Az Educatio Társadalmi Szolgáltató Közhasznú Társaság

Szolgáltatási szabályzat fokozott biztonságú, nem minősített elektronikus aláíráshoz kapcsolódó szolgáltatásokhoz

v 2.3

OID: 1.3.6.1.4.1.27537.1.2.2.3

Hatálybalépés dátuma: 2009. január 20.

Időpont	**Jóváhagyta**	**Aláírás**
2008.dec.18.	Kerekes Gábor ügyvezető	

Időpont	**Készítette**	**Aláírás**
2008.dec.10.	Dr. Polyák Edit, Matolcsi Zoltán Tóth Elemér	

Változáskövetés

Időpont	**Referencia**	**Tartalom**
2007.aug. 6.	Tóth Elemér	v1.0: alapverzió; a független szakértők véleménye alapján több pontosítás történt, a részleteket egy külön dokumentum tartalmazza
2007.aug. 27.	Tóth Elemér	v1.1: a független szakértők véleménye alapján több pontosítás történt, a részleteket egy külön dokumentum tartalmazza
2007.aug. 29.	Tóth Elemér	v1.2 az adatkezelési és adatvédelmi szabályzat szerepeltetése; UserNotice módosítása
2007.aug. 30.	Kiszler Ferenc	v1.3: az NHH által átvett dokumentumverzió
2007. szept.25	Tóth Elemér	v1.4: az NHH észrevételei alapján módosított verzió
2007. okt. .16.	Polyák Edit, Tóth Elemér	v1.41: az NHH észrevételei alapján módosított verzió
2007. okt. .19.	Tóth Elemér	v2.0: Educatio Kht. HR megszüntetése
2007.dec. 10.	Tóth Elemér	v2.1: az NHH észrevételei alapján módosított verzió a független szakértőkkel egyeztetett változat az NHH-val egyeztetett változat
2008. márc.10	Tóth Elemér	v2.2: elérhetőségi adatok változásának átvezetése, 3.2.3.1 pontban megadott határidő megváltoztatása; MÁV Informatika Kft. átalakulás után Zrt.
2008.dec.10.	Tóth Elemér	v2.3: LDAP kivétele; OCSP szolgáltatás bevezetése; átléptetés kivétele

Tartalom

1. Bevezetés

Az Educatio Társadalmi Szolgáltató Közhasznú Társaság (továbbiakban: Educatio Kht., vagy Szolgáltató) célként fogalmazta meg, hogy az általa biztosított hitelesítés szolgáltatás biztosítsa azt, hogy:

- egyrészről az Oktatási és Kulturális Minisztérium, a közoktatásról szóló 1993. évi LXXIX. tv-ben (Közoktatási törvény) meghatározott általános iskolák és középfokú oktatási intézmények vezetői, továbbá a képviselettel meghatalmazott helyettesítő személyek, másrészről az Educatio Kht. közötti, a közoktatásról szóló törvény végrehajtásáról szóló 20/1997 (II. 13.) Kormányrendeletben megadott kommunikációban is,

- továbbá egyrészről a felsőoktatásról szóló 2005. évi CXXXIX. tv-ben (Felsőoktatási törvény) meghatározott felsőoktatási intézmények vezetői, valamint ezen személyek képviselettel meghatalmazottjai, másrészről az Educatio Kht. közötti, a felsőoktatási törvényben és a felsőoktatási törvény egyes rendelkezéseinek végrehajtásáról szóló 79/2006 (IV.5.) Kormányrendeletben meghatározott kommunikációban is

alkalmazható legyen.

A Szolgáltató a fentieken felül szerződést köt más igénybe vevőkkel is.

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény értelmében, a jelen Szolgáltatási Szabályzat mint Hitelesítés Szolgáltatási Szabályzat (továbbiakban: HSZSZ) alapján nyújtott hitelesítés szolgáltatás, nyilvános, fokozott biztonságú aláíráshoz kapcsolódó, nem minősített szolgáltatásnak minősül.

A Szolgáltató ügyfeleinek chipkártyát biztosít az elektronikus aláíráshoz. Jelen dokumentum tartalmazza chipkártyán (mint aláírás-létrehozó eszközön) az elektronikus aláíráshoz szükséges kriptográfiai kulcs (aláírás-létrehozó adat elhelyezéséhez) kapcsolódó szabályokat is.

Jelen Szolgáltatási Szabályzat teljesíti a Hitelesítés Szolgáltatási Szabályzatokkal szemben támasztott elvárásokat, ennek körében rögzíti a közigazgatási célra felhasználható, nem minősített, aláíró tanúsítványokra vonatkozó általános szabályokat, a következő pontban megadott hitelesítési rendek szerint.

1.1 Alkalmazott hitelesítési rendek

A szabályzat az alábbi hitelesítési rendek elvárásait teljesíti :

- a „Közigazgatási, ügyfélhez kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend”, azonosítója: „[EHR+_Ü], OID: 0.2.216.1.100.42.101.3.2.1”

- a „Közigazgatási, köztisztviselőhöz kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend”, azonosítója: „[EHR+_K], OID: 0.2.216.1.100.42.101.4.2.1”

Ez a szabályzat nyilvánosan hozzáférhető az Educatio Kht. honlapján.

1.1.1 A Szabályzat

A Szolgáltatási Szabályzat a szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó dokumentum.

A Szolgáltatási Szabályzat célja, hogy összefogja azokat a szabályzatokat és információkat, melyeket a Szolgáltatóval valamilyen módon kapcsolatba kerülő feleknek érdemes tudni. Mint ilyen, biztosítja a Szolgáltató működésének átláthatóságát, s lehetővé teszi az igénybevevők (felhasználók) számára, hogy megállapítsák a Szolgáltató által kialakított szolgáltatási rendszer megfelelőségét.

A Szolgáltatási Szabályzat alapján a Hitelesítés Szolgáltatás által kibocsátott tanúsítványok elfogadóinak egyértelműen meg kell tudni állapítani a tanúsítványok kezelésének módját, az általuk garantált biztonság mértékét, és az erre vonatkozó technikai, üzleti és pénzügyi garanciákat, jogi felelősségvállalásokat.

A tanúsítványok végfelhasználóinak tevékenységére vonatkozóan jelen szabályzattól független egyéb, az Educatio Kht-ban hatályos belső szolgáltatói szabályzatok is élhetnek előírásokkal. Amennyiben e szabályzatok bármely vonatkozásban ellentmondással vagy eltérő kikötéssel élnének, jelen szolgáltatási szabályzat előírásai tekintendők magasabb szintűnek, s ezek alkalmazandóak.

Jelen Szolgáltatási Szabályzat az áttekinthetőség érdekében követi az európai szabványosítás keretében kidolgozott, az 1.8 pont alatti [6]-ban definiált specifikációt. Ugyanakkor számos helyen eltér attól, tovább pontosítja, illetve konkretizálja a követelményeket, az egységes és biztonságos felhasználhatóság, valamint a hazai jogszabályi előírásoknak való megfelelőség érdekében.

1.1.2 A Szabályzat hatálya

Csak az Educatio Kht. ügyvezetőjének az aláírásával ellátott Szolgáltatási Szabályzat változata tekinthető hitelesnek.

Tárgyi hatály:	A tárgyi hatály az 1.1.4 fejezetben ismertetett szolgáltatások nyújtását és igénybevételét foglalja magában.
Időbeli hatály:	Az időbeli hatály a fedőlapon feltüntetett jelen szabályzati verzióra érvényes hatálybalépés dátumától kezdődően határozatlan időre szól (hatálya megszűnik a szolgáltatási tevékenység beszüntetésekor, illetve egy újabb szabályzat verzió hatályba lépésékor).
Személyi hatály:	A személyi hatály a PKI szereplők közösségének (lásd. 1.3 pont), az érintett felek (aláírás ellenőrzők) kivételével minden tagjára, jogi és természetes személyekre egyaránt kiterjed.
NHH nyilvántartásba vételi azonosító:	HL-3218-1/2008 ügyiratszámú határozat

1. táblázat

1.1.3 A Hitelesítés Szolgáltató

Jelen szabályzat alapján az Educatio Kht. és a vele kapcsolatban álló alvállalkozók együttesen nyújtják az elektronikus aláíráshoz kapcsolódó hitelesítés szolgáltatásokat. A Hitelesítés Szolgáltatót jogi és üzleti értelemben az Educatio Kht. képviseli. A szervezet elérhetőségi adatai a 1.5.1 pontban találhatók.

Az Educatio Kht-t a felsőoktatási felvételi rendszer fejlesztése és üzemeltetése, a felsőoktatási felvételi eljárás lebonyolítása és a felsőoktatási felvételihez kapcsolódó tájékoztatási feladatok ellátása céljából alapította az Oktatási Minisztérium 2000-ben.

Az Oktatási Minisztérium döntésének eredményeképpen – a Minisztériummal kötött közhasznú szerződés módosításai alapján – a Társaság feladatai az Országos Felsőoktatási Felvételi Iroda (jelenlegi nevén Országos Felsőoktatási Információs Központ - OFIK) működtetése mellett 2001-ben kibővültek a SuliNET Programiroda és a győri Közoktatási Információs Iroda (KII), 2002-ben a Hallgatói Információs Központ (HIK), majd 2003-tól a Diákigazolvány Ügyfélszolgálat (jelenlegi nevén Oktatási Kártyaközpont) működtetésével.

A közoktatási intézménytörzset az Educatio Kht. keretein belül működő győri Közoktatási Információs Iroda kezeli. Ebben szerepelnek az intézményi egyedi azonosítók, illetve az elhelyezkedéssel, feladat-ellátással, telephelyekkel stb. kapcsolatos adatok. Az adatok megtekintése és a módosítások bejelentése Internetes felületen az Educatio Kht. portáljain

keresztül is lehetséges.

Az Oktatási Minisztérium (OM) a felsőoktatási felvételi rendszer kialakítása, üzemeltetése, és fejlesztése érdekében hozta létre az OFIK elődjét, az Országos Felsőoktatási Felvételi Irodát (OFI) 1985-ben. A felsőoktatási felvételi eljárás lebonyolítása és a felsőoktatási felvételi tájékoztatás jelentős - országosan egyedülálló - informatikai hátteret igényel. Az ügyintézés lelkét, az OFIK-ban kialakított központi adatbázisok és programok jelentik, ezekhez a felsőoktatási intézmények kliens-programokkal kapcsolódnak. Ez a rendszer teszi lehetővé a tömeges mennyiségű adat és információ tárolását, kezelését.

A Diákigazolvány Ügyfélszolgálatot azzal a céllal hozták létre, hogy gondoskodjon a diákigazolvány-igénylések feldolgozásáról és a diákigazolványok előállításáról. Az igénylők tájékoztatása érdekében az Ügyfélszolgálat külön call-centert üzemeltet, ahol minden érdeklődő személyre szabottan is választ kaphat kérdéseire.

Az Educatio Kht. által 2006-ban létrehozott zártkörű, fokozott biztonságú hitelesítés szolgáltatás során az Educatio Kht.

- a Közoktatási törvényben meghatározott általános iskolák és középfokú oktatási intézmények vezetői, továbbá a képviselettel meghatalmazott helyettesítő személyek, másrészről az Educatio Kht. közötti szerződéses viszony szerint, valamint

- a Felsőoktatási törvényben meghatározott felsőoktatási intézmények vezetői, valamint ezen személyek képviselettel meghatalmazottjai, másrészről az Educatio Kht. közötti szerződéses viszony szerint

biztosít szolgáltatásokat. A zártkörű szolgáltatás hitelesítési rendje, a hitelesítés szolgáltatási szabályzat, és az általános szerződéses feltételek megtalálhatók az Educatio Kht. nyilvános web-lapján (http://www.educatio.hu/).

1.1.4 Szolgáltatások és tevékenységek

A Szolgáltató az elektronikus aláírással kapcsolatos szolgáltatások keretében az alábbi tevékenységeket, illetve szolgáltatásokat végzi:

az elektronikus aláírás hitelesítés szolgáltatás keretében

- kezdeti regisztrálás és személyazonosság megállapítása,
- tanúsítványkérelem feldolgozása,
- tanúsítvány kibocsátás szolgáltatás,
- tanúsítvány elfogadás,
- tanúsítvány megújítás és módosítás szolgáltatás,
- tanúsítvány visszavonás és felfüggesztés szolgáltatás,
- tanúsítvány állapot szolgáltatás,
- tanúsítványarchiválás,
- kulcsmenedzsment,
- egyedi névképzés,
- adattárolás,
- viszontazonosítás.

aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatás során

- regisztrálás és személyazonosság megállapítása,
- aláírás-létrehozó eszköz kibocsátás,
- kulcsmenedzsment,
- kulcsgenerálás az aláírás-létrehozó eszközön,
- a kulcshoz tartozó tanúsítvány elhelyezése az aláírás-létrehozó eszközön,
- adattárolás.

1.1.5 Szabványok és előírások

A jelen Szolgáltatási Szabályzat (melynek a HSZSZ a meghatározó része), az EU elvárásai, illetve a X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány politika és szolgáltatási szabályzat keretrendszer ajánlás [6] figyelembe vételével készült. A HSZSZ az áttekinthetőség érdekében az RFC 3647 ajánlásban [6] megadott struktúrát követi, tartalmilag azonban egyes esetekben eltérhet az ajánlástól.

A HSZSZ megfelel az elektronikus aláírásról szóló 2001. évi XXXV. törvény [1] (továbbiakban: Eat.) vonatkozó előírásainak és ajánlásainak.

A HSZSZ megfelel – a közigazgatásban alkalmazható tanúsítványt kibocsátók számára kiadott – az 1.1 pontban megnevezett hitelesítési rendekben előírtaknak.

1.1.6 Tanúsítványfajták

A Hitelesítés Szolgáltató az alábbi tanúsítványfajtákat bocsátja ki:

S.	Megnevezés	Tranzakciós limit	Korlátozás
1.	Személyes (végfelhasználói) tanúsítvány	0 Ft	Nem használható pénzügyi tranzakciókban!
2.	Szervezeti képviseletre alkalmas, személyes (végfelhasználói) tanúsítvány	0 Ft	Nem használható pénzügyi tranzakciókban!
3.	Szolgáltatói tanúsítvány (végfelhasználói és eszköz tanúsítványok)	0 Ft	A Szolgáltató saját maga számára kibocsátott tanúsítvány.

2. táblázat

Hitelesítés Szolgáltató az egyes tanúsítványok profiljait külön dokumentumban [8] rögzítette. Írásban benyújtott kérelem elfogadása esetén az érdeklődők, ezt a dokumentumot

megtekinthetik. A kérelmet a Szolgáltató 1.5.1 pontban megadott címére, a hitelesítés szolgáltatásért általánosan felelős vezetőnek szólóan kell küldeni.

1.1.7 Aláírás-létrehozó eszköz szolgáltatás

A Szolgáltató az ügyfelei és saját munkatársai számára aláírás-létrehozó eszközön (kriptográfiai hardver eszközön; ú.n. chipkártyán) aláírás-létrehozó adat elhelyezése szolgáltatást végez. Ez a chipkártya megfelelő biztonsági garanciát nyújtó nemzetközi tanúsítvánnyal rendelkezik, a chipkártya által megvalósított kriptográfiai algoritmusok és paramétereik megfelelnek a magyar szabályozásnak is [20], ezzel együtt a nemzetközi elvárásoknak is[1].

