MICROSEC

e-Szignó Hitelesítés Szolgáltató

eIDAS Rendelet szerinti elektronikus aláírás/bélyegző létrehozására alkalmas távoli kulcsmenedzsment szolgáltatás szolgáltatási szabályzat

ver. 3.10

Hatálybalépés: 2023-10-30

Azonosító	1.3.6.1.4.1.21528.2.1.1.207
Verzió	3.10
Első verzió hatálybalépése	2022-03-31
Biztonsági besorolás	NYILVÁNOS
Jóváhagyta	Vanczák Gergely
Jóváhagyás dátuma	2023-10-26
Hatálybalépés dátuma	2023-10-30

Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság

1033 Budapest, Ángel Sanz Briz út 13.

Verzió	Hatálybalépés	A változás leírása
2.25	2022-03-31	Új dokumentum.
3.1	2022-08-31	- Általános felülvizsgálat. - Szolgáltatási rend OID szabályok változása.
3.3	2022-11-30	- Általános felülvizsgálat. - Kapcsolattartó személy. - Ügyféltér bevezetése. - Szabályzat OID szabályok változása.
3.7	2023-08-30	- Általános felülvizsgálat. - Biztonsági incidensek kezelése. - Támogatott kriptográfiai algoritmusok.
3.10	2023-10-30	- JWT bevezetése.

Table of Contents

1 Bevezetés

Jelen dokumentum a Microsec Számítástechnikai Fejlesztő zrt. (továbbiakban: Microsec vagy *Távoli kulcsmenedzsment szolgáltató*) által üzemeltetett e-Szignó Hitelesítés Szolgáltató távoli kulcsmenedzsment szolgáltatásra vonatkozó *Távoli kulcsmenedzsment szolgáltatási szabályzat*a.

A *Távoli kulcsmenedzsment szolgáltató* szolgáltatásait a vele szerződéses viszonyban álló *Ügyfel*ek részére biztosítja.

Jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* a fenti szolgáltatások nyújtásának kereteit, a részletes eljárási és egyéb működési szabályokat tartalmazza.

A *Távoli kulcsmenedzsment szolgáltatási szabályzat* megfelel az eIDAS Rendelet [1] által támasztott követelményeknek. A Távoli kulcsmenedzsment szolgáltatást a Microsec mint eIDAS szerinti minősített bizalmi szolgáltató egy önálló szolgáltatás komponensként nyújtja. A Távoli kulcsmenedzsment szolgáltatás kapcsolódik a *Távoli kulcsmenedzsment szolgáltató* által nyújtott további szolgáltatásokhoz, amelyek szükségesek a Távoli kulcsmenedzsment szolgáltatás igénybe vételéhez:

- az *Ügyfél*nek rendelkeznie kell egy Tanúsítvánnyal, amely a Távoli kulcsmenedzsment szolgáltatás keretében kezelt végfelhasználói magánkulcshoz tartozó nyilvános kulcsot tartalmazza
- az *Ügyfél*nek rendelkeznie kell egy mobil eszközzel, amely alkalmas a Microsec által biztosított PassByME mobil azonosító alkalmazás futtatására.

A Távoli kulcsmenedzsment szolgáltatás keretében a *Távoli kulcsmenedzsment szolgáltató* megfelelően biztonságos körülmények között kezeli az *Ügyfel*ek magánkulcsait, amelyek teljes életciklusuk folyamán az *Ügyfel*ek kizárólagos kontrollja alatt állnak.

A *Távoli kulcsmenedzsment szolgáltató* biztosítja a szükséges műszaki és eljárási feltételeket annak érdekében, hogy az *Ügyfel*ek – a *Távoli kulcsmenedzsment szolgáltató* által tárolt magánkulcsaikkal – kulcs műveleteket végezhessenek el.

A Távoli kulcsmenedzsment szolgáltatás igénybevételével az *Ügyfel*ek elektronikus aláírásokat vagy bélyegzőket is létrehozhatnak.

1.1 Áttekintés

Jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* célja, hogy összefoglalja mindazokat az információkat, amelyeket a *Távoli kulcsmenedzsment szolgáltató*val kapcsolatba kerülő *Ügyfel*eknek tudniuk érdemes. Ezzel elő kívánja segíteni, hogy *Ügyfel*ei és leendő *Ügyfel*ei:

- minél könnyebben megismerhessék a *Távoli kulcsmenedzsment szolgáltató* által kínált szolgáltatások részleteit, feltételeit és a szolgáltatás nyújtásának gyakorlati hátterét;
- átláthassák a *Távoli kulcsmenedzsment szolgáltató* működését, és ennek révén minél könnyebben eldönthessék, hogy a szolgáltatások megfelelnek-e, illetve az egyes szolgáltatások melyik típusa felel meg igényeiknek, elvárásaiknak.

Jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* tartalmilag és formailag az IETF RFC 3647 [14] keretrendszer követelményein alapul, de nem maradéktalanul követi az ott meghatározott

struktúrát. Vannak olyan fejezetek az IETF RFC 3647 szabványban, amelyek csak Hitelesítés-szolgáltatás esetében értelmezhetők és nincs jelentőségük a Távoli kulcsmenedzsment szolgáltatás esetében. Ezek a fejezetek teljesen hiányoznak a jelen szabályzatból, így a meglévő fejezetek számozása nem követi pontosan az IETF RFC 3647 fejezet számozását. Másrészt a *Távoli kulcsmenedzsment szolgáltatási szabályzat* tartalmaz olyan további új részeket, amelyek a Távoli kulcsmenedzsment szolgáltatás esetében lényegesek.

A végfelhasználóknak az igénybe vett szolgáltatással kapcsolatos tevékenységére vonatkozó előírásokat jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat*on kívül az Általános Szerződési Feltételek, a szolgáltatóval kötött Szolgáltatási szerződés, illetve egyéb, a *Távoli kulcsmenedzsment szolgáltató*tól független szabályzat illetve dokumentum is tartalmazhat.

A jelen dokumentum 1.5 fejezete számos fogalmat definiál, amelyeket más területeken nem, vagy nem teljesen ilyen értelmezésben használnak. Az ilyen értelemben használandó fogalmakat a dokumentumban minden esetben nagy kezdőbetűvel írva, döntött betűk használatával jelöljük.

1.2 Dokumentum neve és azonosítója

Kibocsátó	e-Szignó Hitelesítés Szolgáltató
Dokumentum címe	eIDAS Rendelet szerinti elektronikus aláírás/bélyegző létrehozására alkalmas távoli kulcsmenedzsment szolgáltatás szolgáltatási szabályzat
Dokumentum verziószáma	3.10
Hatálybalépés ideje	2023-10-30

1.2.1 Szolgáltatási rend

A jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* az alábbi ETSI TS 119 431-1 [12] szerinti bizalmi szolgáltatási rendnek való megfelelést vállalja fel:

- LSCP (OID: 0.4.0.19431.1.1.1)

1.2.2 Hatály

Tárgyi hatály

A *Távoli kulcsmenedzsment szolgáltatási szabályzat* az 1.3.1. fejezetben ismertetett szolgáltatások nyújtására és igénybevételére vonatkozik.

Időbeli hatály

A *Távoli kulcsmenedzsment szolgáltatási szabályzat* jelen verziója 2023-10-30 -i hatálybalépési dátumtól visszavonásig hatályos. A hatályosság automatikusan megszűnik a szolgáltatások beszüntetésekor vagy a *Távoli kulcsmenedzsment szolgáltatási szabályzat* újabb verziójának hatályba lépésekor.

Személyi hatály

A *Távoli kulcsmenedzsment szolgáltatási szabályzat* személyi hatálya kiterjed az 1.3. alfejezetben azonosított közösség minden tagjára.

A *Távoli kulcsmenedzsment szolgáltató* elsősorban az Európai Unió állampolgárai és az Európai Unió területén bejegyzett szervezetek részére nyújtja bizalmi szolgáltatásait, de nem zárja ki szolgáltatásaiból más országok természetes és jogi személyeit sem, amennyiben azok elfogadják a *Távoli kulcsmenedzsment szolgáltató* által követett szabályrendszert és a szolgáltatások nyújtásához szükséges ellenőrzések kellően biztonságosan és gazdaságosan megvalósíthatók.

Fogyatékkal élők

A *Távoli kulcsmenedzsment szolgáltató* törekszik arra, hogy az általa nyújtott szolgáltatásokhoz a lehető legmagasabb színvonalon biztosítsa az egyenlő esélyű hozzáférést.

A szolgáltatás esélyegyenlőségének megteremtése érdekében minden lehetséges és ésszerű eszköz alkalmazásával törekszik arra, hogy szolgáltatásai akadálymentesen elérhetőek legyenek a fogyatékkal élő személyek számára is. Különösen fontos számára, hogy a fogyatékkal élő ügyfelek a fogyatékossággal nem érintett ügyfelekkel azonos minőségű, speciális igényeikhez igazodó szolgáltatásban részesülhessenek.

A *Távoli kulcsmenedzsment szolgáltató* az ügyfelekkel együttműködve, a *Távoli kulcsmenedzsment szolgáltatási szabályzat* által meghatározott keretek között törekszik a személyes igényeknek leginkább megfelelő ügyintézési forma biztosítására.

Területi hatály

A jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* szerint nyújtott Távoli kulcsmenedzsment szolgáltatás az egész világon elérhető.

A használat előfeltétele a megfelelő minőségű internet szolgáltatás elérhetősége.

A jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* szerint létrehozott elektronikus aláírások iletve bélyegzők érvényessége független attól, hogy mely földrajzi helyről aktiválták a magánkulcsokat.

A Távoli kulcsmenedzsment szolgáltatás igénybevételével létrehozott elektronikus aláírások joghatásáról a magánkulcshoz tartozó *Tanúsítvány*t kibocsátó Hitelesítésszolgáltató vonatkozó Szolgáltatási szabályzatában található információ.

A jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* szerint nyújtott Távoli kulcsmenedzsment szolgáltatás kizárólag a jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat*ban leírtak szerint használható fel.

1.3 PKI szereplők

1.3.1 Bizalmi Szolgáltató

A *Távoli kulcsmenedzsment szolgáltató* adatai

Név:	Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság
Cégjegyzékszám:	01-10-047218 Fővárosi Törvényszék Cégbírósága
Székhely:	1033 Budapest, Ángel Sanz Briz út 13.
Telefonszám:	(+36-1) 505-4444
Telefax szám:	(+36-1) 505-4445
Internet cím:	`https://www.microsec.hu`, `https://www.e-szigno.hu`

Ügyfélszolgálati iroda

A szolgáltató egység neve:	e-Szignó Hitelesítés Szolgáltató
Ügyfélszolgálati iroda:	
	1033 Budapest, Ángel Sanz Briz út 13., Graphisoft Park Déli Terüet, SP3 épület
Ügyfélszolgálati iroda nyitvatartási ideje:	munkanapokon 8:30-16:30 között előzetes időpont egyeztetés alapján
Ügyfélszolgálati iroda telefonszáma:	(+36-1) 505-4444
Ügyfélszolgálati iroda email címe:	`info@e-szigno.hu`
Visszavonási kérelmek fogadása:	`visszavonas@e-szigno.hu`
A szolgáltatással kapcsolatos információk elérése:	`https://www.e-szigno.hu`
Panaszok bejelentésének helye:	Microsec zrt.
	1033 Budapest, Ángel Sanz Briz út 13., Graphisoft Park Déli Terület, SP3 épület
Illetékes fogyasztóvédelmi felügyelőség:	Budapest Főváros Kormányhivatal Fogyasztóvédelmi Felügyelőség 1052 Budapest, Városház u. 7. 1364 Budapest, Pf. 144.
Illetékes békéltető testület elérhetősége:	Budapesti Békéltető Testület 1016 Budapest, Krisztina krt. 99. III. em. 310. Levelezési cím: 1253 Budapest, Pf.: 10.

A Szolgáltató bemutatása

A Microsec zrt. a 910/2014/EU rendelet [1] (továbbiakban: eIDAS) szerinti EU minősített bizalmi szolgáltató.

A Microsec zrt. (illetve jogelődje, a Microsec Kft.) az elektronikus aláírással kapcsolatos szolgáltatásainak nyújtását a 2001. évi XXXV. törvény [3] (továbbiakban: Eat.) hatálya alatt indította

el:

- 2002. május 30-tól kezdve nyújt az Eat. szerinti nem minősített elektronikus aláírás hitelesítés-szolgáltatást, időbélyegzés szolgáltatást és aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatást (regisztrációs szám: MH 6834 1/2002);
- 2005. május 15-től kezdve nyújt az Eat. szerinti minősített hitelesítés-szolgáltatást, időbélyegzés szolgáltatást és aláírás-létrehozó adat elhelyezése aláírás-létrehozó eszközön szolgáltatást;
- 2007. február 1-től kezdve nyújt az Eat. szerinti minősített elektronikus archiválás szolgáltatást (a nyilvántartásba vételről szóló határozat ügyiratszáma: HL-3549- 2/2007).

2016. július 1-én az eIDAS és az azt kiegészítő 2015. évi CCXXII törvény [6] hatálybalépésével európai szinten egységesen megváltozott az elektronikus aláírással kapcsolatos szolgáltatások teljes rendszere.

A Microsec 2016. július 1-jétől nyújtja eIDAS Rendelet szerinti nem minősített bizalmi szolgáltatásait, valamint elindította természetes személyek számára az eIDAS Rendelet szerinti minősített aláíró tanúsítványok kibocsátását.

A Microsec 2016. december 20-ától nyújtja az alábbi eIDAS Rendelet szerinti minősített bizalmi szolgáltatásait:

- minősített elektronikus bélyegző tanúsítványok kibocsátása
- minősített elektronikus időbélyegzés
- minősített elektronikus archiválás.

Microsec 2019. január 2-ától nyújtja az alábbi eIDAS Rendelet szerinti minősített bizalmi szolgáltatást:

- minősített weboldal hitelesítő tanúsítvány kibocsátás.

Microsec 2020. május 29-étől nyújtja az alábbi eIDAS Rendelet szerinti minősített bizalmi szolgáltatás komponenst

- minősített elektronikus aláírás/bélyegző létrehozására alkalmas távoli kulcsmenedzsment szolgáltatás.

Minőség és információbiztonság

A Microsec kiemelten fontosnak tartja *Ügyfel*ei elégedettségét. A magas színvonalú szolgáltatások fenntartása érdekében a Microsec az ISO 9001 szabványnak megfelelő minőségirányítási rendszert üzemeltet 2002. január 23. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

A Microsec nagy figyelmet fordít az általa üzemeltetett rendszerek biztonságára, ezért fő tevékenységi területein a ISO/IEC 27001-nek megfelelő információbiztonság-irányítási rendszert (korábban BS 7799) üzemeltet 2003. május 19. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

A minőségirányítási rendszer és az információbiztonság-irányítási rendszer hatóköre kiterjed a Microsec által nyújtott bizalmi szolgáltatásokra is.

A Microsec kétszintű kockázatelemzése az információ technológiai kockázatokon túlmenően kiterjed a teljes szervezetre és az üzleti kockázatokra is. A kockázatelemzés legalább évente felülvizsgálatra kerül. A kockázatelemzés eredménye alapján a *Távoli kulcsmenedzsment szolgáltató*

- intézkedéseket hoz a feltárt sérülékenységek megszüntetésére, és/vagy
- elfogadja az azonosított maradvány kockázatokat a döntés indokainak rögzítésével.

A *Távoli kulcsmenedzsment szolgáltató* honlapján minden érintett fél számára elérhetővé teszi Információbiztonsági Politikáját az alábbi linken:

`https://www.microsec.hu/hu/biztonsagi-garanciak`

Az Információbiztonsági politika minden változása ily módon kerül publikálásra a web oldalon keresztül.

A *Távoli kulcsmenedzsment szolgáltató* a szükséges mértékben tájékoztatja a harmadik feleket az Információbiztonsági politika változásairól, beleértve az előfizetőket, az érintett feleket, a tanúsító szervezeteket, a felügyelő és egyéb hatóságokat.

A *Távoli kulcsmenedzsment szolgáltató* azok bizalmas jellege miatt nem hozza nyilvánosságra belső Biztonsági szabályzatait. Alvállalkozót, szerződéses partnereit és az egyéb érintett feleket a szerződés megkötésekor a szükséges mértékben tájékoztatja a rájuk vonatkozó biztonsági szabályokról.

Hitelesítés-szolgáltatást nyújtó üzletág

A Microsec szervezetén belül önálló üzleti egységként működő e-Szignó Hitelesítés Szolgáltató látja el a bizalmi szolgáltatások nyújtásával kapcsolatos feladatokat.

Szolgáltatások

A *Távoli kulcsmenedzsment szolgáltató* az eIDAS Rendelet [1] által meghatározott alábbi bizalmi szolgáltatásokat nyújthatja az *Előfizető* számára jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* keretében:

- távoli kulcsmenedzsment szolgáltatás

1.3.2 Ügyfelek

A *Távoli kulcsmenedzsment szolgáltató* által nyújtott Távoli kulcsmenedzsment szolgáltatások *Ügyfel*ei:

- *Előfizető*
  - Szolgáltatási szerződést köt a *Távoli kulcsmenedzsment szolgáltató*val

  - elfogadja az Általános Szerződési Feltételeket,
  - meghatározza a felhasználók körét,
  - kijelölhet *Szervezeti ügyintéző*ket,
  - felelős a szolgáltatás igénybevételével kapcsolatos díjak megfizetéséért.

- *elektronikus aláírás létrehozója*
  - a Távoli kulcsmenedzsment szolgáltatást igénybevevő fél, aki a szolgáltatás felhasználásával elektronikus aláírást vagy elektronikus bélyegzőt hozhat létre.

1.3.3 Érintett felek

Érintett fél, aki ellenőrzi és felhasználja az *Ügyfel*ek által a Távoli kulcsmenedzsment szolgáltatás segítségével létrehozott elektronikus aláírásokat vagy elektronikus bélyegzőket. Az *Érintett fél* nem áll szerződéses kapcsolatban a *Távoli kulcsmenedzsment szolgáltató*val. Az *Érintett fél* nem feltétlenül tudja, hogy az elektronikus aláírást vagy elektronikus bélyegzőt a Távoli kulcsmenedzsment szolgáltatás felhasználásával hozták létre.

1.3.4 Egyéb szereplők

A megfelelőség értékelést végző független auditor.

A szolgáltatás felügyeletét ellátó hatóság.

1.4 A dokumentum adminisztrálása

1.4.1 A dokumentum adminisztrációs szervezete

Jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* adminisztrációját ellátó szervezet adatai az alábbi táblázatban találhatók:

Szervezet neve	Microsec e-Szignó Hitelesítés Szolgáltató
Szervezet címe	Magyarország, H-1033 Budapest, Ángel Sanz Briz út 13.
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
Email cím	`info@e-szigno.hu`

1.4.2 Kapcsolattartó személy

Jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat*tal kapcsolatos kérdésekben közvetlenül az alábbi személyhez lehet fordulni:

Kapcsolattartó	e-Szignó Hitelesítés Szolgáltató igazgató helyettes
Szervezet neve	Microsec zrt.
Szervezet címe	Magyarország, H-1033 Budapest, Ángel Sanz Briz út 13.
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
Email cím	`info@e-szigno.hu`

1.4.3 A Szolgáltatási szabályzat *Bizalmi szolgáltatási rend*nek való megfelelőségéért felelős személy/szervezet

A jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat*nak a benne meghivatkozott *Bizalmi szolgáltatási rend*nek való megfelelőségéért felelős személy:

Felelős	e-Szignó Hitelesítés Szolgáltató igazgató
Szervezet neve	Microsec zrt.
Szervezet címe	Magyarország, H-1033 Budapest, Ángel Sanz Briz út 13.
Telefonszám	+36 1 505-4444
Fax szám	+36 1 505-4445
Email cím	info@e-szigno.hu

1.4.4 A Szolgáltatási szabályzat elfogadási eljárása

A *Távoli kulcsmenedzsment szolgáltatási szabályzat* új verziójának illetve tetszőleges módosításának megírása, elfogadása és kibocsátása egységes folyamatok szerint – a 7.12.1 fejezetben részletezett módon – történik.

