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

Bizalmi Szolgáltatási Rend tárolt kulcsos elektronikus aláírás és elektronikus bélyegző elhelyezés szolgáltatáshoz (BR-NISZ-TKASZ)

Verziószám	1.1
OID	0.2.216.1.200.1100.100.42.3.8.29.1.1
Hatályba lépés dátuma	2020.10.11.
Dokumentum besorolása	nyilvános

Dátum:
2020.10.01
06:33:09 +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 Rendje, mely a tárolt kulcsos elektronikus aláírás és elektronikus bélyegző elhelyezés szolgáltatására vonatkozik (továbbiakban: BR-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), a 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.

[1] {Sz11} RFC 8017

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

Jelen bizalmi szolgáltatási rend a Szolgáltatásra vonatkozó eljárási és működtetési szabályokat tartalmazza.

1.1 Áttekintés

A BR-NISZ-TKASZ egy olyan szabálygyűjtemény, amely a Szolgáltatás használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára, valamint meghatározza a Szolgáltatás felhasználhatóságát.

Jelen bizalmi szolgáltatási rend az {Sz1} RFC 3647 nemzetközi ajánlás alapján készült, felépítésében és tartalmában szigorúan 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.

Jelen bizalmi szolgáltatási rend előírja a Szolgáltatás nyújtása során teljesíteni szükséges összes követelményt, melyeket az alábbi nemzetközi 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 Security Requirements {Sz4}

Ezen követelmények teljesítésének módját, illetve az itt megnevezett eljárások részletes leírását a „Bizalmi Szolgáltatási Szabályzat tárolt kulcsos elektronikus aláírás és elektronikus bélyegző elhelyezés szolgáltatáshoz” (BSZ-NISZ-TKASZ) dokumentum tartalmazza.

1.2 Dokumentum neve és azonosítása

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

A bizalmi szolgáltatási rend rövid neve: BR-NISZ-TKASZ.

A bizalmi szolgáltatási rend objektum azonosítója és verziószáma a címlapon található.

A jelen BR-NISZ-TKASZ hatálya alatt létrehozott elektronikus aláírások/bélyegzők felhasználására vonatkozó részletes szabályokat a BSZ-NISZ-TKASZ szolgáltatási szabályzat tartalmazza.

Jelen BR-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.

A Szolgáltató saját szervezetén kívül más szervezetek is közreműködhetnek a Szolgáltatás nyújtásában, azonban a Szolgáltató teljes körű felelősséggel tartozik azért, hogy a jelen szabályzatban foglalt követelmények teljesülnek.

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: 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 (a 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 Szolgáltató a tárolt magánkulcsok használatára további korlátozásokat szabhat, melyeket a szolgáltatási szabályzatban kell megadnia.

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 Szolgáltatónak szervezetén belül Hitelesítési Rend és Szabályozási Csoportot kell működtetnie, amely többek között jelen bizalmi szolgáltatási rend karbantartásáért is felelős.

1.5.2 Kapcsolat

A SZEÜSZ Ügyfélszolgálat elérhetőségét, nyitva tartását, a Szolgáltatóval való kapcsolattartás módját és az illetékes fogyasztóvédelmi szerv elérhetőségét a szolgáltatási szabályzat tartalmazza.

1.5.3 Szabályzat alkalmasságának meghatározása

A Szolgáltató legalább évente egyszer meg kell vizsgálja 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 kell vegye.

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

Szolgáltatónak rendelkeznie kell a szabályzatainak jóváhagyására és kiadására vonatkozó eljárásrenddel, melyet a szolgáltatási szabályzatában ismertetnie kell. Az eljárásrendben meg kell jelölni az eljárásért felelős személyt, valamint az egyéb fontos részleteket (pl. hatályba lépés napja).

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 meghatározása az alábbiakban olvasható.

Aláírás Érték: A Felhasználó (Aláíró vagy Bélyegző Létrehozó) által, a TKASZ-HSM modulban tárolt magánkulcsának felhasználásával, távolról aktivált és végrehajtott Kriptográfiai Művelet eredménye, azaz az aláírandó dokumentum(ok) lenyomatának a magánkulccsal történő titkosításával előállított digitális jelsorozat. Jelen dokumentum fogalomrendszerében az Aláírás Érték az elektronikus aláírásban, illetve elektronikus bélyegzőben elhelyezett aláírás értéket (az AdES szabványokban a `SignatureValue`) értelemszerűen, egyaránt jelenti.

Aláíró: Az elektronikus aláírás célú tanúsítvány alanya - a természetes személy - aki a tanúsítvány és a kapcsolódó elektronikus aláírás létrehozásához használt adat felhasználásával elektronikus aláírásokat hoz létre. Jelen dokumentum fogalomrendszerében az Aláíró az Előfizetővel kapcsolatban álló természetes személyt (képviseleti joggal rendelkező vagy cégjegyzésre jogosult személyt, vagy Előfizető szervezete által foglalkoztatott személyt) jelenti.

Autentikációs Folyamat: az Aláírók azonosítását elvégző folyamat, amely meg kell feleljen az ezen dokumentumban szereplő biztonsági és műszaki követelményeknek. Az Autentikációs Folyamat sikeressége előfeltétele az Aláíró TKASZ-HSM modulban tárolt magánkulcsa távolról történő aktiválásának, és így az elektronikus aláírás Aláíró által távolról történő létrehozásának.

Bélyegző Létrehozó: az elektronikus bélyegzés célú tanúsítvány alanya - a jogi személy, illetve közhiteles nyilvántartásban szereplő jogi személyiség nélküli szervezet (vagy annak valamely szervezeti egysége) - amely a tanúsítvány és a kapcsolódó elektronikus bélyegző létrehozásához használt adat felhasználásával elektronikus bélyegzőket hoz létre

CHSM: az SCDev (TKASZ-HSM) felhőalapú[2] műszaki megvalósításában elhelyezett, olyan, kizárólag csak a Szolgáltatás nyújtásához használt kriptográfiai modul (hardver elem), amely:

- olyan megbízható rendszer, melynek értékelése az MSZ/ISO/IEC 15408 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 követelményeinek; vagy
- megfelel a FIPS 140-2 3-as, illetve annál magasabb szintű követelményeknek.