Ezen szolgáltatás során a Szolgáltató:

a) megszemélyesíti a chipkártyát, amely során vizuálisan megszemélyesíti a kártyát, elhelyezi a chipmodulon az elektronikus aláírás alkalmazást, beállítja a biztonságos működéshez szükséges kulcsokat, az aktivizáló adatot (PIN-t) és más adatokat, elkészíti a zárt PIN-borítékot

b) az átadásra felkészített kártyát és PIN-borítékot az ügyfélhez történő átadásig biztonságosan tárolja és szállítja

c) az aláírás-létrehozó adat (kriptográfiai magánkulcs) az ügyfél közreműködésével jön létre a chipmodulban, amely során az ügyfél a PIN-boríték felhasználásával megadja a chipmodult védő PIN-kódot a Szolgáltató által rendelkezésére bocsátott szoftvernek, mire az utasítást ad a chipmodul számára, hogy az az aláírás létrehozó adatot megfelelően védett körülmények között hozza létre

A PIN-kód megváltoztatása az ügyfél részéről a műveletet megelőzően is, és azt követően az ügyfél által biztonságos körülmények között is biztosított. A Szolgáltató gondoskodik arról, hogy a rendszerében és az átadás során ne kerüljenek letárolásra a chipkártyához tartozó kulcsok és aktivizáló adatok, a munkafolyamatokban gondoskodik arról, hogy az abban dolgozó munkatársak se ismerhessék meg ezeket a kulcsokat és aktivizáló adatokat.

A chipmodul biztosítja az aláírás létrehozó adat titkosságát és sértetlenségét.

1.1.7.1 Chipkártya paraméterek

A Szolgáltató által jelenleg alkalmazott chipkártya az Axalto Cyberflex 64K típusú terméke. Ennek alkalmazási jellemzőit (paramétereit) mutatja be az alábbi táblázat.

[1] Magyarországon az Eat. [1] a Nemzeti Hírközlési Hatóságot jelöli ki arra, hogy határozatba foglalja, és érvényesítse a szolgáltatók által szolgáltatásaik nyújtása során használható biztonságos kriptográfiai algoritmusokat és az azok meghatározott paraméterekkel történő alkalmazására vonatkozó követelményeket.

Paraméter megnevezése	Érték	Megjegyzés
Kártya címke:	Educatio.cm1.typecard	
A kártya technológiája	Java card	Több alkalmazásra is megfelel
Initial PIN	nincs	az alkalmazott technológia alapján nem szükséges
User PIN és Unblock PIN	igen, mindkettő	PIN és PUK megadása
GINA	nem	Microsoft szolgáltatás
Aláíró kulcsok száma	3	
Aláíró kulcsok mérete	1024 bit, illetve 2048 bit a FIR-hez kiadott kártyáknál	
Titkos terület mérete	10 000 byte	
Nyilvános terület mérete	20 000 byte	
Crypto API	engedélyezett, illetve a FIR-hez kiadott kártyáknál nem engedélyezett	Microsoft szolgáltatás
PKCS#11	nem engedélyezett, illetve a FIR-hez kiadott kártyáknál engedélyezett	egyéb szolgáltatás
Protected Mode	igen	
Generate Key on Card	igen	A regisztráció során keletkezik a kulcs.
PIN hossz legalább	6	
PIN hossz legfeljebb	12	
Ismételhető karakterek	2	
PIN próbálkozások száma	3	hibás megadások száma
PIN váltás	engedélyezett	ügyfél lecseréli
PIN history	nincs	adható többször is ugyanaz a PIN
Hibát követő feloldás	engedélyezett Unblock PIN-nel	PIN boríték tartalmazza
Megadható PIN karakterek	alfanumerikus és nem alfanumerikus is	kisbetű, nagybetű, szám és jel
Unblock PIN hossz legalább	8	PUK érték
Unblock PIN hossz legfeljebb	12	PUK érték
Unblock PIN próbálkozások száma	10	PUK érték! Ezt követően a kártya hozzáférhetetlen lesz!

Unblock PIN váltás	engedélyezett	ügyfél lecserélheti
Unblock PIN history	1	az előzőtől eltérőt fogad el!

3. táblázat

A Szolgáltató belső szabályzatai alapján más chipkártyákat is alkalmazhat. Ezek megnevezését és alkalmazási jellemzőit a Szolgáltató honlapján nyilvánossá teszi.

1.2 A dokumentum neve és azonosítója

A jelen dokumentumban meghatározott Szolgáltatási Szabályzat neve és azonosítói az alábbiak:

Megnevezés: Szolgáltatási szabályzat fokozott biztonságú, nem minősített elektronikus aláíráshoz kapcsolódó szolgáltatásokhoz

Azonosító: EDUCAHSZSZ-2

OID: 1.3.6.1.4.1.27537.1.2

1.3 PKI szereplők

A kibocsátott tanúsítványok és aláírás-létrehozó eszközök alkalmazó közössége, a Szolgáltató, a tanúsítványok végfelhasználói (a Hitelesítés Szolgáltató ügyfelei) és az érintett felek.

1.3.1 Hitelesítés szolgáltató

A Hitelesítés Szolgáltató tanúsítvány kibocsátó szervezetet (CA-t) működtet, melynek feladata a tanúsítványok központi létrehozása, kibocsátása és menedzsmentje, a regisztrációs egységtől (RA), és/vagy a Hitelesítés Szolgáltató általános felelős vezetőjétől kapott kérelmeknek, továbbá a szabályozásnak megfelelően.

A Hitelesítés Szolgáltató megfelel a jelen dokumentumban megnevezett hitelesítési rendeknek, és a magyar Közigazgatási Gyökér Hitelesítés-Szolgáltató (ld. 1.3.5 pontban) által felülhitelesített hitelesítés szolgáltatást biztosít.

Hitelesítés Szolgáltató szervezete a szabályzatok menedzsmentjével kapcsolatos feladatokat is ellátja.

1.3.2 Regisztráló szervezet

Hitelesítés Szolgáltató – saját szervezetén belül, valamint partnerein keresztül – regisztrációs egységet (RA) hozott létre. Az RA a Hitelesítés Szolgáltató általános felelős vezetőjének felügyelete mellett, a szabályozás alapján, az alábbi feladatokat látja el:

- kezdeti regisztráció: amely az ügyfelek igénylésének az átvételéből és az átvett adatok ellenőrzéséből tevődik össze; ezen feladatokat
    - o a közoktatási intézményi igénylők esetében az Educatio Kht. Közoktatási Információs Irodája (KII) látja el, az igénylők a KII http://www.kir.hu honlapján keresztül közlik igényeiket;
    - o a felsőoktatási intézmény igénylők esetében az Educatio Kht. Országos Felsőoktatási Információs Központja látja el, az igénylők a http://www.felvi.hu/ honlapon jelentik be igényüket;
    - o további igényeket az Educatio Kht. Ügyfélszolgálatához eljuttatott levélben lehet megadni, ld. kapcsolati pont az 1.5.2 szerint

- a személyazonosítást, az aláíró eszköz, valamint az aktivizáló adat (PIN) átadását, az aláírás létrehozó adat és aláírás ellenőrző adat generálásának felügyeletét, a tanúsítvány lekérését a hitelesítő egységtől (CA), és a tanúsítvány elhelyezését az aláíró eszközön, valamint a biztonságos környezet helyi menedzselését egy külső regisztrációt végző munkatárs (XRO) látja el az ügyfélnél; a Szolgáltató telephelyén ezeket a feladatokat biztonságos körülmények között a regisztrációs munkatárs (RO) látja el

- a tanúsítvány kibocsátásával kapcsolatos egyéb feladatok elvégzését a Hitelesítés Szolgáltató, tanúsítvány-adminisztrációs (cert admin) szerepkörben dolgozó munkatársai a kijelölt biztonsági felelős és PKI szakértő munkatársakkal együttműködve biztosítják,

- a további tanúsítványmenedzsment feladatok ellátása során a felhasználókkal történő kapcsolattartást a Hitelesítés Szolgáltató tartozó Ügyfélszolgálat munkatársai (DÜ) látják el.

b) A regisztrálók (XRO, RO) feladata a regisztrációhoz és visszavonáshoz kapcsolódó ügyféltájékoztatási teendők ellátása, illetve az XRO-k felelősek a tanúsítványtár elérésének infokommunikációs biztosításáért és a tanúsítványállapotok ellenőrzés ügyfél oldali beállításáért is (az ügyfél számítógépének alkalmassá tételéért, hogy az elektronikus aláírásra használható legyen).

A nyilvántartásba vételi feladatokat, továbbá a nyilvántartáshoz kapcsolódó szükséges ellenőrzéseket az RO végzi.

A regisztrációs munkatársak a feladataikat, jelen szabályzat előírásainak és a szolgáltató belső szabályozásának megfelelően végzik.

1.3.3 Előfizetők és aláírók (végfelhasználók)

Az előfizetők a jelen szabályzat 1.6 pontjában meghatározott személyek, azzal a kitétellel, hogy a közigazgatási alanyok esetén az előfizetők: közigazgatási szervek, illetve más alanyok esetén előfizetők lehetnek az ügyfelek által képviselet szervezetek is.

Jelen szabályzatban az aláírók (végfelhasználók) csoportjai, akik/amelyek speciális igényeit és kötelezettségeit a Szolgáltató figyelembe veszi, a jelen szabályzat szerint kiszolgálja:

- a magyar elektronikus közigazgatás szolgáltatásait igénybe vevő ügyfelek, akik a magyar elektronikus közigazgatási rendszerben elektronikus ügyintézést kívánnak lebonyolítani,

- a magyar közigazgatás köztisztviselői, akik a magyar elektronikus közigazgatási rendszerben egymással, illetve az ügyfelekkel kommunikálnak a rendszer keretén belül,

- azok, akik az Educatio Kht. informatikai rendszereivel, jogszabályi feltételek alapján kommunikálnak,

- egyéb alanyok.

1.3.4 Érintett felek (aláírás ellenőrzők)

A jelen szabályzat vonatkozásában az érintett fél (aláírás ellenőrző) a Hitelesítés Szolgáltató által kibocsátott tanúsítvány megfelelőségét és érvényességét ellenőrzi a Hitelesítés Szolgáltató nyilvántartásai, valamint a Szolgáltató által kibocsátott szabályzatok szerint.

A közigazgatási felhasználás tekintetében érintett fél minden olyan felhasználó a közigazgatási bizalmi tartományon belül és kívül, aki a magyar közigazgatási nyilvános kulcsú infrastruktúrában kibocsátott tanúsítványokat ellenőrzi, alkalmazza.

1.3.5 Egyéb szereplők: Közigazgatási Gyökér Hitelesítés-szolgáltató

A Közigazgatási Gyökér Hitelesítés-Szolgáltató (KGyHSz) a magyar közigazgatásban használható tanúsítványokat kibocsátó hitelesítés-szolgáltatók szolgáltatói tanúsítványát felülhitelesítő szervezet.

A KGyHSz a tanúsítvány kiadásával igazolja, hogy a hitelesítés szolgáltató és a tanúsítvány adatainak egyezését, valamint hogy a megfelelő Hitelesítési rend és Szolgáltatási Szabályzat előírásainak megfelelőségét ellenőrizte, illetve a felültanúsított hitelesítés szolgáltató a tanúsítvány elfogadásával magára nézve kötelezőnek ismeri el a KGyHSz által kiadott szabályzatokat és a KGyHSz felügyeleti, ellenőrzési jogát.

1.4 Tanúsítvány használat

A Hitelesítés Szolgáltató az 1.1 pontban megadott hitelesítési rendeknek megfelelően bocsát ki tanúsítványokat.

Az 1.1 pontban megadott, alább felsorolt hitelesítési rendek megfelelnek a közigazgatási felhasználásra vonatkozó követelményeknek:

- az ügyfél által használt aláíráshoz kapcsolódó Hitelesítési rendek között – az 1.8 pontban megadott [9], és

- a hivatali aláíráshoz kapcsolódó Hitelesítési rendek között – az 1.8 pontban megadott [9a].

Ezek a hitelesítési rendek szerepelnek a Nemzeti Hírközlési Hatóság (NHH) Hivatala hatósági nyilvántartásában.

1.4.1 Tiltott tanúsítvány használat

A tanúsítványt csak az arra jogosítottak, és csak a tanúsítványhoz tartozó hitelesítési rendben ([9], [9a] hivatkozással) meghatározott célra használhatják. A tanúsítvány minden más célú használata tiltott.

1.4.1.1 Közlemény (User Notice)

A tanúsítványok az alábbi közleményeket tartalmazzák (ld. Certificate Policies kiterjesztés):

- közigazgatási ügyfél esetén: „A tanúsítvány közigazgatási ügyfél számára készült, értelmezése az Educatio Kht. által alkalmazott hitelesítési rend (HR) és HSZSZ szerint. A KGYHSZ felelőssége kizárva a saját HR-je szerint.”

- köztisztviselő esetén: „A tanúsítvány tulajdonosa köztisztviselő, értelmezése az Educatio Kht. által alkalmazott hitelesítési rend (HR) és HSZSZ szerint. A KGYHSZ felelőssége kizárva a saját HR-je szerint.”

1.5 Kapcsolattartás

1.5.1 A Szolgáltató adatai

A szervezet adatai	
Szervezet neve:	**EDUCATIO Társadalmi Szolgáltató Közhasznú Társaság**
Szervezet címe:	1134 Budapest, Váci út 37.
Cégjegyzékszám:	01-14-000308
Telefonszám:	+36(1)477-3100
Faxszám:	+36(1)477-3136
Email cím:	pkica@edukht.hu
Honlap:	http://www.educatio.hu/

4. táblázat

1.5.2 Ügyfélkapcsolat

A biztosított szolgáltatásokkal és szerződéskötéssel kapcsolatban, valamint a szerződések teljesítésével, a szerződési problémákkal, továbbá a tanúsítványok felfüggesztésével és visszavonással kapcsolatos eljárásokban (ld. 4.9 pontban) az ügyfél a Szolgáltató Ügyfélszolgálatához fordulhat, az alábbi táblázatban megadott elérhetőségeken.

Az ügyfélszolgálat adatai	
Neve:	**Ügyfélszolgálat**
Cím:	1134 Budapest, Váci út 37. 133. szoba
Telefonszám:	+36(1) 266-7733
Faxszám:	+36(1) 477-3196
Email cím:	pkica@edukht.hu
Honlap:	http://www.educatio.hu/

5. táblázat

Szolgáltató a fent jelzett telefonszámokon, munkanapokon 8 és 16 óra között érhető el.

A tanúsítványok felfüggesztésével és visszavonási kéréssel kapcsolatban, amikor az Ügyfélszolgálat nem elérhető (munkaidőben, vagy azon túl, pihenő- és ünnepnapokon), az ügyfél a Szolgáltató alábbi szerződéses partnerének 24-órás Help Desk csoportjához fordulhat.

Az ügyfélszolgálat adatai	
Neve:	MÁV Informatika Zrt. Help Desk
Telefonszám:	+36(80) 39 93 93

6. táblázat

Szolgáltató webes információs rendszere, a http://www.educatio.hu folyamatosan információkat nyújt a szolgáltatásokról, e-mail-ben pedig minden nap 0-24 óráig fogadják a bejelentéseket, beleértve az esetleges panaszokat is.

Szolgáltató a bejelentésre legkésőbb a következő munkanapon reagál, válasz e-mail, illetve postai cím vagy faxszám birtokában küldi meg a válaszát. Amennyiben a válasz tartalmilag nem teljes (kivizsgálási igény merül fel), a komplett válasz várható elkészültének idejét a Szolgáltató megadja. A válasz megküldésének az ideje legfeljebb 30 nap lehet.