1.5 Fogalmak és rövidítések

1.5.1 Fogalmak

Adatközpont	Számítógépes rendszerek és a hozzájuk kapcsolódó komponensek elhelyezésére és üzemeltetésére kialakított létesítmény. Ezek a komponensek rendszerint magukba foglalják a távközlési rendszereket és kommunikációs kapcsolatokat, redundáns áramforrást, adattárolókat, légkondicionáló, tűzvédelmi és biztonsági rendszereket.
Bizalmi felügyelet	"A *Bizalmi szolgáltatás*ok felügyeletét ellátó hatóság a Nemzeti Média- és Hírközlési Hatóság." (2015. évi CCXXII. törvény [6] 91.§ 1. bekezdés)
Bizalmi szolgáltatás (Trust Service)	"Rendszerint díjazás ellenében nyújtott, az alábbiakból álló elektronikus szolgáltatások: • elektronikus aláírások, elektronikus bélyegzők vagy elektronikus időbélyegzők, ajánlott elektronikus kézbesítési szolgáltatások, valamint az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok létrehozása, ellenőrzése és érvényesítése; vagy • *Weboldal-hitelesítő tanúsítvány*ok létrehozása, ellenőrzése és érvényesítése; vagy • elektronikus aláírások, bélyegzők vagy az ilyen szolgáltatásokhoz kapcsolódó tanúsítványok megőrzése; " (eIDAS [1] 3. cikk 16. pont)

Bizalmi szolgáltatási rend (Trust Service Policy)	"Olyan szabálygyűjtemény, amelyben egy *Bizalmi szolgáltató*, igénybe vevő vagy más személy valamely *Bizalmi szolgáltatás* használatának feltételeit írja elő igénybe vevők valamely közös biztonsági követelményekkel rendelkező csoportja vagy meghatározott alkalmazások számára. " (2015. évi CCXXII. törvény [6] 1. § 8. pont)
Bizalmi szolgáltató (Trust Service Provider)	"Egy vagy több *Bizalmi szolgáltatás*t nyújtó természetes vagy jogi személy; a *Bizalmi szolgáltató* lehet minősített vagy nem minősített *Bizalmi szolgáltató*." (eIDAS [1] 3. cikk 19. pont)
Elektronikus dokumentum	"Elektronikus formában, különösen szöveg, hang-, képi vagy audiovizuális felvétel formájában tárolt bármilyen tartalom." (eIDAS [1] 3. cikk 35. pont)
Elektronikus időbélyegző (Electronic Time Stamp)	"Olyan elektronikus adatok, amelyek más elektronikus adatokat egy adott időponthoz kötnek, amivel igazolják, hogy utóbbi adatok léteztek az adott időpontban." (eIDAS [1] 3. cikk 33. pont)
Előfizető (Subscriber)	A Szolgáltatóval valamely szolgáltatás igénybevétele érdekében Szolgáltatási szerződést kötő személy vagy szervezet.
Érintett fél (Relying Party)	Az elektronikus dokumentum elfogadója, aki elfogadja a dokumentum elektronikus aláírását vagy bélyegzőjét.
Felfüggesztés	A *Tanúsítvány* érvényességének ideiglenes megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* felfüggesztése nem végleges, a felfüggesztett *Tanúsítvány* érvényessége visszaállítható.
Gyökér tanúsítvány (Root Certificate)	Más néven legfelső szintű tanúsítvány. Önhitelesített *Tanúsítvány*, amelyet adott *Hitelesítő egység* saját maga számára bocsátott ki, azaz saját magánkulcsával van aláírva, így a saját – a tanúsítványban szereplő – nyilvános kulcsával ellenőrizhető.
Hardver kriptográfiai eszköz (HSM: Hardware Security Module)	Egy olyan hardver alapú biztonságos eszköz, mely előállítja, tárolja és védi a kriptográfiai kulcsokat, valamint biztonságos környezetet biztosít a kriptográfiai funkciók végrehajtására.

Hitelesítés-szolgáltató	Olyan *Bizalmi szolgáltató*, aki/amely a hitelesítés-szolgáltatás keretében azonosítja az igénylő személyét, *Tanúsítvány*t bocsát ki, nyilvántartásokat vezet, fogadja a *Tanúsítvány*okkal kapcsolatos változások adatait, valamint nyilvánosságra hozza a *Tanúsítvány*hoz tartozó szabályzatokat, és a *Tanúsítvány* aktuális állapotára (különösen esetleges visszavonására) vonatkozó információkat.
Hitelesítő egység	A *Hitelesítés-szolgáltató* rendszerének egy egysége, amely *Tanúsítvány*ok elektronikus aláírását vagy bélyegzését végzi. Egy *Hitelesítő egység*hez mindig egy elektronikus aláírás vagy bélyegző létrehozásához használt adat (magánkulcs) tartozik. Előfordulhat, hogy egy *Hitelesítés-szolgáltató* egyszerre több *Hitelesítő egység*et is működtet.
Kompromittálódás	Egy kriptográfiai kulcs abban az esetben tekintendő kompromittálódottnak, ha vélelmezhető, hogy illetéktelen személynek is hozzáférése van hozzá.
Köztes hitelesítő egység	Olyan *Hitelesítő egység* amelynek *Tanúsítvány*át egy másik *Hitelesítő egység* bocsátotta ki.
Kriptográfiai kulcs (Cryptographic Key)	Olyan – kriptográfiai transzformációt vezérlő – egyedi digitális jelsorozat, amelynek ismerete szükséges titkosításhoz és dekódoláshoz, illetve elektronikus aláírás vagy bélyegző előállításához és ellenőrzéséhez.
Kulcsgondozás (Key Management)	A kriptográfiai kulcsok előállítása, a felhasználókhoz történő eljuttatása vagy ennek algoritmikus megvalósítása, továbbá a kulcsok nyilvántartása, tárolása, archiválása, visszavonása, törlése, amely szoros kapcsolatban áll az alkalmazott biztonsági eljárásmóddal.
Magánkulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet az *Alany*nak szigorúan titokban kell tartania. A *Hitelesítés-szolgáltató* a *Tanúsítvány*ok kibocsátása során a *Hitelesítő egység* magánkulcsát használja arra, hogy a *Tanúsítvány*t védő elektronikus aláírást vagy bélyegzőt elhelyezze rajta.
Nyilvános kulcs	A Nyilvános kulcsú infrastruktúrában egy szereplőhöz tartozó aszimmetrikus kriptográfiai kulcspár azon eleme, amelyet nyilvánosságra kell hozni. A nyilvánosságra hozatal jellemzően egy *Tanúsítvány* formájában történik, amely összekapcsolja a szereplő nevét az ő nyilvános kulcsával. A *Tanúsítvány*ok hitelességét az őket kibocsátó *Hitelesítő egység* nyilvános kulcsa segítségével lehet ellenőrizni.

Nyilvános kulcsú infrastruktúra (Public Key Infrastructure, PKI)	Aszimmetrikus kulcsú kriptográfiára épülő infrastruktúra, beleértve a kriptográfiai algoritmusokat, kulcsokat, tanúsítványokat, a rájuk vonatkozó szabványokat és jogszabályokat, a mögöttes intézményrendszert, a különböző szolgáltatókat és eszközöket is.
Rendkívüli üzemeltetési helyzet	Olyan, a *Távoli kulcsmenedzsment szolgáltató* üzemmenetében zavart okozó rendkívüli helyzet, amikor a *Távoli kulcsmenedzsment szolgáltató* rendes üzemmenetének folytatására ideiglenesen vagy véglegesen nincsen lehetőség.
Szervezet	Jogi személy.
Szervezeti tanúsítvány	Olyan *Tanúsítvány*, amelynek *Alany*a *Szervezet*, vagy amely egy természetes személy *Alany* valamely *Szervezet*hez való tartozását mutatja. Ilyen esetben a *Tanúsítvány* "O" mezejében a *Szervezet* neve feltüntetésre kerül.
Szolgáltatási szabályzat (Trust Service Practice Statement)	"A *Bizalmi szolgáltató* nyilatkozata az egyes *Bizalmi szolgáltatás*ok nyújtásával kapcsolatosan alkalmazott részletes eljárási vagy más működési követelményekről." (2015. évi CCXXII. törvény [6] 1. § 41. pont)
Szolgáltatási szerződés	"A *Bizalmi szolgáltató* és a *Bizalmi szolgáltatás*i ügyfél között létrejött szerződés, amely a *Bizalmi szolgáltatás* nyújtására és a szolgáltatás igénybevételére vonatkozó feltételeket tartalmazza." (2015. évi CCXXII. törvény [6] 1. § 42. pont)
Tanúsítvány (Certificate)	"Az elektronikus aláírás tanúsítvány, az elektronikus bélyegző tanúsítvány és a *Weboldal-hitelesítő tanúsítvány*, valamint mindazon, a *Bizalmi szolgáltatás* keretében a szolgáltató által kibocsátott elektronikus igazolás, amely tartalmazza a tanúsítványra vonatkozó érvényesítési adatot és a tanúsítvány használatához szükséges kapcsolódó adatokat, és amely elektronikus dokumentum megbízhatóan védve van a kibocsátáskor és az érvényességi ideje alatt rendelkezésre álló technológiákkal elkövetett hamisítás ellen." (2015. évi CCXXII. törvény [6] 1. § 44.)
Tanúsítványkérelem	Az *Igénylő* által, a Szolgáltató számára a *Tanúsítvány* kibocsátás érdekében benyújtott adatok és nyilatkozatok, amelyekben többek között az *Igénylő* megerősíti a *Tanúsítvány*ba kerülő adatok valódiságát.

Tanúsítványtár	Különböző *Tanúsítvány*okat tartalmazó adattár. Tanúsítványtára van egy Szolgáltatónak is, amelyben az általa kibocsátott *Tanúsítvány*okat publikálja, de Tanúsítványtárnak nevezzük az *Érintett fél* számítógépén a használt alkalmazás számára elérhető *Tanúsítvány*okat tartalmazó rendszert is.
Távoli kulcsmenedzsment szolgáltatás	Olyan bizalmi szolgáltatás, amely keretében a szolgáltató biztonságos körülmények között kezeli az Ügyfelek magánkulcsait, biztosítja a szükséges műszaki és eljárási feltételeket annak érdekében, hogy az Ügyfelek – a szolgáltató által tárolt magánkulcsaikkal – kulcs műveleteket végezhessenek el, például elektronikus aláírásokat vagy elektronikus bélyegzőket hozhassanak létre.
Távoli kulcsmenedzsment szolgáltatási rend	Olyan Bizalmi szolgáltatási rend, amely meghatározza a Távoli kulcsmenedzsment szolgáltatás által betartandó eljárási követelményeket.
Ügyfél	Az *Előfizető* másik elnevezése.
Ügyféltér	Az e-Szignó Hitelesítés Szolgáltató által kialakított és folyamatosan továbbfejlesztett web alapú szolgáltatás, amelyben az ügyfelek egyszerűen, egy helyen intézhetik a szolgáltatásokkal kapcsolatos egyes ügyeiket, és az igénybe vett szolgáltatásokról azonnali, naprakész információt kaphatnak.
Visszavonás	A *Tanúsítvány* érvényességének megszüntetése a *Tanúsítvány*ban is feltüntetett érvényességi idő lejárta előtt. A *Tanúsítvány* visszavonása végleges, visszavont *Tanúsítvány* többet nem tehető érvényessé.
Visszavonási állapot nyilvántartás	A *Hitelesítés-szolgáltató* által vezetett belső nyilvántartás a felfüggesztett, illetőleg a visszavont *Tanúsítvány*okról, amelyek tartalmazzák legalább a felfüggesztés vagy visszavonás tényét, és a felfüggesztés vagy visszavonás időpontját másodperc pontossággal.

1.5.2 Rövidítések

eIDAS	electronic Identification, Authentication and Signature	A 910/2014/EU rendelet általánosan használt hivatkozása
EUSCP	EU SSASC Policy	EU SSASC bizalmi szolgáltatási rend
LDAP	Lightweight Directory Access Protocol	Protokoll címtár szolgáltatás eléréséhez

LSCP	Ligthweight SSASC Policy	Könnyített SSASC bizalmi szolgáltatási rend
NMHH		Nemzeti Média- és Hírközlési Hatóság
NSCP	Normalized SSASC Policy	Normalizált SSASC bizalmi szolgáltatási rend
OCSP	Online Certificate Status Protocol	Online tanúsítvány-állapot protokoll
OID	Object Identifier	Objektum azonosító
PKI	Public Key Infrastructure	Nyilvános kulcsú infrastruktúra
SAD	Signature Activation Data	Aláírás aktiváló adat
SAP	Signature Activation Protocol	Aláírás aktiváló protokol
SCA	Signature Creation Application	Aláírás létrehozó alkalmazás
SCAL	Sole Control Assurance Level	Ellenőrzési szint
SCDev	Signature Creation Device	Aláírás létrehozó eszköz
SIC	Signer's Interaction Component	Aláíró interakciós komponens
SCP	SSASC Policy	SSASC bizalmi szolgáltatási rend
SSA	Server Signing Application	Szerver aláíró alkalmazás
SSASC	Server Signing Application Service Component	Távoli aláírás létrehozó szolgáltatás komponens
SSASP	Server Signing Application Service Provider	Távoli aláírás létrehozó szolgáltatás szolgáltató
TSP	Trust Service Provider	Bizalmi szolgáltató
TW4S	Trustworthy System Supporting Server Signing	Szerver aláírást támogató megbízható rendszer

2 Közzététel és adattár felelősségek

2.1 Adattárak

A *Távoli kulcsmenedzsment szolgáltató* nyilvánosságra hozza szerződéses feltételeit és szabályzatait a honlapján elektronikus formában az alábbi linken:

`https://e-szigno.hu/dokumentumok-es-szabalyzatok`

A honlapon a hatálybalépés előtt publikálásra kerülnek a bevezetésre váró új dokumentumok tervezetei.

A honlapon az érvényben levő dokumentumokon kívül elérhető valamennyi dokumentum összes korábbi verziója is.

A szabályzatok és szerződési feltételek aktuális verziója olvasható a *Távoli kulcsmenedzsment szolgáltató* ügyfélszolgálati irodájában.

A *Távoli kulcsmenedzsment szolgáltató* a szerződéskötést követően weboldalán publikálva teszi letölthetővé elektronikusan aláírt PDF fájl formájában az *Ügyfél* részére az Általános Szerződési Feltételeket, és a *Távoli kulcsmenedzsment szolgáltatási szabályzat*ot. A *Távoli kulcsmenedzsment szolgáltató* az egyedi Szolgáltatási szerződést papíralapon kézi aláírással és pecséttel hitelesítve, vagy minősített elektronikus aláírással vagy minősített elektronikus bélyegzővel ellátott PDF formátumú elektronikus dokumentum formájában bocsátja az *Ügyfél* rendelkezésére.

A *Távoli kulcsmenedzsment szolgáltató* értesíti *Ügyfel*eit az Általános Szerződési Feltételek változásáról.

2.2 A tanúsítványokra vonatkozó információk közzététele

A Távoli kulcsmenedzsment szolgáltatás keretében menedzselt kulcsokhoz tartozó végfelhasználói *Tanúsítvány*okkal kapcsolatban a *Távoli kulcsmenedzsment szolgáltató* nem hoz nyilvánosságra semmilyen információt sem. Ezen információk közzétételére vonatkozó információ megtalálható az adott *Tanúsítvány*t kibocsátó Hitelesítés Szolgáltató vonatkozó Szolgáltatási Szabályzatában.

2.3 A közzététel időpontja vagy gyakorisága

2.3.1 Kikötések és feltételek közzétételi gyakorisága

A Távoli kulcsmenedzsment szolgáltatás szempontjából leglényegesebb kikötéseket és feltételeket tartalmazza az *Ügyfél* által a szerződéskötés során aláírandó szolgáltatási szerződés, vagy az abban meghivatkozott Általános Szerződési Feltételek [17] dokumentum.

A *Távoli kulcsmenedzsment szolgáltató* évi rendszerességgel illetve rendkívüli változtatási igény esetén soron kívül átvizsgálja az Általános Szerződési Feltételek dokumentumot és elvégzi a szükségesnek tartott változtatásokat. A dokumentum a legkisebb változtatás után is új verziószámot kap és az elfogadási procedúra időigényét figyelembe véve meghatározásra kerül a tervezett hatálybalépés időpontja is.

A *Távoli kulcsmenedzsment szolgáltató* a jóváhagyott dokumentumot legalább 30 nappal a tervezett hatálybalépés előtt véleményezésre megküldi a Nemzeti Média- és Hírközlési Hatóság részére és publikálja honlapján.

A *Távoli kulcsmenedzsment szolgáltató* a közzétett új Általános Szerződési Feltételek tervezettel kapcsolatos észrevételeket a hatálybalépést megelőző 14. napig fogadja az alábbi email címen:

`info@e-szigno.hu`

Érdemi változtatást igénylő észrevétel esetén a dokumentumot megváltoztatja.

Az Általános Szerződési Feltételek észrevételekkel módosított változatát a *Távoli kulcsmenedzsment szolgáltató* a hatálybalépést megelőző 7. napon lezárja és közzé teszi.

2.4 Az adattárak elérésének szabályai

A *Távoli kulcsmenedzsment szolgáltató* által közzétett információk nyilvánosak, olvasás céljából bárki számára biztosított a hozzáférési lehetőség a közzététel sajátosságainak megfelelően.

A *Távoli kulcsmenedzsment szolgáltató* által közölt információkat kizárólag csak a *Távoli kulcsmenedzsment szolgáltató* egészítheti ki, törölheti vagy módosíthatja. A *Távoli kulcsmenedzsment*

szolgáltató különböző védelmi mechanizmusokkal akadályozza meg az információk jogosulatlan módosítását.

3 A Szolgáltatás részletes ismertetése

3.1 Általános követelmények

3.1.1 Kulcs előállítás

A *Távoli kulcsmenedzsment szolgáltató* a végfelhasználói kulcsok menedzselésére olyan általános célú *HSM eszköz*t használ, amely:

- rendelkezik FIPS 140-2 level 3 [15] tanúsítvánnyal.

A *Távoli kulcsmenedzsment szolgáltató* valamennyi végfelhasználói kulcsot a fenti *HSM eszköz*ben hozza létre és teljes életciklusa alatt ott kezeli.

A *Távoli kulcsmenedzsment szolgáltató* az eszköz tanúsításában szereplő kriptográfiai algoritmusok közül csak az alábbiakat használja:

- Kriptográfiai algoritmus: RSA
  - Kulcshossz: 2048 bit
  - lenyomatképző függvény: SHA-256
  - Kitöltő algoritmus: PKCS#1 ver.1.5
- Kriptográfiai algoritmus: ECC
  - Kulcshossz: 256 bit
  - lenyomatképző függvény: SHA-256
  - Görbe: ECC NIST P-256

A végfelhasználói és szolgáltatói infrastruktúrális magánkulcsok csak biztonsági másolat készítése céljából hagyják el a *HSM eszköz*t. A biztonsági másolat állományok minden esetben csak titkosított formában kerülnek ki a *HSM eszköz*ből. A magánkulcsok titkosítására a *Távoli kulcsmenedzsment szolgáltató* AES256 szimmetrikus kulcsokat használ.

A *HSM eszköz* üzembe helyezéséhez legalább 2 adminisztrátor közreműködése szükséges. A *Távoli kulcsmenedzsment szolgáltató* eljárásrendje biztosítja, hogy az eszközön minden létrehozott adminisztrátor konkrét személyhez kapcsolódik, és egy személynek csak egy adminisztrátori fiókja lehet.

A *Távoli kulcsmenedzsment szolgáltató* minden esetben az aktuális kriptográfiai követelményeknek megfelelő algoritmusokat és paramétereket használ.

A *Távoli kulcsmenedzsment szolgáltató* a kulcsok használata előtt minden esetben ellenőrzi a hozzá tartozó *Tanúsítvány* érvényességi idejét, és a kriptográfiai algoritmusok használhatósági idejénél később lejáró *Tanúsítvány* esetében a kulcs használatát elutasítja.

A jelenleg használt kriptográfiai algoritmus készlet esetén a felhasználhatóság határideje 2022. december 31.

A *Távoli kulcsmenedzsment szolgáltató* nem generál előre végfelhasználói kulcsokat, a végfelhasználói kulcsok generálása minden esetben az *Alany* sikeres azonosítását követően történik közvetlenül a Távoli kulcsmenedzsment szolgáltatás aktiválását megelőzően.

A *Távoli kulcsmenedzsment szolgáltató* a magánkulcshoz tartozó legelső *Tanúsítvány* kibocsátásához egy PKCS#10 kérést állít össze, amelyet a magánkulcs segítségével ír alá. A magánkulcs használata már ebben az esetben is az *Alany* azonosításához és egyértelmű jóváhagyásához kötött.

A *Hitelesítés-szolgáltató* a *Tanúsítvány* kibocsátása előtt ellenőrzi a PKCS#10 kérést, ezzel biztosított a kulcs feletti kontroll megléte és a *Tanúsítvány*ba kerülő adatok helyessége.

A magánkulcshoz tartozó bármely okból (megújítás, módosítás) kibocsátott további *Tanúsítvány*ok esetén nincs szükség kulcs műveletre.

3.1.2 Elektronikus azonosító hozzárendelése

A *Távoli kulcsmenedzsment szolgáltató* az *Alany*ok azonosítására a Microsec által kifejlesztett és üzemeltetett PassByME elektronikus felhasználó azonosító rendszert használja. A PassByME egy magas biztonsági szintet nyújtó, mobil alapú személy azonosító rendszer, amely lehetővé teszi a felhasználók azonosítását, az általuk végzett elektronikus tranzakciók egyedi validálását. A PassByME rendszer működése az *Alany* mobil eszközén onboard generált kulcsokhoz kibocsátott autentikációs illetve aláíró tanúsítványok használatán alapul. A rendszerben minden kapcsolat kétoldali PKI alapú azonosításra épül és minden tranzakció elektronikus aláírással védett.