Delegált Autentikáció: az {Sz4} EN 419 241-1 szabvány lehetővé teszi, hogy az Autentikációs Folyamatot külső fél végezze és meghatározza az erre vonatkozó műszaki és biztonsági követelményeket. A Delegált Autentikáció folyamatábráját az {Sz3} TS 119 431-1 szabvány 4.4

[2] felhőalapú számítástechnika: angolul „cloud computing” a számítástechnika egyik ágazata, melynek lényege, hogy a szolgáltatásokat nem egy meghatározott hardvereszközön üzemeltetik, hanem a szolgáltató eszközein elosztva, annak üzemeltetési részleteit a felhasználótól elrejtve. A szolgáltatásokat a felhasználók az Interneten keresztül érhetik el.

fejezete tartalmazza. Szolgáltató a {D2} TKASZ Szolgáltatási Szerződés megkötését megelőzően ellenőrzi, hogy a külső fél maradéktalanul teljesíti a számára meghatározott, a {D11} KDA-TKASZ követelményrendszerben szereplő, a Delegált Autentikációra vonatkozó valamennyi műszaki és biztonsági követelményt.

Előfizető: a Szolgáltatóval kapcsolatban álló jogi személy, illetve közhiteles nyilvántartásban szereplő, jogi személyiség nélküli szervezet, amely megrendeli a Szolgáltatótól a NISZ-TKASZ szolgáltatást, jellemzően a tárolt magánkulccsal a Kriptográfiai Műveletek elvégzését – a TK-EÜSZ elektronikus aláírások vagy bélyegzők létrehozása során - az általa megnevezett Felhasználók számára

Előfizető Autentikációs Tanúsítványa: a {D13} TK-EÜSZ Csatlakozási Kérelem benyújtását és Szolgáltató általi befogadását követően, a {D2} TKASZ Szolgáltatási Szerződés megkötésekor vagy azt megelőzően, Előfizető számára kiadott autentikációs tanúsítvány, amelyet a HTTPS protokoll szerinti PKI autentikációra használ

Interfész Specifikáció: ({D10}) a NISZ-TKASZ szolgáltatást kiközvetítő TK-EÜSZ-re vonatkozó műszaki dokumentáció, amely meghatározza, hogy az Előfizető által működtetett Szakrendszer milyen módon kapcsolódhat a TK-EÜSZ, illetve a NISZ-TKASZ szolgáltatáshoz, abból célból, hogy a Felhasználók (Aláírók és Bélyegző Létrehozók) a tárolt magánkulcsukkal távolról elektronikus aláírásokat/bélyegzőket hozzanak létre

Felhasználó: az Előfizető szervezetével kapcsolatban álló (pl. munkaviszonyban) természetes személy (Aláíró), valamint Előfizető szervezete, vagy annak valamely szervezeti egysége, vagy Előfizető, mint jogi személy (Bélyegző Létrehozó), aki/amely a NISZ-TKASZ szolgáltatást a TK-EÜSZ közvetítésével használja

Kriptográfiai Művelet: az elektronikus aláírás/bélyegző létrehozásához szükséges, az {Sz11} RFC 8017 szabvány által meghatározott kriptográfiai műveletek összessége, amely kiszámítja az Aláírás Értéket (a hitelesítendő dokumentum(ok) lenyomatának a Felhasználó TKASZ-HSM-ben tárolt magánkulcsával történő titkosításával előállított digitális jelsorozatot). A Kriptográfiai Műveletet a Felhasználó távolról hajtja végre, azt követően, hogy a Szolgáltatásban tárolt magánkulcsát aktiválta.

NETHSM: az SCDev (TKASZ-HSM) nem felhőalapú[3]-műszaki megvalósításában, a Szolgáltató saját informatikai rendszereinek belső hálózatában elhelyezett, kizárólag csak a Szolgáltatás nyújtásához használt hálózati kriptográfiai modul (hardver elem), amely:

- olyan megbízható rendszer, melynek értékelése az MSZ/ISO/IEC 15408 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 követelményeinek; vagy
- megfelel a FIPS 140-2 3-as, illetve annál magasabb szintű követelményeknek.

NISZ-TKASZ: a bizalmi szolgáltatás keretében tárolt magánkulcsokkal a Kriptográfiai Műveletet elvégző szolgáltatás, melynek eredményét a TK-EÜSZ közvetíti a Felhasználók felé

SCDev: az {Sz3} TS 119 431-1 szabvány 3.1 fejezetében definiált fogalom, azaz olyan konfigurált szoftver és hardver elemek összessége, melynek működési célja a tárolt magánkulcs felhasználásával az Aláírás Érték kiszámítása (a Kriptográfiai Művelet végrehajtásával)

Szakrendszer: Előfizető által működtetett informatikai rendszer, amely az Interfész Specifikáció szerint megvalósított gépi interfészen keresztül, a TK-EÜSZ közvetítésével kapcsolódik a NISZ-

[3] felhőalapú számítástechnika: angolul „cloud computing” a számítástechnika egyik ágazata, melynek lényege, hogy a szolgáltatásokat nem egy meghatározott hardvereszközön üzemeltetik, hanem a szolgáltató eszközein elosztva, annak üzemeltetési részleteit a felhasználótól elrejtve. A szolgáltatásokat a felhasználók az Interneten keresztül érhetik el.