1.5.3 Az illetékes fogyasztóvédelmi felügyelőség

Nemzeti Fogyasztóvédelmi Hatóság Közép-magyarországi Regionális Felügyelősége, Fogyasztókapcsolati Iroda,

1088 Budapest, József krt. 6., Levélcím: 1364. Budapest, Pf. 270.,

telefon: + 36 1 459 4999, +36 1 459 4836, Ingyenes zöldszám: +36 80 201 205

telefax: + 36 1 303-9075

1.5.4 A jelen szabályzat megfelelőségéért felelős személy/szervezet

a) Az Educatio Kht. ügyvezetője általánosan felelős a jelen szabályzatban foglaltak megfelelőségéért és teljesítéséért.

b) A Hitelesítés Szolgáltatásért általánosan felelős vezető (ld. 5.2.1 pontban) felelős a szolgáltatási szabályzat jelen dokumentumban meghatározott hitelesítési rendeknek történő megfelelőségéért és az ezekben foglaltak szerinti szolgáltatás nyújtásáért.

1.5.5 A Szolgáltatási szabályzat elfogadási eljárása

a) A jelen szabályzatot, a Hitelesítés Szolgáltatásért általánosan felelős vezető (ld. 5.2.1 pontban) felelős javaslata alapján az Educatio Kht. ügyvezetője hagyja jóvá.

1.5.6 Önkéntes akkreditációs rendszer

A Szolgáltató nem alkalmaz önkéntes akkreditációs rendszert.

1.6 Meghatározások

Alany	A hitelesítés-szolgáltató által kiadott tanúsítványban azonosított természetes személy, aki a tanúsítványban szereplő aláírás-ellenőrző adatnak (nyilvános kulcsnak) megfelelő aláírás-létrehozó adatot (kriptográfiai magánkulcsot) birtokolja, vagy szervezet, amely a szerver tanúsítványában szereplő aláírás-ellenőrző adatnak (nyilvános kulcsnak) megfelelő aláírás-létrehozó adatot (kriptográfiai magánkulcsot) birtokolja.

Aláíró	Az a természetes személy, aki az aláírás-létrehozó eszközt, ezen az aláírás-létrehozó adatot birtokolja és a saját vagy más személy nevében aláírásra jogosult.
Bizalmi közösség	Azokat a PKI szereplőket, akik, illetve amelyek elfogadják és alkalmazzák a Szolgáltatási szabályzatban, és a kapcsolódó hitelesítési rendben rögzített meghatározásokat, leírásokat és feltételeket, valamint korlátozásokat, egy Bizalmi közösségbe tartozónak tekintjük.
Elektronikus aláírás	Elektronikusan aláírt elektronikus dokumentumhoz azonosítás céljából logikailag hozzárendelt vagy azzal elválaszthatatlanul összekapcsolt elektronikus adat.
Előfizető	A hitelesítés-szolgáltatónál egy vagy több aláíró nevében előfizető természetes, vagy jogi személy, vagy jogi személyiség nélküli szervezet, aki közvetlenül vagy közvetve elfogadja a hitelesítés-szolgáltató kikötéseit és feltételeit, valamint a szolgáltatás díjának megfizetésére köteles.
Entitás	Személyek, szervezetek és eszközök (általában, de nem kizárólagosan: szerverek).
Érintett fél	Az érintett fél az az entitás, aki az aláírás ellenőrzése során, a Szolgáltató által kibocsátott tanúsítványon alapuló nyilvános kulcsú technikára (elektronikus aláírásra) hagyatkozva jár el.
Hitelesítési rend	Olyan szabálygyűjtemény, mely egy tanúsítvány felhasználhatóságát határozza meg egy közös biztonsági követelményekkel rendelkező közösség és/vagy alkalmazások egy osztálya számára.
Hitelesítés szolgáltató (HSz)	A tanúsítványba foglalt nyilvános kulcs és a tulajdonos azonosító adatainak hiteles összekapcsolásáért felelős, a kommunikációban résztvevő felek mindegyike által hitelesnek tartott szervezet.
Időbélyegzés	Az a folyamat, melynek során az elektronikus dokumentumhoz olyan igazolás rendelődik, amely tartalmazza a bélyegzés hiteles időpontját, és amely a dokumentumhoz oly módon kapcsolódik, hogy minden - az igazolás kiadását követő - módosítás érzékelhető.
Igénylő	Az a személy, aki a tanúsítvány alanya képviseletében, számára tanúsítvány kiadását kérelmezi, és elfogadja a hitelesítés-szolgáltató

	kikötéseit és feltételeit.
Magánkulcs	A 2001. évi XXXV. törvény szerinti „aláírás-létrehozó adat” egyik elterjedt megnevezése. Kriptográfiai kulcs, „privát kulcsnak” is nevezik. jelen dokumentumban a „magánkulcs” jelenik meg.
Nyilvános kulcs	A 2001. évi XXXV. törvény szerinti „aláírás-ellenőrző adat” egyik elterjedt megnevezése. Kriptográfiai kulcs, „publikus kulcsnak” is nevezik. Jelen dokumentumban a „nyilvános kulcs” jelenik meg.
Nyilvános kulcsú infrastruktúra (PKI)	A tanúsítványok és kulcsok kezelését biztosító jogszabályok, irányelvek, eljárások, szervezetek, hardver- és szoftvereszközök összessége.
Szervezeti, személyes (végfelhasználói) tanúsítvány	Olyan tanúsítvány, amely az aláíró személy szervezeti hovatartozásának megjelölését is tartalmazza. Szükséges, hogy az adott szervezet – a jogszabályi kötelezettségei alapján – megfelelő dokumentummal igazolja, hogy a személy jogosult a tanúsítványt a szervezet képviseletében használni.
Szolgáltatási szabályzat	A szolgáltató tevékenységével kapcsolatos részletes eljárási és egyéb működési szabályokat tartalmazó szabályzat.
Szolgáltató	A jelen dokumentumban: az Eat. [1] elektronikus aláírással kapcsolatos szolgáltatások közül a elektronikus aláírás hitelesítés-szolgáltatást és a aláírás-létrehozó eszközön az aláírás-létrehozó adat elhelyezése szolgáltatást nyújtó szervezet.
Szolgáltatói kulcspár	A szolgáltatói aláírás-létrehozó adat (kriptográfiai magánkulcs) és a szolgáltatói aláírás-ellenőrző adat (kriptográfiai nyilvános kulcs).
Szolgáltatói magánkulcs	Olyan kriptográfiai magánkulcs, amelyet a hitelesítésszolgáltató saját szolgáltatásának igazolására, így különösen a tanúsítvány kibocsátásához, a visszavonási nyilvántartások aláírásához, az időbélyegzéshez, a naplózáshoz, az archiváláshoz használ.
Szolgáltatói nyilvános kulcs	Olyan kriptográfiai nyilvános kulcs, amelyet a szolgáltatói magánkulcs használatával létrehozott elektronikus aláírás ellenőrzésére használnak.
Tanúsítvány	Hitelesítés-szolgáltató által kibocsátott digitális igazolás, amely a belefoglalt nyilvános kulcsot egy

	meghatározott személyhez kapcsolja, és igazolja e személy személyazonosságát vagy valamely más tény fennállását, ideértve a hatósági (hivatali) jelleget.
Tanúsítvány visszavonási lista (CRL)	Valamely okból visszavont, vagy felfüggesztett, azaz érvénytelenített tanúsítványok azonosítóit, valamint a visszavonás tényét és időpontját tartalmazó, nemzetközi elvárásoknak megfelelő elektronikus lista, melyet a hitelesítés-szolgáltató bocsát ki, s aláírásával hitelesít.

1.7 Rövidítések és jelölések

CRL	tanúsítvány visszavonási lista	Certificate Revocation List
DN	megkülönböztetett név	Distinguished Name
KHE	kriptográfiai hardver eszköz	
EHR	egységesített Hitelesítési rend	Normalized Certification Policy
EHR+	kriptográfiai hardver eszköz használatát megkövetelő Egységesített Hitelesítési rend	(extended) Normalized Certification Policy
OCSP	valós idejű tanúsítvány állapot protokoll	On-line Certificate Status Protocol
OID	objektum azonosító	
PKI	publikus kulcsú infrastruktúra	Public Key Infrastructure
URI	egységes forrás azonosító	Object Identifier Uniform Resource Identifier
URL	egységes forrás meghatározó	Uniform Resource Locator
UTF	egységes átalakítás formátum	Unicode Transformation Format

1.8 Hivatkozások

[1] 2001. évi XXXV. törvény az elektronikus aláírásról (rövidítve: Eat)

[2] FIPS PUB 140: "Kriptográfiai modulok biztonsági követelményei"

[3] MSZ/ISO/IEC 15408 1999: Informatika - Biztonságtechnika - Az informatikai biztonságértékelés közös szempontjai (1-3 részek)

[4] CEN CWA 14167-2: Védelmi profil hitelesítés-szolgáltató aláírási műveletét végző, mentési funkcióval rendelkező kriptográfiai moduljára

[5] ETSI TS 102 042 Szabályozási követelmények a nyilvános kulcsú tanúsítványokat kibocsátó hitelesítés-szolgáltatók számára (Műszaki specifikáció) v1.2.1 (2005-05

[6] RFC 3647 Internet X.509 Nyilvános kulcsú infrastruktúra – tanúsítvány politika és szolgáltatási szabályzat keretrendszer

[8] Az Educatio Kht. elektronikus aláíráshoz kapcsolódó hitelesítés szolgáltatásának tanúsítvány-profilja

[9] „Közigazgatási, ügyfélhez kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend.”, azonosító: [EHR+_Ü], OID: 0.2.216.1.100.42.101.3.2.1

[9a] A „Közigazgatási, köztisztviselőhöz kapcsolódó, kriptográfiai hardver eszköz használatát megkövetelő, egységesített hitelesítési rend”, azonosítója: „[EHR+_K], OID: 0.2.216.1.100.42.101.4.2.1”

[10] „Az Educatio Társadalmi Szolgáltató Közhasznú Társaság ÁLTALÁNOS SZERZŐDÉSI FELTÉTELEK fokozott biztonságú aláíráshoz kapcsolódó elektronikus aláírás hitelesítés szolgáltatások igénybevételéhez”

[11] „Országos Felsőoktatási Információs Központ Informatikai szabályzata”

[12] „Az Educatio Társadalmi Szolgáltató Közhasznú Társaság hitelesítés szolgáltatási rendszerének adatkezelési és adatvédelmi szabályzata”

[13] ETSI TS 102 280 X.509 V.3 a természetes személyek számára kiadandó tanúsítvány profilja

[14] RFC 3280 a X.509 3-as verziójú tanúsítványok és 2-es verziójú CRL-ek

[15] 2004. évi CXL. törvény a közigazgatási hatósági eljárás és szolgáltatás általános szabályairól (rövidítve: Ket.)

[16] 193/2005. (IX. 22.) Kormányrendelet az elektronikus ügyintézés részletes szabályairól

[17] Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban a hitelesítés-szolgáltatók által végzett viszontazonosítás protokolljának műszaki specifikációjára, 2005. december 6.

[18] RFC 2986 Tanúsítványkérés specifikáció (PKCS #10: Certification Request Syntax Specification)

[19] Az Educatio Társadalmi Szolgáltató Közhasznú Társaság Kulcsmenedzsment dokumentumai.

[20] Az NHH által a Szolgáltatónak küldött HL-21917-2/2008. határozata az

algoritmusokról.

[21] RFC 2560 valós idejű tanúsítvány állapot protokoll (Online Certificate Status Protocol) specifikáció

2. Közzétételre és tárolásra vonatkozó felelősségek

2.1 Szolgáltatói információ közzététele

A Szolgáltató szerződéses feltételeit és szabályzatait elektronikus formában hozza nyilvánosságra a honlapján. A honlapon az érvényben levő dokumentumokon kívül a korábbi verziók is elérhetőek.

Szolgáltató nyilvános szabályzataiban csak azon eljárásait hozza nyilvánosságra, melyek ismerete a szolgáltatás biztonságát nem veszélyezteti.

2.2 Rendkívüli információk közzététele

A Szolgáltató a rendkívüli információkat késlekedés nélkül közzéteszi a jogszabályi előírásoknak megfelelően, illetve akkor, amikor arra szükség van.

2.3 A tanúsítványokra vonatkozó információk közzététele

A Hitelesítés Szolgáltató a http://www.educatio.hu honlapján keresztül folyamatosan elérhetővé teszi a jelen szabályzat, valamint az Általános szerződési feltételek [10], továbbá a hitelesítési rend dokumentumokat.

A Hitelesítés Szolgáltató a http://crl.pkica2.educatio.hu/certenroll/educatio-ca2.crl fájlban adja meg a visszavonási listát.

A valós idejű tanúsítvány állapot lekérdezése szolgáltatás a http://educa2.educatio.hu/ocsp/ címen érhető el.

A Hitelesítés Szolgáltató tanúsítványkibocsátó egység (CA) tanúsítványának elérése a http://crl.pkica2.educatio.hu/certenroll/educatio-ca2.crt azonosító megadásával történhet.

Mindazon ügyfelekre vonatkozóan, akik nyilatkozatban hozzájárultak ahhoz, hogy a tanúsítványaikat nyilvánosságra hozhatja a Hitelesítés Szolgáltató web-es lekérdezési lehetőséget biztosít. A web-lap címe: http://pkica2.educatio.hu/certsearch/educertsearch.aspx.

2.4 A közzététel gyakorisága

Tanúsítványok, kikötések és feltételek nyilvánosságra hozatala:

a) A Hitelesítés Szolgáltató biztosítja saját szolgáltatói tanúsítványai, valamint az általa kibocsátott tanúsítványok használatára vonatkozó kikötések és feltételek folyamatos elérhetőségét (a 4.10.2 pontban meghatározott rendelkezésre állás mellett).

Az általa kibocsátott végfelhasználói tanúsítványok nyilvánosságra hozatala csak az érintett alany, illetve előfizető hozzájárulása esetén megengedett.

Visszavonási állapot információ nyilvánosságra hozatala:

b) A Hitelesítés Szolgáltató ügyfélszolgálata a telefonon érkező visszavonási és felfüggesztési kérelem fogadásakor megállapítja a kérelem érvényességét és a kérelmező jogosultságát.

c) Az ügyfélszolgálat a jogos felfüggesztési kérelem esetén elvégzi a felfüggesztési műveletet és utasítást ad a rendszernek, hogy ezen eseményhez kapcsolódóan módosított visszavonási állapotot tegyen közzé. A felfüggesztett tanúsítvány -- a PKI technológia alapján -- a visszavonási állapotot mutató adatsorozatban (CRL-visszavonási lista információk listája) visszavont tanúsítványként jelenik meg[2], amíg az ügyfél felfüggesztésre vonatkozó törlési (visszaállítási) igénye alapján szolgáltatói eljárás nem hajtódik végre. Továbbiak a 4.9 és a 4.9.13-20. pontokban, a felfüggesztési kérelemre vonatkozó kivárási idő a 4.9.4 b) és c) pontokban találhatók.

d) A jogos visszavonási kérelem esetén a Hitelesítés Szolgáltató ügyfélszolgálata tájékoztatja az ügyfelet, hogy a visszavonási művelet két szakaszból áll. Az első szakaszban a megjelölt tanúsítvány felfüggesztésre kerül, majd a Hitelesítés Szolgáltató további jogosultság ellenőrzést végez. Továbbiak a 4.9 és a 4.9.1-12. pontokban, a visszavonási kérelemre vonatkozó kivárási idő a 4.9.4 b) és c) pontokban találhatók.

e) A Hitelesítés Szolgáltató a tanúsítvány visszavonási listákat rendszeresen („CRL fájlokat") közzé teszi. Továbbiakat ld. a „4.9.7 A visszavonási lista kibocsátás gyakorisága" pontban. Emellett a Szolgáltató valós idejű tanúsítvány állapot szolgáltatást is biztosít.