A PassByME rendszerben használatos elektronikus azonosító kiadása és az *Alany*hoz rendelése a magánkulcshoz tartozó legelső *Tanúsítvány* kibocsátását megelőző azonosítási eljárás keretében történik, így garantált a Távoli kulcsmenedzsment szolgáltatást igénybevevő *Alany* magas megbízhatóságú, az eIDAS követelmények szerinti azonosítása és az azonosító adatnak az *Alany*hoz való hozzárendelése.

A magánkulcshoz tartozó bármely okból (megújítás, módosítás) kibocsátott további *Tanúsítvány*ok esetén az azonosító nem változik, az a kulcs teljes élettartama alatt állandó.

A PassByME rendszer rendelkezik Common Criteria alapú tanúsítvánnyal.

A *Hitelesítés-szolgáltató* által kiadott *Tanúsítvány* minden esetben tartalmazza a *Hitelesítés-szolgáltató* által az *Alany*hoz rendelt egyedi azonosítót (OID). A PassByME rendszerben történt regisztráció során a Microsec hozzárendeli ezt az egyedi azonosító OID értéket a PassByME szolgáltatásban kibocsátott tanúsítványokhoz. A kulcs használata során az *Alany* kiválasztja a használni kívánt *Tanúsítvány*t és megadja a kulcs aktiválásához szükséges - a *Tanúsítvány*tól függetlenül érvényes, a felhasználó által megváltoztatható - jelszót. A megadott adatok alapján a PassByME rendszer azonosítja az aktuális felhasználót, és az általa regisztrált mobil eszközre elküldi a jóváhagyást kérő üzenetet. A jóváhagyás alapján a *Távoli kulcsmenedzsment szolgáltató* aktiválja a megfelelő kulcsot és elvégzi a kért kulcsműveletet.

Az elektronikus azonosító kibocsátása során a *Távoli kulcsmenedzsment szolgáltató* nem veszi igénybe alvállalkozók közreműködését.

3.1.3 Tanúsítvány hozzárendelése

A kulcshoz tartozó bármely okból kibocsátott új *Tanúsítvány* kibocsátása esetén a *Távoli kulcsmenedzsment szolgáltató* ellenőrzi a kibocsátott *Tanúsítvány*t, meggyőződik a generált kulcs és a kiállított *Tanúsítvány* összetartozásáról és eltárolja a *Tanúsítvány*t. A *Távoli kulcsmenedzsment szolgáltató* minden esetben a kulcshoz tartozó legkésőbb kibocsátott *Tanúsítvány*t rendeli a kulcshoz. A kulcs használata előtt a *Távoli kulcsmenedzsment szolgáltató* minden esetben meggyőződik a kiválasztott és a tárolt *Tanúsítvány* egyezéséről.

Az *Alany*hoz tartozó magánkulcs első használata a PKCS#10 kérés aláírása. A magánkulcs használata már ebben az esetben is és minden további esetben az *Alany* azonosításához és jóváhagyásához kötött.

3.1.4 Elektronikus azonosító biztosítása

A PassByME alapú azonosító adatok létrehozásához az *Alany* személyes találkozás során - vagy már létező biztonságos ügyfél kommunikációs csatorna felhasználásával - kapja meg az aktiváláshoz szükséges, rövid érvényességi idejű egyedi azonosító adatokat.

3.1.5 Kulcs használata

A *Távoli kulcsmenedzsment szolgáltató* csak az *Alany* sikeres azonosítása és a megfelelő jóváhagyás után teszi lehetővé az *Alany* részére a magánkulcs használatát.

A *Távoli kulcsmenedzsment szolgáltató* által használt rendszerek és protokollok megfelelő védelmet biztosítanak, amelyek megakadályozzák a magánkulcs jogosulatlan felhasználását.

Az *Alany*oknak és tetszőleges harmadik külső feleknek nincs közvetlen hozzáférésük a rendszerekben tárolt adatokhoz. Az *Alany*ok jól definiált protokollon keresztül aktiválhatnak funkciókat, amelyeket az *Alany* a *Távoli kulcsmenedzsment szolgáltató* belső rendszereinek közreműködésével végezhet el.

A *Távoli kulcsmenedzsment szolgáltató* által üzemeltetett rendszerek biztosítják, hogy az *Alany* által előállított aláírandó adat (DTBS/R) aláírása csak az *Alany* által kiválasztott *Tanúsítvány*hoz tartozó magánkulcs felhasználásával történhet meg.

A magánkulcs aktiválásához az *Alany*nak be kell mutatnia a kulcs aktiváló jelszót és egy egyedi, rövid érvényességi idejű jelszót (TOTP) vagy egy erre a célra kibocsátott aláírt JWT adatcsomagot.

A *Távoli kulcsmenedzsment szolgáltató* kockázatelemzésen alapuló védelmi intézkedéseket alkalmaz az aktiváló adatokkal kapcsolatos fenyegetettségek kivédésére.

A magánkulcs kizárólag az aktiváló protokollban kapott aláírandó adatok (DTBS/R) aláírására használható fel.

A *Távoli kulcsmenedzsment szolgáltató* a magánkulcs használata előtt minden esetben ellenőrzi a magánkulcshoz tartozó *Tanúsítvány* érvényességét. Érvénytelen (lejárt, felfüggesztett vagy visszavont) *Tanúsítvány*hoz tartozó magánkulcs használatát a *Távoli kulcsmenedzsment szolgáltató* nem engedi.

A magánkulcs használata minden esetben az *Alany* azonosításához és jóváhagyásához kötött.

3.1.6 Kulcs törlése

A *Távoli kulcsmenedzsment szolgáltató* megsemmisíti az *Alany* magánkulcsát, amennyiben:

- a magánkulcshoz tartozó valamennyi *Tanúsítvány* érvényessége lejár
- a magánkulcshoz tartozó valamennyi *Tanúsítvány*t visszavonják
- megszűnik a Szolgáltatási szerződés érvényessége
- az *Alany* kérése esetén
- amennyiben megszűnik a hozzárendelés a magánkulcs és az *Alany* között.

A *Távoli kulcsmenedzsment szolgáltató* az aktív rendszeréből úgy törli ki a feleslegessé vált magánkulcsokat, hogy azokat nem lehet visszaállítani.

A törölt magánkulcsokat tartalmazó mentéseket a *Távoli kulcsmenedzsment szolgáltató* 30 napon belül megsemmisíti.

3.1.7 Kulcs mentés és visszaállítás

A mentési példányokban a magánkulcsok csak titkosított formában vannak jelen. A *Távoli kulcsmenedzsment szolgáltató* megfelelő védelmet biztosító kriptográfiai algoritmusokat használ (AES256). A mentett adatállományok csak a biztonságos üzemvitelhez szükséges számú példányban léteznek.

A *Távoli kulcsmenedzsment szolgáltató* a mentési állományok védelmére csak olyan kriptográfiai algoritmusokat és paramétereket használ, amelyek a magánkulcs teljes tervezett használati idejére megfelelő védelmet nyújtanak.

A végfelhasználói és infrastruktúrális magánkulcsok mentését és visszaállítását csak bizalmi szerepkörrel rendelkező munkatársak láthatják el. A mentések titkosítására használatos szolgáltatói magánkulcsok mentése csak két, bizalmi szerepkörrel rendelkező munkatárs közreműködésével valósulhat meg.

4 Elhelyezési, eljárásbeli és üzemeltetési előírások

A *Távoli kulcsmenedzsment szolgáltató* széles körben elismert szabványoknak megfelelő fizikai, eljárásbeli és személyzeti biztonsági óvintézkedéseket, valamint az ezeket érvényre juttató adminisztratív és irányítási eljárásokat alkalmaz.

A *Távoli kulcsmenedzsment szolgáltató* nyilvántartást vezet a szolgáltatás nyújtásával kapcsolatos rendszerelemekről és erőforrásokról, és ezekkel kapcsolatos kockázatelemzést végez. Az egyes elemekkel kapcsolatban a kockázatokkal arányos védelmi megoldásokat alkalmaz.

A *Távoli kulcsmenedzsment szolgáltató* figyelemmel kíséri a kapacitás igényeket és biztosítja, hogy megfelelő feldolgozási teljesítmény és tárolási kapacitás álljon rendelkezésre a Távoli kulcsmenedzsment szolgáltatás nyújtásához.

4.1 Fizikai követelmények

A *Távoli kulcsmenedzsment szolgáltató* gondoskodik arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen és a kritikus szolgáltatások eszközeit érintő fizikai kockázatát minimalizálja.

A fizikai óvintézkedések célja a *Távoli kulcsmenedzsment szolgáltató* által birtokolt információra illetve fizikai zónáira irányuló jogosulatlan hozzáférés, károkozás és illetéktelen behatolás megakadályozása.

A kritikus és érzékeny információt feldolgozó szolgáltatásokat biztonságos helyszíneken valósítják meg a *Távoli kulcsmenedzsment szolgáltató* rendszerében.

A biztosított védelem mértéke megfelel a *Távoli kulcsmenedzsment szolgáltató* által végzett kockázatelemzésben megállapított fenyegetettség mértékének.

A megfelelő védelem biztosítása érdekében:

- A *Távoli kulcsmenedzsment szolgáltató* védett számítógéptermében valósítja meg a szigorúban védendő szolgáltatásokat. Ez a számítógépterem speciálisan erre a célra lett tervezve és kialakítva, tervezésénél különböző védelmi szempontok [a telephely elhelyezése és szerkezeti felépítése, a fizikai hozzáférés (beléptetés ellenőrzése és felügyelete), áramellátás, légkondicionálás, beázás és elárasztódás elleni védekezés, tűzmegelőzés és tűzvédelem, adathordozók tárolása stb.] egységes érvényesítésére került sor.

- A *Távoli kulcsmenedzsment szolgáltató* valamennyi kritikus szolgáltatását egy külön biztonsági zónában valósítja meg, az ehhez szükséges valamennyi eszközt egy – a biztonsági zóna részét képező – védett számítógépteremben helyezi el.

4.1.1 A telephely elhelyezése és szerkezeti felépítése

A *Távoli kulcsmenedzsment szolgáltató* informatikai rendszereit fizikai és logikai védelemmel ellátott, megfelelően biztonságos *Adatközpont*ban helyezte el és üzemelteti, amely megakadályozza az illetéktelen hozzáférést. Az *Adatközpont* elhelyezése és kialakítása során egymásra épülő és egymást támogató védelmi megoldásokat alkalmaz – őrzés, biztonsági zárak, behatolás érzékelők, videó megfigyelő rendszer, beléptető rendszer stb. – amelyek együttesen egy erős védelmi szintet biztosítanak a szolgáltatásban részt vevő informatikai rendszerek és a szolgáltató által tárolt bizalmas adatok megóvására.

4.1.2 Fizikai hozzáférés

A *Távoli kulcsmenedzsment szolgáltató* védi a szolgáltatás nyújtásában részt vevő eszközeit és berendezéseit a jogosulatlan fizikai hozzáféréstől az eszközök manipulálásának megakadályozása érdekében. A *Távoli kulcsmenedzsment szolgáltató* biztosítja, hogy:

- az *Adatközpont*ba történő minden belépés regisztrálásra kerül;

- az *Adatközpont*ba csak a megfelelő jogosultságokkal rendelkező, bizalmi szerepkört betöltő munkatársak léphetnek be önállóan;

- az önálló jogosultsággal nem rendelkező személyek csak indokolt esetben, a szükséges ideig tartózkodhatnak a gépteremben megfelelő jogosultságú kísérő személyzettel;
- a belépési logokat folyamatosan archiválják és legalább hetente megvizsgálják.

Az eszközök aktiváló adatai (jelszavak, PIN kódok) a géptermen belül sem tárolhatók nyílt formában.
Jogosulatlan személyek jelenlétében:

- a bizalmas adatokat tartalmazó adathordozókat fizikailag elzárva tartják;
- a bejelentkezett terminálokat nem hagyják felügyelet nélkül;
- nem végeznek olyan munkafolyamatot, amely során bizalmas adat felfedésre kerülhet.

A gépterem elhagyásakor az adminisztrátornak ellenőriznie kell, hogy:

- az *Adatközpont* minden berendezése megfelelően biztonságos üzemállapotban van;
- egyetlen terminálon sem maradt bejelentkezve;
- a fizikai tároló eszközök megfelelően be lettek zárva;
- a fizikai védelmet biztosító rendszerek, berendezések megfelelően működnek;
- a riasztó rendszer aktiválva lett.

A rendszeres fizikai biztonsági vizsgálatokat kijelölt felelősök végzik. A vizsgálatok eredményét megfelelő naplóbejegyzésekben rögzítik.

4.1.3 Áramellátás és légkondicionálás

A *Távoli kulcsmenedzsment szolgáltató Adatközpont*jában olyan szünetmentes áramellátó rendszert alkalmaz, amely:

- megfelelő teljesítménnyel rendelkezik az adatközpont informatikai és a kisegítő létesítményi rendszerei áramellátásának biztosítására;
- megvédi az informatikai berendezéseket a külső hálózatból érkező feszültség ingadozások, feszültség kimaradások, tüskék és egyéb zavarok ellen;
- tartós áramszünet esetére saját áramtermelő berendezéssel rendelkezik, amely - üzemanyag utántöltést lehetővé téve - tetszőleges időtartamig képes a szükséges energia biztosítására.

Az *Adatközpont*ba nem juthat be közvetlenül a külső környezet levegője. Az *Adatközpont* levegőjének tisztaságát megfelelő szűrőrendszer alkalmazása biztosítja, amely kiszűri a levegőből a különféle szennyeződéseket (por, szennyező anyagok, korrozív anyagok, mérgező vagy gyúlékony anyagok). A szellőző rendszer megfelelő szűrés mellett biztosítja az operátorok biztonságos munkavégzéséhez szükséges mennyiségű friss levegőt.
A levegő nedvességtartalma az informatikai rendszerek által megkívánt szintre van csökkentve.
A *Távoli kulcsmenedzsment szolgáltató* megfelelő teljesítményű hűtőrendszert használ a szükséges üzemi hőmérséklet biztosítása, az informatikai eszközök túlhevülésének megakadályozása érdekében.

4.1.4 Beázás és elárasztódás veszély kezelése

A *Távoli kulcsmenedzsment szolgáltató* biztonsági zónájának kialakítása során fontos szempont volt a beázás és elárasztódás veszélyének minimalizálása. A biztonsági zóna teljes területe mentes a vizesblokkoktól, nincs a közelében sem csatorna sem vízvezeték.

A védett számítógépteremben a biztonságot tovább növeli az álpadló alkalmazása.

4.1.5 Tűz megelőzés és tűzvédelem

A *Távoli kulcsmenedzsment szolgáltató Adatközpont*jában az illetékes tűzoltóparancsnokság által jóváhagyott tűzvédelmi rendszer működik.

Minden helyiségben jól látható helyen található a vonatkozó előírásoknak megfelelő típusú és mennyiségű kézi tűzoltó készülék.

4.1.6 Adathordozók tárolása

A *Távoli kulcsmenedzsment szolgáltató* megvédi valamennyi adathordozóját a jogosulatlan hozzáféréstől és a véletlen rongálódástól. Minden napló és archív adatot legalább két példányban hoz létre. A példányokat egymástól fizikailag elkülönítve tárolja tűzálló páncélszekrényekben, egymástól biztonságos távolságra lévő helyszíneken a bizalmi szolgáltatások nyújtásához használt adatközpontok operátori helyiségeiben.

A tárolt adathordozókat védi a káros környezeti behatásoktól, mint pl. alacsony vagy magas hőmérséklet, szennyeződés, nedvesség, napfény, erős mágneses tér, erős sugárzás.

4.1.7 Hulladék megsemmisítése

A *Távoli kulcsmenedzsment szolgáltató* a környezetvédelmi előírások betartásával gondoskodik feleslegessé vált eszközeinek, adathordozóinak megsemmisítéséről.

A *Távoli kulcsmenedzsment szolgáltató* a bizalmas minősítésű adatokat tartalmazó elektronikus adathordozókat még tartalmuk törlése után sem használja fel nem bizalmas minősítésű adatok tárolására, az ilyen eszközök nem vihetők ki a *Távoli kulcsmenedzsment szolgáltató* területéről. A *Távoli kulcsmenedzsment szolgáltató* a meghibásodott vagy bármely más okból használhatatlanná, feleslegessé vált, bizalmas minősítésű adatokat tartalmazó adathordozókat – a selejtezési szabályzatának megfelelően – fizikailag megsemmisíti:

- a papíralapú dokumentumokat iratmegsemmisítő géppel felaprítja;
- a merevlemezeket szétszereli és a kritikus alkatrészeket összetöri;
- az optikai lemezeket erre alkalmas iratmegsemmisítő géppel megsemmisíti.

4.1.8 A mentési példányok fizikai elkülönítése

A *Távoli kulcsmenedzsment szolgáltató* legalább heti rendszerességgel előállít olyan mentést, amiből meghibásodás esetén a teljes szolgáltatás helyreállítható. A mentéseket - legalább az utolsó teljes mentést is beleértve - egy olyan külső helyszínen tárolja, amelynek a fizikai és működési

védelme azonos az elsődleges helyszínével. Az elsődleges és a tartalék helyszínek között biztosítja az adatok biztonságos továbbítását.

A mentett állományokból legalább évente szúrópróbaszerű kiválasztással jegyzőkönyvezett helyreállítási tesztet végez.

4.2 Eljárásbeli előírások

A *Távoli kulcsmenedzsment szolgáltató* gondoskodik arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltesse.

Az eljárásbeli óvintézkedések célja, hogy a bizalmi szerepkörök kijelölésével és elkülönítésével, az egyes szerepkörök felelősségének dokumentálásával, az egyes feladatokhoz szükséges személyzeti létszámok, a kizáró szerepkörök, valamint az egyes szerepkörökben elvárt azonosítás és hitelesítés meghatározásával kiegészítse, egyúttal fokozza a fizikai környezetre és személyzetre vonatkozó óvintézkedések hatásosságát.

A *Távoli kulcsmenedzsment szolgáltató* belső irányítási rendszere biztosítja a jogszabályoknak és belső szabályzatainak megfelelő működést. Rendszerében minden rendszerelemhez és minden folyamathoz egyértelműen hozzárendelhető az adott rendszerelemért, vagy folyamatért felelős személy. A *Távoli kulcsmenedzsment szolgáltató* rendszerében élesen elkülönülnek egymástól a fejlesztési és üzemeltetési folyamatok. A rendszer megfelelő működését a független rendszervizsgáló és a *Távoli kulcsmenedzsment szolgáltató* belső folyamatainak rendszeres ellenőrzése biztosítja.

4.2.1 Bizalmi szerepkörök

A *Távoli kulcsmenedzsment szolgáltató* feladatai ellátásához bizalmi szerepköröket hozott létre. A jogosultságok és funkciók oly módon lettek megosztva az egyes bizalmi szerepkörök között, hogy egyedül egyetlen felhasználó se legyen képes a biztonsági védelmi intézkedések megkerülésére.

A *Távoli kulcsmenedzsment szolgáltató* a következő bizalmi szerepköröket határozza meg az alábbi felelősségi körökkel:

A *Távoli kulcsmenedzsment szolgáltató* informatikai rendszeréért általánosan felelős vezető

Az informatikai rendszerért felelős személy.

Biztonsági tisztviselő
Biztonságtechnikai főmunkatárs, a szolgáltatás biztonságáért általánosan felelős személy.

Rendszeradminisztrátor
Infrastruktúra adminisztrátor. Feladata a *Távoli kulcsmenedzsment szolgáltató* rendszereinek telepítése, konfigurálása, karbantartása. Felelős a rábízott rendszerelemek megbízható és folyamatos működéséért, valamint a technológia fejlődésének nyomon követéséért, az egyes rendszerelemekben való biztonsági rések felderítéséért és megoldási javaslatok kidolgozásáért.

Operátor
Rendszerüzemeltető, az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását végző személy.

Független rendszervizsgáló

A *Távoli kulcsmenedzsment szolgáltató* naplózott, illetve archivált adatállományát vizsgáló, a *Távoli kulcsmenedzsment szolgáltató* által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy.

A bizalmi szerepkörök ellátására a *Távoli kulcsmenedzsment szolgáltató* biztonságért felelős vezetője formálisan kinevezi a *Távoli kulcsmenedzsment szolgáltató* munkatársait.

Bizalmi szerepkört csak a *Távoli kulcsmenedzsment szolgáltató*val munkaviszonyban álló személyek láthatnak el, megbízási szerződés keretében a bizalmi szerepkörök nem láthatók el.

A bizalmi szerepkörökről a *Távoli kulcsmenedzsment szolgáltató* naprakész nyilvántartást vezet, a változásokat haladéktalanul bejelenti a Nemzeti Média- és Hírközlési Hatóságnak.

