TKASZ-HSM modul tanúsítási jelentésében foglalt előírásokat is.

6.2 Magánkulcs védelme és kriptográfiai modul műszaki szabályozások

6.2.1 Kriptográfiai modul szabványok és műszaki szabályozások

Szolgáltató a szolgáltatói infrastrukturális és vezérlő kulcsok, valamint az előfizető kulcspárok olyan kriptográfiai modult (TKASZ-HSM) alkalmaz, amely:

- olyan megbízható rendszer, amelynek értékelése az MSZ/ISO/IEC 15408 {Sz8} szerint, illetve azzal egyenértékű biztonsági kritériumok szerint – az AVA_VAN.5 garancia összetevővel kiegészítve - 4-es vagy magasabb értékelési garancia szinten történt meg; vagy
- megfelel az ISO/IEC 19790 {Sz9} követelményeinek; vagy
- megfelel a FIPS 140-2 {Sz10} 3-as, illetve annál magasabb szintű követelményeknek.

Szolgáltató havi rendszerességgel ellenőrzi minden, a Szolgáltatásban használt HSM és TKASZ-HSM modul tanúsított állapotának meglétét, és figyelemmel kíséri a tanúsítás lejáratának időpontját. A tanúsítás lejárata előtt legalább hat hónappal intézkedik új, megfelelő HSM eszközök beszerzéséről és üzembe állításáról.

6.2.2 Több szereplős ("n-ből m") ellenőrzés

Szolgáltató alkalmazza a több szereplős "n-ből m" ellenőrzést minden, a Szolgáltatásban használt TKASZ-HSM modul esetében, az adminisztrátori- és kulcsgondozási funkcióinak aktivizálásánál.

6.2.3 Magánkulcs mentése

A Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok biztonsági okokból mentésre kerülnek. A mentés titkosított formában, speciális eszközök alkalmazásával történik, hasonlóan szigorú fizikai, biztonsági óvintézkedések és eljárási szabályok betartásával, mint ahogy a kulcsok előállítása eredetileg történt.

Szolgáltató az előfizetői kulcspárokról a Szolgáltató infrastrukturális kulcsain alapuló titkosított export állományok formájában biztonsági mentést készít. A titkosításhoz használt szolgáltatói infrastrukturális kulcs algoritmusa és hossza erősebb, mint az általa védett előfizetői kulcspárok algoritmusa, illetve hossza. A titkosított export állomány előállítása a TKASZ-HSM modul erre szolgáló, tanúsítással rendelkező biztonsági funkciójával történik.

6.2.4 Magánkulcs visszaállítása

Szolgáltató a szolgáltatói kulcsokat rendkívüli üzemi helyzetek esetén a 6.2.3 fejezetben leírt titkosított mentésből visszaállíthatja, hasonlóan szigorú fizikai, biztonsági óvintézkedések és eljárási szabályok betartásával, mint ahogy a kulcsok előállítása eredetileg történt.

Szolgáltató az előfizetői kulcspárokat a 6.2.3 fejezetben leírt titkosított mentésből visszaállíthatja, hasonlóan szigorú fizikai, biztonsági óvintézkedések és eljárási szabályok betartásával, mint ahogy a kulcspárok előállítása eredetileg történt. A titkosított mentésből történő visszaállítás a TKASZ-HSM modul erre szolgáló, tanúsítással rendelkező biztonsági funkciójával történik.

6.2.5 Magánkulcs bejuttatása a kriptográfiai modulba

A Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok teljes életciklusuk alatt a 6.2.1 fejezetben leírt HSM modulban kerülnek tárolásra.

[CHSM] Az előfizető kulcspárok bejuttatása a [CHSM] modulba a Szolgáltató infrastrukturális kulcsain alapuló titkosított export állományokból a [CHSM] modul erre szolgáló, tanúsítással rendelkező biztonsági funkciójával történik (lásd 6.1.1.2 fejezet).

[NETHSM] Az előfizetői kulcspárok teljes életciklusuk alatt a NETHSM modulban maradnak, bejuttatásuk nem szükséges.

6.2.6 Magánkulcs kriptográfiai modulban történő tárolásának módja

A Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok teljes életciklusuk alatt a 6.2.1 fejezetben leírt HSM modulban kerülnek tárolásra. A kulcsok tárolása során Szolgáltató betartja a HSM modul tanúsítási jelentésében foglalt előírásokat.

[CHSM] Az előfizetői kulcspárok felhasználása minden esetben a CHSM modulból történik, olyan módon, hogy az adott előfizető kulcspár a használatot megelőzően (a magánkulcs aktiválása során) bejuttatásra kerül a CHSM modulba, a 6.2.5 fejezetben leírt módon.

[NETHSM] Az előfizetői kulcspárokat teljes életciklusuk alatt a NETHSM modulban kerülnek tárolásra, felhasználásuk onnan történik.

6.2.7 Magánkulcs aktiválásának módja

A Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok aktiválását Szolgáltató a HSM modul gyártói dokumentációjában előírtak szerint végzi el. Szolgálató biztosítja, hogy az aktivált HSM modul jogosulatlan hozzáférés ellen védett legyen.