TKASZ rendszerhez, és amellyel a Bélyegző Létrehozók, illetve az Aláírók a tárolt magánkulcsukkal végzendő Kriptográfiai Műveleteket kezdeményeznek

TK-EÜSZ: a {J7} 84/2012. (IV. 21.) Korm. rendelet 4. §-ban meghatározott, olyan, elektronikus dokumentumok hitelesítésére irányuló, a Kormány által kötelezően biztosított szabályozott elektronikus ügyintézési szolgáltatás (SZEÜSZ) vagy központi elektronikus ügyintézési szolgáltatás (KEÜSZ), melyeknél az elektronikus aláírások és bélyegzők létrehozásához szükséges Kriptográfiai Műveletek elvégzése bizalmi szolgáltatásban tárolt magánkulcsok felhasználásával is történhet

TKASZ-HSM: a Szolgáltatásban működtetett SCDev, melyet a Felhasználók távoli elektronikus aláírás/bélyegző létrehozó eszközként, távolról használnak az Aláírás Érték kiszámítására irányuló Kriptográfiai Művelet elvégzésére. A „TKASZ-HSM" jelölés a CHSM-t és a NETHSM-t együttesen jelenti. Egy Felhasználó valamely magánkulcsa vagy a CHSM-ben; vagy a NETHSM-ben kerül tárolásra. A Szolgáltatásra vonatkozó szabályzatok közösen, „TKASZ-HSM" jelöléssel tárgyalják azokat a követelményeket és előírásokat, melyek a CHSM-re és NETHSM-re azonosan vonatkoznak. Azok a fejezetek, melyek a CHSM-re és NETHSM-re vonatkozó, de eltérő, nem azonos követelményeket vagy előírásokat tárgyalnak, „[CHSM]" és „[NETHSM]" mintával jelölt külön-külön bekezdéseket tartalmaznak, melyek értelemszerűen vagy csak a CHSM-re, vagy csak a NETHSM-re vonatkoznak.

TKASZ Szolgáltatási Szerződés: Előfizető és Szolgáltató között, a NISZ-TKASZ igénybevételére megkötött szolgáltatási szerződés

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	PDF aláírási formátum

	Signature	
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 Szolgáltatónak gondoskodnia kell arról, hogy a Szolgáltatással kapcsolatos szabályzatok, valamint az egyéb közérdekű szolgáltatói információk az Előfizetők és Érintett Felek részére folyamatosan, napi 24 órában, heti hét napban rendelkezésre álljanak. A Szolgáltatónak mindent meg kell tennie annak érdekében, hogy az információk elérhetetlensége ne haladhassa meg a szolgáltatási szabályzatban meghatározott időtartamot.

2.2 A szolgáltatói információ közzététele

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

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 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.

Szolgáltatónak a Szolgáltatás nyújtása során teljesítenie kell 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 vehet. Ebben az esetben Szolgáltató teljes körűen felel a külső fél tevékenységéért, és biztosítania kell, hogy a külső fél a jelen szabályzatban előírt, vonatkozó biztonsági követelményeket maradéktalanul teljesítse.

3.2 Bélyegző Létrehozók azonosítása és jogosultság ellenőrzése

Szolgáltatónak azonosítania és hitelesítenie kell a Bélyegző Létrehozókat, mielőtt a tárolt kulcsukat használhatnák. Ennek eljárását a szolgáltatási szabályzatban kell ismertetni.

3.3 Aláírók azonosítása és jogosultság ellenőrzése

Szolgáltatónak vagy az Autentikációs Folyamatot végző külső félnek azonosítania és hitelesítenie kell az Aláírókat, mielőtt a tárolt kulcsukat használhatnák. Ennek eljárását a szolgáltatási szabályzatban kell ismertetni.

4 A SZOLGÁLTATÁS ÉS ÉLETCIKLUSA

4.1 Szolgáltatás igénylése

A szolgáltatás igénylésének folyamata röviden a következő:

- Előfizető előzetes tájékoztatása;
- {D13} TK-EÜSZ Csatlakozási Kérelem Szolgáltatóhoz történő beküldése Előfizető által;
- Előfizető teszt rendszerhez csatlakozása, Szolgáltató ellenőrzi a szükséges műszaki-technikai és biztonsági követelmények teljesülését, különös tekintettel az Előfizető (illetve az általa használt Szakrendszer) által a természetes személyek azonosítására használt Autentikációs Folyamat megfelelőségére;
- a Szolgáltatásra vonatkozó {D2} TKASZ Szolgáltatási Szerződés, valamint a minősített tanúsítványra vonatkozó BSZ-MTT {D9} szerinti - Szolgáltatási Szerződés megkötése;
- a megkötött szerződések, valamint az ehhez kapcsolódó kulcsgenerálási űrlapok ({D7}) alapján a kulcspárok generálása, azokhoz minősített tanúsítványok igénylése.

Szolgáltatónak a szolgáltatási szabályzatban kell ismertetnie a fenti folyamat eljárását és az egyes lépéseket.

4.2 Szolgáltatás üzembe állítása

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

Szolgáltatónak biztosítania kell a Szolgáltatás teljes életciklusában a tárolt kulcs és az ahhoz tartozó minősített tanúsítvány közötti összerendelés sértetlenségét.

4.3 Szolgáltatás elérhetősége és rendelkezésre állása

Szolgáltatónak a szolgáltatási szabályzatában meg kell adnia a szolgáltatás elérhetőségét és rendelkezésre állását.

4.4 A Szolgáltatás használata

Felhasználók a Szolgáltatást úgy használhatják, hogy az Interfész Specifikációnak megfelelően összeállított kérést a Szakrendszerrel – megfelelő azonosítást követően - beküldik az Interfész Specifikációban meghatározott web címre, melyre válaszként megkapják a tárolt kulccsal aláírt (elektronikus bélyegzővel vagy elektronikus aláírással hitelesített) dokumentumot tartalmazó választ.

4.4.1 Kérés elfogadása vagy visszautasítása

Szolgáltatónak ellenőriznie kell a kapott kérés formai és tartalmi megfelelőségét.

Szolgáltatónak vissza kell utasítania 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.