2.5 Az adatbázisok elérésének szabályozása

Tanúsítványok, kikötések és feltételek elérhetősége:

a) A tanúsítványtár egy 2.3 pont szerint web-es lekérdezéssel érhető el. A szolgáltatói tanúsítványok, valamint a tanúsítványok használatára vonatkozó kikötések és feltételek (a jelen szabályzat, valamint a megfelelő hitelesítési rendek ([9], [9a], Általános szerződési

[2] Ez egy technikai megoldás, amelyet a PKI létrehozói teremtettek meg; a tanúsítványhoz kapcsolódó egyéb nyilvántartásból kitűnik, hogy felfüggesztés történt.

feltételek [10]) nyilvánosak és a szokásos böngészőkkel elérhetők az Interneten.

b) Külön kérésre a jelen jelen szabályzat, Általános szerződési feltételek [10] a Hitelesítés Szolgáltató ügyfélszolgálatán nyomtatásban is átvehetők. Ezért a szolgáltatásért a Hitelesítés Szolgáltató eseti megállapodás alapján külön díjat számolhat fel.

Visszavonási állapot információ elérhetősége:

A Hitelesítés Szolgáltató a visszavonási állapot információt tanúsítvány visszavonási lista (CRL) formájában is, és valós idejű tanúsítvány állapot szolgáltatással is közzéteszi.

Ezek a szolgáltatások nyilvánosan és korlátozás nélkül (nemzetközileg is) elérhetők.

3. Azonosítás és hitelesítés

3.1 Megnevezési konvenciók

Az azonosítók a Hitelesítés Szolgáltató belső szabályzatai alapján vannak kezelve. Az ékezetes magánhangzók használatánál a Hitelesítés Szolgáltató magyar helyesírás szabályait alkalmazza. Ennek megfelelően a Hitelesítés Szolgáltató a nevekben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve az UTF-8 kódolásban rögzíti

3.1.1 Név típusok

a) A Hitelesítés Szolgáltató által kiállított tanúsítványokra a következő névkonvenció érvényes:

- X.500 formátum (ITU-T X.501 /ISO/IEC 9594-2:1997, RFC 3280),

  A Hitelesítés Szolgáltató neve:

  A Hitelesítés Szolgáltató a tanúsítványban a tanúsítvány kiadói nevét (common name; cn) „EDUCA-2” megnevezéssel szerepelteti.

  A Hitelesítés Szolgáltató technikai azonosító nevét (X.509 distinguished name; dn) a következők alkotják:

  - a cn szerinti név,
  - a szervezeti megjelölés (organization; o): „Educatio Társadalmi Szolgáltató Kht”, és
  - országnév jelzése (country; c): „HU”.

  Az ügyfél, aki természetes személy / aláíró neve:

  A Szolgáltató a tanúsítvány birtokosának névmezőjébe (Subject), az alany személyazonosságának igazolására elfogadott hatósági igazolványban (lásd 3.2.3 c)

pont) foglalt névvel betű szerint megegyezően, a névben szereplő ékezetes betűket eredeti írásmódjuk szerint feltüntetve szerepelteti.

A hatósági igazolvány szerinti név a tanúsítvány egyedi megkülönböztető név (DN) szerint: CN és SN mezőkben (CN = Teljes név = Vezetéknév + Keresztnév/Keresztnevek, SN = Vezetéknév), az UTF-8 kódolást használva kell szerepeljen.

Az ügyfél technikai azonosító nevét (X.509 distinguished name; dn) a következők alkotják:

- a cn szerinti név,
- a szervezeti megjelölés, ha meg van adva (organization; o), és
- az oktatási azonosító/pedagógus azonosítója, oktatáson kívüli felhasználás esetén egy egyedi azonosító kód.

A tanúsítvány „SubjectAltname” mezőjében szereplő elektronikus levelezési cím tartalmazza az ügyfél címét, melynek struktúrája megfelel az RFC 822 előírásainak.

3.1.2 Igény a nevek értelmezhetőségére

a) A Hitelesítés Szolgáltató betartja a [8] 6. táblázata (Ügyfelek tanúsítványának subject beállítása) által a nevek értelmezhetőségére vonatkozó szabályokat.

3.1.3 Álnevek használata

A Hitelesítés Szolgáltató a regisztráció során felhívja az ügyfél figyelmét arra, hogy az alábbi szabályokat alkalmazza:

a) A közigazgatási célú hitelesítési rendek ([9], és [9a]) alapján kiadott tanúsítványokban az álnév használata tilos!

3.1.4 A különböző elnevezési formák értelmezési szabályai

A nevek és azonosítók értelmezése során az ügyfeleknek és a Hitelesítés Szolgáltatónak a jelen szabályzatban leírtak alapján kell eljárniuk. Amennyiben a nevek és azonosítók, illetve a tanúsítványban foglalt adatok értelmezésével kapcsolatban további információra van szükség, akkor ezt a Hitelesítés Szolgáltató a jelen szabályzatra támaszkodva megadja.

3.1.5 A nevek egyedisége

A Hitelesítés Szolgáltató gondoskodik arról, hogy az általa kiadott tanúsítványokban használt egyedi technikai azonosító neveket (X.509 distinguished name; dn) sohasem fogja egy másik entitáshoz rendelni.

3.1.6 Márkanevek elismerése, azonosításuk és szerepük

Nem alkalmazható.

3.2 Kezdeti regisztrálás /személyazonosság megállapítása

A regisztrációhoz kapcsolódó eljárások helyét és időpontját az igénylő telefonon, esetleg levélben egyezteti a Hitelesítés Szolgáltató ügyfélszolgálatával, vagy regisztrációs munkatársaival.

A regisztrációt megelőzően az igénylőnek

- vagy személyesen meg kell jelennie a regisztrációt végző szervezet előtt

- vagy – külön egyeztetés és megállapodás alapján – a regisztrációt végző szervezet külső helyszínen találkozik a személyesen megjelenő igénylővel.

Az igénylő személyazonosságának ellenőrzését biztonságos eljárás keretében végzi el a Hitelesítés Szolgáltató, az alábbiak szerint:

3.2.1 A magánkulcs birtoklásának igazolása

o Természetes személy esetén: a Hitelesítés Szolgáltató megbízható rendszere biztosítja a tanúsítvány generálása előtt – a jelen szabályzat 1.1.7 pontja szerint –, hogy az igénylő ténylegesen birtokolja a tanúsítványba foglalandó aláírás-ellenőrző adatnak (kriptográfiai nyilvános kulcsnak) megfelelő aláírás-létrehozó adatot (kriptográfiai magánkulcsot).

3.2.2 Szervezet azonosságának hitelesítése

3.2.2.1 Az Educatio Kht. zárkörű hitelesítés szolgáltatását igénybe vevő intézményvezető, illetve a képviselettel meghatalmazott személy esetén

A Hitelesítés Szolgáltató a jelen szabályzat 3.2.3.1 pontja szerint regisztrált ügyfeleknél nem vizsgálja egy Aláíró jogi szervezethez, jogi személyiség nélküli szervezethez, gazdálkodó szervezethez kapcsolódó képviseleti jogát, illetve ebben az értelemben nem azonosít szervezetet.

3.2.2.2 Más személyek esetén

a) Ha az ügyfél tanúsítványával kifejezetten jelezni kívánja, hogy ő egy adott szervezethez tartozik, akkor a regisztráció során be kell mutatnia az adott szervezet nevében aláírásra jogosult személy által hivatalosan kiállított és aláírt, az adott szervezet nevét is tartalmazó meghatalmazást arra, hogy a szervezet képviseletében a tanúsítványt használja, az aláírásra jogosító aláírási címpéldányt, valamint a szervezet azonosságát is hitelesítő dokumentumot.

Egy közigazgatási szervet képviselő természetes személynek a regisztrációhoz magával kell vinnie egy, az adott közigazgatási szerv által kiállított és közokiratba foglalt, a közigazgatási szerv nevét is tartalmazó meghatalmazást arra, hogy a hivatal képviseletében a Hitelesítés

Szolgáltatónál előforduló ügyekben eljárjon, mely meghatalmazás egyúttal a szervezet azonosságát is hitelesíti.

A regisztrációs felelős munkatársak (RO-k) ellenőrzik ezeket a meghatalmazásokat.

A Hitelesítés Szolgáltató köteles a meghatalmazást kiállító hatóságot - a hivatali aláírást kiváltó személy adatainak megadása nélkül - a hivatali aláírás kiállításának tényéről és a hatóság által kiadott meghatalmazásban foglalt iktatószámról értesíteni.

3.2.3 Személy azonosságának hitelesítése

a) A regisztrációra az igénylő alanynak személyesen meg kell jelennie a Hitelesítés Szolgáltató regisztrációt ellátó munkatársánál (RO-nál). Az RO a regisztrációt egy erre a célra elkülönített, megfelelő biztonsági feltételekkel üzemeltetett regisztrációs helyiségben (RA helyiség) végzi el.

A Hitelesítés Szolgáltató az Educatio Kht. ügyvezetőjének írásos utasítása alapján, az RO a regisztrációt külső helyszínen is lefolytathatja, amennyiben a biztonsági feltételek egyenértékűek az RA helyiség biztonsági feltételeivel, valamint a regisztráció helyszínének és lefolytatásának megfelelőségét a Hitelesítés Szolgáltató egy, a biztonsági feladatok ellátásáért felelős munkatársa (SO) ellenőrzi, és ezt a tényt az RO, valamint a SO által saját kezűleg aláírt jegyzőkönyvvel igazolja.

A hivatali aláíráshoz tartozó ([EHR+_K], [9a] szerinti) tanúsítvány kibocsátását megelőző regisztrációt kezdeményezheti a hatóság, ha a regisztrációs szervezet a természetes személy azonosítását külső helyszíni regisztráció útján, szükség szerint a hatóság által kijelölt közigazgatási szerv közreműködésével végzi el.

b) A Hitelesítés Szolgáltató a regisztráció során az igénylő személyazonosságát a személyazonosság igazolására alkalmas hatósági igazolvány alapján, szemrevételezéssel ellenőrzi.

c) A regisztráció és a személyazonosság ellenőrzése alapjául szolgáló, rögzítendő adatok helyességét, valamint a kriptográfiai eszköz birtoklását, az igénylő nyilatkozatban, saját kezű aláírásával ellátva igazolja.

d) A b) pont szerinti hatósági igazolvány azonosító adatait, a megadott adatok egyezését és a hatósági igazolvány érvényességét az RO közhiteles elektronikus nyilvántartásban ellenőrizi.

e) A Hitelesítés Szolgáltató regisztrációban részt vevő munkatársa (RO) aláírással igazolja, hogy a hatósági igazolványon szereplő arckép megfeleltethető az igénylő arcának, és az igazolványban szereplő aláírás azonos a c) pont szerinti nyilatkozatot igazoló aláírással.

f) A Hitelesítés Szolgáltató ellenőrzi a képviseletre feljogosító dokumentumokat, és megállapítja a kibocsátandó tanúsítvány fajtáját, az 1.1.6 pont szerint.

3.2.4 Viszontazonosítás

A Hitelesítés Szolgáltató a közigazgatási ügyintéző hatóság elektronikus üzenetben történő megkeresésére viszontazonosítást végez a 2004. évi CXL. törvény [15], valamint a kapcsolódó 193/2005. (IX. 22.) Korm. rendelet [16], és az IHM ajánlása [17] alapján. Ezen szolgáltatás keretében a Hitelesítés Szolgáltató összeveti a közigazgatási ügyintéző hatóság által küldött természetes személyazonosító adatokat az általa regisztrált és kezelt természetes személyazonosító adatokkal. A megkeresésre válaszként elküldi a viszontazonosítást kérő hatóságnak az egyezőség eredményét (pontos találat, vagy sikertelenség tényét), valamint a viszontazonosítási kérést azonosító adatot.

A viszontazonosítás címe: https://educa2.educatio.hu/

3.3 Azonosítás és hitelesítés kulcs megújítás kérelem esetén

Tanúsítvány kulcscseréjét a Hitelesítés Szolgáltató nem támogatja. Amennyiben kulcscsere válna szükségessé, abban az esetben új tanúsítvány-igénylést kell beadni a jelen szabályzatban meghatározottak szerint. (Ld. a 4. pontot)

3.4 Azonosítás és hitelesítés tanúsítvány visszavonási kérelem esetén

Az ügyfél (alany) a tanúsítványát a Hitelesítés Szolgáltató ügyfélszolgálatán keresztül (ld. 1.5.2 pontot) vonhatja vissza, illetve (átmenetileg) függeszteti fel.

Az ügyfélszolgálat a visszavonó, illetve a felfüggesztést kérő személy azonosságát a rendszerben tárolt titkos kérdés – válasz párral állapítja meg. Az ügyfélszolgálat csak azon esetekben kezdeményezi a visszavonást, illetve a felfüggesztési kérelmet, ha az ügyfél mind a kérdést, mind a választ helyesen adta meg.

A titkos kérdés – válasz bonyolultságát és összetettségét az ügyfélszolgálat véleményezi, de az ezzel kapcsolatos felelősséget az ügyfél viseli.

Az ügyfélszolgálat először a titkos kérdésre kérdez. Amennyiben az ügyfél erre nem emlékezne, lehetőség van arra, hogy egy rávezető szóval, vagy szavakkal segítsen az ügyfélszolgálat. Amennyiben ez nem lenne sikeres, az azonosítás hiányában a kérelem elutasításra kerül.

A titkos válasznál az ügyfél nem kap segítséget. Amennyiben a választ nem helyesen kapja meg az ügyfélszolgálat, még kétszer próbálkozhat. Ha ez sem volt sikeres, akkor az azonosítás hiányában a kérelem elutasításra kerül.

(Példa: titkos kérdés volt: „az első autóm színe”. Válasz: „korálpiros”. A kérelmező nem emlékszik a titkos kérdésre, ezért az ügyfélszolgálat segít: „autó”. Ebből kell emlékeznie az ügyfélnek, hogy mi volt a titkos kérdés, és tudnia kell, hogy mi a válasz!)

4. A tanúsítvány életciklusra vonatkozó követelmények

4.1 Tanúsítványkérelem

4.1.1 Ki nyújthat be tanúsítványkérelmet

a) Tanúsítványkérelmet azok az igénylők nyújthatnak be, akik vállalják, hogy a Hitelesítés Szolgáltatóval szerződéses kapcsolatot létesítenek.

b) A Hitelesítés Szolgáltató azt megelőzően, hogy az igénylővel szerződéses kapcsolatot létesít, tájékoztatja az igénylőt a tanúsítvány használatával kapcsolatos kikötésekről és feltételekről, valamint a nyilvánosan elérhető, jelen szolgáltatási szabályzat, a alkalmazott hitelesítési rend ([9], [9a]), továbbá az Általános szerződési feltételek [10] dokumentumok rendelkezésre állásáról, valamint a felhasználás technikai lehetőségeiről.

c) Amennyiben az aláíró (alany) nem azonos az előfizetővel, őt is tájékoztatni kell kötelességeiről.

d) A Hitelesítés Szolgáltató a b) pontban említett kikötéseket és feltételeket tartalmazó, közérthető nyelven megfogalmazott dokumentumokat elektronikusan letölthető formában és egyedi kérésre, tartós eszközön (pl. papírra vagy CD-re írva) egyaránt hozzáférhetővé teszi.