[CHSM] A CHSM modulban tárolt előfizetői magánkulcsok aktiválásához szükséges, hogy az adott magánkulcshoz kapcsolódó minősített tanúsítvány a Szolgáltatás nyújtásához használt informatikai rendszer nyilvántartásába felvételre kerüljön, a tanúsítvány érvényes legyen, valamint a Bélyegző Létrehozó, illetve az Aláíró azonosítása és jogosultságának ellenőrzése a 3.2, illetve a 3.3 fejezetben leírtak szerint sikeresen megtörténjen. Ekkor az adott előfizető magánkulcs aktív állapotba kerül, ha az adott kulcspár éppen nincs fizikailag jelen a CHSM modulban, akkor automatikusan betöltésre kerül a titkosított export állományból, a 6.1.1.2 fejezetben leírt módon, ezt követően képes a Felhasználó a magánkulcsát használni az elektronikus aláírásának vagy bélyegzőjének létrehozásához szükséges Kriptográfiai Művelet elvégeztetésére. A CHSM modul kulcsmenedzsment algoritmusa az utolsó használatot követően bizonyos idő elteltével automatikusan eltávolítja az adott kulcspárt a CHSM modulból. Szolgáltató biztosítja, hogy az aktivált CHSM modul jogosulatlan hozzáférés ellen védett legyen.

[NETHSM] A NETHSM modulban tárolt előfizetői magánkulcsok aktiválásához szükséges, hogy az adott magánkulcshoz kapcsolódó minősített tanúsítvány a Szolgáltatás nyújtásához használt informatikai rendszer nyilvántartásába felvételre kerüljön, a tanúsítvány érvényes legyen, valamint a Bélyegző Létrehozó, illetve az Aláíró azonosítása és jogosultságának ellenőrzése a 3.2, illetve a 3.3 fejezetben leírtak szerint sikeresen megtörténjen. Ekkor az adott előfizető magánkulcs aktív állapotba kerül, a Felhasználó képes a magánkulcsát használni az elektronikus aláírásának vagy bélyegzőjének létrehozásához szükséges a Kriptográfiai Művelet elvégeztetésére. Szolgáltató biztosítja, hogy az aktivált NETHSM modul jogosulatlan hozzáférés ellen védett legyen.

6.2.8 Magánkulcs aktív állapotának megszüntetési módja

Az előfizetői magánkulcs aktív állapota automatikusan megszűnik a NISZ-TKASZ kérés kiszolgálásának végeztével, azaz a kért Kriptográfiai Művelet elvégeztét követően.

6.2.9 Magánkulcs megsemmisítésének módja

Szolgáltató a Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsokat visszaállíthatatlan módon megsemmisíti, amikor használatuk már nem szükséges. A kulcsok és az aktiválásukhoz szükséges minden adat megsemmisítését

olyan módon végzi, hogy annak végrehajtása után a kulcs semmilyen része ne legyen kikövetkezhető vagy levezethető.

Szolgáltató az előfizetői kulcspárokat megsemmisíti, amikor:

- a hozzá kapcsolódó tanúsítvány lejárt vagy visszavonásra került;
- vagy előfizető kéri a kulcspár törlését.

Az előfizetői kulcspárokat és az aktiválásukhoz szükséges minden adat megsemmisítése olyan módon történik, hogy annak végrehajtása után a magánkulcs semmilyen része nem lesz kikövetkezhető vagy levezethető. Az előfizetői kulcspár megsemmisítésével egyidejűleg a Szolgáltatás nyújtásához használt informatikai rendszer nyilvántartásából törlésre kerül a kulcspárhoz tartozó tanúsítvány.

6.2.10 Kriptográfiai modul értékelése

A 6.2.1 fejezet tartalmazza.

6.3 Kulcspár gondozás egyéb szempontjai

6.3.1 Tanúsítvány érvényességi időszaka és kulcspár felhasználás időtartama

Szolgáltató biztosítja, hogy egy előfizetői kulcspár csak azt követően használható, hogy a kulcspárhoz kibocsátott minősített tanúsítvány a Szolgáltatás nyújtásához használt informatikai rendszer nyilvántartásába felvételre került – ez alól egyetlen kivétel a PKCS#10 formátumnak megfelelő tanúsítványkérelem előállítása.

Szolgáltató biztosítja, hogy egy előfizetői kulcspár csak és kizárólag érvényes tanúsítvány esetén használható, azaz érvényességi időszakon belül és akkor, ha a tanúsítvány nincs felfüggesztve vagy visszavonva.

6.4 Aktivizáló adatok

6.4.1 Aktivizáló adatok előállítása és telepítése

Szolgáltató a TKASZ-HSM modulban tárolt előfizetői magánkulcsok védelmére a TKASZ-HSM modul gyártói dokumentációjában és tanúsítási jelentésében előírt eljárásokat alkalmazza az aktivizáló adatok előállítása és telepítése során.

6.4.2 Aktivizáló adatok védelme

Szolgáltató biztosítja, hogy a TKASZ-HSM modulban az előfizetői magánkulcshoz kapcsolódó aktivizáló adat kizárólag csak az Előfizető, valamint a Felhasználó sikeres azonosítását és hitelesítését követően legyen használható.

6.5 Informatikai biztonsági óvintézkedések

6.5.1 Informatikai biztonsági műszaki követelmények meghatározása

Az informatikai biztonság műszaki követelményeit a Szolgáltató az {Sz2} EN 319 401, {Sz3} TS 119 431-1 és {Sz4} EN 419 241-1 szabványoknak a nem minősített bizalmi szolgáltatás nyújtására vonatkozó, informatikai biztonsági műszaki követelményeiben határozza meg.