4.2.2 Az egyes feladatok ellátásához szükséges személyzeti létszámok

A *Távoli kulcsmenedzsment szolgáltató* biztonsági és üzemeltetési szabályzata előírja, hogy csak védett környezetben, kettő, bizalmi szerepkört betöltő munkatárs egyidejű fizikai jelenlétében végezhetők el az alábbi műveletek:

- a *Távoli kulcsmenedzsment szolgáltató* saját szolgáltatói kulcspárjának generálása;
- a szolgáltatói magánkulcs mentése;
- a szolgáltatói magánkulcs aktiválása;
- a szolgáltatói magánkulcs megsemmisítése.

A felsorolt műveleteket végrehajtó személyek közül legalább az egyiknek rendszeradminisztrátornak kell lennie és a másik személy nem lehet független rendszervizsgáló.

A felsorolt műveletek végrehajtása során illetéktelen személy nem lehet jelen a helyiségben.

4.2.3 Az egyes szerepkörökben elvárt azonosítás és hitelesítés

A *Távoli kulcsmenedzsment szolgáltató* informatikai rendszerét kezelő felhasználók egyedi azonosító adatokkal rendelkeznek, amely lehetővé teszi a felhasználók biztonságos azonosítását és hitelesítését.

A felhasználók a hitelesítés-szolgáltatás szempontjából kritikus informatikai rendszerekhez csak azonosítás és hitelesítés után férhetnek hozzá.

Az azonosító és hitelesítő adatok a felhasználói jogosultságok megszűnésekor haladéktalanul visszavonásra kerülnek.

Az informatikai rendszer minden felhasználója és az adminisztratív folyamatok minden szereplője személy szerint kerül azonosításra.

A fizikai hozzáférés ellenőrzéséhez a *Távoli kulcsmenedzsment szolgáltató* RFID kártyára épülő beléptető rendszert használ, a logikai hozzáférés ellenőrzése *Elektronikus aláírást létrehozó eszköz*ön kiadott VPN *Tanúsítvány*ok segítségével történik. Sikeres hitelesítés nélkül egyetlen biztonsági szempontból kritikus feladatot sem lehet végrehajtani. A *Távoli kulcsmenedzsment szolgáltató* minden munkatársa annak megfelelő hozzáférési jogosultsággal rendelkezik, amely a feladatköre ellátásához elengedhetetlenül szükséges.

4.2.4 Egymást kizáró szerepkörök

A *Távoli kulcsmenedzsment szolgáltató* munkatársai egyidejűleg több bizalmi szerepkört is betölthetnek, de a *Távoli kulcsmenedzsment szolgáltató* biztosítja, hogy:

- a biztonsági tisztviselő és a regisztrációs felelős nem töltheti be a független rendszervizsgálói szerepkört;
- a rendszeradminisztrátor nem töltheti be a biztonsági tisztviselő és a független rendszervizsgálói szerepkört;
- az informatikai rendszerért általánosan felelős vezető nem láthatja el a biztonsági tisztviselő és a független rendszervizsgáló feladatkörét.

A fentieken túl a *Távoli kulcsmenedzsment szolgáltató* törekszik a bizalmi szerepkörök teljes szétválasztására.

4.3 Személyzetre vonatkozó előírások

A *Távoli kulcsmenedzsment szolgáltató* gondoskodik arról, hogy személyzeti politikája, illetve a munkatársak alkalmazására vonatkozó gyakorlata fokozza és támogassa a *Távoli kulcsmenedzsment szolgáltató* működésének megbízhatóságát. A személyzetre vonatkozó óvintézkedések célja az emberi hibák, lopás, csalás és a visszaélések kockázatának csökkentése.

A *Távoli kulcsmenedzsment szolgáltató* már a felvételi szakaszban foglalkozik a személyi biztonsággal, beleértve a szerződések megkötését, illetve azok alkalmazás során történő ellenőrzését. Valamennyi bizalmi szerepkör esetén a szerepkört betöltő személyeknek kinevezésükkor érvényes erkölcsi bizonyítvánnyal kell rendelkezniük. Minden bizalmi szerepkört betöltő alkalmazottnak és külső félnek – aki a *Távoli kulcsmenedzsment szolgáltató* szolgáltatásaival kapcsolatba kerül – titoktartási nyilatkozatot kell aláírnia.

A *Távoli kulcsmenedzsment szolgáltató* egyúttal biztosítja valamennyi munkakör betöltéséhez a szükséges közös, általános, illetve az egyes szerepkörök betöltéséhez szükséges speciális szakmai ismeretek megszerzését, illetve továbbfejlesztését.

4.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

Felvételi követelményként a *Távoli kulcsmenedzsment szolgáltató* minden dolgozója számára legalább középfokú végzettséget ír elő, de a *Távoli kulcsmenedzsment szolgáltató* a továbbiakban is gondot fordít arra, hogy dolgozói megfelelő képzésben részesüljenek. Közvetlenül a felvételt követően a *Távoli kulcsmenedzsment szolgáltató* új dolgozóit képzésben részesíti, melynek keretében el kell sajátítania a munkája elvégzéséhez szükséges ismereteket. A *Távoli kulcsmenedzsment szolgáltató* általában támogatja a dolgozók szakmai fejlődését, valamint elvárja, hogy a dolgozók saját szakterületükön önállóan fejlesszék tudásukat. A *Távoli kulcsmenedzsment szolgáltató* bizonyos dolgozóinak munkaköri kötelessége a technikai és üzleti újdonságok felderítése és összegyűjtése, rendszerezése, és ezen ismeretek megosztása munkatársaikkal.

A *Távoli kulcsmenedzsment szolgáltató*nál bizalmi szerepkört csak olyan személy tölthet be, akinek a befolyásmentességét és szakértelmét a *Távoli kulcsmenedzsment szolgáltató* igazolni tudja. A

bizalmi szerepkört betöltő személyeknek mentesnek kell lenniük az összeférhetetlenségtől, amely veszélyeztethetné a *Távoli kulcsmenedzsment szolgáltató* tevékenységének pártatlanságát.

Az informatikai rendszerért általánosan felelős vezető csak olyan személy lehet, aki rendelkezik:

- szakirányú felsőfokú végzettséggel (matematikusi, fizikusi egyetemi végzettség vagy a műszaki tudományterületre tartozó mérnöki szakon szerzett főiskolai vagy egyetemi végzettség);
- legalább három év, az informatikai biztonsággal összefüggésben szerzett szakmai gyakorlattal.

4.3.2 Előélet vizsgálatára vonatkozó eljárások

A *Távoli kulcsmenedzsment szolgáltató* vezető munkakörben illetve bizalmi szerepkörben csak olyan alkalmazottakat foglalkoztat, akik:

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

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

A *Távoli kulcsmenedzsment szolgáltató* a felvételi eljárás során ellenőrzi a jelentkező önéletrajzában megadott releváns információk valódiságát, úgy mint előző munkahely, szakmai referenciák, legfontosabb képzettség.

4.3.3 Képzési követelmények

A *Távoli kulcsmenedzsment szolgáltató* az újonnan felvett alkalmazottakat képzésben részesíti, amely során elsajátítják az adott munkakör ellátásához szükséges mértékben:

- a PKI alapismereteket;
- a *Távoli kulcsmenedzsment szolgáltató* informatikai rendszerének sajátosságait és kezelésének módját;
- a szerepkörük ellátásához szükséges speciális ismereteket;
- a *Távoli kulcsmenedzsment szolgáltató* nyilvános és belső szabályzataiban meghatározott folyamatokat, eljárásokat;
- az egyes tevékenységek jogi következményeit;
- az alkalmazandó informatikai biztonsági szabályokat;
- az adatvédelmi szabályokat.

A *Távoli kulcsmenedzsment szolgáltató* éles informatikai rendszereihez csak a képzést sikeresen teljesítő alkalmazottak kapnak hozzáférési jogosultságot.

4.3.4 Továbbképzési gyakoriságok és követelmények

A *Távoli kulcsmenedzsment szolgáltató* gondoskodik arról, hogy az alkalmazottak folyamatosan a megfelelő tudással rendelkezzenek, így szükség esetén továbbképzést, vagy ismétlő jellegű képzést kell tartani.

A *Távoli kulcsmenedzsment szolgáltató* továbbképzést tart, ha folyamataiban vagy informatikai rendszerében változás áll be.

A képzési anyag legalább 12 havonta felülvizsgálatra kerül, és tartalmazza az új fenyegetéseket és biztonsági megoldásokat.

A továbbképzés megfelelően dokumentálásra kerül, amelyből egyértelműen megállapítható a továbbképzés tematikája és a résztvevő dolgozók köre.

4.3.5 Munkabeosztás körforgásának sorrendje és gyakorisága

A *Távoli kulcsmenedzsment szolgáltató* nem alkalmaz kötelező jellegű körforgást az egyes munkabeosztások között.

4.3.6 Felhatalmazás nélküli tevékenységek büntető következményei

A *Távoli kulcsmenedzsment szolgáltató* a dolgozókkal kötendő munkaszerződésben szabályozza a dolgozók felelősségre vonásának lehetőségeit a dolgozó által elkövetett mulasztások, hibák, vétlen vagy szándékos károkozások esetére. Amennyiben egy munkatárs – szándékosan vagy gondatlanul – kötelezettségeit megsérti, vele szemben a *Távoli kulcsmenedzsment szolgáltató* szankciót alkalmazhat, amelyet az elkövetés módjára és következményeire tekintettel állapít meg. Szankcióként alkalmazható a jutalom megvonása, fegyelmi eljárás, elbocsátás, kinevezés visszavonása vagy büntetőjogi felelősségre vonás kezdeményezése.

Valamennyi bizalmi szerepkört betöltő munkatárs a szerepkörbe kinevezéskor a foglalkoztatási dokumentumok részeként:

- írásos tájékoztatást kap jogszabályi kötelezettségeiről, jogairól, a személyes adatai kezelésére vonatkozó minősítési és kezelési szabályokról;
- munkaköri leírást kap, mely tartalmazza az őt érintő biztonsági feladatokat;
- titoktartási nyilatkozatot ír alá, melyben a biztonsági intézkedések be nem tartásával járó, őt érintő következmények (büntető szankciók) is megtalálhatóak.

A felsorolt dokumentumok tartalmazzák azokat a munkajogi következményeket és egyéb szankciókat, amelyek kötelezettségszegés esetén alkalmazhatóak.

4.3.7 Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

A *Távoli kulcsmenedzsment szolgáltató* bizalmi munkakörben csak vele munkaviszonyban álló személyt alkalmaz.

Az egyéb feladatok ellátására alvállalkozói vagy megbízásos szerződésben foglalkoztatott szerződő személyeket a *Távoli kulcsmenedzsment szolgáltató* lehetőség szerint a korábban már

minősített beszállítók listájáról választ. A beszállítókkal a *Távoli kulcsmenedzsment szolgáltató* a munkavégzést megelőzően írásban szerződést köt.

Valamennyi szerződő fél – még a tényleges munkavégzés megkezdése előtt – titoktartási nyilatkozatot ír alá, melyben vállalja, hogy a munkavégzés során későbbiekben megismert üzleti/vállalati titkokat illetéktelen személynek nem fedi fel, egyéb módon nem hasznosítja. A titoktartási nyilatkozat tartalmazza a megszegése esetén alkalmazandó szankciókat is. A szerződés alapján foglalkoztatott külső munkavállalókkal szemben elvárás a megfelelő szakismeret megléte, részükre a *Távoli kulcsmenedzsment szolgáltató* nem tart képzéseket.

4.3.8 A személyzet számára biztosított dokumentációk

A *Távoli kulcsmenedzsment szolgáltató* folyamatosan biztosítja a dolgozók részére a szerepkörük ellátásához szükséges aktuális dokumentációk, szabályzatok rendelkezésre állását.

Minden bizalmi munkakört betöltő munkatárs írásban megkapja a következő dokumentumokat:

- a *Távoli kulcsmenedzsment szolgáltató* szervezeti biztonsági szabályzata;
- aláírandó titoktartási nyilatkozat;
- egyéni munkaköri leírás;
- a tervezett és rendkívüli továbbképzések alkalmával az adott oktatási formához tartozó oktatási segédanyagokat.

A szervezeti biztonsági szabályzatban bekövetkező változásokról írásos értesítő formájában minden dolgozó tájékoztatást kap.

4.4 Naplózási eljárások

A *Távoli kulcsmenedzsment szolgáltató* a biztonságos informatikai környezet fenntartása érdekében a teljes informatikai rendszerét átfogó eseménynaplózó és ellenőrző rendszert üzemeltet.

4.4.1 A tárolt események típusai

A *Távoli kulcsmenedzsment szolgáltató* az általánosan elfogadott informatikai biztonsági gyakorlatnak megfelelően naplóz minden olyan biztonsággal kapcsolatos eseményt, amely információt szolgáltathat az informatikai rendszerben vagy annak fizikai környezetében történt eseményekről, változásokról. Minden naplóbejegyzésnél eltárolja:

- az esemény időpontját;
- az esemény típusát;
- a felhasználó vagy rendszer azonosítóját, aki/amely az eseményt kiváltotta;
- a végrehajtás sikerességét illetve sikertelenségét.

Minden új naplóbejegyzés hozzáadódik a korábban elmentett bejegyzésekhez, az egyszer már elmentett bejegyzés nem kerülhet módosításra vagy törlésre.

Az összes lényeges naplóbejegyzést elérhetővé teszi a független rendszervizsgálók részére, akik a *Távoli kulcsmenedzsment szolgáltató* működésének megfelelőségét vizsgálják.

A *Távoli kulcsmenedzsment szolgáltató* naplózza minimálisan az alábbi eseményeket:

- BELSŐ ÓRA
  - a belső óra szinkronizációja az UTC időhöz, beleértve az üzemszerű újrakalibrálásokat is;
  - a szinkronizáció elvesztése;
- REMOTE KEY MANAGEMENT
  - jelentős TW4S környezeti események;
  - felhasználói aláírási események (például az aláíró aláíró kulcsával történő sikeres aláírás és a DTBS/R kéréskezelés);
  - felhasználói hitelesítés az SAP során;
  - az aláíró SAD kezelése;

  A felhasználói aláírási eseményeknek tartalmazniuk kell az aláírási kulcshoz tartozó tanúsítványt.
- NAPLÓZÁS
  - a naplózó rendszer vagy egyes komponenseinek leállítása, újraindítása;
  - a naplózás bármilyen beállításának módosítása, mint pl. gyakoriság, riasztási küszöb érték, vizsgált esemény;
  - a tárolt naplózási adatok módosítása vagy törlése;
  - a naplózó rendszer hibája miatt végzett tevékenységek;
- RENDSZER BEJELENTKEZÉSEK
  - sikeres bejelentkezések, sikertelen bejelentkezési próbálkozások bizalmi szerepkörökbe;
  - jelszó alapú azonosítás esetén:
    - az engedélyezett sikertelen bejelentkezési próbálkozások számának megváltoztatása;
    - az engedélyezett sikertelen bejelentkezési próbálkozások számának elérése felhasználói bejelentkezéskor;
    - sikertelen bejelentkezések miatt zárolt felhasználó újbóli engedélyezése;
  - az azonosítási technika változtatása (például jelszó alapúról PKI alapúra);
- KULCSKEZELÉS
  - a szolgáltatói kulcsok teljes életciklusára vonatkozó valamennyi esemény (kulcsgenerálás, elmentés, betöltés, megsemmisítés stb.);

  - a felhasználói aláíró kulcsok kezelésével kapcsolatos események (generálás, használat, megsemmisítés);

- TANÚSÍTVÁNY KEZELÉS
- ADATMOZGÁSOK
  - bármilyen, a biztonság szempontjából kritikus adat manuális bevitele a rendszerbe;
  - a rendszer által fogadott, biztonsági szempontból fontos adatok, üzenetek;
- *HSM eszköz*
  - *HSM eszköz* installálása;
  - *HSM eszköz* eltávolítása;
  - *HSM eszköz* selejtezése, megsemmisítése;
  - *HSM eszköz* szállítása;
  - *HSM eszköz* tartalmának törlése (nullázás);
  - *HSM eszköz* feltöltése kulcsokkal, tanúsítványokkal;
- KONFIGURÁCIÓ VÁLTOZÁSA
  - hardver;
  - szoftver;
  - operációs rendszer;
  - javító csomag;
  - szoftver telepítése, frissítése vagy eltávolítása a *Távoli kulcsmenedzsment szolgáltató* rendszerében;
- FIZIKAI HOZZÁFÉRÉS, TELEPHELY BIZTONSÁG
  - személy belépése a bizalmi szolgáltatást nyújtó rendszer komponenseket tartalmazó biztonsági területre és onnan kilépése;
  - hozzáférés egy bizalmi szolgáltatást nyújtó rendszer komponenshez;
  - a fizikai biztonság ismert vagy gyanított megsértése;
  - tűzfal és router forgalmak;
- MŰKÖDÉSI RENDELLENESSÉGEK
  - rendszerösszeomlás, hardver hiba;
  - szoftveres hibák;
  - szoftverintegritás ellenőrzési hiba;
  - hibás vagy rossz helyre továbbított üzenetek;
  - hálózatot ért támadások, támadási kísérletek;
  - berendezés hiba;

  - elektromos hálózati üzemzavar;
  - szünetmentes tápegység hiba;
  - lényeges hálózati szolgáltatás hozzáférési hiba;
  - a *Távoli kulcsmenedzsment szolgáltatási szabályzat* megsértése;
  - operációs rendszer órájának törlése;
- EGYÉB ESEMÉNYEK
  - személy kinevezése biztonsági szerepkörbe;
  - operációs rendszer telepítése;
  - PKI alkalmazás telepítése;
  - rendszer elindítása;
  - belépési kísérlet a PKI alkalmazásba;
  - jelszó módosítási, beállítási kísérlet;
  - a belső adatbázis elmentése, visszaállítása mentésből;
  - fájl műveletek (pl. létrehozás, átnevezés, áthelyezés);
  - adatbázis hozzáférés.

4.4.2 A naplófájl feldolgozásának gyakorisága

A *Távoli kulcsmenedzsment szolgáltató* független rendszervizsgálói a keletkezett naplóbejegyzéseket minden munkanapon átvizsgálják.

A kiértékelés során meggyőződnek a vizsgált naplóállományok hitelességéről és sértetlenségéről, ellenőrzik a bejegyzésekben talált hibaüzeneteket, szükség esetén dokumentálják az eltérést és intézkedéseket hoznak az eltérés okának megszüntetése érdekében.

Az informatikai rendszerek ellenőrzésére a *Távoli kulcsmenedzsment szolgáltató* automatizált ellenőrző rendszereket is használ, amelyek előre beállított szempontok szerint folyamatosan figyelik a keletkező naplóbejegyzéseket és szükség esetén riasztják az üzemeltetés munkatársait.

Az automatizált ellenőrző rendszerekből kapott értesítéseket az IT üzemeltetés munkatársai 24 órán belül feldolgozzák és az eredményeket kiértékelik.

A vizsgálat ténye, a vizsgálat eredményei és az esetleges feltárt hiányosságok elhárítása érdekében meghozott intézkedések megfelelően dokumentálásra kerülnek.

4.4.3 A naplófájl megőrzési időtartama

Az online rendszerből való kitörlés előtt a naplóállományokat a *Távoli kulcsmenedzsment szolgáltató* archiválja és gondoskodik azok biztonságos megőrzéséről az 4.5.2 fejezetben meghatározott ideig, de legalább a keletkezésüktől számított 10 évig.

Ezen időtartamig a *Távoli kulcsmenedzsment szolgáltató* biztosítja az archivált adatok olvashatóságát, megőrzi az ehhez szükséges szoftver és hardver eszközöket.

4.4.4 A naplófájl védelme

A *Távoli kulcsmenedzsment szolgáltató* az előírt megőrzési ideig tárolja és védi a keletkezett naplóállományokat. A megőrzési idő teljes időtartama alatt biztosítja a naplóadatok:

- védelmét az illetéktelen felfedés ellen: a naplóállományokhoz csak az arra jogosultak – elsősorban a független rendszervizsgálók – férhetnek hozzá;
- rendelkezésre állását: a jogosultak számára biztosítja a naplóállományokhoz való hozzáférést;
- integritását: megakadályozza például a naplóállományokban bármilyen adat módosítását, törlését, bejegyzések sorrendjének megváltoztatását.

A *Távoli kulcsmenedzsment szolgáltató* a naplóbejegyzéseket minősített *Időbélyegző*vel látja el, a naplóbejegyzések törlések és beszúrások észrevétlen végrehajtását kizáró módon kerülnek tárolásra.