4.1.2 A tanúsítvány igénylés folyamata és a résztvevők felelőssége

a) Az igénylőnek a tanúsítványigénylés folyamatában meg kell adnia azon cím- és egyéb adatokat, melyek alapján a későbbiekben az aláíróval illetve az előfizetővel fel lehet venni a kapcsolatot.

b) A Hitelesítés Szolgáltató nyilvántartásba vesz minden, az alany azonosságának igazolására használt információt, beleértve az igazoláshoz használt dokumentáció regisztrációs számát és az annak érvényességével kapcsolatos esetleges korlátozásokat.

c) A Hitelesítés Szolgáltató nyilvántartásba vesz több, az aláíróval illetve előfizetővel aláírt nyilatkozatot és megállapodást[3], beleértve az alábbiakat:

- annak megerősítését, hogy a regisztráció során megadott információk valódiak és pontosak,
- az aláíró illetve az előfizető nyilatkozatát arra vonatkozóan, hogy kötelezettségeit megismerte és azok betartását vállalja,
- az aláíró illetve az előfizető nyilatkozatát arra vonatkozóan, hogy a részére biztosított kriptográfiai hardver eszköz használatával kapcsolatos kötelezettségeit megismerte és azok

[3] Az előfizető ezen megállapodás különböző pontjaihoz, a regisztráció különböző fázisai során is hozzájárulhat. Például a tanúsítványban szereplő információk korrektségére vonatkozó megállapodás, a megállapodás egyéb szempontjait követően is megköthető.

betartását vállalja,

- az érintett hozzájárulását az egyes szolgáltatások során felhasznált információk Hitelesítés Szolgáltató által történő nyilvántartásba vételéhez,

- azt, hogy az előfizető megköveteli-e, az aláíró pedig hozzájárul-e a tanúsítvány közzétételéhez és milyen feltételek mellett,

Az eljárás során a Hitelesítés Szolgáltató nyilvántartásba veszi az Aláíró az igazolásához bemutatott dokumentumok regisztrációs számát és az azok érvényességével kapcsolatos esetleges korlátozásokat is.

A fentiek elektronikus formát is ölthetnek.

d) A fent megnevezett nyilvántartásokat a Hitelesítés Szolgáltató legalább a tanúsítvány érvényességének lejártától számított 10 évig megőrzi (archiválja), illetve jogi eljárásokban a tanúsítványon keresztüli bizonyításához szükséges ideig. Továbbiakat ld. 5.5 pontokban.

4.2 A tanúsítványkérelem feldolgozása

4.2.1 Az azonosítási és hitelesítési funkciók megvalósítása

a) A Hitelesítés Szolgáltató igény esetén új aláíró eszközt biztosít. A Hitelesítés Szolgáltató csak az általa támogatott/rendszeresített aláíró eszközzel (például chipkártyával) biztosítja a szolgáltatást. Az aláírás-létrehozó eszközt kizárólag az Aláíró veheti át személyesen, és az átvétel során hitelesen kell igazolnia a személyazonosságát, a személyazonosság igazolására alkalmas hatósági igazolvány alapján. Ennek hiányában az eszköz nem kerül átadásra.

b) A regisztrációs munka igazolásához szükséges eljárás részeként a Hitelesítés Szolgáltató – az aláíró hozzájárulása esetén – archiválja a bemutatott hatósági igazolvány fénymásolóval készült képét. A hatósági igazolvány fénymásolóval történő lemásolásakor keletkező lapon a Hitelesítés Szolgáltató megbízottja az adatkezeléshez nem szükséges adatokat fekete tollal kifesti, hogy azok a továbbiakban olvashatatlanok legyenek. Ezt a kifestett lapot mind az Aláíró, mind a Hitelesítés Szolgáltató megbízottja aláírásával hitelesíti. Hozzájárulás hiányában az aláíró teljes bizonyító erejű okiratban nyilatkozatot ad, amelyben kijelenti, hogy a Hitelesítés Szolgáltató által rögzített személyes adatok megfelelnek a valóságnak, valamint a személyazonosító igazolványban rögzítetteknek.

c) A regisztráció során bemutatott hatósági igazolvány azonosító adatait, a megadott adatok egyezését és a hatósági igazolvány érvényességét a Hitelesítés Szolgáltató (regisztrációs egység) közhiteles nyilvántartásban ellenőrzi. Eltérés esetén a szolgáltatás megtagadható.

d) A regisztráció során a regisztrációs munkatárs (RO, vagy XRO) a szolgáltatási szerződés kitöltésével rögzíti a regisztrációs adatokat, és a regisztráció és a személyazonosság ellenőrzése alapjául szolgáló, rögzítendő adatok helyességét az igénylő saját kezű aláírásával ellátva igazolja.

e) A regisztrációs munkatárs (RO, vagy XRO) tájékoztatja az aláírót a hitelesítés szolgáltatásról és az aláírás-létrehozó eszköz (kriptográfiai hardver eszköz) használatáról.

f) Ezt követően az aláírók illetve az előfizető aláírja a szolgáltatási szerződést.

g) A regisztrációt végző szervezet regisztrációban részt vevő munkatársa (RO, vagy XRO) aláírásával igazolja, hogy az aláírót a személyes regisztráció során azonosította és az aláíró a szolgáltatási szerződést az ő jelenlétében aláírta.

h) A tanúsítványkérelmet a Hitelesítés Szolgáltató (RO) az eseménynaplójában rögzíti, a kapcsolódó dokumentumokat, valamint az eseménynapló bejegyzéseket a Hitelesítés Szolgáltató biztonsági felelősei (SO-k) begyűjtik és archiválják.

4.2.2 A tanúsítványkérelem jóváhagyása vagy visszautasítása

a) A Szolgáltató csak akkor fogadja el a tanúsítványkérelmet, ha a következő feltételek teljesülnek:
   - benyújtották a kérelmét a tanúsítvány kibocsátónak,
   - az ügyfél természetes személy, és azonos a kérelemben szereplő alannyal,
   - a kérelemben szereplő adatok ellenőrizhetők és pontosak.

4.2.3 A tanúsítványigénylések feldolgozásának időtartama

A tanúsítványigénylések feldolgozásának időtartama legfeljebb 30 nap.

4.3 Tanúsítvány kibocsátás

A tanúsítvány kibocsátás a regisztrációs eljárás alatt történik a Hitelesítés Szolgáltató által meghatározott regisztrációs pontokon (a Hitelesítés Szolgáltató telephelyén, az RA helyiségben, vagy az ügyfélnél – külső helyszínen). Ezeken a helyeken a Hitelesítés Szolgáltató bemutatja a regisztrációs eljáráshoz szükséges eljárást, dokumentációt és az eszközöket. A tanúsítvány kibocsátás biztonsági körülményeinek meghatározását a Hitelesítés Szolgáltató, a teljesítést a Hitelesítés Szolgáltató és az ügyfél együttesen biztosítja. Véleményeltérés esetén a Hitelesítés Szolgáltató megtagadhatja a tanúsítvány kibocsátását. Ez esetben is készül egy jegyzőkönyv.

A megfelelő körülmények betartásáért a Hitelesítés Szolgáltató jelen levő, a regisztrációt végrehajtó (meghatalmazott) munkatársa (RO, XRO) felel, az alábbi pontok szerint.

4.3.1 A hitelesítés-szolgáltató tevékenysége a tanúsítvány kibocsátás során

A tanúsítvány létrehozása a regisztrációs eljárás során keletkező automatikus tanúsítvány kérelemre történik. Ez egy zárt technológiai folyamat.

A Szolgáltató a tanúsítványkiadást biztonsági naplózás mellett hajtja végre.

4.3.2 Az előfizető értesítése a tanúsítvány kibocsátásról

Külön értesítésre nincs szükség, ld. az előző 4.3.1 pontot, kivéve a 4.4.3. pontban foglaltakat.

4.3.3 A tanúsítvány kibocsátásának időpontja

A tanúsítvány kibocsátásának az időpontja a tanúsítvány létrehozásának az időpontjának felel meg.

4.3.4 A tanúsítvány érvényessége

A tanúsítvány érvényessége a tanúsítvány kibocsátásának az időpontjától számított 1 év.

4.4 Tanúsítvány elfogadás

4.4.1 A tanúsítvány elfogadás esetei

a) Az ügyfél a tanúsítvány használatba vétele előtt köteles igazolni a tanúsítvány átvételét, és a tanúsítvány adatainak helyességét. Az igazolás egyben a jelen szabályzat, valamint a megfelelő hitelesítési rend ([9],[9a]), és az Általános szerződési feltételek [10], továbbá az esetleges egyedi szerződéses kikötések elfogadását is jelenti.

4.4.2 A tanúsítvány közzététele a hitelesítés-szolgáltató által

A tanúsítvány nyilvánosságra hozatala csak az érintett előfizető, illetve alany hozzájárulása esetén megengedett. Ld. fent 2.3 pontban.

4.4.3 A további szereplők értesítése a tanúsítvány kibocsátásról.

A Hitelesítés Szolgáltató értesíti az ügyfél számára szervezeti képviseletre jogot adó szervezetet.

A Hitelesítés Szolgáltató a hivatali aláírással és a hivatali aláíráshoz tartozó tanúsítvány elkészítésével kapcsolatban – 194/2005 (IX. 22.) Korm. rendelet 10. § (3) alapján – köteles a meghatalmazást kiállító hatóságot - a hivatali aláírást kiváltó személy adatainak megadása nélkül - a hivatali aláírás kiállításának tényéről és a hatóság által kiadott meghatalmazásban foglalt iktatószámról értesíteni.

4.5 Kulcspár- és tanúsítvány használat

4.5.1 Az alany magánkulcs- és tanúsítvány használata

a) Az alany magánkulcsát és tanúsítványát csak a Hitelesítés Szolgáltatóval szerződésben rögzített korlátozásnak megfelelően használhatja.

b) Az alany csak a megfelelő tanúsítvány elfogadása után (lásd 4.4.) használhatja magánkulcsát.

c) Az alany a megfelelő tanúsítvány lejárta után nem használhatja tovább magánkulcsát.

d) Az alanynak az adott helyzetben általában elvárható gondosságot kell tanúsítania annak érdekében, hogy megelőzze magánkulcsának illetéktelen felhasználását.

e) Az alany különböző magánkulcsait csak olyan célokra és olyan alkalmazásokkal használhatja, melyek összhangban vannak a megfelelő tanúsítványok „kulcshasználat" és „kiterjesztett kulcshasználat" mezőinek tartalmával (lásd még 6.1.7 és 7.1.2).

4.5.2 Az érintett felek nyilvános kulcs- és tanúsítvány használata

Annak érdekében, hogy az érintett fél megalapozottan hagyatkozhasson a tanúsítvánnyal igazolt kriptográfiai kulcspár használatával működő alkalmazásra ajánlott a kulcspár megfelelő használatát és a hozzá tartozó tanúsítványt az adott helyzetben tőle általában elvárható gondossággal ellenőriznie.. Ennek során – a Hitelesítés Szolgáltató ajánlása szerint – szükséges, hogy figyelembe vegye az alábbiakat:

a) Az érintett fél csak olyan célokra és olyan alkalmazásokkal fogadjon el nyilvános kulcsokat, melyek összhangban vannak a megfelelő tanúsítványok „kulcshasználat" és „kiterjesztett kulcshasználat" mezőinek tartalmával.

b) Mielőtt egy tanúsítványba foglalt nyilvános kulcsot felhasználna, ajánlott, hogy az érintett fél ellenőrizze a tanúsítvány érvényességét, valamint azt, hogy a tanúsítvány nincs-e felfüggesztve, illetve visszavonva az érvényes visszavonási állapot információ alapján – a tanúsítványt kibocsátó szolgáltató szabályzatai szerint.

c) Amennyiben – ésszerű módon – egy tanúsítványra kíván hagyatkozni, az érintett fél számára ajánlott, hogy vegye figyelembe a tanúsítvány felhasználására vonatkozó valamennyi korlátozást, mely a tanúsítványban és a tanúsítványt kibocsátó szolgáltató szabályzataiban szerepel.

4.6 Tanúsítvány megújítás

A tanúsítvány megújítás az a folyamat, amelynek során a hitelesítés-szolgáltató úgy bocsát ki egy megújított tanúsítványt, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai (köztük a nyilvános kulcs is) változatlanok.

4.6.1 A tanúsítvány megújítás körülményei

a) A tanúsítvány megújítása akkor lehetséges, ha valamennyi alábbi feltétel teljesül:

- a tanúsítvány érvényes,
- a tanúsítvány nem szerepel a tanúsítvány visszavonási listán,
- a kezdeti regisztráció alkalmával rögzített, tanúsítványba foglalt összes adat még érvényes,
- a tanúsítványhoz tartozó magánkulcs nem kompromittálódott,
- a tanúsítvány még nem volt korábban megújítva.

4.6.2 Ki kérelmezheti a megújítást

a) A tanúsítvány megújítást olyan személy kezdeményezheti, aki a kezdeti tanúsítvány kérelem benyújtására is jogosult volt, vagy jelenlegi felhatalmazása alapján jogosult lett volna.

4.6.3 A tanúsítvány megújítási kérelmek feldolgozása

A hitelesítés-szolgáltatónak gondoskodik arról, hogy egy már korábban nála nyilvántartásba vett alany tanúsítványára vonatkozó megújítási kérelem teljes, pontos és kellőképpen hiteles legyen. Különösképpen:

a) A Hitelesítés Szolgáltató ellenőrizi a tanúsítvány létezését és érvényességét, valamint azt, hogy az alany azonosságának és jellemzőinek igazolására használt információ még mindig érvényes-e.

b) Amennyiben a Hitelesítés Szolgáltató bármely feltétele, illetve kikötése megváltozott, azokat közölnie kell az előfizetővel, és azok előfizető általi elfogadását a 4.1.2 c) pontjának megfelelően rögzítenie kell.

c) Amennyiben bármilyen az aláíróra vagy az előfizetőre vonatkozó információ megváltozott, azt a 3.2.3 pontnak megfelelően a hitelesítés-szolgáltatónak ellenőriznie kell, nyilvántartásba kell vennie, és ehhez az előfizető hozzájárulását be kell szereznie.

d) A Hitelesítés Szolgáltató csak akkor bocsát ki egy új tanúsítványt az aláíró korábbiakban tanúsított nyilvános kulcsának felhasználásával, ha annak kriptográfiai biztonsága még megfelelő az új tanúsítvány tervezett élettartamára, és nincsenek arra utaló jelek, hogy az aláíró magánkulcsa kompromittálódott.

A fent leírt eljárásnak az a célja, hogy a Hitelesítés Szolgáltató meggyőződjön arról, hogy a tanúsítvány megújításra vonatkozó kérelmet az arra jogosult kérelmezi, az előfizető a megváltozott szolgáltatói feltételekről, kikötésekről tudomást szerezzen, azokat elfogadja, illetve a megújítás során a szolgáltató megbízható tanúsítványt állítson elő.

4.6.4 Az aláíró értesítése az új tanúsítvány kibocsátásáról

A Hitelesítés Szolgáltató az aláírót elektronikus levélben értesíti az új tanúsítvány kibocsátásáról annak kibocsátását megelőzően.

4.6.5 A megújított tanúsítvány elfogadása

Lásd. a 4.4.1 pontban.

4.6.6 A megújított tanúsítványok közzététele

Lásd. a 4.4.2 pontban.

4.6.7 A további szereplők értesítése a tanúsítvány kibocsátásról

Lásd. a 4.4.3 pontban.

4.7 Kulcscsere

A kulcscsere az a folyamat, amelynek során a hitelesítés-szolgáltató úgy bocsát ki egy megújított tanúsítványt, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai közül csak a nyilvános kulcs kerül lecserélésre.