6.5.2 Informatikai biztonsági értékelés

Szolgáltató az informatikai rendszerek biztonsági értékelését az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rendelkezései szerint végzi.

6.6 Életciklusra vonatkozó műszaki óvintézkedések

6.6.1 Rendszerfejlesztési óvintézkedések

Szolgáltató gondoskodik arról, hogy az általa vagy a nevében végzett valamennyi rendszerfejlesztési projektjében a biztonság követelményeit már a tervezési és követelmény meghatározási fázisban figyelembe vegyék annak érdekében, hogy a biztonság beépüljön az informatikai rendszerekbe.

Az IT életciklusra vonatkozó rendszerfejlesztési szabályokat a Szolgáltató belső információbiztonsági szabályzata tartalmazza, amely pontosan meghatározza a tervezés és előkészítés, a projekt és kivitelezés, a működtetés és a menedzselés, valamint a visszacsatolás, illetve visszavonás/rekonstrukció ciklus időszakok feladatait és az alkalmazott módszertanokat. A belső információbiztonsági szabályzat figyelembe veszi az {Sz2} EN 319 401 szabvány 7.7 fejezetében előírt követelményeket.

6.6.2 Biztonságkezelési óvintézkedések

Szolgáltató olyan eszközöket és eljárásokat alkalmaz, melyek garantálják a Szolgáltatást megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

A biztonságkezelési szabályokat a Szolgáltató {D5} informatikai biztonsági szabályzata tartalmazza.

6.6.3 Életciklus biztonsági óvintézkedések

Szolgáltató az alábbi táblázatban megadott rendszerességgel elvégzi a Szolgáltatást megvalósító, megbízható informatikai rendszereinek konfigurációs beállításai, az operációs rendszer beállítások, a hálózati konfigurációs beállítások, továbbá az alkalmazott biztonsági mechanizmusok sértetlenségének és helyes működésének ellenőrzését.

biztonsági ellenőrzés típusa		végzi	rendszeresség
operatív	IT infrastruktúra	rendszerüzemeltető operátorok	naponta

	szolgáltatás nyújtásához használt alkalmazások és naplóik	rendszervizsgálók	naponta
belső ellenőrzés	IT infrastruktúra	biztonsági tisztviselő	évente egyszer
	szolgáltatás nyújtásához használt alkalmazások és naplóik	biztonsági tisztviselő	évente egyszer
külső ellenőrzés	IT infrastruktúra	külső auditor	évente egyszer
	szolgáltatás nyújtásához használt alkalmazások és naplóik	külső auditor	évente egyszer

6.7 Hálózatbiztonsági óvintézkedések

A hálózati védelmi intézkedéseket a Szolgáltató a {D5} biztonsági szabályzatában meghatározott követelményeknek megfelelően valósítja meg, melyek figyelembe veszik az {Sz2} EN 319 401 szabvány 7.8 fejezetében leírt követelményeket is.

6.8 Időforrások

A Szolgáltatás nyújtásához használt megbízható rendszereket Szolgáltató 24 óránként legalább egyszer, megbízható időforrásokkal (NTP) szinkronizálja az UTC időhöz.

A megbízható időforrások Szolgáltató saját rendszerén belüli, redundáns kialakítású, speciális célberendezések (referencia időforrások), melyek pontossága századmásodpercen belüli, és amelyek GPS alapúak, így visszavezethetők az UTC időforrásra.

7 TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK

7.1 Tanúsítvány profil

Az előfizetői kulcspárokhoz kibocsátott minősített tanúsítvány profilja megfelel a {D9} „Bizalmi Szolgáltatási Szabályzat minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BSZ-MTT) 7.1 fejezetében leírtaknak.

7.2 CRL profil

Az előfizetői kulcspárokhoz kibocsátott minősített tanúsítvány visszavonási állapotának ellenőrzéséhez használható CRL-ek profilja megfelel a {D9} „Bizalmi Szolgáltatási Szabályzat minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BSZ-MTT) 7.2 fejezetében leírtaknak

7.3 OCSP profil

Az előfizetői kulcspárokhoz kibocsátott minősített tanúsítvány visszavonási állapotának ellenőrzéséhez használható OCSP válaszok profilja megfelel a {D9} „Bizalmi Szolgáltatási Szabályzat minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BSZ-MTT) 7.3 fejezetében leírtaknak.

8 MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

Jelen bizalmi szolgáltatási szabályzat tartalmazza az összes, a tárolt kulcsos Kriptográfiai Műveletek elvégzésére irányuló bizalmi szolgáltatás nyújtása során teljesíteni szükséges követelményt, melyeket különösen az alábbi szabványok határoznak meg:

- EN 319 401: General policy requirements for Trust Service Providers {Sz2}
- TS 119 431-1: Policy and security requirements for Trust Service Providers;
  Part 1: TSP service components operating a remote QSCD/SCDev {Sz3}
- EN 419 241-1: Trustworthy Systems Supporting Server Signing;
  Part 1: General System Security Requirements {Sz4}

8.1 Vizsgálatok gyakorisága és körülményei

Szolgáltató külső és belső vizsgálatokat végez, illetve végeztet annak érdekében, hogy a Szolgáltatással kapcsolatos folyamatai, eszközei, személyzete és környezete mindenkor megfeleljenek a vonatkozó jogszabályi és szabványi követelményeknek. A Szolgáltató érintett szervezetei és munkatársai kötelesek együttműködni a Szolgáltató által kijelölt auditorral, és biztosítani az ellenőrzéshez szükséges feltételeket.