A naplóállományt a véletlen és szándékos rongálások ellen biztonsági mentések védik. A személyes adatokat tartalmazó naplóbejegyzések esetében a *Távoli kulcsmenedzsment szolgáltató* gondoskodik az adatok bizalmas tárolásáról. A naplóállományokhoz való hozzáférésre csak azok jogosultak, akiknek erre munkakörük folytán feltétlenül szükségük van. A *Távoli kulcsmenedzsment szolgáltató* a hozzáféréseket biztonságos módon ellenőrzi. A naplóállományokat a *Távoli kulcsmenedzsment szolgáltató* biztonságos környezetben őrzi. Az állományokról a működés másodlagos helyszínén másolati példányokat is tart.

4.4.5 A naplófájl mentési eljárásai

Az üzemeltetés során az egyes rendszerekben folyamatosan keletkező naplóbejegyzésekből napi naplóállományok generálódnak.

A napi naplóállományokat a *Távoli kulcsmenedzsment szolgáltató* 2 példányban archiválja és a példányokat egymástól fizikailag elkülönülő helyszíneken az előírt ideig megőrzi.

A mentés operatív folyamatait a *Távoli kulcsmenedzsment szolgáltató* mentési szabályzatai írják le részletesen.

4.4.6 A naplózás adatgyűjtési rendszere

A naplóbejegyzéseket az egyes alkalmazások automatikusan gyűjtik és továbbítják a naplózó rendszer felé.

A naplózó funkciók automatikusan indulnak a rendszer indításakor és a rendszer működésének teljes időtartama alatt folyamatosan működnek.

Az automatikus vizsgáló és naplózó rendszerek működési rendellenessége esetén a *Távoli kulcsmenedzsment szolgáltató* felfüggeszti az érintett területek működését az üzemzavar elhárításáig.

4.4.7 Az eseményeket kiváltó alanyok értesítése

A hibaeseményt kiváltó személyeket, szervezeteket és alkalmazásokat a *Távoli kulcsmenedzsment szolgáltató* nem feltétlenül értesíti minden esetben, szükség esetén azonban bevonhatja őket az esemény kivizsgálásába. Az esemény kiváltásában érintett *Ügyfel*eknek ilyen esetben kötelességük a *Távoli kulcsmenedzsment szolgáltató*val való együttműködés a hiba feltárása érdekében.

4.4.8 Sebezhetőség felmérése

A naplóbejegyzések napi rendszerességgel végzett feldolgozásán túl a *Távoli kulcsmenedzsment szolgáltató* szakemberei figyelik a nyilvánosan elérhető információt a lehetséges sérülékenységekről, szoftver javító csomagokról. Elemzik a gyűjtött információt, osztályba sorolják a sérülékenységet és szükség esetén értesítik a vezetőséget az eredményről és intézkedési tervet javasolnak a rendszer biztonságának növelésére.

Minden nagyobb jelentőségű feltárt hiányosság vagy külső fenyegetettség esetén az észlelésétől számított 48 órán belül, de legalább évente egyszer a *Távoli kulcsmenedzsment szolgáltató* szakemberei átfogó sebezhetőség vizsgálatot végeznek, amely segítségével feltérképezik a potenciális belső és külső fenyegetettségeket, amelyek jogosulatlan hozzáféréseket eredményezhetnek.

A vizsgálat eredményei alapján a *Távoli kulcsmenedzsment szolgáltató*

- intézkedési tervet hoz létre és hajt végre a sérülékenységek megszüntetése érdekében, vagy
- dokumentálja a döntés alapjául szolgáló tényeket, elfogadja a maradvány kockázatokat és nem hoz intézkedési tervet a sérülékenység megszüntetésére.

Az új program verziókat vagy program javító csomagokat a *Távoli kulcsmenedzsment szolgáltató* először a teszt rendszeren telepíti és csak a sikeres tesztek elvégzése után kerülnek telepítésre a szolgáltatásokat nyújtó éles rendszeren.

Az új szoftver verziók vagy javító csomagok nem kerülnek bevezetésre az éles rendszeren, amennyiben olyan további sérülékenységet vagy instabilitást okoznak a rendszer működésében, ami nagyobb gondot eredményez az alkalmazásukból származó előnynél. Az alkalmazás mellőzésének okát a *Távoli kulcsmenedzsment szolgáltató* dokumentálja.

4.5 Adatok archiválása

4.5.1 Az archivált adatok típusai

A *Távoli kulcsmenedzsment szolgáltató* felkészült elektronikus és papíralapú dokumentumok megfelelően biztonságos, hosszú idejű archiválására.

A *Távoli kulcsmenedzsment szolgáltató* minimálisan az alábbi jellegű információt archiválja:

- a *Távoli kulcsmenedzsment szolgáltató* akkreditációjával kapcsolatos valamennyi irat;
- a *Távoli kulcsmenedzsment szolgáltatási szabályzat*(ok) valamennyi kibocsátott verziója;
- az Általános Szerződési Feltételek valamennyi kibocsátott verziója;
- a *Távoli kulcsmenedzsment szolgáltató* működésével kapcsolatos szerződések;
- valamennyi elektronikus és papíralapú naplóbejegyzés.

4.5.2 Az archívum megőrzési időtartama

A *Távoli kulcsmenedzsment szolgáltató* az archivált adatokat az alábbi időtartamokig őrzi meg:

- a *Távoli kulcsmenedzsment szolgáltatási szabályzat*ot a hatályon kívül helyezéstől számított legalább 10 évig;
- Általános Szerződési Feltételeket a hatályon kívül helyezéstől számított legalább 10 évig;
- minden egyéb archiválandó dokumentomot a keletkezésétől számított legalább 10 évig.

4.5.3 Az archívum védelme

A *Távoli kulcsmenedzsment szolgáltató* valamennyi archivált adatot két példányban, két egymástól fizikailag elkülönült helyszínen őrzi. Az egyetlen hiteles példányban rendelkezésre álló papíralapú dokumentumról hiteles papíralapú, vagy elektronikus másolatot készít a vonatkozó jogszabályok betartásával.

A két helyszín mindegyike teljesíti az archiválással szemben támasztott biztonsági és egyéb követelményeket.

Az archivált adatok megőrzése során a *Távoli kulcsmenedzsment szolgáltató* gondoskodik az archivált adatok

- sértetlenségének megőrzéséről;
- illetéktelen megismerés elleni védelméről;
- rendelkezésre állásáról;
- hitelességének megőrzéséről.

Az archivált elektronikus adatokat legalább fokozott biztonságú elektronikus aláírással vagy bélyegzővel és minősített *Időbélyegző*vel látja el.

4.5.4 Az archívum mentési folyamatai

A *Távoli kulcsmenedzsment szolgáltató* a papíralapú dokumentumok eredeti példányáról hiteles elektronikus másolatot készít a vonatkozó jogszabályok betartásával.

Az elektronikus másolatokat a többi védendő elektronikus dokumentummal azonos szabályok szerint tárolja.

A *Távoli kulcsmenedzsment szolgáltató* a hiteles elektronikus másolatok archiválása után az eredeti papíralapú dokumentumokat megsemmisítheti.

4.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Valamennyi elektronikus naplóbejegyzés tartalmaz időjelzést, amelyen legalább másodperc pontossággal fel van tüntetve a rendszer által szolgáltatott időpont.

Az időpontot a *Távoli kulcsmenedzsment szolgáltató* belső órája adja, amelyet a *Távoli kulcsmenedzsment szolgáltató* két egymástól független Stratum-1 UTC referencia időforrással szinkronizál:

- az egyik pontos idő forrás a műhold alapú GNSS (GPS és Galileo) rendszert használja;
- a másik pontos idő forrás a hosszúhullámú pontos idő szolgáltatásra (DCF77) támaszkodik.

A *Távoli kulcsmenedzsment szolgáltató* a fenti két független Stratum-1 időforráshoz 0,1 másodperc pontossággal szinkronizálja saját belső óráját. E szinkronizációt a *Távoli kulcsmenedzsment szolgáltató* naponta legalább négy alkalommal elvégzi.

A *Távoli kulcsmenedzsment szolgáltató* a belső óra pontosságának ilyen szinten tartásával garantálja, hogy valamennyi időjelzés pontossága legfeljebb 1 másodperccel tér el az UTC időalaptól.

A *Távoli kulcsmenedzsment szolgáltató* a napi naplóállományokat minősített *Időbélyegző*vel látja el.

Az archivált adatok megőrzése során szükség esetén (pl. algoritmusváltás, az eredeti *Időbélyegző* érvényességének lejárata) a *Távoli kulcsmenedzsment szolgáltató* gondoskodik az adatok hitelességének megőrzéséről.

4.5.6 Az archívum gyűjtési rendszere

A *Távoli kulcsmenedzsment szolgáltató* védett informatikai rendszerén belül keletkeznek a naplóbejegyzések, onnan csak az elektronikusan aláírt, minősített *Időbélyegző*vel védett naplóállományok kerülhetnek ki.

A Távoli kulcsmenedzsment szolgáltatás nyújtása során keletkezett papíralapú iratok egy eredeti példányát a *Távoli kulcsmenedzsment szolgáltató* az általa működtetett belső adattárban tárolja és őrzi.

4.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások

A *Távoli kulcsmenedzsment szolgáltató* a naplóállományok előállítását automatikusan végzi, a hitelesített naplóállományokat naponta állítja elő.

Az archivált adatállományokat védi a jogosulatlan hozzáféréstől.

Az arra jogosultaknak biztosítja az archivált adatokhoz való ellenőrzött hozzáférést:

- az *Ügyfel*ek jogosultak a róluk tárolt adatok megtekintésére;
- jogi eljárásokban bizonyíték nyújtása céljából biztosítani kell a szükséges adatokat.

4.6 Kompromittálódást és katasztrófát követő helyreállítás

A *Távoli kulcsmenedzsment szolgáltató* katasztrófa esetén minden szükséges intézkedést meghoz annak érdekében, hogy a szolgáltatáskiesésből eredő károkat minimalizálja és a szolgáltatásokat a lehető legrövidebb időn belül helyreállítsa.

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

A hiba elhárítása után az eseményt jelenti a Nemzeti Média- és Hírközlési Hatóságnak, mint felügyeleti szervnek.

4.6.1 Váratlan esemény és kompromittálódás kezelési eljárások

A *Távoli kulcsmenedzsment szolgáltató* rendelkezik üzletmenet folytonossági tervvel.

A *Távoli kulcsmenedzsment szolgáltató* megnövelt biztonságú eszközökkel és rendszerekkel rendelkezik a hardver és szoftver meghibásodások valamint az adatsérülések okozta szolgáltatáskiesés minimalizálása érdekében. A szolgáltatások helyreállíthatóságát a *Távoli kulcsmenedzsment szolgáltató* háttérszerződései és saját tartalék eszközei garantálják.

A *Távoli kulcsmenedzsment szolgáltató* belső szabályzatai részletesen meghatározzák a biztonsági incidensek kezelésével kapcsolatos feladatokat. A normál működéstől való bármilyen eltérésről az észlelés után feljegyzés készül a belső feladatkezelő rendszerben. A *Távoli kulcsmenedzsment szolgáltató* az eltérés észlelése után haladéktalanul megkezdi az eltérés kivizsgálását, a lehető leghamarabb megszünteti az észlelt eltérést és szükség esetén megelőző intézkedéseket hoz az eltérés ismételt előfordulásának megakadályozása érdekében.

A *Távoli kulcsmenedzsment szolgáltató* minden esetben biztonsági incidensnek tekinti és kiemelten kezeli az olyan eltérést, amely kihatással lehet a szolgáltatások elérhetőségére, integritására vagy bizalmasságára (pl. szolgáltatás kieséssel jár).

A *Távoli kulcsmenedzsment szolgáltató* a szolgáltatás kiesésről és a súlyosnak ítélt biztonsági incidensről az incidens keletkezésétől számított 24 órán belül hivatalosan értesíti a Nemzeti Média- és Hírközlési Hatóságot.

4.6.2 Meghibásodott IT erőforrások, szoftverek és/vagy adatok

A *Távoli kulcsmenedzsment szolgáltató* informatikai rendszereit megbízható hardver és szoftver komponensekből építette fel. A kritikus funkciókat redundáns rendszerelemek alkalmazásával valósította meg úgy, hogy azok egy elem meghibásodása esetén is képesek legyenek a további működésre.

A *Távoli kulcsmenedzsment szolgáltató* naponta teljes mentést készít az adatbázisairól és a keletkezett naplózási eseményekről.

A *Távoli kulcsmenedzsment szolgáltató* olyan gyakorisággal készít teljes rendszermentést, amely biztosítja, hogy abból katasztrófa esetén a teljes szolgáltatás helyreállítható legyen.

A *Távoli kulcsmenedzsment szolgáltató* üzletmenet folytonossági terve pontos előírásokat tartalmaz a kritikus rendszerkomponensek meghibásodásának esetén végrehajtandó feladatokra.

A *Távoli kulcsmenedzsment szolgáltató* a hiba elhárítása és a rendszer integritásának helyreállítása után a lehető leghamarabb újraindítja a szolgáltatásait.

4.6.3 Működés folyamatosságának biztosítása katasztrófát követően

A *Távoli kulcsmenedzsment szolgáltató* üzletmenet folytonossági tervében meghatározta a természeti vagy egyéb katasztrófa miatt bekövetkezett szolgáltatás leállás esetén végrehajtandó feladatokat.

A katasztrófa bekövetkezése esetén haladéktalanul életbe lépteti a rendelkezéseket és megkezdi a károk elhárítását, a szolgáltatások helyreállítását.

A *Távoli kulcsmenedzsment szolgáltató* a lehető legrövidebb időn belül köteles értesíteni az érintett felhasználókat a katasztrófa bekövetkezéséről.

A szolgáltatások helyreállítása után a *Távoli kulcsmenedzsment szolgáltató* a lehető legrövidebb időn belül helyreállítja a katasztrófa során tönkrement eszközeit és az eredeti szolgáltatás biztonsági szintet.

4.7 A szolgáltatás leállítása

A *Távoli kulcsmenedzsment szolgáltató* a Távoli kulcsmenedzsment szolgáltatás tervezett megszüntetése esetén legkevesebb 60 nappal a Távoli kulcsmenedzsment szolgáltatás leállítását megelőzően értesíti a végfelhasználókat és a Nemzeti Média- és Hírközlési Hatóságot.

A *Távoli kulcsmenedzsment szolgáltató* a Távoli kulcsmenedzsment szolgáltatás leállítására vonatkozó bejelentéssel egyidejűleg leállítja a következő szolgáltatásait:

- új előfizetői szerződések kötése,
- kulcs előállítás,
- kulcscsere.

A leállás időpontjával egyidejűleg a *Távoli kulcsmenedzsment szolgáltató* a következő szolgáltatásokat állítja le:

- távoli kulcs használat,
- műszaki segítségnyújtás,
- információ szolgáltatás.

A *Távoli kulcsmenedzsment szolgáltató* a Távoli kulcsmenedzsment szolgáltatás leállítását követően haladéktalanul kezdeményezi a Hitelesítés szolgáltatótól a szolgáltatásban menedzselt végfelhasználói kulcsokhoz tartozó *Tanúsítvány*ok visszavonását. A *Távoli kulcsmenedzsment szolgáltató* megsemmisíti valamennyi, a rendszerében kezelt végfelhasználói kulcsot, beleértve a kulcsokról készült valamennyi mentési állományt is. A *Távoli kulcsmenedzsment szolgáltató* a kulcsok megsemmisítéséről jegyzőkönyvet vesz fel.

A *Távoli kulcsmenedzsment szolgáltató* a tervezett megszűnés előtt tárgyalásokat kezd más vele azonos besorolású bizalmi szolgáltatókkal szolgáltatásainak átvételéről. Nyilvántartásait a bizalmas felhasználói adatokkal együtt a 7.3 fejezet szerint mindenképpen átadja egy ilyen bizalmi szolgáltatónak, vagy megállapodás hiányában a Nemzeti Média- és Hírközlési Hatóságnak, egyéb szolgáltatásait a tárgyalások eredményétől függően átadja vagy átadás nélkül megszünteti.

A *Távoli kulcsmenedzsment szolgáltató* a tárgyalások végeredményéről tájékoztatja az *Ügyfel*eket és a Nemzeti Média- és Hírközlési Hatóságot. A *Távoli kulcsmenedzsment szolgáltató* az *Ügyfel*eket elektronikus levélben, az *Érintett felek*et a honlapján történő közzététel útján tájékoztatja.

A *Távoli kulcsmenedzsment szolgáltató* a Távoli kulcsmenedzsment szolgáltatás befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, minősített *Időbélyegző*vel ellátott mentést készít.

A *Távoli kulcsmenedzsment szolgáltató* – annak érdekében, hogy adatait átadhassa egy másik bizalmi szolgáltatónak – az adatokat az új bizalmi szolgáltató által fogadni képes médián és formátumban helyezi el vagy biztosítja az új bizalmi szolgáltató számára az adatok eredeti formátumban

történő feldolgozásának lehetőségét, amelyekhez átadja a megfelelő eszközöket, dokumentációkat és ismereteket. A Távoli kulcsmenedzsment szolgáltatás leállítását követően a *Távoli kulcsmenedzsment szolgáltató* visszaállíthatatlan módon törli az *Előfizető*k magánkulcsait és azonosító adatait a rendszereiből.

5 Műszaki biztonsági óvintézkedések

A *Távoli kulcsmenedzsment szolgáltató* módosítás ellen védett, megbízható, biztonságtechnikailag értékelt termékekből álló informatikai rendszereket használ szolgáltatásai nyújtásához. A *Távoli kulcsmenedzsment szolgáltató* a szolgáltatói és végfelhasználói kriptográfiai magánkulcsokat teljes életciklusuk alatt megfelelő tanúsítással rendelkező *HSM eszköz*ökben kezeli.

Mind a *Távoli kulcsmenedzsment szolgáltató*, mind a rendszert szállító és kivitelező vállalkozók jelentős tapasztalatokkal rendelkeznek PKI alapú rendszerek és bizalmi szolgáltatások kiépítésében és nemzetközileg elismert technológiát alkalmaznak.

A *Távoli kulcsmenedzsment szolgáltató* folyamatosan nyomon követi a kapacitás igényeket és a trendek felállításával becslést ad a jövőbeni várható kapacitás igényekre. Igény esetén gondoskodik a szűkös kapacitások bővítéséről, ezáltal biztosítja a szükséges feldolgozási és tárolási kapacitások folyamatos rendelkezésre állását.

5.1 Kulcspár előállítása és telepítése

A *Távoli kulcsmenedzsment szolgáltató* gondoskodik valamennyi általa – az *Alany*ok illetve saját IT rendszerei számára – generált magánkulcs biztonságos, a hatályos jogszabályi előírásoknak és az ipari szabványoknak megfelelő előállításáról és kezeléséről.

5.1.1 Kulcspár előállítása

A *Távoli kulcsmenedzsment szolgáltató* a kulcspárok generálásához mindenkor csak olyan kulcsgenerálási algoritmusokat használ, amelyek megfelelnek az alábbi normatívákban megfogalmazott követelményeknek:

- ETSI TS 119 312 [11];
- az Eüt. [6] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

Szolgáltatói infrastruktúrális kulcspárok előállítása

A *Távoli kulcsmenedzsment szolgáltató* a saját IT rendszereiben használt infrastruktúrális kulcsok előállítása esetén biztosítja, hogy:

- a szolgáltatói infrastruktúrális kulcs előállítását fizikailag védett környezetben (lásd 4.1 pont), bizalmi szerepkört (lásd 4.2.1 pont) betöltő, erre feljogosított személy végzi, más illetéktelen személyek jelenlétét kizárva;
- a kulcs előállítása során maradéktalanul betartja az eszköz felhasználói dokumentációjában szereplő előírásokat.

Végfelhasználói kulcspárok előállítása és ellenőrzése

A *Távoli kulcsmenedzsment szolgáltató* által az *Alany*ok számára előállított kulcspár előállítása esetén biztosítja, hogy:

- A kulcsok előállítását fizikailag védett környezetben végzi automatikusan, vagy kizárólag bizalmi szerepkört betöltő személyek részvételével.
- A *Távoli kulcsmenedzsment szolgáltató* a végfelhasználói kulcsokat saját *HSM eszköz*én generálja, ami lehetetlenné teszi a magánkulcs felfedését.
- A *Távoli kulcsmenedzsment szolgáltató* meggyőződik arról, hogy az előállított kulcspár megfelel a 5.1.4 és 5.1.5 fejezetekben meghatározott követelményeknek, és a nyilvános kulcs nem egy ismert gyenge kulcspár tagja.

5.1.2 Magánkulcs eljuttatása az igénylőhöz

A Távoli kulcsmenedzsment szolgáltatás esetében:

- A *Távoli kulcsmenedzsment szolgáltató* az általa az *Alany*ok részére generált magánkulcsokat a szolgáltatás teljes időtartama alatt biztonságos módon tárolja, amely megakadályozza a kulcsok felfedését, lemásolását, módosítását, sérülését, illetéktelenek általi használatát.
- A *Távoli kulcsmenedzsment szolgáltató* olyan azonosítási eljárást alkalmaz, amely biztosítja, hogy a magánkulcsot csak az arra jogosult *Alany* használhassa.
- A *Távoli kulcsmenedzsment szolgáltató* megfelelő bizonyítékot tárol el arról, hogy a magánkulcs feletti rendelkezést az *Alany* számára adott hiteles időpontban átadta.
- A magánkulcs feletti rendelkezés *Alany* számára történő átadását követően biztosítja, hogy kizárólag az *Alany* legyen képes a magánkulcs használatához szükséges azonosítási folyamat lefolytatására.