Tanúsítvány kulcscseréjét a Hitelesítés Szolgáltató csak abban az értelemben támogatja, hogy új tanúsítvány-igénylési kérelemként kezeli. Ld. még a 3.3 pontban.

4.8 Tanúsítvány módosítása

A tanúsítvány módosítás az a folyamat, amelynek során a hitelesítés-szolgáltató úgy bocsát ki egy módosított tanúsítványt, hogy abban az eredeti tanúsítvány alanyra vonatkozó adatai - a nyilvános kulcs kivételével - változnak, és a tanúsítvány az új adatokkal, valamint a régi nyilvános kulccsal kerül kiadásra.

Tanúsítvány módosítását a Hitelesítés Szolgáltató csak abban az értelemben támogatja, hogy új tanúsítvány-igénylési kérelemként kezeli

4.9 Tanúsítvány visszavonás és felfüggesztés

A Hitelesítés Szolgáltató gondoskodik arról, hogy hiteles és érvényes tanúsítvány visszavonási (felfüggesztési) kérelmek esetén a tanúsítványok visszavonásra (felfüggesztésre) kerüljenek, s erről az aláírók, előfizetők, illetve érintett felek hiteles és megbízható információt kapjanak (a 2.3 pontban meghatározottak szerint).

4.9.1 A visszavonás körülményei

a) A Hitelesítés Szolgáltató köteles intézkedni a tanúsítvány visszavonásáról az alábbi esetekben:

- jogos visszavonási kérés esetén,
- kulcscsere (ld. a fenti 4.7 pontot),és tanúsítvány megújítása (ld. a fenti 4.8 pontot), esetén
- a tanúsítvány felfüggesztésének az ideje lejárt (ld. a 4.9.16 pontban)
- a szolgáltatással kapcsolatos - jogszabályban, a szolgáltatási szabályzatban vagy az Általános szerződési feltételekben [10] meghatározott - rendellenességről szerez tudomást, s ez a rendellenesség nem orvosolható,
- a Hitelesítés Szolgáltató tudomására jut, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy a magánkulcs nem az aláíró kizárólagos birtokában van,
- az aláíró intézmény-vezetői illetve képviselettel meghatalmazotti státusza megszűnik és nem kerül továbbfoglalkoztatásra pedagógus munkakörben (nevelő- és oktatómunkát közvetlenül segítő alkalmazotti munkakörben, pedagógiai előadó vagy pedagógiai szakértő munkakörben), vagy oktatói, kutatói, tanári munkakörben, avagy ilyen foglalkoztatását a megszűnéstől számított 30 napon belül nem jelentik be a közoktatás vagy a felsőoktatás információs rendszerébe,
- a Hitelesítés Szolgáltató és az aláíró illetve előfizető között a szerződés megszűnt,
- a Hitelesítés Szolgáltató tevékenységét befejezte, vagy
- a tanúsítvány érvényességi ideje lejárt,
- a visszavonást jogszabály kötelezővé teszi, vagy egy jogerős és végrehajtható hatósági határozat elrendeli.

4.9.2 Ki kérelmezheti a visszavonást

a) Tanúsítvány visszavonási kérelmet az alábbiak kezdeményezhetik:

- olyan személy, aki ismeri a visszavonási ellenőrző adatokat
- a Hitelesítés Szolgáltató (ld. 4.9.1 és 5.8 pontok szerint).

4.9.3 Visszavonási kérelemre vonatkozó eljárás

a) A tanúsítványok visszavonásának eljárásai:

- a kérelem beadásának módja: telefonon keresztül a Hitelesítés Szolgáltató ügyfélszolgálatánál történik. A bejelentő a neve e-mail címe, majd a titkos kérdésre történő válasz megadásával azonosítja magát. Kéri a visszavonást. Az ügyfélszolgálat

munkatársa megállapítja a kérelem jogosságát. Jogos kérelem esetén, ismerteti a visszavonási eljárás menetét. Felhívja a figyelmet arra, hogy a visszavonás előtt felfüggesztésre kerül a tanúsítvány, amely alkalmas arra, hogy a tanúsítvány sorszáma felkerüljön a visszavonási listára, így ezt követően a tanúsítvánnyal nem lehet visszaélni. Emellett az ügyfélszolgálat munkatársa értesíti a regisztrációs munkatársat (RO-t), hogy az adott felfüggesztett tanúsítványra visszavonást kért egy hitelesített bejelentő. A visszavonás még a felfüggesztési idő lejárta előtt, de legkésőbb a következő munkanapon belül megtörténik. Visszavonás esetén az ügyfélszolgálat munkatársa felhívja az ügyfél figyelmét arra, hogy a Hitelesítés Szolgáltatóval megkötött, a tanúsítványhoz kapcsolódó Szolgáltatási Szerződése megszűnik.

- eljárás abban az esetben, ha a bejelentő nem tudja jogosultságát igazolni. Ebben az esetben személyesen kell megjelennie a Hitelesítés Szolgáltatónál, ahol a regisztrációs munkatárs (RO) a Hitelesítés Szolgáltató nyilvántartása alapján azonosítja a bejelentőt, majd jogos kérelem esetén, a tanúsítványt visszavonja.

b) Amennyiben a visszavonási kérés jogtalan, az elutasítást közölni kell a bejelentővel, és tájékoztatni kell, hogy a kérésről feljegyzés készült.

c) A visszavonási kéréseket a Hitelesítés Szolgáltató az eseménynaplójában rögzíti. Az eseménynaplókat a Hitelesítés Szolgáltató biztonsági felelősei (SO-k) gyűjtik és archiválják.

d) A visszavonásra vonatkozó kérelmeket és jelentéseket hitelesíteni kell, és ellenőrizni kell, hogy hiteles forrásból származnak-e. Amennyiben ismeretlen fél kérelmezi a visszavonást, a visszavonási kérelem hitelességének megállapítása érdekében, a regisztrációs munkatárs (RO) döntése alapján, kiegészítő ellenőrzések végrehajtására kerülhet sor. A kiegészítő ellenőrzések csak a Hitelesítés Szolgáltató nyilvántartásában szereplő adatokra, és ezek érvényességére vonatkozhatnak.

e) Felelősségi szabályok a visszavont/visszavonandó tanúsítvány elfogadásából eredendő károkra:

- a visszavonási/felfüggesztési kérelem Hitelesítés Szolgáltatóhoz történő megérkezéséig az Aláíró felelős a felmerülő károkért,
- a visszavonási/felfüggesztési kérelem megérkezésétől az érvénytelen állapot tanúsítványtárban való megjelenésig (azaz a kérelem érvényességének megállapításáig) szintén a Hitelesítés Szolgáltató felelős a felmerülő károkért,
- amennyiben a felfüggesztési kérelmet a Hitelesítés Szolgáltató tudomásul vette, és a benyújtást követően 3 órán belül nem jelenik meg a tanúsítványtárban, akkor a benyújtás követő 3 óra eltelte után az érvénytelen állapot közzétételéig a Hitelesítés Szolgáltató felelős a felmerülő károkért,
- az érvénytelen állapot közzététele után a Hitelesítés Szolgáltató nem felelős az aláírás elfogadásából származó, felmerülő károkért.

4.9.3.1 A visszavonás jogkövetkezményei

f) Egy visszavont tanúsítványban szereplő aláírót (alanyt), és ahol ez alkalmazható az előfizetőt, tájékoztatni kell a tanúsítvány állapotának megváltozásáról.

g) Ha egy tanúsítvány véglegesen visszavonásra került (azaz nem felfüggesztésre), azt technikailag nem lehet érvényesre visszaállítani.

h) a Szolgáltatási Szerződés visszavonás következtében történő megszűnéséről az ÁSZF 5. 4. pontja rendelkezik

4.9.4 A visszavonási kérelemre vonatkozó kivárási idő

a) A Hitelesítés Szolgáltató a visszavonási kérelemre vonatkozó kivárási idő betartását úgy teljesíti, hogy a kivárási időn belül a tanúsítványt a szolgáltató nem visszavonja, hanem felfüggeszti, és a visszavonást később - esetleg összetettebb ellenőrzést Ld. 4.9.3 pontban) követően végzi el.

b) A Hitelesítés Szolgáltató a visszavonási, illetve felfüggesztési kérelem fogadását követő 3 órán belül megállapítja a kérelem érvényességét (a kérelmező jogosultságát), és érvényes kérelem esetén a tanúsítványállapot megváltozását a nyilvántartásában átvezeti.

c) Az a) pontban foglaltak teljesítését követő, 1 órán belül a hitelesítés-szolgáltató a módosított visszavonási listát közzéteszi.

4.9.5 A visszavonási eljárás maximális hossza

a) A Hitelesítés Szolgáltató a benyújtott visszavonási (felfüggesztési) kérelmeket a fenti 4.9.3 pontban foglaltak szerint feldolgozza, és az arra jogosult által benyújtott kérelmeket teljesíti.

b) A visszavonást megelőző felfüggesztési eljárást követően, a visszavonáshoz kapcsolódó tevékenységeket a Hitelesítés Szolgáltató a munkarendjében feltűntetett munkaidőben végzi. A Hitelesítés Szolgáltató ezek a tevékenységeket legfeljebb 4 munkaóra alatt végzi el.

4.9.6 A visszavonási információ ellenőrzésére az érintett felek részéről

a) Amennyiben az érintett felek kellő gondossággal kívánnak eljárni a tanúsítvány visszavonási állapotának ellenőrzésekor, akkor indokolt meggyőződniük a tanúsítvány visszavonási információ hitelességéről és sértetlenségéről is.

4.9.7 A visszavonási lista kibocsátás gyakorisága

a) A Hitelesítés Szolgáltató legalább 24 óránként bocsát ki tanúsítványokhoz tartozó visszavonási listákat („CRL” fájlokat). A Szolgáltató legkésőbb a lista érvényességi idejének lejártakor új CRL-t bocsát ki új érvényességi idővel, amely legfeljebb 24 óra lehet.

b) A tanúsítványok állapotára vonatkozó jelentős változás esetén (pl. egy tanúsítvány visszavonásakor) a Hitelesítés Szolgáltató 1 órán belül CRL-t bocsát ki.

4.9.8 A visszavonási lista előállítása és közzététele közötti idő maximális hossza

a) A visszavonási lista előállítása és közzététele között legfeljebb 1 óra telhet el (lásd 4.9.4 c).

4.9.9 Valósidejű tanúsítvány állapot ellenőrzés elérhetősége

a) A hitelesítés-szolgáltató valósidejű tanúsítvány állapot szolgáltatást is nyújt.

4.9.10 A valósidejű tanúsítvány állapot ellenőrzése

a) A Szolgáltató web-es tanúsítvány-lekérdezési lehetőséget és valós idejű visszavonási állapot-szolgáltatásokat is nyújt. Az elérési címek a jelen szabályzat 2.3 pontjában találhatók.

A Szolgáltató javasolja, hogy az OCSP szolgáltatás által kiadott elektronikusan aláírt válaszokat az elfogadó fél ellenőrizze. Érvénytelen OCSP válasz esetén az elfogadó fél a visszavonási listára támaszkodhat.”

4.9.11 A visszavonási hirdetmények egyéb elérhető formái

A Szolgáltató a korábbi LDAP lekérdezési szolgáltatást megszűntette.

4.9.12 A kulcs kompromittálódásra vonatkozó speciális követelmények

Megegyezik a tanúsítvány visszavonási követelményekkel.

4.9.13 A felfüggesztés körülményei

i) A Hitelesítés Szolgáltató köteles intézkedni a tanúsítvány felfüggesztéséről az alábbi esetekben:

- jogos felfüggesztési kérés esetén, és
- a szolgáltatással kapcsolatos - jogszabályban, a szolgáltatási szabályzatban vagy az Általános szerződési feltételekben [10] meghatározott - rendellenességről szerez tudomást, s ez a rendellenesség nem orvosolható,
- a Hitelesítés Szolgáltató tudomására jut, hogy a tanúsítványban foglalt adatok nem felelnek meg a valóságnak, vagy a magánkulcs nem az aláíró kizárólagos birtokában van,
- a felfüggesztést jogszabály kötelezővé teszi, vagy egy jogerős és végrehajtható hatósági határozat elrendeli.

4.9.14 Ki kérelmezheti a felfüggesztést

Tanúsítvány felfüggesztési kérelmet az alábbiak kezdeményezhetik:

- olyan személy, aki ismeri a visszavonási ellenőrző adatokat
- a hitelesítés-szolgáltató, esetlegesen a jogosultságot érintő ellenőrzések idejére, vagy azonnali visszavonás esetén (ld. 4.9.1 és 5.8 pontok szerint).

A Szolgáltató is kezdeményezheti egy tanúsítvány felfüggesztését a következő okok esetén:

- • Ha az Ügyfél vagy az Előfizető határidőig nem fizet.
- • Ha a Hitelesítés Szolgáltató valószínűsíti, hogy a tanúsítványban szereplő adatok nem felelnek meg a valóságnak,

4.9.15 A felfüggesztési kérelemre vonatkozó eljárás

A tanúsítványok felfüggesztésének eljárásai:

- a kérelem beadásának módja: telefonon keresztül a Hitelesítés Szolgáltató ügyfélszolgálatánál történik. A bejelentő a neve és az oktatási azonosítója, majd a titkos kérdésre bemondott válasz megadásával azonosítja magát. Kéri a felfüggesztést. Az ügyfélszolgálat munkatársa megállapítja a kérelem jogosságát. Jogos kérelem esetén, a figyelmeztet arra, hogy a felfüggesztésre kerülő tanúsítvány, sorszáma felkerül a visszavonási listára, így ezt követően a tanúsítvánnyal nem lehet visszaélni.
- eljárás abban az esetben, ha a bejelentő nem tudja jogosultságát igazolni. Ebben az esetben személyesen kell megjelennie a Hitelesítés Szolgáltató (RO-nál), a regisztrációs adatok ellenőrzésére.

4.9.16 A felfüggesztés maximális ideje

A felfüggesztéstől a visszaállításig – más néven az aktiválásig –, legfeljebb 5 munkanap telhet el. Ezt követően a még felfüggesztett tanúsítványokat a Hitelesítés Szolgáltató automatikusan visszavonja.

4.9.17 A felfüggesztésből visszaállítás körülményei

j) A Hitelesítés Szolgáltató köteles intézkedni a tanúsítvány visszaállításáról az alábbi esetekben:

- jogos visszaállítási/aktiválási kérés esetén.

4.9.18 Mikor szabad a felfüggesztésből visszaállítani a tanúsítványt?

A felfüggesztésből csak abban az esetben szabad a tanúsítványt visszaállítani, ha hitelt érdemlően megállapítható, hogy

- az aláírás-létrehozó adatot nem használhatta fel senki jogtalanul. Amennyiben ez nem állapítható meg, a tanúsítvány visszavonását kell kérni. Minden olyan kárért az alanyt terheli a felelősség, amely abból adódik, hogy az ő kérésére, a visszaállított tanúsítványt érvényesítette a Hitelesítés Szolgáltató.

- az aláírást létrehozó adat az aláíró kizárólagos birtokában van.

4.9.19 Ki kérelmezheti a felfüggesztésből visszaállítást?

Felfüggesztett tanúsítvány visszaállítására vonatkozó kérelmet az alábbiak kezdeményezhetik:

- olyan személy, aki ismeri a visszavonási ellenőrző adatokat, ebben a titkos kérdést.