Szabályzatainak megfelelőségét Szolgáltató saját szervezete részéről a Hitelesítési Rend és Szabályozási Csoport vizsgálja meg. A Szolgáltatás megfelelőségének vizsgálatára Szolgáltató saját belső ellenőrzéseket hajt végre.

A Szolgáltató nyilvános szabályzatait a Bizalmi Felügyelet is megvizsgálja a nyilvántartásba vételi eljárása során, valamint a szabályzatok módosításakor, és megfelelőség esetén közzé teszi a kötelezően benyújtandó szabályzatokat.

Szolgáltató rendelkezik minőségbiztosítási rendszerrel és információbiztonsági irányítási rendszerrel, melyek megfelelő működését független rendszervizsgáló ellenőrzési tevékenysége biztosítja.

Szolgáltató a külső, illetve a saját ellenőrző szervezet által végzett belső vizsgálatokat a {D5} PKI szolgáltatások biztonsági szabályzatában megjelölt rendszerességgel – évente legalább egyszer biztosítja.

8.2 Auditor azonosítása és képesítése

A külső rendszervizsgálói auditokat a Szolgáltató olyan szakértővel vagy szakértői szolgáltatásokat nyújtó szervezettel végzi el, aki független Szolgáltatótól, illetve az ellenőrzött rendszertől, területtől, és szakértelmét biztosítani tudja a PKI és az informatikai biztonság, valamint az ezen területekre vonatkozó technikai, technológiai, jogi, szabályzati ismeretek és auditálási módszertanok vonatkozásában.

A Szolgáltató tevékenységére és az informatikai biztonságra vonatkozó belső ellenőrzéseket a Szolgáltató belső szervezete végzi, az ott dolgozó biztonsági tisztviselők bevonásával.

8.3 Auditor függetlensége

A külső vizsgálatokat végző szervezet, illetve annak munkatársai teljes mértékben függetlenek Szolgáltatótól.

8.4 Audit során vizsgált területek

Az audit az alábbi területeket fedi le:

- szabályzatok és dokumentációk;
- irányítási és ellenőrzési követelmények;
- személyzeti biztonsági követelmények;
- a szolgáltatói kulcsok kezeléséhez kapcsolódó követelmények;
- üzemeltetési és hozzáférési biztonság;
- fizikai és környezeti biztonság;
- folyamatos szolgáltatás biztosítása;
- adatbiztonság és archiválás.

Az audit során megvizsgálásra kerül, hogy Szolgáltató és az általa nyújtott Szolgáltatás megfelelnek-e:

- a hatályos jogszabályoknak és szabványoknak;
- a szolgáltatási szabályzatnak, illetve a bizalmi szolgáltatási rendnek.

8.5 Hiányosságok esetén végrehajtandó tevékenységek

Az üzemszerű ellenőrzések, belső és külső auditok, szakértői elemzések által feltárt hiányosságok, hibás gyakorlatok kezelésére Szolgáltató intézkedési tervet készít. A hiányosságokat késlekedés nélkül orvosolja, az intézkedéseket dokumentálja és ellenőrzi.

A Bizalmi Felügyelet által végzett helyszíni ellenőrzések során feltárt esetleges hiányosságokat Szolgáltató a hatóság által előírt határidőn belül megszünteti a hatályos jogszabályok alapján és a hatóságtól kapott információk és ajánlások figyelembe vételével.

8.6 Eredmény kommunikációja

A belső és külső auditot, szakértői elemzést végző személyek csak a megbízójuknak adhatnak információt a Szolgáltató tevékenységével kapcsolatban. Az audit és az ellenőrzés eredményei a Szolgáltató bizalmas üzleti információi, ezért azokat a társaság titokvédelmi előírásai szerint kell kezelni. Szolgáltató nem köteles a konkrét hiányosságot nyilvánosságra hozni.

9 EGYÉB ÜZLETI ÉS JOGI KÉRDÉSEK

9.1 Díjak

A szolgáltatási díjakat Szolgáltató a Szolgáltatás internetes honlapján teheti közzé, vagy ártájékoztatót küldhet az érdeklődők számára. Szolgáltató jogosult a díjakat egyoldalúan meghatározni, módosítani.

Az Előfizetőre vonatkozó szolgáltatási díjak a {D2} TKASZ Szolgáltatási Szerződésben kerülnek rögzítésre.

9.2 Anyagi felelősség

A Szolgáltató anyagi felelősségének mértékéről, illetve annak korlátairól a {D1} Általános Szerződési Feltételek rendelkezik.

9.2.1 Biztosítási fedezet

A Szolgáltató rendelkezik olyan felelősségbiztosítással, mely egyaránt kiterjed az elektronikus aláírással vagy bélyegzővel, illetve az ezzel ellátott elektronikus dokumentummal szerződésen kívül okozott károkra és szerződésszegéssel okozott károkra, és amely fedezetet biztosít az összes károsultnak okozott kárra, a {D1} Általános Szerződési Feltételekben rögzített mértékig. A biztosítási szerződésben szereplő felelősségvállalási érték 3.000.000 Ft, vagy ennél esetenként magasabb összeg.