5.1.3 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

A *Távoli kulcsmenedzsment szolgáltató* által betartandó követelmények:

- a nyilvános kulcsot olyan módon kell eljuttatni a *Tanúsítvány*t kibocsátó Hitelesítés szolgáltatóhoz, hogy az egyértelműen az *Alany*hoz rendelhető legyen;
- a *Tanúsítványkérelem* folyamatának bizonyítania kell, hogy az *Alany* valóban rendelkezik a nyilvános kulcshoz tartozó magánkulccsal.

A Távoli kulcsmenedzsment szolgáltatás keretében a *Távoli kulcsmenedzsment szolgáltató* az általa előállított végfelhasználói kulcsok esetében egy PKCS#10 formátumú *Tanúsítványkérelmet* juttat el a Hitelesítés szolgáltatóhoz, amit a *Tanúsítvány*ba kerülő nyilvános kulcshoz tartozó magánkulccsal aláír. A PKCS#10 formátumú *Tanúsítványkérelem* tartalmazza az *Alany Tanúsítvány*ba kerülő nyilvános kulcsát és a *Tanúsítvány*ba kerülő azonosító adatait, ezáltal mindkét követelmény teljesül.

5.1.4 Kulcsméretek

A *Hitelesítés-szolgáltató* mindenkor csak olyan kriptográfiai algoritmusokat és minimális kulcsméreteket használ, amelyek megfelelnek az alábbi normatívákban megfogalmazott követelményeknek:

- ETSI TS 119 312 [11];
- az Eüt. [6] 92. § (1) b) pontja szerinti aktuális Nemzeti Média- és Hírközlési Hatóság által kiadott algoritmusokkal kapcsolatos határozat.

A *Távoli kulcsmenedzsment szolgáltató* kizárólag az alábbi RSA kulcshosszakat támogatja:

- RSA-2048 (2048 bit)
- RSA-3072 (3072 bit)
- RSA-4096 (4096 bit)

A *Távoli kulcsmenedzsment szolgáltató* kizárólag az alábbi ECC görbéket támogatja:

- ECC NIST P-256 (256 bit)
- ECC NIST P-384 (384 bit)
- ECC NIST P-521 (521 bit)

Az ECC kulcs minden esetben egy érvényes pont egy támogatott elliptikus görbén.

5.1.5 A nyilvános kulcs paraméterek előállítása, a minőség ellenőrzése

A *Távoli kulcsmenedzsment szolgáltató* a kulcsok generálását a 5.1.1. fejezetben leírtak szerint végzi.

A paraméterek megfelelőségének ellenőrzése

A *Hitelesítés-szolgáltató* valamennyi szolgáltatói és végfelhasználói *Tanúsítvány* kibocsátása előtt ellenőrzi a kulcs megfelelőségét az alábbi szempontok szerint:

1. RSA kulcsok esetén
    - az RSA kulcshossz a támogatott értékek között szerepel
    - az RSA nyilvános kitevő páratlan
    - az RSA nyilvános kitevő értéke legalább "(2 exp 16)+1" és legfeljebb "(2 exp 256)-1"
    - a modulus páratlan, nem prímhatvány és nincs 752-nél kisebb osztója
2. ECC kulcsok esetén
    - a kulcs egy támogatott elliptikus görbén egy érvényes pont (ECC Full Public-Key Validation Routine a NIST Special Publication 800-56A Revision 3 [16] 5.6.2.3.3 fejezetének megfelelően.)

5.1.6 A kulcshasználat célja (az X.509 v3 kulcs használati mező tartalmának megfelelően)

A *Távoli kulcsmenedzsment szolgáltató* az általa kezelt végfelhasználói magánkulcsot kizárólag csak a kulcshoz tartozó *Tanúsítvány*ban szereplő kulcshasználati beállításoknak megfelelően használhatja.

5.2 A magánkulcsok védelme

A *Távoli kulcsmenedzsment szolgáltató* gondoskodik a birtokában lévő magánkulcsok biztonságos kezeléséről, megakadályozza a magánkulcsok felfedését, lemásolását, törlését, módosítását, jogosulatlan használatát. A *Távoli kulcsmenedzsment szolgáltató* csak addig őrzi a magánkulcsokat, ameddig azt a Távoli kulcsmenedzsment szolgáltatás nyújtása feltétlenül megköveteli.

5.2.1 Kriptográfiai modulra vonatkozó szabványok és előírások

A *Távoli kulcsmenedzsment szolgáltató* kulcsmenedzsment rendszerei a végfelhasználói magánkulcsokat olyan biztonságos hardver eszközökben tárolják, amelyek

- megfelelnek a FIPS 140-2 [15] Level 3-as szintű követelményeknek.

A *Távoli kulcsmenedzsment szolgáltató* a szolgáltatói és végfelhasználói magánkulcsokat a *HSM eszköz*ön kívül csak kódolt formában tárolja. A kódoláshoz csak az Eüt. [6] 92. § (1) b) szerint kiadott aktuális Nemzeti Média- és Hírközlési Hatóság határozat szerinti algoritmusokat és kulcsparamétereket használ, amelyek várhatóan a kulcs teljes élettartama alatt képesek ellenállni a kriptográfiai támadásoknak.

A *Távoli kulcsmenedzsment szolgáltató* a szolgáltatói magánkulcsokat kódolt formában is fizikailag biztonságos helyszínen tárolja az *Adatközpont* páncélszekrényében, ahol azokhoz csak az arra jogosultak férhetnek hozzá.

A *Távoli kulcsmenedzsment szolgáltató* a kriptográfiai algoritmusok vagy kulcsparaméterek gyengülése esetén a kódolt kulcsokat megsemmisíti vagy erősebb védelmet biztosító algoritmus és kulcsparaméterek felhasználásával tovább kódolja.

5.2.2 Magánkulcs többszereplős (n-ből m) használata

A *Távoli kulcsmenedzsment szolgáltató* alkalmazza az "n-ből m" ellenőrzést a magánkulcsokkal kapcsolatos kulcsgondozási funkciók aktivizálásánál. A paraméterek úgy lettek meghatározva, hogy a szolgáltatói magánkulcsaival végzett kritikus műveletek végrehajtásához legalább kettő, bizalmi szerepkört betöltő munkatárs egyidejű jelenlétére legyen szükség.

5.2.3 Magánkulcs letétbe helyezése

A *Távoli kulcsmenedzsment szolgáltató* a szolgáltatói és végfelhasználói magánkulcsokat nem helyezi letétbe.

5.2.4 Magánkulcs mentése

A *Távoli kulcsmenedzsment szolgáltató* biztonsági másolatot készít minden szolgáltatói magánkulcsáról még a magánkulcs használatbavételét megelőzően illetve minden végfelhasználói magánkulcsról legalább napi rendszerességgel a 5.2.1. fejezetben leírtak szerint védett környezetben, legalább két bizalmi szerepkört betöltő személy együttes jelenlétében, más személyek kizárásával. A mentés során a magánkulcs titkosított formában hagyja el a modult, e titkosított kulcsot később másik modulba be lehet tölteni. Mind a mentés, mind a visszatöltés csakis a 5.2.2. fejezetben leírt védelmi mechanizmus mellett végezhető.

A *Távoli kulcsmenedzsment szolgáltató* a biztonsági másolatot két példányban tárolja, ebből legalább az egyik példányt a szolgáltatás nyújtásától eltérő helyszínen.

A biztonsági másolatok kezelésére és megőrzésére ugyanolyan szigorú biztonsági előírások vonatkoznak, mint az éles rendszer üzemeltetésére.

5.2.5 Magánkulcs archiválása

A *Távoli kulcsmenedzsment szolgáltató* nem archiválja szolgáltatói magánkulcsait és az *Ügyfel*ek végfelhasználói magánkulcsait.

5.2.6 Magánkulcs bejuttatása hardver kriptográfiai eszközbe, vagy onnan történő exportja

A *Távoli kulcsmenedzsment szolgáltató* valamennyi szolgáltatói magánkulcsát illetve az általa kezelt végfelhasználói magánkulcsokat a követelményeknek megfelelő *HSM eszköz*ben állítja elő.

A magánkulcsok nem léteznek nyílt formában a *HSM eszköz*ön kívül.

A *Távoli kulcsmenedzsment szolgáltató* a magánkulcsot csak biztonsági másolat készítése céljából exportálja a *HSM eszköz*ből.

A magánkulcs *HSM eszköz*ök közötti szállítása csak biztonsági másolat formájában engedélyezett.

A szolgáltatói magánkulcsok exportálása vagy betöltése minden esetben a 5.2.2. fejezetben leírt módon történik.

5.2.7 Magánkulcs tárolása hardver kriptográfiai eszközben

A *Távoli kulcsmenedzsment szolgáltató* a Távoli kulcsmenedzsment szolgáltatás nyújtásához használt magánkulcsait illetve az általa kezelt végfelhasználói magánkulcsokat a 5.2.1. fejezet szerinti kriptográfiai modulokban tartja.

A *HSM eszköz*ben a magánkulcsokat az eszköz tanúsításában meghatározott módon tárolja és használja a vonatkozó kezelési utasítások maradéktalan betartásával.

5.2.8 A magánkulcs aktiválásának módja

A *Távoli kulcsmenedzsment szolgáltató* szolgáltatói magánkulcsait biztonságos *HSM eszköz*ben tárolja, a használat során betartja a *HSM eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott követelményeket. A *HSM eszköz*t csak a hozzá tartozó operátori kártyákkal lehet aktiválni, a *HSM eszköz*ben lévő magánkulcsokat a modul aktiválása előtt

nem lehet használni. A *HSM eszköz*höz tartozó operátori kártyákat a *Távoli kulcsmenedzsment szolgáltató* biztonságos környezetben tárolja és e kártyákat kizárólag a *Távoli kulcsmenedzsment szolgáltató* erre jogosult munkatársai érhetik el.

5.2.9 A magánkulcs deaktiválásának módja

A *Távoli kulcsmenedzsment szolgáltató* által használt hardver kriptográfia eszközök által kezelt szolgáltatói magánkulcs akkor deaktiválódik, ha az eszköz (szabályos vagy szabálytalan módon) kikerül az aktív állapotból. Ez az alábbi esetekben következik be:

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

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

5.2.10 A magánkulcs megsemmisítésének módja

A *Távoli kulcsmenedzsment szolgáltató* használatból kivont, lejárt érvényességű vagy kompromittálódott szolgáltatói magánkulcsait olyan módon semmisíti meg, amely lehetetlenné teszi a magánkulcs további használatát.

A *Távoli kulcsmenedzsment szolgáltató* a biztonságos *HSM eszköz*ében tárolt szolgáltatói magánkulcsok megsemmisítését a felhasznált *HSM eszköz* felhasználói útmutatójában és a tanúsítási dokumentumokban megfogalmazott eljárásoknak, követelményeknek megfelelően végzi a *Távoli kulcsmenedzsment szolgáltató* két munkatársának (egy infrastruktúra adminisztrátor és egy biztonsági tisztviselő) együttes jelenlétében más személyek jelenlétének kizárásával.

A *Távoli kulcsmenedzsment szolgáltató* dokumentált módon megsemmisíti a magánkulcsról készült minden mentett példányt olyan módon, hogy annak visszaállítása, használata lehetetlenné váljon.

5.2.11 A hardver kriptográfiai eszközök értékelése

A 5.2.1 fejezet előírásaival összhangban a *Távoli kulcsmenedzsment szolgáltató* az összes végfelhasználói magánkulcsot olyan *HSM eszköz*ben tárolja, amely rendelkezik:

- a CEN 419 241-1 [13] követelményeinek való megfelelést igazoló legalább EAL-4 szintű Common Criteria alapú eszköz tanúsítvánnyal, és szerepel az Európai Bizottság honlapján [1].

[1] European Commission eIDAS Dashboard
Qualified Signature/Seal Creation Devices and Secure Signature Creation Devices
`https://eidas.ec.europa.eu/efda/browse/notification/qscd-sscd`

5.3 A kulcspár kezelés egyéb szempontjai

5.3.1 A tanúsítványok és kulcspárok használatának periódusa

A *Tanúsítvány*ok és a magánkulcsok érvényességi idejét befolyásolhatja, ha a Nemzeti Média- és Hírközlési Hatóság új algoritmusokkal kapcsolatos határozatot ad ki, amely szerint a felhasznált kriptográfiai algoritmus vagy kulcsparaméter már nem biztonságos a kibocsátáskor tervezett felhasználási idő végéig.

Amennyiben ez bekövetkezik, a *Hitelesítés-szolgáltató* visszavonja az érintett *Tanúsítvány*okat. A visszavont *Tanúsítvány*okhoz tartozó magánkulcsokat a *Távoli kulcsmenedzsment szolgáltató* megsemmisíti.

5.4 Aktiváló adatok

5.4.1 Aktiváló adatok előállítása és telepítése

A *Távoli kulcsmenedzsment szolgáltató* a felhasznált *HSM eszköz* felhasználói útmutatójában és az eszköz tanúsítványban megfogalmazott eljárásoknak, követelményeknek megfelelő aktiváló módszereket alkalmaz szolgáltatói magánkulcsainak védelmére.

Jelszó alapú aktiváló adatok használata esetén a jelszavak kellően bonyolultak a megkívánt védelmi szint biztosítása érdekében.

5.4.2 Az aktiváló adatok védelme

A *Távoli kulcsmenedzsment szolgáltató* alkalmazottai a magánkulcsok aktiválásához szükséges eszközöket, aktiváló adatokat biztonságosan kezelik, műszaki és szervezési intézkedések segítségével védik, a jelszavakat csak kódolt formában tárolják.

5.4.3 Az aktiváló adatok kezelésének egyéb szempontjai

Nincs megkötés.

5.5 Informatikai biztonsági előírások

5.5.1 Speciális informatikai biztonsági műszaki követelmények

A *Távoli kulcsmenedzsment szolgáltató* informatikai rendszereinek konfigurálása és üzemeltetése során biztosítja az alábbi követelmények teljesülését:

- a rendszerhez vagy alkalmazáshoz való hozzáférés engedélyezése előtt a felhasználó azonosságát többfaktoros azonosítással ellenőrzi kártyán tárolt VPN tanúsítvány felhasználásával;
- a felhasználókhoz szerepköröket rendel és biztosítja, hogy minden felhasználó csak a szerepkörének megfelelő jogosultságokkal rendelkezzen;
- minden tranzakcióról naplóbejegyzést állít elő és a naplóbejegyzéseket archiválja;

- a biztonságkritikus folyamatok részére biztosítja, hogy a *Távoli kulcsmenedzsment szolgáltató* belső hálózati tartományai kellően védettek legyenek a jogosulatlan hozzáféréstől;
- megfelelő eljárásokat alkalmaz a kulcsvesztés vagy rendszerhiba után a szolgáltatás visszaállítása érdekében.

5.5.2 Az informatikai biztonság értékelése

A Microsec kiemelten fontosnak tartja *Ügyfel*ei elégedettségét. A magas színvonalú szolgáltatások fenntartása érdekében a Microsec az ISO 9001 szabványnak megfelelő minőségirányítási rendszert üzemeltet 2002. január 23. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

A Microsec nagy figyelmet fordít az általa üzemeltetett rendszerek biztonságára, ezért fő tevékenységi területein a ISO/IEC 27001-nek megfelelő információbiztonság-irányítási rendszert (korábban BS 7799) üzemeltet 2003. május 19. óta. A szabványnak való megfelelést a Lloyd's Register Quality Assurance tanúsította.

A minőségirányítási rendszer és az információbiztonság-irányítási rendszer hatóköre kiterjed a Microsec által nyújtott bizalmi szolgáltatásokra is.

A Microsec kétszintű kockázatelemzése az információ technológiai kockázatokon túlmenően kiterjed a teljes szervezetre és az üzleti kockázatokra is. A kockázatelemzés legalább évente felülvizsgálatra kerül. A kockázatelemzés eredménye alapján a *Távoli kulcsmenedzsment szolgáltató*

- intézkedéseket hoz a feltárt sérülékenységek megszüntetésére, és/vagy
- elfogadja az azonosított maradvány kockázatokat a döntés indokainak rögzítésével.

5.6 Életciklusra vonatkozó műszaki előírások

5.6.1 Rendszerfejlesztési előírások

A *Távoli kulcsmenedzsment szolgáltató* az éles szolgáltatást nyújtó informatikai rendszereiben csak olyan eszközöket, alkalmazásokat használ, amelyek:

- kereskedelmi dobozos szoftverek, amelyeket dokumentált tervezési módszertan szerint terveztek és fejlesztettek;
- a *Távoli kulcsmenedzsment szolgáltató* saját maga által kifejlesztett egyedi hardver és szoftver megoldások, amelyek tervezése során strukturált fejlesztési módszereket és ellenőrzött fejlesztési környezetet használt;
- a *Távoli kulcsmenedzsment szolgáltató* részére megbízható fél által kifejlesztett egyedi hardver és szoftver megoldások, amelyek tervezése során strukturált fejlesztési módszereket és ellenőrzött fejlesztési környezetet használtak;
- olyan nyílt forráskódú szoftverek, amelyek teljesítik a biztonsági követelményeket és amelyek megfelelőségét szoftver verifikáció, strukturált fejlesztés és életciklus menedzsment biztosítja.

Az informatikai eszközök beszerzése a hardver és szoftver komponensek módosítását kizáró módon történik, megbízható és rendszeresen minősített szállítók felhasználásával.

A *Távoli kulcsmenedzsment szolgáltató* a Távoli kulcsmenedzsment szolgáltatások nyújtásához használt kritikus informatikai eszközöket más célra nem használja.

A *Távoli kulcsmenedzsment szolgáltató* megfelelő védelmi intézkedésekkel megakadályozza, hogy kártékony szoftver kerülhessen a hitelesítés-szolgáltatás nyújtása körében használt eszközökbe.

A hardver és szoftver komponenseket az első használat előtt és azt követően rendszeresen ellenőrzi kártékony kódok után kutatva.

A *Távoli kulcsmenedzsment szolgáltató* a programfrissítések vásárlása vagy fejlesztése során ugyanolyan gondossággal jár el, mint az első verzió beszerzésekor.

A *Távoli kulcsmenedzsment szolgáltató* megbízható, megfelelően képzett személyzetet alkalmaz a szoftverek és eszközök telepítése során.

A *Távoli kulcsmenedzsment szolgáltató* csak a szolgáltatás nyújtásához szükséges szoftvereket telepíti a szolgáltatást nyújtó informatikai berendezéseire.

A *Távoli kulcsmenedzsment szolgáltató* rendelkezik változáskövető rendszerrel, amelyben az informatikai rendszer minden lényeges változtatása dokumentálásra kerül.

A *Távoli kulcsmenedzsment szolgáltató* a jogosulatlan változások észlelése érdekében automatikus monitorozó rendszert üzemeltet, amely rögzíti minden állomány változását és a figyelt állományok változása esetén naplóbejegyzést generál vagy figyelmeztető jelzést küld a rendszer üzemeltetőknek.

5.6.2 Biztonságkezelési előírások

A *Távoli kulcsmenedzsment szolgáltató* változáskövető rendszert használ a szolgáltatásban használt rendszerek telepítésének, konfigurációjának dokumentálására, üzemeltetésére, ellenőrzésére, monitorozására és karbantartására, beleértve a módosításokat és továbbfejlesztéseket is. A változáskövető rendszer alkalmas arra, hogy észleljen a rendszerben történt bármilyen jogosulatlan változtatást, adatbevitelt, amely érinti a szolgáltatásban használt rendszert, a tűzfalakat, routereket, programokat és egyéb komponenseket. A szolgáltatásban használt program telepítésekor a *Távoli kulcsmenedzsment szolgáltató* minden esetben meggyőződik arról, hogy a telepítendő program a megfelelő verziójú és mentes mindenféle jogosulatlan módosítástól. A *Távoli kulcsmenedzsment szolgáltató* rendszeresen ellenőrzi a szolgáltatói rendszereiben használt programok integritását.

A *Távoli kulcsmenedzsment szolgáltató* által alkalmazott valamennyi *HSM eszköz* ellenőrzésre, bevizsgálásra és értékelésre került. A *Távoli kulcsmenedzsment szolgáltató* ellenőrzi a modulok sértetlenségét:

- az eszközök beszerzését követően az átvétel során,
- a használatbavételt közvetlenül megelőzően,
- rendszeresen az üzemeltetés során.

A használatból véglegesen vagy időlegesen kivont *HSM eszköz*ből a *Távoli kulcsmenedzsment szolgáltató* törli a szolgáltatói kulcsokat.