4.9.20 A felfüggesztésből visszaállítási kérelemre vonatkozó eljárás

A tanúsítványok felfüggesztésből visszaállítás eljárásai:

- a kérelem beadásának módja: telefonon keresztül a Hitelesítés Szolgáltató ügyfélszolgálatánál történik. A bejelentő a neve és az oktatási azonosítója, majd a titkos kérdésre bemondott válasz megadásával azonosítja magát. Kéri a felfüggesztésből a visszaállítást. Az ügyfélszolgálat munkatársa megállapítja a kérelem jogosságát. Jogos kérelem esetén, a felhívja a figyelmet arra, hogy a visszaállított/aktivált tanúsítvány, sorszáma lekerül a visszavonási listáról, így ezt követően a tanúsítványt elektronikus aláírásra és aláírás ellenőrzésre is fel lehet használni.

- eljárás abban az esetben, ha a bejelentő nem tudja jogosultságát igazolni. Ebben az esetben személyesen kell megjelennie a Hitelesítés Szolgáltatónál (RO-nál), a regisztrációs adatok ellenőrzésére.

4.10 Tanúsítvány állapot szolgáltatások

4.10.1 Működési jellemzők

A Hitelesítés Szolgáltató a visszavont tanúsítványok listáját az általa kibocsátott tanúsítványokban meghatározott URL-en teszi elérhetővé. A megfelelő cím a 2.3 (A tanúsítványokra vonatkozó információk közzététele) pontban olvasható.

A Hitelesítés Szolgáltató a tanúsítvány-állapot lekérdezését OCSP szolgáltatással is biztosítja. Az elérési címek a jelen szabályzat 2.3 pontjában találhatók.

Az aktuális OCSP aláíró tanúsítványok és a kapcsolódó visszavonási listák a Szolgáltató tanúsítványtárában érhetőek el.

4.10.2 A szolgáltatás rendelkezésre állása

a) A hitelesítés-szolgáltatónak biztosítja a tanúsítványtár, valamint a szolgáltató által kibocsátott tanúsítványok használatára vonatkozó kikötések és feltételek folyamatos elérhetőségét, 99%-os rendelkezésre állás mellett, ahol az eseti szolgáltatás-kiesések nem haladhatják meg a 24 órát.

b) A Hitelesítés Szolgáltató biztosítja a visszavonási nyilvántartások és a visszavonás kezelési szolgáltatás legalább 99%-os rendelkezésre állását, az eseti szolgáltatás-kiesések nem haladhatják meg a 24 órát.

4.11 A tanúsítvány előfizetés vége

A Hitelesítés Szolgáltató által kiadott tanúsítványok érvényességi ideje és az adott tanúsítvány előfizetési ideje megegyezik.

Amennyiben az alany még a tanúsítványban feltüntetett érvényességi idő lejárta előtt fel kívánja mondani az előfizetést (a szolgáltatási szerződést), a Hitelesítés Szolgáltató – a visszavonásra vonatkozó szabályok betartása mellett -- visszavonja a tanúsítványt. A visszavonással egy időben szűnik meg a szolgáltatási szerződés.

4.12 Kulcs letétbe helyezése és visszaállítása

Az ügyfeleknek készített aláíró magánkulcsokról a Hitelesítés Szolgáltató nem készít másolatot és nem tárolja. (Ld. 1.1.7 pontot.)

A kulcsok kezelését a Hitelesítés Szolgáltató a kulcskezeléshez kapcsolódó dokumentációjában, határozza meg. (Ld. kulcsmenedzsment dokumentumok [19].)

5. Elhelyezési, irányítási és működtetési előírások

A biztonsági előírásokról általában:

A Szolgáltató megfelelő tervezéssel, megfelelő eszközök üzembe állításával, továbbá megfelelő, szakmailag képzett személyzettel, valamint kontrollok alkalmazásával gondoskodik arról, hogy a hitelesítés szolgáltatás az elvárt színvonalon működjön és kellő, az elismert szabványoknak megfelelő adminisztratív és irányítási eljárások kerüljenek alkalmazásra. Különösképpen:

a) A Hitelesítés Szolgáltató felelősséget vállal minden hitelesítési szolgáltatásáért, még akkor is, ha bizonyos funkciókat alvállalkozóknak ad ki. A harmadik felek felelősségét a Hitelesítés Szolgáltató egyértelműen meghatározza, és megfelelő szerződéses konstrukciókat és technikákat biztosít ahhoz, hogy a harmadik felek a Hitelesítés Szolgáltató által megkövetelt

összes ellenőrzés végrehajtására legyenek szorítva. A Hitelesítés Szolgáltató felelősséget vállal a szabályzatban és a megfelelő hitelesítési rendben ([9], [9a]) leírt szabályaira és ezek gyakorlati megvalósítására vonatkozóan.

b) A Hitelesítés Szolgáltató a biztonságkezeléshez szükséges informatika biztonsági infrastruktúrát folyamatosan fenntartja. A hitelesítés szolgáltatási rendszer működtetéséért az a Hitelesítés Szolgáltató a hitelesítés szolgáltatásért általánosan felelős vezetője a felelős. A biztonság szintjére hatást gyakorló bárminemű változtatást a Hitelesítés Szolgáltató felső vezetésének kell jóváhagynia.

c) A Hitelesítés Szolgáltató gondoskodik az informatikai biztonság fenntartásáról akkor is, ha a szolgáltatói funkciók egy körülhatárolt részének az elvégzésével egy más szervezetet bízott meg. A tanúsítványkiadó (CA), ebben a tanúsítványtár és ügyfélnyilvántartás működtetését, a tanúsítványállapot információk nyilvánossá tételét (LDAP szerverről történő lekérdezés lehetősége), tanúsítvány visszavonási lista információk biztosítását (CRL), valamint a viszontazonosítási szolgáltatás ellátását, továbbá a munkaidőn túli felfüggesztési eljárás kezelését, a Hitelesítés Szolgáltatóval megkötött szerződés és felelősségvállalási nyilatkozatok alapján, egy külső szervezet végzi.

A Hitelesítés Szolgáltató és a MÁV Informatika Kft., jelenleg MÁV Informatika Zrt. (a külső szervezet; továbbiakban: Tanúsítványkiadó) által megkötött szolgáltatási szerződés biztosítja mindazon funkcionális és garanciális feltételeket, amelyek a jelen szolgáltatási szabályzatban meghatározott minőségű szolgáltatás folyamatos biztosításához szükségesek.

A Tanúsítványkiadó a saját, biztonságos, hitelesítés szolgáltatási célokra kialakított informatikai rendszerében nyújtja a fent megnevezett funkciókat, illetve működteti az informatikai elemeket, biztosítja a megfelelő infrastruktúrát. A szerződés alapján kialakított informatikai rendszer megfelelő módon el van választva a Tanúsítványkiadó egyéb szolgáltatásaitól.

d) A Hitelesítés Szolgáltató felső vezetősége felelős a jelen szabályzat betartásáért. A Hitelesítés Szolgáltató biztonsági műveletei el vannak különítve az egyéb műveletektől. A Hitelesítés Szolgáltató biztonsági műveleteivel kapcsolatos felelősségek közé tartoznak az alábbiak:

- az informatikai biztonság vonatkozásában:
    - üzemeltetési eljárások és felelősségek,
    - erőforrás gazdálkodás,
    - hálózat menedzselés,
    - adathordozó eszköz kezelése és biztonsága,
    - biztonsági rendszerek tervezése és elfogadása,
    - folyamatos működés biztosítása,
    - káros szoftver elleni védelem,
    - kockázatkezelés,

- fizikai biztonság,

- továbbá kifejezetten a hitelesítés szolgáltatásra vonatkozóan
  - üzemeltetési felelősség,
  - PKI CA/RA biztonsági rendszerek tervezése és elfogadása,
  - PKI CA rendszer folyamatos működésének biztosítása,
  - a biztonsági napló aktív felügyelete, eseményelemzések és nyomkövetések,
  - adat és szoftver csere, valamint változásmenedzsment.

A fenti felelősségeket alapján a Hitelesítés Szolgáltatónál dolgozó, nem szakértő üzemeltető személyzet csak megfelelő felügyelet és a felelősségre vonhatóságot biztosító ellenőrzési rend mellett hajthatja végre.

Az értékek osztályozása, minősítése és kezelése

A Szolgáltató gondoskodik arról, hogy eszközei és információi megfelelő szintű védelemben részesüljenek.

A Szolgáltató valamennyi informatikai értékéről leltárt vezet, ezek védelmi követelményeit osztályokba kell sorolja, és minősíti ezeket a kockázatelemzés eredményével, a kockázatkezelés során előállított maradványkockázatokkal összhangban.

5.1 Fizikai előírások

A Szolgáltató gondoskodik arról, hogy a kritikus szolgáltatásokhoz történő fizikai hozzáférés ellenőrzött legyen, és a kritikus szolgáltatások eszközeinek fizikai kockázatát minimalizálja.

5.1.1 Feladatmegosztás

Az 5. c) pontban megadott funkciókat biztosító Tanúsítványkiadó üzemi területét (szerver szoba, raktárak) megfelelő biztonsági berendezésekkel (beléptető-rendszer, tűzjelző, riasztó, stb.) védik, és oda illetéktelenek nem léphetnek be. A zárt helyiségekbe csak a Tanúsítványkiadó dolgozói, illetve az egyedi engedéllyel rendelkezők – beleértve a Szolgáltató biztonságért felelős munkatársait (SO-kat) – léphetnek be. Munkavégzés céljából átmenetileg, felügyelet alatt, idegen személyek is tartózkodhatnak a helyiségekben.

A Hitelesítés Szolgáltató számára fenntartott és működtetett/menedzselt szolgáltatási rendszer el van különítve a Tanúsítványkiadó által biztosított egyéb szolgáltatásoktól, külön biztonsági zónában üzemel. A Hitelesítés Szolgáltató ügyfélnyilvántartása olyan biztonsági feltételek között (elkülönített zónában) üzemel, amelyet a MÁV Informatika Zrt. üzemeltet, de ezt a Hitelesítés Szolgáltató felügyeli.

A regisztrációs tevékenység infrastruktúrája a Hitelesítés Szolgáltató telephelyén van biztosítva. A regisztrációs helyiség zárt helyiség, megfelelő beléptetési eljárással van védve, és oda illetéktelenek nem léphetnek be. A helyiségekbe csak a Hitelesítés Szolgáltató kijelölt munkatársai (RO, SO), illetve az egyedi engedéllyel rendelkezők léphetnek be. Munkavégzés céljából átmenetileg, felügyelet alatt, idegen személyek is tartózkodhatnak a helyiségekben.

A kulcsmenedzsment adott szinten megosztott a két társaság között. A titkok-megosztást, a kulcsceremóniát, és az eljárásokat és a kapcsolódó adatkezelést a kulcsmenedzsment dokumentumok [19] szabályozzák.

A Hitelesítés Szolgáltató és a MÁV Informatika Zrt. által megkötött szerződés, valamint a felelősségvállalási nyilatkozatok, továbbá a társaságok szabályozási dokumentumai garantálják a szolgáltatáshoz kapcsolódó fizikai és informatikai infrastruktúra megfelelő (biztonságos) felhasználását. Ezen dokumentumok alapján valósulnak meg az alábbi (5.1.2-5.1.9) pontokban meghatározott biztonsági megoldások.

5.1.2 A telephely elhelyezése és szerkezeti felépítése

A hitelesítés szolgáltatás i általános tevékenységekkel kapcsolatosan a Hitelesítés Szolgáltató

a) biztosítja az értékek elvesztésének, sérülésének, és kompromittálódásának, valamint a működési tevékenységek megzavarásának elkerülését,

b) érvényre juttatja az előírásokat és más adminisztratív intézkedéseket az információ és az információ feldolgozó berendezések kompromittálódásának, illetve ellopásának elkerülése érdekében.

Tanúsítvány előállítással, alanyok kriptográfiai hardver eszközzel való ellátásával, visszavonás kezeléssel kapcsolatosan a Hitelesítés Szolgáltató

c) fizikai védelmet biztosít a tanúsítvány előállítás, az alanyok kriptográfiai hardver eszközeinek tárolása és szállítása, illetve a visszavonás-kezelés szolgáltatások köré; ehhez biztosítja az egyértelműen meghatározott, működtetett és menedzselt biztonsági eszközök alkalmazását,

d) érvényt szerez azon előírásoknak és más adminisztratív intézkedéseknek, melyek a Hitelesítés szolgáltató szolgáltatásokkal kapcsolatos berendezéseinek, információinak, adathordozóinak és szoftvereinek jogosulatlan elvitelét akadályozzák meg.

5.1.3 Fizikai hozzáférés

a) A hitelesítés szolgáltatás nyújtásával összefüggésben használt elektronikus aláírási termékeket, illetve azokat a helyiségeket, amelyekben a szolgáltató ilyen termékeket helyez el, a jogosulatlan hozzáféréstől a Szolgáltató fizikailag is védi.

b) A Szolgáltató biztosítja, hogy a fenti a) pontban említett helyiségekbe csak olyan személyek jussanak be, akik erre jogosultak.

5.1.4 Áramellátás és légkondicionálás

A Szolgáltató által igénybevett infrastruktúrája biztosítja a folyamatos/szünetmentes áramellátást és a rendszer elemeinek üzemeltetéséhez szükséges klíma viszonyokat.

5.1.5 Beázás és elárasztódás veszély kezelése

A Szolgáltató által igénybevett infrastruktúra beázás és elárasztódás ellen védett.

5.1.6 Tűzmegelőzés és tűzvédelem

A Szolgáltató által igénybevett helyiségekben a tűzmegelőzés és tűzvédelem biztosított. A Tanúsítványkiadó szervereinél tűzvédelmi rendszer működik.

5.1.7 Adathordozók tárolása

a) Szolgáltató az adathordozó eszközöket biztonságosan kezeli azok sérülése, ellopása és jogosulatlan hozzáférés elleni védelme érdekében.

b) Az adathordozó eszközök biztonságos kezelése a Szolgáltató szabályzataiban megfogalmazott követelmények szerint történik.

5.1.8 Hulladék megsemmisítése

a) Az érzékeny adatokat tartalmazó adathordozó eszközöket – amennyiben azokra már nincs szükség – a Szolgáltató biztonságosan megsemmisíti. A következő eljárások valósulnak meg:
   - a papíralapú dokumentumokat aprítógéppel felaprítják,
   - a hajlékony lemezeket a házából való kibontás után aprítógéppel felaprítják,
   - egyéb más mágneses adathordozókat, demagnetizálás után összetörik,
   - egyéb más adathordozókat összetörik.

5.1.9 A mentési példányok fizikai elkülönítése

A tanúsítványkiadó rendszer (CA; beleértve a kapcsolódó alrendszereket is, mint például a naplózás rendszerét), valamint a regisztrációs rendszer (RA; beleértve például a kommunikációs rendszert is) biztonság-kritikus adatainak és szoftvereinek mentési példányait biztonsági kategóriánként, személyi felelősség mellett, a Hitelesítés Szolgáltató és a Tanúsítványkiadó telephelyenként, biztonsági zónáiban tárolja.

5.2 Eljárásbeli előírások

A Szolgáltató eljárásbeli előírásainak megfelelnek a személyes adatok védelmére, valamint a jogszabályban nevesített, vagy az aláíróval illetve az előfizetővel kötött szerződésben meghatározott titokfajták kezelésére vonatkozó jogszabályi és mértékadó dokumentumokban meghatározott, a legjobb gyakorlatot tükröző műszaki-szervezési előírásoknak. (lásd 9.15 a)

A Szolgáltató gondoskodik arról, hogy rendszereit biztonságosan, szabályszerűen, a meghibásodás minimális kockázata mellett üzemeltesse. Ennek keretében

a) A személyzetnek olyan adminisztratív és kezelési eljárásokat és folyamatokat kell végeznie, amely szinkronban van a Szolgáltató informatika biztonság kezelési (ellenőrzési és üzemeltetési) eljárásaival (lásd 5. e. pontot).