A felelősségbiztosítási szerződés megfelel a {J8} 24/2016 rendelet előírásainak is.

9.3 Üzleti információk bizalmassága

9.3.1 Bizalmasan kezelendő információk köre

Szolgáltató minden olyan adatot és információt bizalmasnak tekint, melyek nem kerültek felsorolásra a 9.3.2 fejezetben.

9.3.2 Nem bizalmasnak tekintett információk köre

Nem bizalmasnak tekintett információk az alábbiak:

- Előfizető tanúsítványba foglalt adatai;
- a tanúsítványokhoz kapcsolódó visszavonási információk;
- a Szolgáltató internetes honlapján közzétett nyilvános információk, szabályzatok és egyéb dokumentumok;
- az olyan adatok, melyek nyilvános adatforrásból elérhetők.

9.3.3 Bizalmas információk védelmének felelőssége

Szolgáltató a bizalmas információkhoz való hozzáférést csak az arra feljogosított személyek és szervezetek számára teszi lehetővé. A bizalmas információk védelmét a személyzet megfelelő

képzésével, továbbá a munkavállalókkal, szerződéses partnerekkel megkötött szerződésekkel juttatja érvényre.

9.4 Személyes adatok védelme

9.4.1 Adatvédelmi terv

Szolgáltató rendelkezik mind társasági szintű adatvédelmi tervvel ({D4}), mind pedig a Szolgáltatásra vonatkozó adatvédelmi tájékoztatóval, melyek nyilvános dokumentumok, és elérhetők Szolgáltató internetes honlapján. Ezen dokumentumok összhangban vannak a nemzetközi és hazai vonatkozó jogszabályokkal.

9.4.2 Bizalmasként kezelendő személyes adatok

Szolgáltató csak Előfizetőtől közvetlenül gyűjt személyes adatot és csak olyan mértékben, ami a Szolgáltatás nyújtásához, valamint Aláíró tájékoztatásához, személyazonosságának megállapításához szükséges.

Szolgáltató bizalmasként kezelendő személyes adatnak tekinti:

- Előfizető részéről a {D2} TKASZ Szolgáltatási Szerződésben érintett személyek (pl. cégjegyzésre jogosult vezető, vagy Előfizető Kapcsolattartója) minden adatát;
- Aláírónak azon adatait, melyek a tanúsítványba nem kerülnek befoglalásra.

9.4.3 Bizalmasként nem kezelendő személyes adatok

Szolgáltató nem bizalmasként kezelendő személyes adatnak tekinti Aláírónak a tanúsítványba foglalt adatait, amennyiben Aláíró tanúsítványa közzétételéhez írásban hozzájárult.

Továbbá, nem bizalmas adat a tanúsítványhoz kapcsolódó státusz információ, minden tanúsítvány vonatkozásában. A státusz információba beleértendő a tanúsítvány - esetleges - visszavonásának oka és időpontja.

9.4.4 Személyes adatok védelmének felelőssége

Szolgáltató gondoskodik a személyes adatok védelméről, működése és szabályzatai megfelelnek a {J11} GDPR rendelkezéseinek.

9.4.5 Hozzájárulás a személyes adatok felhasználásához

Aláírás célú kulcspár esetén Aláírónak tudomásul kell vennie a kulcspár generálásához szükséges adatoknak a Szolgáltató által történő nyilvántartásba vételét, kezelését és tárolását.

Bélyegzés célú kulcspár esetén Előfizető Kapcsolattartójának a kulcsgenerálási űrlap kitöltésével és aláírásával hozzá kell járulnia a kulcspár generálásához szükséges adatok Szolgáltató által történő nyilvántartásba vételéhez, kezeléséhez és tárolásához.

Előfizetőnek a {D2} TKASZ Szolgáltatási Szerződés aláírásával hozzá kell járulnia a szerződés megkötéséhez szükséges adatok Szolgáltató által történő nyilvántartásba vételéhez, kezeléséhez és tárolásához.

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 érintett Előfizetőt és/vagy Felhasználót.

9.4.7 Egyéb, felfedést eredményező körülmények

Szolgáltató a szolgáltatási tevékenység, illetve a Szolgáltatás nyújtásának megszüntetése esetén Előfizetők és Felhasználók adatait a jogszabályi kötelezettségeire tekintettel átadja harmadik félnek.

9.5 Szellemi tulajdonjogok

A Szolgáltató által ügyfelei részére generált kulcspár tulajdonosa az Előfizető, teljes jogú használója pedig az adott Felhasználó (Aláíró vagy Bélyegző Létrehozó), aki/amely számára a kulcspár előállításra került, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.

Szolgáltató kizárólagos tulajdonát képezik a szabályzatai, szerződéses feltételei és egyéb, a Szolgáltatás internetes honlapján közzétett dokumentumai. Ezen dokumentumok felhasználása csak és kizárólag a Szolgáltatás használatával összefüggésben engedélyezett, minden egyéb kereskedelmi vagy egyéb célú felhasználása szigorúan tilos.