Szolgáltatónak el kell fogadnia és ki kell szolgálnia 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

Szolgáltatónak a szolgáltatási szabályzatában meg kell határoznia az előfizetés megszűnésének módját és eseteit.

5 FIZIKAI, ELJÁRÁSBELI ÉS SZEMÉLYZETI BIZTONSÁGI ÓVINTÉZKEDÉSEK

Szolgáltatónak gondoskodnia kell arról, hogy kellő, az irányadó szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedések, illetve az ezeket érvényre juttató adminisztratív és irányítási eljárások kerüljenek alkalmazásra.

5.1 Fizikai óvintézkedések

5.1.1 Telephely elhelyezése és szerkezeti felépítése

A Szolgáltatónak a Szolgáltatás nyújtásában közreműködő informatikai rendszereit fizikai és logikai védelemmel ellátott, legmagasabb védelmi szintet képező objektumaiban kell elhelyeznie és üzemeltetnie. A telephely elhelyezése és kialakítása során olyan egymásra épülő és egymást támogató védelmi megoldásokat kell alkalmazni, melyek képesek megakadályozni az illetéktelen hozzáférést és alkalmasak az informatikai rendszerek és Szolgáltató által tárolt bizalmas adatok megóvására.

5.1.2 Fizikai hozzáférés

Szolgáltatónak védenie kell a Szolgáltatás nyújtásában közreműködő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében.

Ehhez biztosítania kell 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

Szolgáltató a gépteremben olyan szünetmentes áramellátó rendszert kell biztosítson, 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.

Szolgáltatónak a gépteremben olyan légkondicionáló berendezést kell alkalmazni, 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

Szolgáltatónak a géptermet meg kell védenie a beázástól, víz betöréstől és elárasztástól.

5.1.5 Tűzmegelőzés és tűzvédelem

Szolgáltatónak a géptermet füst- és tűzérzékelőkkel kell felszerelni, melyek automatikusan riasztják az illetékes személyzetet. Minden helyiségben jól látható helyen kell elhelyezni a vonatkozó előírásoknak megfelelő típusú és mennyiségű tűzoltó készüléket. A gépteremben automatikus tűzoltó rendszert kell kialakítani, amely emberi egészségre nem veszélyes és nem károsítja az informatikai eszközöket.

5.1.6 Adathordozók tárolása

Szolgáltatónak meg kell védenie valamennyi adathordozóját a jogosulatlan hozzáféréstől, a megsemmisüléstől vagy véletlen rongálódástól.

5.1.7 Selejt kezelése és megsemmisítése

Szolgáltatónak a környezetvédelmi előírások betartásával kell gondoskodnia feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről. A felesleges eszközöket és adathordozókat az erre kijelölt munkatárs személyes felügyelete mellett, széleskörűen elfogadott módszerekkel használhatatlanná kell tenni vagy visszaállíthatatlan módon törölni kell.

5.1.8 Fizikailag elkülönítetten őrzött mentési példányok

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

Szolgáltatónak biztosítania kell, hogy az adatmentést vagy abból a helyreállítást csak rendszerüzemeltető bizalmi munkakört betöltő személy végezze el.

5.2 Eljárásbeli előírások

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

5.2.1 Bizalmi munkakörök

Szolgáltatónak egyértelműen azonosítania kell azokat a munkaköröket, amelyektől a Szolgáltatás biztonsága függ. Ezeket a bizalmi munkaköröket és felelősségeket dokumentálni kell. A jogosultságokat és funkciókat olyan módon kell megosztani az egyes bizalmi munkakörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére. Szolgáltatónak biztosítania kell, hogy minden bizalmi munkakör betöltésre kerüljön.

A bizalmi munkakört betöltő személynek munkaviszonyban kell állnia Szolgáltatóval. Bizalmi munkakörbe a Szolgáltató felső vezetősége kell kinevezze a munkatársakat.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

Szolgáltató biztonsági szabályzataiban elő kell írni, hogy csak védett környezetben, legalább kettő, bizalmi munkakört betöltő munkatárs egyidejű fizikai jelenlétében 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 személyeket azonosítani és hitelesíteni kell, mielőtt a Szolgáltatás nyújtásában érintett, kritikus informatikai rendszerekhez hozzáférnének.

5.2.4 Egymást kizáró munkakörök

A Szolgáltatónak biztosítania kell, 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) meg kell valósítani a bizalmi munkakörök teljes személyi szétválasztását.

5.3 Személyzetre vonatkozó előírások

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

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

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

5.3.2 Biztonsági háttér ellenőrzés eljárásai

A Szolgáltató vezetői munkakörben, illetve bizalmi munkakörben csak olyan alkalmazottakat foglalkoztathat, 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.

5.3.3 Képzési követelmények

A bizalmi munkakörökben Szolgáltató olyan személyeket foglalkoztathat, akik az adott munkakör 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

Szolgáltatónak gondoskodnia kell arról, hogy a munkatársak folyamatosan a megfelelő tudással rendelkezzenek, szükség esetén továbbképzést vagy ismétlő jellegű képzést kell tartania.

Rendszeresen (pl. évente egyszer) továbbképzést kell biztosítani az újonnan ismertté vált sebezhetőségekről, az IT biztonság aktuális gyakorlatáról, a munkatársak saját szakterületét érintően.

5.3.5 Felhatalmazás nélküli tevékenységek büntető következményei

Szolgáltatónak a dolgozókkal kötendő munkaszerződésben szabályoznia kell 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 foglalkoztathat.

Az egyéb feladatok ellátására, vállalkozási vagy megbízási szerződésben foglalkoztatott személyeket Szolgáltató csak előzetes biztonsági ellenőrzést követően foglalkoztathatja. Az ellenőrzött személyekkel írásos megállapodást kell kötni, melyben rögzíteni kell az esetleges biztonsági szabályokat és a titoktartásra vonatkozó kikötéseket.