A *Távoli kulcsmenedzsment szolgáltató* a használaton kívüli *HSM eszköz*öket fizikailag védett helyszínen tárolja.

5.6.3 Életciklusra vonatkozó biztonsági előírások

A *Távoli kulcsmenedzsment szolgáltató* gondoskodik a felhasznált *HSM eszköz*ök védelméről azok teljes életciklusa alatt.

A szolgáltatások nyújtásához használt informatikai eszközök, rendszerek üzemeltetése során a *Távoli kulcsmenedzsment szolgáltató* figyelembe veszi az eszközök életciklusára vonatkozó biztonsági szempontokat, melyek szerint:

- megfelelő tanúsítással rendelkező *HSM eszköz*öket használ rendszereiben;
- a *HSM eszköz*ök átvételekor a minőség ellenőrzése során meggyőződik róla, hogy a szállítás folyamán biztosították a *HSM eszköz*ök feltörés elleni védelmét;
- a *HSM eszköz*öket biztonságos helyen tárolja, a tárolás során biztosítja a *HSM eszköz*ök feltörés elleni védelmét;
- az üzemeltetés során folyamatosan betartja a *HSM eszköz*ök biztonsági előirányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeket;
- a használatból kivont *HSM eszköz*ökben tárolt magánkulcsokat olyan módon törli, hogy lehetetlené válik a kulcsok visszaállítása;
- a használatból kivont *HSM eszköz*öket a biztonsági előirányzatában, használati útmutatójában és a tanúsítási jelentésben szereplő követelményeknek megfelelően kezeli és semmisíti meg.

5.7 Hálózati biztonsági előírások

A *Távoli kulcsmenedzsment szolgáltató* a hálózati biztonság biztosítása érdekében követi a legjobb ipari gyakorlatot.

A *Távoli kulcsmenedzsment szolgáltató* szigorú ellenőrzés alatt tartja az alkalmazott IT rendszereinek konfigurációját, minden változást dokumentál, beleértve a legkisebb módosítást, fejlesztést, szoftverfrissítést is.

A *Távoli kulcsmenedzsment szolgáltató* megfelelő eljárásokat használ az IT rendszereiben bekövetkezett tetszőleges hardver vagy szoftver változás észlelésére, a rendszer telepítésére, karbantartására.

A *Távoli kulcsmenedzsment szolgáltató* minden szoftverkomponens első betöltésekor ellenőrzi a komponens eredetiségét, integritását.

A *Távoli kulcsmenedzsment szolgáltató* megfelelő hálózatbiztonsági intézkedéseket alkalmaz, mint például:

- IT rendszereit jól elválasztott biztonsági zónákra osztja;
- elkülöníti az IT rendszer üzemeltetését támogató rendszereit az éles szolgáltatást nyújtó rendszereitől;
- elkülöníti az éles szolgáltatást nyújtó rendszereit a fejlesztésre és tesztelésre szolgáló rendszerektől;

- az elkülönített megbízható rendszerek között csak olyan megbízható kommunikációs csatornákon keresztül létesít kapcsolatot, amelyek logikailag el vannak választva más kommunikációs csatornáktól, megbízható végponti azonosítást használnak és védik a csatornákon küldött adatokat a módosítástól és a felfedéstől;
- az éles szolgáltatást nyújtó IT rendszereit biztonságos hálózati zónában üzemelteti;
- a zónákhoz való hozzáférést és a zónák közötti kommunikációt csak a Távoli kulcsmenedzsment szolgáltatás nyújtásához szükségesre korlátozza;
- letiltja a nem használt protokollokat és felhasználókat;
- letiltja a használaton kívüli hálózati portokat és szolgáltatásokat;
- csak az IT rendszer megfelelő működéséhez feltétlenül szükséges hálózati alkalmazásokat futtat.
- a használt szabályrendszert rendszeresen felülvizsgálja.

A *Távoli kulcsmenedzsment szolgáltató* sérülékenységvizsgálatot végez vagy végeztet a *Távoli kulcsmenedzsment szolgáltató* nyilvános és privát IP címein:

- a CA/Browser Forum kérésétől számított egy héten belül;
- a *Távoli kulcsmenedzsment szolgáltató* által jelentősnek minősített rendszer vagy hálózati változtatás után;
- legalább minden három (3) hónapban.

A *Távoli kulcsmenedzsment szolgáltató* legalább 3 havonta ellenőrzi a helyi hálózati eszközök (pl. router) konfigurációjának megfelelőségét a *Távoli kulcsmenedzsment szolgáltató* által meghatározott követelményeknek.

A *Távoli kulcsmenedzsment szolgáltató* évente illetve az informatikai rendszerén történt minden jelentős változás után sebezhetőségvizsgálatot végeztet egy külső, független szakemberrel, aki rendelkezik az ilyen vizsgálat elvégzéséhez szükséges képességekkel, szakértelemmel, eszközökkel és etikai kódexekkel.

5.8 Időbélyegzés

A *Távoli kulcsmenedzsment szolgáltató* a naplóbejegyzések és egyéb archiválandó elektronikus állományok hitelesítésére az e-Szignó Hitelesítés Szolgáltató által kibocsátott minősített elektronikus *Időbélyegző*ket használja.

6 A megfelelőség vizsgálata

A *Távoli kulcsmenedzsment szolgáltató* rendszeres időközönként megvizsgáltatja működését külső független auditorral. Az audit során felülvizsgálatra kerül, hogy a *Távoli kulcsmenedzsment szolgáltató* működése megfelel-e az alábbi normatív dokumentumoknak:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];
- ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers [10]

A megfelelőségértékelési vizsgálat eredménye bizalmas dokumentum, csak az arra jogosultak számára hozzáférhető.

A megfelelőségértékelési jelentés alapján kiállított megfelelőségi tanúsítványt a *Távoli kulcsmenedzsment szolgáltató* honlapján közzéteszi.

A *Távoli kulcsmenedzsment szolgáltató* vizsgált és tanúsított elemeket (elektronikus aláírási termékeket, informatikai rendszerelemeket stb.) alkalmaz a szolgáltatásaihoz kapcsolódóan.

A *Távoli kulcsmenedzsment szolgáltató* a szolgáltatások nyújtásához használt valamennyi rendszerelemet biztonsági osztályokba sorolta kockázatmenedzsment rendszere alapján. Ezen rendszerelemekről és a hozzájuk tartozó biztonsági besorolásról a *Távoli kulcsmenedzsment szolgáltató* a kockázatmenedzsment rendszere keretében nyilvántartást vezet.

A *Távoli kulcsmenedzsment szolgáltató* a külső auditon túl saját belső ellenőrzési rendszerrel is rendelkezik, amely segítségével rendszeresen vizsgálja a korábbi auditoknak való megfelelőséget és eltérés esetén megteszi a szükséges lépéseket.

A *Távoli kulcsmenedzsment szolgáltató* 2002 óta rendelkezik az ISO 9001 szabványnak megfelelő minőségirányítási, valamint 2003 óta a ISO/IEC 27001-nek (korábban BS 7799-nek) megfelelő információbiztonság-irányítási rendszerrel, amelyeket külső auditáló szervezet (Lloyd's Register Quality Assurance) auditál és vizsgál felül folyamatosan (lásd: 1.3.1. fejezet) .

6.1 Az ellenőrzések körülményei és gyakorisága

A *Távoli kulcsmenedzsment szolgáltató* évente külső megfelelőségértékelési auditot hajt végre a Távoli kulcsmenedzsment szolgáltatások nyújtását végző informatikai rendszerén.

6.2 Az auditor és szükséges képesítése

A *Távoli kulcsmenedzsment szolgáltató* a belső auditokat a független rendszervizsgáló szerepkörrel felruházott alkalmazottai segítségével rendszeresen végzi.

Az eIDAS és ETSI követelményeknek való megfelelőséget igazoló vizsgálatot olyan szervezet végzi el, amely rendelkezik egy EU tagállam nemzeti akkreditációs szervezete által kiadott erre feljogosító felhatalmazással.

6.3 Az auditor és az auditált rendszerelem függetlensége

A külső auditot olyan személy végzi:

- aki független a vizsgált *Távoli kulcsmenedzsment szolgáltató* tulajdonosi körétől, vezetőségétől és üzemeltetésétől;
- aki független a vizsgált szervezettől, vagyis sem saját maga, sem közvetlen hozzátartozója nincs munkaviszonyban vagy üzleti kapcsolatban a *Távoli kulcsmenedzsment szolgáltató*val;

- akinek díjazása nem függ az audit során végzett tevékenységének megállapításaitól.

6.4 Az auditálás által lefedett területek

Az átvizsgálás lefedi az alábbi területeket:

- hatályos jogszabályoknak való megfelelés;
- műszaki szabványoknak való megfelelés;
- *Bizalmi szolgáltatási rend*(ek)nek és *Távoli kulcsmenedzsment szolgáltatási szabályzat*(ok)nak való megfelelés;
- az alkalmazott folyamatok megfelelősége;
- a dokumentálás;
- a fizikai biztonság;
- a személyi állomány megfelelősége;
- az IT biztonság;
- az adatvédelmi szabályok betartása.

6.5 A hiányosságok kezelése

A független auditor az átvizsgálás eredményét egy részletes átvilágítási jelentésben foglalja össze, amely kitér a vizsgált rendszerelemekre, folyamatokra, tartalmazza az átvilágítás során felhasznált bizonyítékokat és vizsgálói megállapításokat. A jelentésben külön fejezetben rögzíti a vizsgálat során feltárt eltéréseket és az elhárításukra kitűzött határidőket.

A független auditor a vizsgálat során feltárt eltérések, hiányosságok súlyossága alapján a jelentésben rögzíthet:

- opcionálisan figyelembe vehető módosítási javaslatokat;
- kötelezően elhárítandó eltéréseket.

6.6 Az eredmények közzététele

A *Távoli kulcsmenedzsment szolgáltató* a vizsgálat eredményét összefoglaló jelentést nyilvánosságra hozza honlapján az alábbi linken:

`https://e-szigno.hu/eidas/`

A feltárt hiányosságok részleteit nem publikálja, azokat bizalmas információként kezeli.

7 Egyéb üzleti és jogi kérdések

7.1 Díjak

A szolgáltatási díjakat és árakat a *Távoli kulcsmenedzsment szolgáltató* a honlapján közzéteszi és kérelemre ügyfélszolgálati irodájában is biztosítja olvashatóságát.

Az árlista elérhetősége:

- `https://e-szigno.hu/arlista`

A *Távoli kulcsmenedzsment szolgáltató* az árlistát egyoldalúan módosíthatja. Az árlista módosítását a hatálybalépése előtt 30 nappal a *Távoli kulcsmenedzsment szolgáltató* a honlapján közzéteszi.

Az *Ügyfél* számára kedvező változások a 30 naposnál rövidebb határidővel is bevezethetők.

Az előre kifizetett Távoli kulcsmenedzsment szolgáltatások árát a módosítás nem érinti.

A díjak kifizetésével és visszatérítésével kapcsolatos rendelkezéseket a Szolgáltatási szerződés és mellékletei – különösen az Általános Szerződési Feltételek – tartalmazzák.

7.1.1 Visszatérítési politika

Lásd: 7.1. fejezet.

7.2 Anyagi felelősségvállalás

A *Távoli kulcsmenedzsment szolgáltató* megbízhatósága érdekében anyagi felelősséget vállal a jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat*ban, a vonatkozó *Bizalmi szolgáltatási rend*ben valamint az *Ügyfél*lel kötött Szolgáltatási szerződésben megfogalmazott valamennyi rá vonatkozó kötelezettség maradéktalan betartásáért.

7.2.1 Pénzügyi követelmények

A *Távoli kulcsmenedzsment szolgáltató* rendelkezik a szolgáltatások nyújtásával valamint a megszűnésével kapcsolatos költségek biztosításához szükséges anyagi erőforrásokkal.

7.2.2 Felelősségbiztosítás

- A *Távoli kulcsmenedzsment szolgáltató* a megbízhatóság biztosítása érdekében felelősségbiztosítással rendelkezik.
- A felelősségbiztosítási szerződés kiterjed az alábbi, a *Távoli kulcsmenedzsment szolgáltató* által a szolgáltatások nyújtásával összefüggésben okozott károkra:
  - a bizalmi szolgáltatási *Ügyfél*nek a Szolgáltatási szerződés megszegésével összefüggésben okozott károkra;
  - a bizalmi szolgáltatási *Ügyfél*nek és harmadik személynek szerződésen kívüli okozott károkra;

  - a Nemzeti Média- és Hírközlési Hatóságnak a bizalmi szolgáltatási tevékenységet befejező *Távoli kulcsmenedzsment szolgáltató* által okozott költségekre;
  - az eIDAS Rendelet [1] 17. cikk (4) bekezdés e) pontja alapján a Nemzeti Média- és Hírközlési Hatóság által felkért megfelelőségértékelő szervek eljárásának költségeire, ha azt a Nemzeti Média- és Hírközlési Hatóság eljárási költségként érvényesíti.

- A biztosítási szerződésben szereplő felelősségvállalási érték káreseményenként legalább 3.000.000 forint. Több azonos okból bekövetkezett, időben összefüggő káresemény egy biztosítási eseménynek minősül.

- A felelősségbiztosítás a meghatározott összeg erejéig fedezetet nyújt a károsultnak a szolgáltató károkozó magatartásával összefüggésben keletkező teljes kárára, függetlenül attól, hogy a kárt szerződésszegéssel vagy szerződésen kívül okozták.

- Ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

7.3 Bizalmasság

A *Távoli kulcsmenedzsment szolgáltató* az *Ügyfel*ek adatait a jogszabályoknak megfelelően kezeli. A *Távoli kulcsmenedzsment szolgáltató* rendelkezik adatkezelési szabályzattal (lásd 7.4 fejezet), amely a személyes adatok kezelésével kiemelten foglalkozik.

Az *Ügyfél* a Szolgáltatási szerződés aláírásával hozzájárul ahhoz, hogy a személyes adatait a *Távoli kulcsmenedzsment szolgáltató* (az adatkezelési szabályzatnak megfelelő módon) tárolja és kezelje. A hozzájárulás vonatkozik a törvény által meghatározott és nyilvántartásba vett információk harmadik félhez történő továbbítására a *Távoli kulcsmenedzsment szolgáltató* szolgáltatásainak leállítása esetén, valamint – kizárólag a szolgáltatással összefüggő feladatok elvégzése céljából – a *Távoli kulcsmenedzsment szolgáltató* alvállalkozóinak való továbbításra.

A *Távoli kulcsmenedzsment szolgáltató* az *Ügyfel*ek adatait kizárólag a szolgáltatásaival összefüggésben használja fel.

A *Távoli kulcsmenedzsment szolgáltató* a tudomására jutott adatokat a jogszabályi követelményeknek megfelelően, az előírt időtartamig megőrzi. A *Távoli kulcsmenedzsment szolgáltató* az adatok megőrzése során gondoskodik az információk sértetlenségéről, bizalmasságáról és biztonságos tárolásáról. Az információkhoz való hozzáférést csak azon személyeknek engedélyezi, akik feladata azt indokolja.

A *Távoli kulcsmenedzsment szolgáltató* az *Ügyfel*ek adatainak továbbítása során gondoskodik a nem nyilvános információk bizalmasságáról és sértetlenségéről.

7.3.1 Bizalmas információk köre

A *Távoli kulcsmenedzsment szolgáltató* bizalmas információként kezeli:

- az *Ügyfel*ek minden adatát, kivéve azokat, amelyeket a 7.3.2. fejezetben nem bizalmasnak tekintett információnak minősít;

- az *Ügyfel*ek adatain kívül:
  - a tranzakciós és naplóadatokat;
  - a nem nyilvános szabályzatokat;
  - minden olyan adatot, amelynek nyilvánosságra hozatala a szolgáltatás biztonságát előnytelenül befolyásolná.

7.3.2 Bizalmas információk körén kívül eső adatok

A *Távoli kulcsmenedzsment szolgáltató* nyilvánosnak tekint miden olyan adatot, amely nyilvánosan elérhető forrásból beszerezhető, vagy amely nyilvánosságra hozatalához az *Előfizető* előzetesen írásban hozzájárult.

7.3.3 Bizalmas információ védelme

A *Távoli kulcsmenedzsment szolgáltató* felelősséggel tartozik az általa kezelt bizalmas adatok védelméért.

A *Távoli kulcsmenedzsment szolgáltató* szerződésben vagy titoktartási nyilatkozat aláírásával kötelezi alkalmazottait, alvállalkozóit, szerződött partnereit a bizalmas adatok védelmére.

A *Távoli kulcsmenedzsment szolgáltató* a birtokába jutott bizalmas adatokat az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [4] rendelkezéseinek megfelelően kezeli, és kizárólag az alábbi esetben fedi fel azokat:

- **Információszolgáltatás a hatóságok részére**

  A *Távoli kulcsmenedzsment szolgáltató* az Eüt. [6] 90. § (1) bekezdésének megfelelően az általa nyújtott bizalmi szolgáltatások felhasználásával elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdekből – az adatigénylésre külön törvényben meghatározott feltételek teljesülése esetén – a nyomozó hatóságnak és a nemzetbiztonsági szolgálatoknak díjmentesen továbbítja az érintett személyazonosságát igazoló, valamint a *Távoli kulcsmenedzsment szolgáltató* által egyeztetett adatokat.

  A *Távoli kulcsmenedzsment szolgáltató* rögzíti az adatátadás tényét, de arról nem tájékoztatja az érintett *Ügyfel*eket.

- **A tulajdonos kérésére történő felfedés**

  A *Távoli kulcsmenedzsment szolgáltató* az *Ügyfél* személyes kérése vagy az általa hivatalosan, írásban adott felhatalmazása alapján tárja fel a rá vonatkozó bizalmas felhasználói információkat harmadik fél részére.

7.4 Személyes adatok védelme

A *Távoli kulcsmenedzsment szolgáltató* gondoskodik az általa kezelt személyes adatok védelméről, működése és szabályzatai megfelelnek az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény [4] és a 2016/679 EU általános adatvédelmi rendelet [2] rendelkezéseinek.

A *Távoli kulcsmenedzsment szolgáltató* az *Ügyfél*ről nyilvántartott személyes adatokat és információkat a jogszabályi előírásoknak megfelelően

- megőrzi,
- azokat a megőrzési kötelezettség lejártával – amennyiben az *Ügyfél* erről másképpen nem rendelkezik – az ügyfél adatbázisból törli.

A *Távoli kulcsmenedzsment szolgáltató* nyilvántartásában azonosító adatokat, az *Előfizető*ről kizárólag a szolgáltatás igénybevételéhez, valamint a szerződéskötéshez és a számlázáshoz szükséges információkat tárolja.

A *Távoli kulcsmenedzsment szolgáltató* kizárólag olyan esetben adja át harmadik félnek az *Ügyfél* adatait, ha ezt jogszabály előírja vagy ha az *Ügyfél* ebbe írásban beleegyezett.

7.4.1 Adatkezelési terv

A *Távoli kulcsmenedzsment szolgáltató* rendelkezik Adatvédelmi Szabályzattal és Adatkezelési Tájékoztatóval, amelyek részletes előírásokat tartalmaznak a személyes adatok kezelésére.

Az Adatvédelmi Szabályzat megtalálható az e-Szignó Hitelesítés Szolgáltató honlapján az alábbi linken:

`https://e-szigno.hu/minden-dokumentum.html`

Az Adatkezelési Tájékoztató megtalálható az e-Szignó Hitelesítés Szolgáltató honlapján az alábbi linken:

`https://e-szigno.hu/adatkezelesi-tajekoztato.html`

7.4.2 Személyes adatok

A *Távoli kulcsmenedzsment szolgáltató* védi az érintettel kapcsolatba hozható, vagy az érintettre vonatkozó következtetést tartalmazó minden olyan személyes adatot, amely nem érhető el nyilvános adatforrásból.

A *Távoli kulcsmenedzsment szolgáltató* csak az *Előfizető*től közvetlenül, vagy annak egyértelmű előzetes hozzájárulásával gyűjt személyes adatokat és csak olyan mértékben, ami a Távoli kulcsmenedzsment szolgáltatás nyújtásához szükséges.

7.4.3 Személyes adatnak nem minősülő adatok

A *Távoli kulcsmenedzsment szolgáltató* nem köteles bizalmasként kezelni az olyan személyes adatot, amely nyilvános adatforrásból elérhető.

7.4.4 Személyes adatok védelme

A *Távoli kulcsmenedzsment szolgáltató* biztonságosan tárolja és védi az általa kezelt személyes adatokat. Az adatokat megfelelő intézkedésekkel védi különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, valamint nyilvánosságra hozatal ellen.

A *Távoli kulcsmenedzsment szolgáltató* általánosan felelős az Adatkezelési szabályzatában leírtak betartásáért, felelőssége kiterjed az alvállalkozói által végzett tevékenységekre is.