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 Szolgáltató felelőssége és helytállása

Szolgáltató felel a bizalmi szolgáltatási rendben és jelen szolgáltatási szabályzatban, valamint az Előfizetővel megkötött {D2} TKASZ Szolgáltatási Szerződésben megfogalmazott valamennyi kötelezettsége maradéktalan betartásáért, még akkor is, ha a Szolgáltatás nyújtásához kapcsolódó egyes feladatokat egyéb alvállalkozók végeznek.

Szolgáltató a vele szerződéses jogviszonyban nem álló harmadik személlyel szemben a {J5} Polgári Törvénykönyv 6:519. §-a szerint, a vele szerződéses jogviszonyban álló Előfizetővel szemben a szerződésszegésért való felelősség ({J5} Polgári Törvénykönyv 6:142. §) szabályai szerint felelős az elektronikus aláírással vagy bélyegzővel hitelesített elektronikus dokumentummal okozott kárért, ha megszegte a bizalmi szolgáltatási rendben és a jelen szolgáltatási szabályzatban, valamint az Előfizetővel megkötött {D2} TKASZ Szolgáltatási Szerződésben előírtakat, vagy az esemény időpontjában hatályos jogszabály szerinti, rá vonatkozó kötelezettségeket. E kötelezettségek megtartását kétség esetén Szolgáltatónak kell bizonyítania. Szolgáltató sajátjaként felel az egyéb alvállalkozók által a Szolgáltatás nyújtása során okozott kárért.

Szolgáltató a felelősségi körén belül keletkezett, bizonyított károkért az Előfizetővel megkötött {D2} TKASZ Szolgáltatási Szerződésben és a 9.8 fejezetben foglalt korlátozásokkal kártérítést fizet.

Szolgáltató nem felel:

- Előfizető Autentikációs Tanúsítványával kapcsolatos tevékenységéért;

- a Felhasználók (Aláírók és Bélyegző Létrehozók) azonosító eszközükkel kapcsolatos tevékenységéért;
- az Érintett felek elektronikus aláírás vagy bélyegző ellenőrzési és felhasználási tevékenységeiért;
- az Érintett Felek vagy mások által kibocsátott szabályzatokért.

Szolgáltató kötelezettsége

Szolgáltató azzal, hogy generál egy TKASZ-HSM modulban tárolt előfizetői kulcspárt – mely jelen szolgáltatás szabályzat hatálya alatt került előállításra – arra vállal kötelezettséget, hogy a Szolgáltatás nyújtása során ő maga és a Szolgáltatás nyújtásában közreműködő egyéb alvállalkozói a jelen szabályzatban foglaltakat maradéktalanul betartják. Szolgáltató megteszi a szükséges és tőle telhető intézkedéseket ahhoz, hogy az Előfizetők és Felhasználók is jelen szabályzat előírásainak megfelelően járjanak el.

9.6.2 SZEÜSZ Ügyfélszolgálat felelőssége és helytállása

Az ügyfélszolgálati tevékenységeket Szolgáltató saját szervezetén belül üzemeltetett SZEÜSZ Ügyfélszolgálat végzi. A SZEÜSZ Ügyfélszolgálat betartja a rá vonatkozó, jogszabályokban, illetve a Szolgáltató szabályzataiban foglalt előírásokat.

Szolgáltató felelőssége a Szolgáltatás nyújtása során:

- Előfizető szerződéskötést megelőző tájékoztatása;
- Előfizető Kapcsolattartója személyének azonosítása és eljárási jogosultságának megállapítása;
- a Szolgáltatáshoz szükséges adatok rögzítése az erre szolgáló informatikai rendszerben;
- a kulcsgenerálási űrlapok ({D7}) alapján a megfelelő tanúsítvány kérelmek előállítása;
- a {D2} TKASZ Szolgáltatási Szerződés előkészítése és megkötése.

9.6.3 Előfizető felelőssége és helytállása

Előfizető jogai

Előfizető jogosult:

- a Szolgáltatás igénybe vételére a jelen szolgáltatási szabályzatban, a {D2} TKASZ Szolgáltatási Szerződésben és a {D1} Általános Szerződési Feltételekben leírtak szerint;
- kapcsolattartó személyt kijelölni;
- az általa meghatározott Felhasználók számára kulcspár előállítását igényelni;
- az általa meghatározott Felhasználók kulcspárjának törlését kérni.

Előfizető felelőssége

Az Előfizető felelősségét a {D2} TKASZ Szolgáltatási Szerződés és a {D1} Általános Szerződési Feltételek határozzák meg.

Előfizető kötelezettségei

Előfizető kötelessége a Szolgáltató szabályzatainak és szerződéses feltételeinek megfelelően eljárni a Szolgáltatás használata során. Az Előfizető kötelezettségeit a jelen szolgáltatási szabályzat, a {D2} TKASZ Szolgáltatási Szerződés és annak {D1} Általános Szerződési Feltételek melléklete tartalmazzák.

A Felhasználók jogai

Az Aláíró vagy Bélyegző Létrehozó jogosult:

- a számára előállított kulcspárt az 1.4.1 fejezetben leírt célokra és jelen szabályzatban leírt módon használni;
- a tárolt kulcshoz kapcsolódó egyéb szolgáltatásokat használni a jelen szabályzatban leírt módon.