5.3.7 A személyzet számára biztosított dokumentációk

Szolgáltatónak folyamatosan biztosítania kell a személyzet részére a munkakörük ellátásához szükséges dokumentációk és szabályzatok rendelkezésre állását.

5.4 A biztonsági naplózás folyamatai

5.4.1 Naplózott esemény típusok

Szolgáltatónak minden, az informatikai rendszerével és a Szolgáltatás nyújtásával kapcsolatos eseményt naplóznia kell. A naplózott adatállománynak a szolgáltatás nyújtásának teljes folyamatát át kell fognia, és lehetővé tennie, hogy a valós helyzetek megítéléséhez a szükséges mértékben minden, a Szolgáltatással kapcsolatos eseményt rekonstruálni lehessen.

5.4.2 Naplóállomány feldolgozásának gyakorisága

Szolgáltatónak biztosítania kell a naplóállományok rendszeres ellenőrzését és kiértékelését.

5.4.3 Naplóállomány megőrzési időtartama

A naplóállományokat archiválni kell és gondoskodni azok biztonságos megőrzéséről az 5.5.2 fejezetben előírt időtartamig.

5.4.4 Naplóállomány védelme

A naplóállomány minden bejegyzését védeni kell a módosítástól, illetve biztosítani kell, hogy a napló tartalmához csak arra feljogosított személyek férhessenek hozzá.

A naplóállományok kezelését olyan módon kell megoldani, hogy kizárható legyen a napló megsemmisülése, a napló bejegyzések törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása.

5.4.5 Naplóállomány mentési folyamatai

A naplóállományokról rendszeres mentést kell készíteni.

5.4.6 Naplózás gyűjtési rendszere

A naplóbejegyzések gyűjtését belső komponenssel kell megoldani. A naplóbejegyzések gyűjtésének meg kell kezdődnie rendszer indításkor és rendszer leállításig folyamatosan működnie kell, és közben biztosítania kell a gyűjtött bejegyzések integritását és rendelkezésre állását, szükség esetén a bizalmasságát is.

A naplóbejegyzések gyűjtési rendszerének működési rendellenessége esetén Szolgáltatónak fel kell függesztenie az érintett területek működését az üzemzavar elhárításáig.

5.4.7 Rendellenes eseményeket kiváltó alanyok értesítése

Nincs kikötés.

5.4.8 Sebezhetőség értékelések

Szolgáltatónak rendszeres időközönként, a naplóállományok és egyéb információk kiértékelésén alapuló sebezhetőség vizsgálatot és behatolás tesztet kell végeznie, mely segítségével feltérképezi a potenciális belső és külső fenyegetéseket, melyek jogosulatlan hozzáférést eredményezhetnek, vagy a Szolgáltatásban kezelt adatok megmásítását, módosítását, sérülését vagy megsemmisülését eredményezhetik.

Szolgáltatónak folyamatosan figyelemmel kell kísérnie az újonnan ismertté vált, kritikus sebezhetőségeket, és a szükséges ellenintézkedéseket lehetőség szerint 48 órán belül meg kell tennie. Bármely olyan sebezhetőség esetén, melynek kihatása lehet a Szolgáltatás nyújtására, Szolgáltatónak vagy cselekvési tervet kell készítenie és végrehajtania annak érdekében, hogy a sebezhetőség ne legyen kihasználható, illetve annak hatása elhanyagolható legyen, vagy dokumentálnia kell annak ténybeli alapját, hogy az adott sebezhetőség nem igényel intézkedést.

5.5 Adatok archiválása

5.5.1 A tárolt adatok típusai

Szolgáltatónak gondoskodnia kell 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;
- az 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 köteles megőrizni, 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.

5.5.3 Archívum védelme

Szolgáltatónak biztosítania kell valamennyi archivált adatra azok sértetlenségét és hitelességét, a rendelkezésre állását és a bizalmasságát.

5.5.4 Archívum mentési eljárásai

Szolgáltatónak biztosítania kell az iratok, dokumentumok, elektronikus állományok biztonságos, hosszú távú megőrzését, illetve tárolását, továbbá az elektronikus formában archivált állományok adathordozóinak elavulás elleni védelmét a megőrzési időn belül.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi naplóbejegyzést el kell látni olyan időjellel, melyben legalább egy másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

Az elektronikus formában archivált adatokon legalább fokozott biztonságú elektronikus aláírást vagy bélyegzőt, valamint minősített időbélyeget kell elhelyezni.

Az archivált adatok megőrzése során szükség esetén (pl. algoritmus váltás) gondoskodni kell az elektronikus aláírások, bélyegzők és időbélyegzők hitelességének fenntartásáról.

5.5.6 Archívum gyűjtési rendszere

A naplóállományokat és az egyéb elektronikusan keletkezett adatokat a Szolgáltató védett informatikai rendszerén belül kell gyűjteni. A védett informatikai rendszerből történő kimozgatás során az adatokat minősített időbélyeget tartalmazó elektronikus aláírással vagy bélyegzővel kell ellátni.

A papíralapú iratokat Szolgáltató dokumentumtárában kell tárolni.

5.5.7 Archívum hozzáférés és ellenőrzés eljárásai

Szolgáltatónak az archivált adatokat meg kell védenie a jogosulatlan hozzáféréstől. A jogosult hozzáféréseket naplózni kell.

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 köteles meghozni minden szükséges intézkedést 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 meg kell, hogy előzze.

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

A bekövetkezett incidens kiértékelése alapján Szolgáltatónak meg kell hoznia a szükséges módosító, javító intézkedéseket, hogy az incidens jövőbeli előfordulását megakadályozza.

5.7.1 Rendkívüli események és kompromittálódás kezelésének eljárásai

Szolgáltatónak rendelkeznie kell üzletmenet folytonossági tervvel.

Rendkívüli üzemeltetési helyzetben Szolgáltatónak dokumentálnia kell az eseményeket, azok körülményeit, az elhárításukra megtett intézkedéseket.