7.4.5 Személyes adatok felhasználása

A *Távoli kulcsmenedzsment szolgáltató* csak a Távoli kulcsmenedzsment szolgáltatás nyújtásához megkívánt mértékben, az *Ügyfél*lel való kapcsolattartás érdekében használja fel az *Ügyfél* személyes adatait.

7.4.6 Adatkezelés

A *Távoli kulcsmenedzsment szolgáltató* az *Ügyfél* értesítése nélkül is kiadhatja az *Ügyfél*ről tárolt személyes adatokat a vonatkozó jogszabályok által meghatározott esetekben.

7.4.7 Egyéb adatvédelmi követelmények

Nincs előírás.

7.5 Szellemi tulajdonjogok

A *Távoli kulcsmenedzsment szolgáltató* működése során nem sértheti meg harmadik személy szellemi tulajdonjogait.

A jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* a *Távoli kulcsmenedzsment szolgáltató* kizárólagos tulajdonát képezi. Az *Ügyfel*ek és egyéb *Érintett felek* a dokumentumot csak a jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* előírásainak megfelelően jogosultak felhasználni, minden egyéb kereskedelmi vagy egyéb célú felhasználás szigorúan tilos.

A jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* szabadon terjeszthető, de csak változatlan formában, teljes terjedelemben és az eredet feltüntetésével.

A *Távoli kulcsmenedzsment szolgáltató* által a Távoli kulcsmenedzsment szolgáltatás igénybevételéhez biztosított szoftverek használatának szabályait a szoftver leírásában vagy magában a szoftverben elérhető illetve ott meghivatkozott helyen található felhasználói útmutató tartalmazza.

7.6 Tevékenységért viselt felelősség és helytállás

7.6.1 A szolgáltató felelőssége és helytállása

A Szolgáltató felelőssége

A *Távoli kulcsmenedzsment szolgáltató* felelősségét jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat*, a vonatkozó *Bizalmi szolgáltatási rend*, valamint az *Ügyfél*lel kötött Szolgáltatási szerződés és annak mellékletei tartalmazzák, melyek szerint:

- a *Távoli kulcsmenedzsment szolgáltató* felelősséget vállal az általa támogatott *Bizalmi szolgáltatási rend*(ek)ben leírt eljárásoknak való megfelelésért;
- a *Távoli kulcsmenedzsment szolgáltató* sajátjaként felel az alvállalkozói által a Távoli kulcsmenedzsment szolgáltatás nyújtása során okozott károkért;

- a *Távoli kulcsmenedzsment szolgáltató* a vele szerződéses jogviszonyban álló *Ügyfel*ekkel szemben a Polgári Törvénykönyv [5] a szerződésszegésért való felelősség szabályai szerint felelős;
- a *Távoli kulcsmenedzsment szolgáltató* a vele szerződéses jogviszonyban nem álló harmadik személlyel (ilyen az *Érintett fél*) szemben a Polgári Törvénykönyv [5] általános felelősségi szabálya szerint felelős;
- a *Távoli kulcsmenedzsment szolgáltató* a felelősségi körén belül keletkezett, bizonyított károkért a szabályzataiban és az *Ügyfél*lel megkötött Szolgáltatási szerződésekben rögzített korlátozásokkal kártérítést fizet (lásd: Pénzügyi felelősség korlátozása 7.8. fejezet);
- ha egy biztosítási eseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra biztosítási eseményenként a felelősségbiztosítási szerződésben meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a felelősségbiztosítási szerződésben meghatározott összeghez viszonyított arányában történik.

A *Távoli kulcsmenedzsment szolgáltató* nem felelős:

- az *Érintett felek* tanúsítvány ellenőrzési és felhasználási tevékenységeiért,
- az *Érintett felek* vagy mások által kibocsátott szabályzatokért.

A Szolgáltató kötelezettsége

A *Távoli kulcsmenedzsment szolgáltató* alapvető kötelezettsége, hogy a Távoli kulcsmenedzsment szolgáltatást a *Bizalmi szolgáltatási rend*del, a *Távoli kulcsmenedzsment szolgáltatási szabályzat*tal, az Általános Szerződési Feltételekkel, továbbá a vállalati és biztonsági belső szabályzatokkal összhangban nyújtsa. Ezen alapvető kötelezettségek a következők:

- a szolgáltatásnak megfelelő jogi-, szabályozási-, anyagi-, szerződéses stb. keretek megteremtése;
- magas színvonalú és biztonságos szolgáltatások nyújtása a vonatkozó szabályzatok szerint;
- a szolgáltatásokhoz kapcsolódó szervezetek (ügyfélszolgálat stb.) folyamatos működtetése és ellenőrzése;
- a szabályzatokban előírt eljárások betartása és az esetleg bekövetkező helytelen működés elkerülése, illetve megszüntetése;
- a szolgáltatások biztosítása minden olyan igénylő számára, aki elfogadja a szabályzatokban rögzített feltételeket;
- a publikus nyilvántartások és saját szabályzatok karbantartása és folyamatos elérhetővé tétele bárki számára az interneten keresztül.

7.6.2 Az Ügyfél felelőssége és helytállása

Az *Előfizető* felelőssége

Az *Előfizető* felelősségét a Szolgáltatási szerződés és annak mellékletei (köztük az Általános szerződési feltételek) határozzák meg.

Az *Előfizető* kötelezettségei

Az *Előfizető* köteles a *Távoli kulcsmenedzsment szolgáltató* szerződéses feltételeinek és szabályzatainak megfelelően eljárni a Távoli kulcsmenedzsment szolgáltatás igénybevétele során.

Az *Előfizető* kötelezettségeit a jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat*, a Szolgáltatási szerződés és annak elválaszthatatlan részét képező Általános Szerződési Feltételek, valamint a vonatkozó *Bizalmi szolgáltatási rend* tartalmazzák.

Az *Előfizető* jogai

Az *Előfizető* jogosult:

- a szolgáltatások igénybevételére a jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat*ban leírtak szerint;

7.6.3 Az Érintett fél felelőssége

Az *Érintett felek* saját belátásuk és/vagy szabályzataik alapján dönthetnek az egyes *Tanúsítvány*ok és *Időbélyegző*k elfogadásáról és a felhasználás módjáról. Az érvényesség vizsgálata során a *Távoli kulcsmenedzsment szolgáltató* által garantált biztonsági szint megtartásához szükséges, hogy az *Érintett fél* megfelelő körültekintéssel járjon el, ezért különös tekintettel javasolt:

- a *Bizalmi szolgáltatási rend*ben és a *Távoli kulcsmenedzsment szolgáltatási szabályzat*ban megfogalmazott követelmények, előírások betartása;
- megbízható informatikai környezet és alkalmazások használata;
- valamennyi *Tanúsítvány* visszavonási állapotának ellenőrzése az aktuális CRL vagy OCSP válasz alapján;
- valamennyi korlátozás figyelembevétele, amely a a *Távoli kulcsmenedzsment szolgáltatási szabályzat*ban és a vonatkozó *Bizalmi szolgáltatási rend*ben szerepel.

7.6.4 Egyéb szereplők tevékenységéért viselt felelősség és helytállás

Nincs megkötés.

7.7 Helytállás érvénytelenségi köre

A *Távoli kulcsmenedzsment szolgáltató* kizárja felelősségét, amennyiben:

- az *Ügyfel*ek nem tartják be a magánkulcs és az aktiváló adat kezelésével kapcsolatos előírásokat;
- az *Ügyfel*ek nem érik el a Távoli kulcsmenedzsment szolgáltatást a *Távoli kulcsmenedzsment szolgáltató* hibáján kívül fakadó okból;
- az Internet, vagy annak egy részének működési hibájából adódóan a tájékoztatás és egyéb kommunikációs kötelezettségeit nem tudja ellátni;
- a károkozás a Nemzeti Média- és Hírközlési Hatóság algoritmusokkal kapcsolatos határozat által elfogadott kriptográfiai algoritmusok hibájából, illetve gyengeségeiből ered.

7.8 A felelősség korlátozása

A *Távoli kulcsmenedzsment szolgáltató* korlátozza a szolgáltatással kapcsolatos kártérítési kötelezettségét, ezen korlátozás mértéke káreseményenként 100.000,-Ft.

Ha egy káreseménnyel kapcsolatban több jogosult megalapozott kártérítési igénye meghaladja a károkra káreseményenként a fenti korlátozás szerint meghatározott összeget, akkor a kártérítési igények megtérítése az összes kártérítési igénynek a korlátozás szerint meghatározott összeghez viszonyított arányában történik.

7.9 Kártérítési kötelezettség

7.9.1 A szolgáltató kártérítési kötelezettsége

A *Távoli kulcsmenedzsment szolgáltató* kártérítési kötelezettségének részletes szabályait jelen szabályzat (lásd: 7.8. fejezet), a Szolgáltatási szerződés és az *Ügyfel*ekkel kötött szerződések tartalmazzák.

7.9.2 Az előfizető kártérítési kötelezettsége

Az *Előfizető* kártérítési felelősséggel tartozik a *Távoli kulcsmenedzsment szolgáltató*nak azokért a veszteségekért és károkért, amelyeket kötelezettségei és a rá vonatkozó ajánlások be nem tartásával okoz számára.

7.9.3 Az érintett felek kártérítési kötelezettsége

Lásd: 7.8. fejezet

7.10 Érvényesség és megszűnés

7.10.1 Érvényesség

A *Távoli kulcsmenedzsment szolgáltatási szabályzat* adott verziója hatálybalépésének napja a dokumentum címlapján kerül meghatározásra.

7.10.2 Megszűnés

A *Távoli kulcsmenedzsment szolgáltatási szabályzat* visszavonásig – illetve a *Távoli kulcsmenedzsment szolgáltatási szabályzat* újabb verziójának hatályba lépéséig – hatályos időbeli korlátozás nélkül.

7.10.3 A megszűnés következményei

A *Távoli kulcsmenedzsment szolgáltatási szabályzat* visszavonása esetén a *Távoli kulcsmenedzsment szolgáltató* honlapján közzéteszi a visszavonás részletes szabályait és a visszavonás után is fennálló jogokat és kötelezettségeket.

A *Távoli kulcsmenedzsment szolgáltató* garantálja, hogy a *Távoli kulcsmenedzsment szolgáltatási szabályzat* visszavonása esetén is érvényben maradnak a bizalmas adatok védelmére vonatkozó előírások.

7.11 A felek közötti kommunikáció

A *Távoli kulcsmenedzsment szolgáltató* az *Ügyfel*ekkel történő kapcsolattartás érdekében ügyfélszolgálati irodát működtet.

Az *Ügyfel*ek jognyilatkozataikat a *Távoli kulcsmenedzsment szolgáltató* felé kizárólag írásban, aláírt módon tehetik meg. Szervezet képviseletében történő aláírás csak a képviseleti jogosultság igazolásával együtt érvényes.

Az e-Szignó Hitelesítés Szolgáltató elektronikus levélben tájékoztatja *Ügyfel*eit vagy tájékoztatását honlapján teszi közzé.

7.12 Módosítások

A *Távoli kulcsmenedzsment szolgáltató* fenntartja magának a jogot, hogy a normatív szabályok, biztonsági követelmények, piaci környezet vagy egyéb körülmények változása esetén szabályozott módon megváltoztassa a *Távoli kulcsmenedzsment szolgáltatási szabályzat*ot.

7.12.1 Módosítási eljárás

A *Távoli kulcsmenedzsment szolgáltató* nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatások biztonságát nem veszélyezteti. A *Távoli kulcsmenedzsment szolgáltató* több belső biztonsági és egyéb szabályzattal, operatív szintű előírással rendelkezik, melyeket bizalmasan kezel (jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* több ilyet is megemlít). A 6.4. fejezetben leírt eljárások ezeket a dokumentumokat is vizsgálják.

A *Távoli kulcsmenedzsment szolgáltató* szervezetén belül működik egy olyan szervezeti egység, amely felelős a szabályzatok és dokumentációk karbantartásáért. A változtatási igényeket e csoport gyűjti, a módosításokat elvégzi, a belső és külső tájékoztatási kötelezettségeknek eleget tesz. A szabályzatot az e-Szignó Hitelesítés Szolgáltató igazgatója hagyja jóvá.

A változtatásokat gyűjtve a csoport belső, nem nyilvános munkaváltozatokat hoz létre a szabályzatokból, melyek a közzététel előtt belső felülvizsgálaton esnek át. A *Távoli kulcsmenedzsment szolgáltató* törekszik arra, hogy új szabályzatot csak a lehető legritkábban kelljen kibocsátania.

A *Távoli kulcsmenedzsment szolgáltató* évi rendszerességgel illetve rendkívüli változtatási igény esetén soron kívül átvizsgálja a *Távoli kulcsmenedzsment szolgáltatási szabályzat*ot és elvégzi a szükségesnek tartott változtatásokat. A dokumentum a legkisebb változtatás után – illetve az éves rendszeres átvizsgálás esetén változtatás hiányában is – új verziószámot kap, és az elfogadási procedúra időigényét figyelembe véve meghatározásra kerül a tervezett hatálybalépés időpontja.

A *Távoli kulcsmenedzsment szolgáltató* a jóváhagyott dokumentumot a tervezett hatálybalépés előtt publikálja honlapján.

7.12.2 Értesítések módja és határideje

A *Távoli kulcsmenedzsment szolgáltató* a 7.12.1. pontban leírtak szerint értesíti az *Érintett felek*et az új dokumentum verziók kibocsátásáról.

7.12.3 Az OID megváltoztatása

A *Távoli kulcsmenedzsment szolgáltató* a *Távoli kulcsmenedzsment szolgáltatási szabályzat* legkisebb változtatása esetén is az új verziót új verziószámmal adja ki, amelyben a változás mértékétől függően vagy a főverziószám, vagy az alverziószám megváltozik.

Az 1.x és 2.x verziókban a *Távoli kulcsmenedzsment szolgáltatási szabályzat* verziószáma megjelent a dokumentum azonosító OID végén lévő 2 tagban, így két eltérő tartalmú – hatályba léptetett – *Távoli kulcsmenedzsment szolgáltatási szabályzat*nak nem lehetett azonos OID azonosítója.

A 3.1 verziószámú *Távoli kulcsmenedzsment szolgáltatási szabályzat*tól kezdődően a verziószám nem jelenik meg az OID végén, így a *Távoli kulcsmenedzsment szolgáltatási szabályzat* OID azonosítója azonos érték minden kiadott verzióban. Az egyes *Távoli kulcsmenedzsment szolgáltatási szabályzat*ok azonosítása a dokumentum OID és a verziószám együttes használatával lehetséges.

7.13 Vitás kérdések rendezése

A *Távoli kulcsmenedzsment szolgáltató* törekszik a működése során felmerülő vitás kérdések békés, tárgyalásos rendezésére. A rendezés során a fokozatosság elvét követi.

A *Távoli kulcsmenedzsment szolgáltató* és az *Ügyfél* kölcsönösen megállapodnak abban, hogy bármilyen vitás kérdés vagy panasz felmerülése esetén, a vita jogi útra való terelése előtt megkísérlik a békés úton, tárgyalással történő egyeztetést. A kezdeményező fél kötelessége, hogy minden érintett többi felet haladéktalanul értesítsen és teljes körűen tájékoztasson az ügy minden vonatkozását illetően.

Az *Ügyfél* vitás kérdés felmerülése esetén jogosult az esetleges bírósági eljárást megelőzően a Budapesti Békéltető Testülethez fordulni.

A *Távoli kulcsmenedzsment szolgáltató* tevékenységével kapcsolatos kérdéseket, kifogásokat és panaszokat az ügyfélszolgálati iroda címére kell eljuttatni írásos formában. A bejelentés kézhezvételétől számított 3 munkanapon belül a *Távoli kulcsmenedzsment szolgáltató* értesíti a bejelentő felet az általa megadott címen a bejelentés fogadásáról és a kivizsgáláshoz szükséges időről. A megjelölt határidőig a *Távoli kulcsmenedzsment szolgáltató* köteles írásban válaszolni a bejelentőnek. A *Távoli kulcsmenedzsment szolgáltató* a válaszadáshoz szükséges információk

megadását kérheti a bejelentőtől. A *Távoli kulcsmenedzsment szolgáltató* a panaszt 30 napon belül kivizsgálja, és az eredményekről értesíti a bejelentőt.

Amennyiben a választ a bejelentő nem tartja kielégítőnek, vagy az alapján nem sikerül a *Távoli kulcsmenedzsment szolgáltató* bevonása nélkül rendezni a felmerült vitát, akkor a bejelentő egyeztetést kezdeményezhet a *Távoli kulcsmenedzsment szolgáltató*val és az *Érintett felek*kel. Az egyeztetés minden résztvevőjét írásban értesíteni kell az egyeztetés időpontjáról azt megelőzően 10 munkanappal, és írásban meg kell számukra küldeni a bejelentést, a *Távoli kulcsmenedzsment szolgáltató* válaszát és egyéb szükséges információkat tartalmazó dokumentumokat.

Amennyiben az egyeztetés a panasz benyújtásától számított 30 napon belül nem vezet eredményre, akkor a bejelentő peres útra terelheti az ügyet. Az *Érintett felek* kölcsönösen alávetik magukat a Budapesti II. és III. Kerületi Bíróság, illetve a Fővárosi Törvényszék kizárólagos illetékességének.

7.14 Irányadó jog

A *Távoli kulcsmenedzsment szolgáltató* tevékenységét a mindenkor hatályos magyar jogszabályoknak megfelelően végzi. A *Távoli kulcsmenedzsment szolgáltató* szerződéseire és szabályzataira, azok teljesítésére a magyar jog az irányadó, s azok a magyar jog szerint értelmezendők.

7.15 Az érvényben lévő jogszabályoknak való megfelelés

A vonatkozó jogszabályok:

- AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről [1];
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról [4];
- 2013. évi V. törvény a Polgári Törvénykönyvről [5].
- 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól [6];
- 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről [7];
- 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről [8];
- 470/2017. (XII. 28.) Kormányrendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről [9];

7.16 Vegyes rendelkezések

7.16.1 Teljességi záradék

Nincs megkötés.

7.16.2 Átruházás

A jelen *Távoli kulcsmenedzsment szolgáltatási szabályzat* alapján nyújtott szolgáltatásokba bevont alvállalkozók vagy egyéb együttműködő partnerek csak a *Távoli kulcsmenedzsment szolgáltató* előzetes írásbeli engedélyével adhatják tovább jogosultságaikat és delegálhatják kötelezettségeiket harmadik félnek.

7.16.3 Részleges érvénytelenség

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

7.16.4 Igényérvényesítés

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

7.16.5 Vis maior

A *Távoli kulcsmenedzsment szolgáltató* nem felelős a *Bizalmi szolgáltatási rend*ben és a *Távoli kulcsmenedzsment szolgáltatási szabályzat*ban megfogalmazott kötelezettség hibás vagy késedelmes teljesítéséért, illetve nem teljesítéséért, amennyiben a hiba vagy késedelem oka a *Távoli kulcsmenedzsment szolgáltató* ellenőrzési körén kívül eső, előre nem látható elháríthatatlan külső ok.

7.17 Egyéb rendelkezések

Nincs megkötés.

A Hivatkozások

[1] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 910/2014/EU RENDELETE (2014. július 23.) a belső piacon történő elektronikus tranzakciókhoz kapcsolódó elektronikus azonosításról és bizalmi szolgáltatásokról, valamint az 1999/93/EK irányelv hatályon kívül helyezéséről .

[2] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) 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 (általános adatvédelmi rendelet) .

[3] 2001. évi XXXV. törvény az elektronikus aláírásról (hatályon kívül helyezve 2016. július 1-től) .

[4] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról .

[5] 2013. évi V. törvény a Polgári Törvénykönyvről .

[6] 2015. évi CCXXII. törvény az elektronikus ügyintézés és a bizalmi szolgáltatások általános szabályairól .

[7] 24/2016. (VI. 30.) BM rendelet a bizalmi szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről .

[8] 25/2016. (VI. 30.) BM rendelet a bizalmi felügyeletnek fizetendő igazgatási szolgáltatási díjak mértékéről .

[9] 470/2017. (XII. 28.) Korm. rendelet a bizalmi felügyelet által vezetett nyilvántartások tartalmáról és a bizalmi szolgáltatás nyújtásával kapcsolatos bejelentésekről .

[10] ETSI EN 319 401 V2.3.1 (2021-05); Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

[11] ETSI TS 119 312 V1.4.3 (2023-08); Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

[12] ETSI TS 119 431-1 V1.2.1 (2021-05) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service providers; Part 1: TSP service components operating a remote QSCD / SCDev.

[13] CEN EN 419 241-1:2018 (July 2018); Trustworthy Systems Supporting Server Signing - Part 1: General System Security Requirements.

[14] IETF RFC 3647: Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework, November 2003.

[15] FIPS PUB 140-2 (2001 May 25): Security Requirements for Cryptographic Modules.

[16] NIST Special Publication 800-56A Revision 3 (April 2018): Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography.

[17] e-Szignó Hitelesítés Szolgáltató - Általános Szerződési Feltételek .