A Felhasználók felelőssége

Az Aláíró vagy Bélyegző Létrehozó felelős:

- a regisztráció során megadott adatainak valódiságáért, pontosságáért és érvényességéért;
- a tanúsítványba foglalt adatok ellenőrzéséért;
- az adataiban bekövetkezett változás haladéktalan bejelentéséért;
- az Autentikációs Folyamatban használt azonosító eszköze biztonságos kezeléséért;
- a kulcspár szabályzatoknak megfelelő felhasználásáért;
- a Szolgáltató haladéktalan értesítéséért és teljes körű tájékoztatásáért vitás ügyek esetén;
- általában, a jelen szabályzatban előírt kötelezettségei betartásáért.

A Felhasználók kötelezettségei:

Az Aláíró vagy Bélyegző Létrehozó köteles:

- a Szolgáltatás használata előtt megismerni jelen szolgáltatási szabályzatot;
- a Szolgáltató által kért, a Szolgáltatás igénybe vételéhez szükséges adatokat hiánytalanul és a valóságnak megfelelően megadni;
- a Szolgáltatást kizárólag a jogszabályok által megengedett vagy nem tiltott célokra, a jelen szabályzatban és a hivatkozott dokumentumokban foglaltaknak megfelelően használni;
- adat változás esetén haladéktalanul írásban értesíteni erről Szolgáltatót, és beszüntetni a kulcspár használatát;
- biztosítani, hogy a Szolgáltatás igénybe vételéhez szükséges adatokhoz és eszközökhöz (különösen az Autentikációs Folyamatban használt azonosító eszközhöz) illetéktelen személy ne férhessen hozzá;
- haladéktalanul kezdeményezni a tanúsítvány felfüggesztését vagy visszavonását, amennyiben az Autentikációs Folyamatban használt azonosítók illetéktelen kezekbe kerültek vagy megsemmisültek, megrongálódtak, elvesztek, valamint haladéktalanul megszüntetni a Szolgáltatásban tárolt kulcspár használatát;
- jogellenes használat gyanúja esetén a Szolgáltató megkereséseire a Szolgáltató által megadott időtartamon belül reagálni;
- haladéktalanul, írásban értesíteni Szolgáltatót, ha a Szolgáltatás felhasználásával létrehozott elektronikus aláírással vagy bélyegzővel kapcsolatban jogvita indul.

9.6.4 Érintett felek felelőssége és helytállása

Az Érintett Felek a saját belátásuk és/vagy szabályzataik szerint dönthetnek az egyes elektronikus aláírások és bélyegzők elfogadásáról és a felhasználás módjáról. Az elektronikus aláírás vagy bélyegző érvényességének elbírálása során az Érintett Félnek megfelelő körültekintéssel kell eljárnia, ezért különös tekintettel javasolt:

- a szolgáltatási szabályzatban foglalt követelmények és előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- a tőle elvárható magatartás tanúsítása az elektronikus aláírás vagy bélyegző ellenőrzésekor.

Szolgáltató kizárja a felelősségét, amennyiben az Érintett Fél az elektronikus aláírás vagy bélyegző elfogadásakor nem körültekintően, vagy nem a tőle elvárható gondossággal jár el.

9.7 Helytállás érvénytelenségi köre

Szolgáltató kizárja felelősségét, amennyiben:

- az Érintett Fél nem körültekintően jár el az elektronikus aláírások és bélyegzők ellenőrzése és felhasználásra során, azaz nem a mérvadó műszaki szabványoknak vagy a hatályos jogszabályoknak megfelelően jár el;
- az Érintett Felek vagy mások által kibocsátott szabályzatok nem felelnek meg a mérvadó műszaki szabványoknak vagy a hatályos jogszabályoknak;
- az Internet, vagy annak egy részének működési hibájából fakadóan tájékoztatási vagy egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- az Előfizető nem tesz eleget a szolgáltatási szabályzatban előírt kötelezettségeinek;
- a Felhasználó (Aláíró vagy Bélyegző Létrehozó) nem tesz eleget a szolgáltatási szabályzatban előírt kötelezettségeinek;
- a károkozás a Bizalmi Felügyelet Szolgáltatónak kiadott, hatályos határozatában közölt kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

9.8 Felelősség korlátozása

Szolgáltató korlátozza a kártérítési felelősségét:

- a Szolgáltatás keretében történt összes elektronikus aláírással vagy bélyegzővel hitelesített dokumentumokat érintően Szolgáltató hibájából bekövetkezett káreseménnyel kapcsolatban fizetendő kártérítési összeg tekintetében.

Szolgáltató nem felelős az olyan károkért, melyek abból adódnak, hogy az Érintett Fél az Szolgáltatás keretében létrejött elektronikus aláírások és bélyegzők ellenőrzése és felhasználása során nem a hatályos jogszabályok és a mérvadó műszaki szabványok szerint járt el, illetve nem tanúsította a tőle elvárható gondosságot, illetve magatartást.

A Szolgáltató pénzügyi felelősségének mértékét a {D1} Általános Szerződési Feltételek határozza meg. Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja ezt az összeget, akkor az egyes kártérítési igények megtérítése az összes kártérítési igénynek a megadott összeghez viszonyított arányában történik.

9.9 Kártérítések

A kártérítésekről a jelen szabályzat 9.8 fejezetében leírtakon túl a {D2} TKASZ Szolgáltatási Szerződés és a {D1} Általános Szerződési Feltételek rendelkeznek.