Szolgáltatónak ki kell alakítani és fenntartani egy tartalék rendszert, mely a rendkívüli üzemeltetési helyzetben képes a nyilvános szabályzatok elérhetőségét biztosítani.

A rendkívüli üzemeltetési helyzetben Szolgáltatónak a lehető legrövidebb időn belül tájékoztatást kell közzé tennie internetes honlapján, valamint - lehetőség szerint - elektronikus levélben kell értesítenie azokat a személyeket, akiket az esemény érint.

5.7.2 Sérült számítási erőforrások, szoftverek és/vagy adatok

Szolgáltatónak olyan megbízható rendszert kell működtetni, mely a rendszerben bekövetkezett hiba esetén is biztosítja a Szolgáltatás működtetését és elérhetőségét.

5.7.3 Előfizetői magánkulcsok kompromittálódása esetén követendő eljárás

Az előfizetői magánkulcsok kompromittálódása esetén haladéktalanul meg kell tenni a szükséges lépéseket:

- megszüntetni az érintett magánkulcsok használatát;
- értesíteni Előfizető Kapcsolattartóját és kezdeményezni az érintett tanúsítványok visszavonatását;
- intézkedni valamennyi érintett fél értesítéséről.

5.7.4 Üzletmenet folytonosság helyreállás katasztrófát követően

Szolgáltatónak rendelkeznie kell tartalék helyszínnel és informatikai rendszerrel, továbbá megtervezett eljárásokkal az áttelepülésre.

5.8 A szolgáltatási tevékenység megszüntetése

Szolgáltatónak rendelkeznie kell a szolgáltatási tevékenység megszüntetésére vonatkozó, aktualizált tervvel.

Szolgáltatónak rendelkeznie kell 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.

A szolgáltatási tevékenység megszüntetésére vonatkozó tervnek tartalmaznia kell legalább az alábbiakat:

- Előfizetők és Érintett Felek értesítésének módja;

- a Szolgáltatással kapcsolatos azon kötelezettségek átadása egy másik bizalmi szolgáltatónak, melyek arra vonatkoznak, hogy bizonyítékot szolgáltassanak a Szolgáltató működésével kapcsolatban - különösen az 5.5.1 fejezetben meghatározott adatoknak a megőrzése az 5.5.2 fejezetben megjelölt időtartamig;
- Szolgáltató informatikai rendszerében foglalt adatokról teljes körű mentés készítése.

6 MŰSZAKI BIZTONSÁGI ÓVINTÉZKEDÉSEK / TECHNICAL SECURITY CONTROLS

6.1 Kulcspár előállítás és telepítés

6.1.1 Kulcspár előállítás

6.1.1.1 Szolgáltatói kulcsok előállítása

Szolgáltató maga kell előállítsa a Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsokat, fizikailag védett környezetben, kriptográfiai modulban (HSM), legalább két bizalmi munkakört betöltő személy részvételével, illetéktelen személy jelenlétének kizárásával. A kriptográfiai modulnak meg kell felelnie a 6.2.1 fejezet szerinti követelményeknek.

6.1.1.2 Előfizetői kulcspárok előállítása

Szolgáltatónak 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 kell végeznie az előfizetői kulcspárok generálását megelőzően. A TKASZ-HSM modulnak meg kell felelnie a 6.2.1 fejezet szerinti követelményeknek.

Szolgáltató a 6.1.5 és 6.1.6 fejezetek szerinti algoritmusra és kulcshosszra vonatkozó követelményeknek megfelelő előfizetői kulcspárokat az erre szolgáló TKASZ-HSM modulban kell előállítsa, szigorúan védett környezetben, kizárólag bizalmi munkakört betöltő személyek jelenlétében.

[CHSM] A generálást követően az előfizető kulcspárokat a Szolgáltató infrastrukturális kulcsain alapuló titkosított export állományban kell tárolni, majd a CHSM modulból törölni. A titkosításhoz használt szolgáltatói infrastrukturális kulcs algoritmusa és hossza erősebb kell legyen, mint az általa védett előfizető kulcspárok algoritmusa, illetve hossza. A titkosított export állományt a CHSM modul erre szolgáló, tanúsítással rendelkező biztonsági funkciójával kell előállítani. A későbbiekben, az előfizetői magánkulcs aktiválása során, a kulcspárokat a titkosított export állományból kell a CHSM modulba visszatölteni (importálni), használatuk a CHSM modulból történik. Az importálást a CHSM modul erre szolgáló, tanúsítással rendelkező biztonsági funkciójával kell elvégezni.

[NETHSM] Az előfizetői kulcspároknak teljes életciklusuk alatt a NETHSM modulban kell maradniuk.

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 kell eljuttassa 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

A Szolgáltatónak a Szolgáltatás nyújtása során - mind a szolgáltatói, mind az előfizetői kulcsok tekintetében - a Bizalmi Felügyelet vonatkozó határozatának megfelelő olyan szabványos algoritmusokat, paramétereket és kulcshosszakat kell használnia, melyek a kulcs generálását követő legalább két év hosszú időtartamra megfelelően erősnek tekinthetők.

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 kell történjen. A szolgáltatói kulcsok generálása során Szolgáltatónak be kell tartania a HSM modul tanúsítási jelentésében foglalt előírásokat is.

Az előfizetői kulcspárok előállítása a 6.1.1.2 fejezet szerint, szigorúan védett környezetben és tanúsított TKASZ-HSM modulban, kizárólag bizalmi munkakört betöltő személyek jelenlétében kell történjen. Az előfizetői kulcspárok generálása során Szolgáltatónak be kell tartania a TKASZ-HSM modul tanúsítási jelenlétében 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 előállítására, tárolására és használatára csak olyan kriptográfiai modult (TKASZ-HSM) alkalmazhat, 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.

Szolgáltatónak rendszeres időközönként ellenőriznie kell minden, a Szolgáltatásban használt HSM és TKASZ-HSM modul tanúsított állapotának meglétét, és figyelemmel kíséri a tanúsítás lejáratának időpontját. A tanúsított állapot várható megváltozása esetén időben meg kell tennie a szolgáltatási szabályzatában dokumentált, megfelelő intézkedéseket.

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

Szolgáltatónak alkalmaznia kell 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 kell kerüljenek. A mentést titkosított formában, speciális eszközök alkalmazásával kell megvalósítani, megfelelő biztonsági óvintézkedések és eljárási szabályok betartásával.

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

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 kell történjen.

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 előfizetői kulcspárok bejuttatása a CHSM modulba a Szolgáltató infrastrukturális kulcsain alapuló titkosított export állományokból a CHSM modul erre szolgáló, tanúsítással rendelkező biztonsági funkciójával kell történjen (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 tárolásának módja

A Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsok teljes életciklusa alatt a 6.2.1 fejezetben leírt HSM modulban kell történjen.

[CHSM] Az előfizetői kulcspárok felhasználása minden esetben a CHSM modulból kell történjen, olyan módon, hogy az adott előfizetői 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 kell tárolni, 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 kell végezze. Szolgáltatónak biztosítania kell, 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 előfizetői 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. Szolgáltatónak biztosítania kell, 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 előfizetői magánkulcs aktív állapotba kerül, a Felhasználó képes a magánkulcsát használni az elektronikus aláírásának vagy bélyegzőjének létrehozásához szükséges Kriptográfiai Művelet elvégeztetésére. Szolgáltatónak biztosítania kell, hogy az aktivált NETHSM modul jogosulatlan hozzáférés ellen védett legyen.

6.2.8 Magánkulcs aktív állapotának megszüntetési módja

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

6.2.9 Magánkulcs megsemmisítésének módja

A Szolgáltatás nyújtásához használt informatikai rendszer működtetéséhez szükséges infrastrukturális és vezérlő kulcsokat visszaállíthatatlan módon meg kell semmisíteni, amikor használatuk már nem szükséges. A kulcsokat és az aktiválásukhoz szükséges minden adatot

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

Az előfizetői kulcspárokat meg kell semmisíteni, amikor:

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

Az előfizetői kulcspárokat és az aktiválásukhoz szükséges minden adatot olyan módon kell megsemmisíteni, hogy annak végrehajtása után a magánkulcs semmilyen része ne legyen kikövetkezhető vagy levezethető. Az előfizetői kulcspár megsemmisítésével egyidejűleg törölni kell a Szolgáltatás nyújtásához használt informatikai rendszer nyilvántartásából az adott kulcspárhoz tartozó tanúsítványt.

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

Szolgáltatónak biztosítania kell, hogy egy előfizetői kulcspár csak azt követően legyen 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.

Szolgáltatónak biztosítania kell, 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

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

6.4.2 Aktivizáló adatok védelme

Szolgáltatónak biztosítania kell, hogy a TKASZ-HSM modulban tárolt 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.

Ennek alapján Szolgáltatónak olyan megbízható informatikai rendszert (beleértve a redundáns kiépítést) és technikákat kell kialakítania és üzemeltetnie, melyek biztosítják a Szolgáltató megbízható működését a Szolgáltatás nyújtásához. Ennek ismertetését Szolgáltató részben a szolgáltatási szabályzatában (BSZ-NISZ-TKASZ), részben a belső biztonsági szabályzataiban írja le.

6.5.2 Informatikai biztonsági értékelés

Szolgáltatónak az informatikai rendszerek biztonsági értékelését az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény rendelkezései szerint kell elvégeznie.

6.6 Életciklusra vonatkozó műszaki óvintézkedések

6.6.1 Rendszerfejlesztési óvintézkedések

Szolgáltatónak gondoskodnia kell 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.

6.6.2 Biztonságkezelési óvintézkedések

Szolgáltató olyan eszközöket és eljárásokat kell alkalmazzon, 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 belső társasági szintű és rendszer szintű információbiztonsági szabályzata tartalmazza.

6.6.3 Életciklus biztonsági óvintézkedések

Szolgáltatónak a szolgáltatási szabályzatban meghatározott rendszeres időközönként el kell végeznie 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.

6.7 Hálózatbiztonsági óvintézkedések

A hálózati védelmi intézkedéseket a Szolgáltató belső biztonsági szabályzatában meghatározott követelményeknek megfelelően kell megvalósítani, figyelembe véve az {Sz2} EN 319 401 szabvány 7.8 fejezetében leírt követelményeket is.

6.8 Időforrások

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

7 TANÚSÍTVÁNY, CRL ÉS OCSP PROFILOK

7.1 Tanúsítvány profil

Az előfizetői kulcspárokhoz kibocsátott minősített tanúsítvány profilja meg kell feleljen a {D8} „Bizalmi Szolgáltatási Rend minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BR-MTT) 7.1 fejezetében leírtaknak.

7.2 CRL profil

Az előfizetői kulcspárokhoz kibocsátott minősített tanúsítvány visszavonási állapotának ellenőrzéséhez használható CRL-ek profilja meg kell feleljen a {D8} „Bizalmi Szolgáltatási Rend minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BR-MTT) 7.2 fejezetében leírtaknak.

7.3 OCSP profil

Az előfizetői kulcspárokhoz kibocsátott minősített tanúsítvány visszavonási állapotának ellenőrzéséhez használható OCSP válaszok profilja meg kell feleljen a {D8} „Bizalmi Szolgáltatási Rend minősített elektronikus aláírás és elektronikus bélyegzés célú tanúsítványokhoz” (BR-MTT) 7.3 fejezetében leírtaknak.

8 MEGFELELŐSÉG VIZSGÁLAT ÉS EGYÉB ÉRTÉKELÉSEK

Jelen bizalmi szolgáltatás rend előírja 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

Szolgáltatónak külső és belső vizsgálatokat és értékeléseket kell elvégeznie, illetve elvégeztetnie annak érdekében, hogy a Szolgáltatással kapcsolatos folyamatai, személyzete, eszközei és környezete mindenkor megfeleljen a vonatkozó jogszabályi és szakmai követelményeknek.