9.10 Hatályosság és megszűnés

9.10.1 Hatályosság

Időbeli hatály

A szolgáltatási szabályzat egy adott verziójának időbeli hatálya a címlapon feltüntetett hatálybalépés dátumával kezdődik és határozatlan időre szól. Az időbeli hatály megszűnik a szolgáltatási szabályzat újabb verziójának hatályba lépésével vagy a Szolgáltatás befejezésekor.

Tárgyi hatály

A szolgáltatási szabályzat tárgyi hatálya kiterjed a Szolgáltatás nyújtására és igénybe vételére.

Személyi hatály

A szolgáltatási szabályzat személyi hatálya kiterjed Szolgáltatónak a Szolgáltatás nyújtásában közreműködő munkatársaira, továbbá az Előfizető kapcsolattartójaként kijelölt személyekre, az Aláírókra, és Előfizető szervezetén belül az egyes elektronikus bélyegzők felhasználásáért felelős személyekre.

9.10.2 Megszűnés

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

9.10.3 Megszűnés után is hatályban maradó rendelkezések

A megszűnés után is hatályban maradó rendelkezéseket – amennyiben ilyenek vannak – a {D1} Általános Szerződési Feltételek és a {D2} TKASZ Szolgáltatási Szerződés tartalmazza.

9.11 Egyéni hirdetmények és kommunikáció a részvevőkkel

Azokban az esetekben, melyekre jelen szolgáltatási szabályzat nem rendelkezik a felek közötti értesítésről, illetve annak joghatást kiváltó módjáról, a Szolgáltató értesítése írásban vagy emailben, Előfizető Kapcsolattartója vagy az Aláíró saját kezű vagy elektronikus aláírásával hitelesítve a SZEÜSZ Ügyfélszolgálat elérhetőségeire való beküldéssel történik. Az elektronikus értesítés csak a Szolgáltató általi visszaigazolást követően tekinthető kézbesítettnek. Szolgáltató a megkeresésekre 30 napon belül válaszol elektronikus aláírással vagy bélyegzővel ellátott válasz üzenetben.

9.12 Módosítások

9.12.1 Módosítás eljárása

A szolgáltatási szabályzat módosítása az 1.5.3 és 1.5.4 fejezetekben leírt szabályok szerint történik. A szolgáltatási szabályzat módosulását a verziószám megfelelő változása jelzi.

9.12.2 Értesítés módszere és időtartama

A Szolgáltatás jelentős vagy lényeges változása esetén Szolgáltató internetes honlapján közleményt tesz közzé és emailben tájékoztatást küld Előfizetőknek, a hatályba lépést megelőzően kellő időben ahhoz, hogy az érintett a felek a változásokra felkészülhessenek.

9.12.3 OID megváltozását előidéző körülmények

A szolgáltatási szabályzat új verziójával az OID verziószámot jelentő része megfelelően változik.

9.13 Vitás kérdések rendezése

Bármely vitás kérdés felmerülése előtt az Előfizetőnek kötelessége a Szolgáltató haladéktalan értesítése és teljes körű tájékoztatása a kérdés minden vonatkozását illetően, a vita jogi útra terelése előtt.

Panaszt írásban vagy személyesen, a SZEÜSZ Ügyfélszolgálat elérhetőségein lehet előterjeszteni. A panaszt a Szolgáltató az előterjesztéstől számított 30 napon belül kivizsgálja és ennek eredményéről a panaszost írásban tájékoztatja.

A jogviták esetén követendő eljárást a {D1} Általános Szerződési Feltételek tartalmazza.

Bármely vitás kérdés felmerülése esetén Előfizető jogosult az esetleges bírósági eljárást megelőzően békéltető testülethez fordulni, amennyiben jogszabályok szerinti fogyasztónak minősül. Az illetékes békéltető testület megnevezését és elérhetőségeit jelen szabályzat 1.5.2 fejezete tartalmazza.

9.14 Irányadó jog

Szolgáltató szerződéseire, szabályzataira és azok teljesítésére a magyar jog az irányadó és azokat a magyar jog szerint kell értelmezni.

9.15 Hatályos jognak megfelelés

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

9.16 Vegyes rendelkezések

9.16.1 Részleges érvénytelenség

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

9.16.2 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.

9.16.3 Force Majeure (Vis maior)

Vis maior: Az olyan – a Szolgáltató akaratától, cselekedeteitől és személyétől függetlenül bekövetkező és érdekkörén kívül eső elháríthatatlan – esemény (pl. sztrájk, háború, polgári felkelés, természeti katasztrófa, a Felek bármelyikének partnerénél felmerülő elháríthatatlan fizikai vagy jogi akadály vagy más elháríthatatlan szükséghelyzet) minősül vis maiornak, amely megakadályozza vagy lehetetlenné teszi a jelen szolgáltatási szabályzatban foglalt követelmény teljesítését, feltéve, hogy ezen körülmények a jelen szolgáltatási szabályzat hatálybalépését követően keletkeznek, illetőleg azt megelőzően következtek be, ám a jelen szolgáltatási szabályzat teljesítésére kiható következményeik az említett időpontban még nem voltak előre láthatóak.

Szolgáltató nem felelős a vis maior esetekből fakadó károkért.

9.17 Egyéb rendelkezések

Szolgáltató a Szolgáltatást és a Szolgáltatás során alkalmazott végfelhasználói termékeket hozzáférhetővé teszi a fogyatékossággal élő személyek számára, amennyiben az lehetséges.