A Szolgáltató vizsgálatának gyakorisága és körülményei meg kell feleljenek a hatályos jogszabályi előírásoknak.

8.2 Auditor azonosítása és képesítése

A külső rendszervizsgálói auditokra Szolgáltató olyan szakértőt vagy szakértői szolgáltatásokat nyújtó szervezetet kell megbízzon, 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 kell legyenek Szolgáltatótól.

8.4 Audit során vizsgált területek

Az audit az alábbi területeket kell lefedje:

- 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:

- 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 kell készítsen. A hiányosságokat köteles késlekedés nélkül orvosolni, az intézkedéseket dokumentálni és ellenőrizni.

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 Szolgáltatás díjaival kapcsolatos információkat a szolgáltatási szabályzat kell tartalmazza.

9.2 Anyagi felelősség

Szolgáltatónak az anyagi felelősség mértékéről, illetve annak korlátairól a szolgáltatási szabályzatban rendelkeznie kell.

9.2.1 Biztosítási fedezet

Szolgáltatónak felelősségbiztosítással kell rendelkeznie, mely egyaránt kiterjed az elektronikus aláírással vagy bélyegzővel, illetve az ezzel ellátott elektronikus dokumentummal szerződésen kívül okozott károkra és szerződésszegéssel okozott károkra, valamint a Bizalmi Felügyeletnél felmerült jogszabály szerint költségekre, és amely fedezetet biztosít az összes károsultnak okozott kárra, a szolgáltatási szabályzatban leírtak szerint.

A felelősségbiztosítási szerződésnek meg kell felelnie a {J8} 24/2016 rendelet előírásainak is.

9.3 Üzleti információk bizalmassága

9.3.1 Bizalmasan kezelendő információk köre

Szolgáltatónak a szolgáltatási szabályzatban meg kell adnia a bizalmasan kezelendő információk körét.

9.3.2 Nem bizalmasnak tekintett információk köre

Nincs kikötés.

9.3.3 Bizalmas információk védelmének felelőssége

Szolgáltatónak meg kell védenie a bizalmas információkat. A bizalmas információk védelmét a személyzet megfelelő képzésével, továbbá a munkavállalókkal, szerződéses partnerekkel megkötött szerződésekkel kell érvényre juttatni.

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, mely nyilvános dokumentum, és elérhető

Szolgáltató internetes honlapján. Ezen dokumentum összhangban vannak a nemzetközi és hazai vonatkozó jogszabályokkal.

9.4.2 Bizalmasként kezelendő személyes adatok

Szolgáltató csak Előfizetőtől közvetlenül gyűjthet személyes adatot és csak olyan mértékben, ami a Szolgáltatás nyújtásához 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

Szolgáltatónak gondoskodnia kell a személyes adatok védelméről, működése és szabályzatai meg kell feleljenek 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 jelen bizalmi szolgáltatási rendben és a vonatkozó 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 végzik.

9.6.2 SZEÜSZ Ügyfélszolgálat felelőssége és helytállása

Az ügyfélszolgálati tevékenységeket Szolgáltató saját szervezetén belül üzemeltetett SZEÜSZ Ügyfélszolgálata kell végezze. A SZEÜSZ Ügyfélszolgálat be kell tartsa a rá vonatkozó, jogszabályokban, illetve a Szolgáltató szabályzataiban foglalt előírásokat.

Szolgáltató felelőssége a Szolgáltatás nyújtása során:

- szerződéskötést megelőző tájékoztatás;
- 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 TKASZ Szolgáltatási Szerződés előkészítése és megkötése.

9.6.3 Előfizető felelőssége és helytállása

Előfizető jogai

Előfizető jogosult:

- a Szolgáltatást igénybe venni a 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 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 szolgáltatási 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 a 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 tanúsítványok 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.

9.7 Helytállás érvénytelenségi köre

A helytállás érvénytelenségi körét a szolgáltatási szabályzatban meg kell határozni.

9.8 Felelősség korlátozása

Szolgáltató korlátozhatja a kártérítési felelősségét:

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

9.9 Kártérítések

A kártérítésekről a szolgáltatási szabályzatban kell rendelkezni.

9.10 Hatályosság és megszűnés

9.10.1 Hatályosság

Időbeli hatály

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

Tárgyi hatály

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

Személyi hatály

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

9.10.3 Megszűnés után is hatályban maradó rendelkezések

A megszűnés után is hatályban maradó rendelkezéseket a szolgáltatási szabályzatban meg kell határozni.

9.11 Egyéni hirdetmények és kommunikáció a részvevőkkel

A szolgáltatási szabályzatban rendelkezni kell a felek és részvevők közötti kommunikáció joghatást kiváltó módjairól.

9.12 Módosítások

9.12.1 Módosítás eljárása

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

9.12.2 Értesítés módszere és időtartama

A Szolgáltatás jelentős vagy lényeges változása esetén Szolgáltatónak internetes honlapján közleményt kell közzé tennie, a hatályba lépést megelőzően kellő időben ahhoz, hogy az érintett felek a változásokra felkészülhessenek.

9.12.3 OID megváltozását előidéző körülmények

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

9.13 Vitás kérdések rendezése

A vitás kérdések rendezéséről a szolgáltatási szabályzatban kell rendelkezni.

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 bizalmi szolgáltatási rend 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 bizalmi szolgáltatási rend más rendelkezésének megsértése esetén is lemondana a kártérítési igény érvényesítéséről.

9.16.3 Force Majeure (Vis maior)

A szolgáltatási szabályzat tartalmazza.

9.17 Egyéb rendelkezések

A Szolgáltatást és a Szolgáltatás során alkalmazott végfelhasználói termékeket hozzáférhetővé kell tenni a fogyatékossággal élő személyek számára, amennyiben az lehetséges.