5.2.1 Bizalmi munkakörök

a) A Szolgáltató szolgáltatási és informatikai biztonsági megfelelése érdekében bizalmi munkaköröket és felelősségeket határozott meg, amelyeket megbízólevéllel, illetve a munkaköri leírásokban is dokumentál.

b) A bizalmi munkakör úgy jön létre, hogy egy munkakörhöz bizalmi szerepkört rendel a

Szolgáltató ügyvezetője.

c) Bizalmi szerepkörök az alábbiak:

- A hitelesítés szolgáltatásért általánosan felelős vezető (rövidítve: Hitelesítés szolgáltatás vezető): felelős a jelen szabályzat megfelelőségéért, és az ebben foglaltak szerinti szolgáltatás nyújtásáért, a vezetői kontrollok érvényesítéséért, az információs rendszer működéséért, a szolgáltatatási tevékenységben dolgozó munkatársakért és alvállalkozókért.

- Biztonsági felelős (SO)[4]: a szolgáltatás biztonságáért, a biztonsági irányelvek és szabályzatok érvényre juttatásáért általánosan felelős személy, felelős az archivált adatok eltárolásáért.

- Rendszeradminisztrátor (sys-admin): az informatikai rendszer tervezését, telepítését, konfigurálását, karbantartását végző, valamint az informatikai rendszer folyamatos üzemeltetését, mentését és helyreállítását biztosító személy. Felelős a hitelesítés szolgáltatási információs rendszer működési paramétereinek a beállításáért, beleértve az elvárt működtetési feltételek biztosítását is.

- Rendszerüzemeltető (operator): az informatikai rendszer folyamatos üzemeltetését, mentését, valamint az archiválást végző személy.

- Független rendszervizsgáló (auditor): a hitelesítés-szolgáltató naplózott, illetve archivált adatállományát vizsgáló, a hitelesítés-szolgáltató által a szabályszerű működés érdekében megvalósított kontroll intézkedések betartásának ellenőrzéséért, a meglévő eljárások folyamatos vizsgálatáért és monitorozásáért felelős személy.

- Regisztrációs felelős (RO): a szolgáltatás igénybe vételéhez kapcsolódó tájékoztatásért, a személyazonosításért, a személyadatok kezeléséért, az aláírást-létrehozó eszköz átadásáért, a tanúsítványok előállításának, kibocsátásának kezdeményezéséért, a tanúsítványok biztonságos visszavonásának és felfüggesztésének jóváhagyásáért felelős személy.

- Megbízott regisztrációs munkatárs (XRO): szolgáltatás igénybe vételéhez kapcsolódó tájékoztatásért, a személyazonosításért, a személyadatok kezeléséért, az aláírást-létrehozó eszköz átadásáért, a tanúsítványok előállításának, kibocsátásának kezdeményezéséért felelős személy.

- Tanúsítvány-profilt menedzselő adminisztrátor (cert-admin): megtervezi a tanúsítványok szerkezetét és tartalmát.

- Kártya-profilt menedzselő adminisztrátor (sc-admin): megtervezi a chipkártyák adatszerkezetét és tartalmát, megtervezi és beállítja a biztonsági paramétereket, beleértve az elvárt működtetési feltételek biztosítását is.

- Kulcsmenedzser (crypto officer): a kriptográfiai eszközök kulcsainak a kezelését végzi.

A Tanúsítványkiadó bizalmi munkakörei össze vannak rendelve a fenti szerepkörökkel.

[4] A 3/2005. (III. 18.) IHM rendelet szerinti megjelölés szerint megfelel: a biztonsági tisztviselőnek.

d) A Szolgáltató üzemeltetési eljárások alapján irányítja és felügyeli azokat a bizalmi és adminisztratív feladatokat, amely hatást gyakorol a hitelesítési szolgáltatásokra. A Szolgáltató ezeket az eljárásokat betartja és betartatja.

5.2.2 Az egyes feladatokhoz szükséges személyzeti létszámok

a) A Szolgáltató biztosítja a biztonságos működés beindításához, fenntartásához és esetleges leállításához szükséges szakképzett létszámot.

b) A kizárólagosan védett környezetben, legalább két, kulcsmenedzser szerepkört betöltő személy együttes részvételével, más személyek jelenlétét kizárva kerülhet sor az alábbi funkciók végrehajtására:

a Hitelesítés Szolgáltató

- saját szolgáltatói kulcsának előállítása (6.1.1),
- szolgáltatói magánkulcsának mentése (6.2.4),
- szolgáltatói magánkulcsának visszaállítása (6.2.2),
- szolgáltatói magánkulcsának megsemmisítése (6.2.10).

5.2.3 Az egyes szerepkörökhöz kapcsolódó elvárt azonosítás és hitelesítés

c) A szolgáltatást ellátó dolgozók a regisztrációval és tanúsítvány kezeléssel kapcsolatos kritikus alkalmazások használata előtt megfelelő azonosítási és hitelesítési eljáráson esnek át.

d) Egyes biztonságilag kritikusnak minősített munkafolyamatok esetén, az egyes szerepkörökben dolgozók csak chipkártyás azonosítással végezhetik a munkájukat.

e) A Szolgáltatáshoz tartozó regisztrációs helyiségbe csak az arra felhatalmazottak léphetnek be. Számunkra névre szóló biztonsági kulcs van rendszeresítve.

f) A Hitelesítés Szolgáltatáshoz tartozó szerverterembe a beléptetés chipkártyával történik. A belépéshez személyazonosítás mellett, a Tanúsítványkiadó biztosítja a körülményeket.

g) A Szolgáltatáshoz ügyfélnyilvántartását kezelő adatbázisrendszer fizikailag el van különítve a Hitelesítés Szolgáltatás más szervereitől. A Hitelesítés Szolgáltatáshoz tartozó szerverek el vannak különítve a helyiségben működő, egyéb szerverektől. A Szolgáltató szervereinek biztonsági felügyeletét a Szolgáltató biztonsági felelősei látják el.

5.2.4 Egymást kizáró munkakörök

a) A bizalmi munkakörök közötti személyi átfedések megakadályozására vonatkozóan a Szolgáltató biztosítja, hogy:

- a biztonsági felelős (SO) szerepkört ellátó dolgozók nem tölthetik be az alábbi

szerepköröket:

- o független rendszervizsgáló (auditor),
- o rendszeradminisztrátor (sys-admin) valamint a rendszerüzemeltető (operator),
- o regisztrációs munkatárs (RO, XRO),
- o tanúsítvány-profilt menedzselő adminisztrátor (cert-admin), kártya-profilt menedzselő adminisztrátor (sc-admin), kulcsmenedzser (crypto officer)

- a független rendszervizsgáló szerepkört ellátó dolgozók nem tölthetik be más bizalmi személy szerepkörét
- az informatikai rendszerért általánosan felelős vezető nem láthatja el a biztonsági tisztviselő, illetve a független rendszervizsgáló feladatait.

5.3 Személyzetre vonatkozó előírások

a) A Szolgáltató gondoskodik arról, hogy a szolgáltatásban dolgozókhoz kapcsolódó személyzeti gyakorlat fokozza és támogassa a Szolgáltató működésének megbízhatóságát.

5.3.1 Képzettségre, gyakorlatra és biztonsági ellenőrzésre vonatkozó követelmények

a) A hitelesítés szolgáltatásban dolgozó munkatársak rendelkeznek az elektronikus aláírással kapcsolatos szolgáltatások nyújtásához szükséges és megfelelően naprakész tudással és tapasztalattal.

b) A Hitelesítés Szolgáltató valamennyi bizalmi munkakört betöltő munkatársa független minden olyan ütköző érdektől, amely hátrányosan érinthetné a Hitelesítés Szolgáltató tevékenységeinek semlegességét.

c) A Hitelesítés Szolgáltató munkatársai munkaköri és szerepköri leírásokkal rendelkeznek. A szerepkörök biztosítják a hitelesítés szolgáltatás és az egyéb tevékenységek ellátásának a szétválasztását. A leírások meghatározzák az elvégzendő feladatok érzékenységét, a feladatok, valamint a hozzáférési jogosultságok, a speciális körülmények, ezek között a háttér-ellenőrzés, az alkalmazott képzettség és tudatosság alapján.

5.3.2 Előélet vizsgálatára vonatkozó eljárások

a) A Szolgáltató a bizalmi szerepkörbe kinevezett személyek büntetlen előéletét ellenőrzi.

5.3.3 Kiképzési követelmények

a) Hitelesítés szolgáltatási feladatokat csak olyan személy láthat el, aki képzésen vett részt, és a

hitelesítés szolgáltatásért általánosan felelős vezető felelősége alapján megfelel

- a nyilvános kulcsú infrastruktúra elméletéből,
- a rendszer használatáról,
- a regisztrációs, tanúsítási és visszavonási eljárásrendekről,
- az egyes tevékenységek jogi következményeiről,
- az informatikai biztonsági követelményekről,
- a jelen szabályzat és a megfelelő hitelesítési rend ([9], [9a]) és alkalmazásának jelentőségéről.

5.3.4 Továbbképzési gyakoriságok és követelmények

A rendszerben történő lényeges változást követően a szolgáltatásban dolgozó személyek képzést kapnak a változás által érintett területen.

A hitelesítés szolgáltatásért felelős vezető biztosítja, hogy a technológiai és technikai fejlesztések követése a rendszeres, legalább az éves továbbképzések során érvényesüljön.

5.3.5 Munkabeosztás körforgásának gyakorisága és sorrendje

Körforgást a munkabeosztások között a Szolgáltató nem alkalmaz.

5.3.6 Felhatalmazás nélküli tevékenységek büntető következményei

Az ide vonatkozó szabályokat, a hatályos jogszabályok és a Hitelesítés Szolgáltató szervezeti és működési szabályozása, valamint az informatikai biztonsági szabályozás, továbbá a megfelelő szerződések szerint, a Hitelesítés Szolgáltató érvényesíti. (Felelős: a hitelesítés szolgáltatásért általánosan felelős vezető.)

5.3.7 Szerződéses viszonyban foglalkoztatottakra vonatkozó követelmények

Az ide vonatkozó szabályokat, a hatályos jogszabályok és a Hitelesítés Szolgáltató szervezeti és működési szabályozása, valamint az informatikai biztonsági szabályozás, továbbá a megfelelő szerződések szerint, a Hitelesítés Szolgáltató érvényesíti. (Felelős: a hitelesítés szolgáltatásért általánosan felelős vezető.)

5.3.8 A személyzet számára biztosított dokumentációk

a) A hitelesítés szolgáltatás ban dolgozók számára biztosítandó dokumentációk tartalmazzák a biztonságos üzemeltetéshez szükséges ismereteket.

5.4 Naplózási eljárások

A Hitelesítés Szolgáltató a biztonságos környezet fenntartása érdekében eseménynaplót vezet, és ellenőrző rendszert használ a megfelelő hitelesítési rend ([9], [9a]) előírásai szerint.

5.4.1 A tárolt események típusai

A hitelesítés-szolgáltató általános tevékenységével kapcsolatosan:

a) A Hitelesítés Szolgáltató rendszerei naplózzák az alábbi eseményeket:

- a működtető rendszerek környezetében bekövetkező, illetve a kulcsok és tanúsítványok kezelésével kapcsolatos események,
- a naplózási funkció elindítása és leállítása,
- a naplózási paraméterek megváltoztatása,
- a naplózás tárolási hibája miatt végzett tevékenységek.

A regisztrációval kapcsolatosan:

b) A Hitelesítés Szolgáltató gondoskodik arról, hogy naplózásra kerüljön valamennyi regisztrációval kapcsolatos esemény, köztük a tanúsítvány megújításra vonatkozó kérelmek is. (Felelős: RO)

A tanúsítvány előállítással kapcsolatosan:

c) A Hitelesítés Szolgáltató naplózza a saját szolgáltatói kulcsai életciklusával kapcsolatos összes eseményt (felelős: kulcsmenedzser, sc-admin), továbbá

d) a saját tanúsítványai életciklusával kapcsolatos összes eseményt, és az általa kibocsátott tanúsítványok életciklusával kapcsolatos összes eseményt (felelős: sys-admin).

Az alanyok kriptográfiai hardver eszközzel való ellátásával kapcsolatosan:

e) A Hitelesítés Szolgáltató naplózza az általa gondozott kulcsok életciklusával kapcsolatos eseményeket, valamint a kriptográfiai hardver eszközök felkészítésével (megszemélyesítésével) és átadásával kapcsolatos valamennyi eseményt (felelős: kulcsmenedzser, sc-admin).

A visszavonás és felfüggesztés kezeléssel kapcsolatosan:

f) A Hitelesítés Szolgáltató gondoskodik arról, hogy a visszavonás és a felfüggesztés kezeléssel kapcsolatos összes kérés és jelentés naplózva legyen (Felelős: RO)

5.4.2 A napló fájl feldolgozásának gyakorisága

A Hitelesítés Szolgáltató folyamatos felügyelő és riasztó eszközöket működtet annak érdekében, hogy a képes legyen felismerni, regisztrálni az erőforrásaihoz történő hozzáférésre irányuló jogosulatlan és/vagy szabálytalan próbálkozásokat, illetve képes legyen időben reagálni ezekre.

A visszavonás állapotokat kezelő alkalmazás hozzáférés ellenőrzést végez a visszavonás állapot információ módosítására irányuló próbálkozások esetében.

a) A Hitelesítés Szolgáltató auditora naponta kiértékeli a napló fájlokat és ennek alapján jelentést készít a menedzsment számára.

5.4.3 A naplófájl megőrzési időtartama

A naplóadatokat a Hitelesítés Szolgáltató archiválja. Az archívum megőrzési idejét lásd az 5.5.2 pontban.

5.4.4 A naplófájl védelme

a) A naplózott adatállomány tartalmazza a naplózott esemény bekövetkezésének dátumát és pontos idejét, az esemény követhetőségéhez, rekonstruálásához szükséges adatokat, az események kiváltásában közreműködő felhasználó vagy más érintett személy nevét.

b) A naplózási rendszer regisztrálja a naplózásra vonatkozó módosítási kísérletet.

c) A naplózott adatállomány védelmét, a tanúsítványokhoz kapcsolódó eljárásoknál a szolgáltatói kulccsal történő elektronikus aláírás, valamint az archiválási eljárás biztosítja, amelynek következében a napló minden bejegyzése védetté válik a módosítástól. A Hitelesítés Szolgáltató biztosítja, hogy a napló tartalmához csak arra feljogosított személy, elsősorban a független rendszervizsgáló férhessen hozzá.

d) A napló kezelését a Hitelesítés Szolgáltató úgy biztosítja, hogy a napló megsemmisítése, a napló bejegyzéseinek törlése, módosítása, a bejegyzések sorrendjének bármilyen módon történő megváltoztatása kizárható legyen. (Felelős: SO)

5.4.5 A naplófájl archiválási eljárásai

A napló fájl napi rendszerességgel archiválásra kerül, két példányban.

5.4.6 A naplózás adatgyűjtési rendszere (belső vagy külső)

A naplózás komplex, a teljes rendszer biztonsági eseményeit kezelő és magába foglaló rendszer.

5.5 Adatok archiválása

A Hitelesítés Szolgáltató gondoskodik arról, hogy az általa kibocsátott tanúsítványokra vonatkozó minden lényeges adat rögzítésre és megőrzésre kerüljön, különösen jogi eljárásokhoz bizonyíték nyújtása érdekében.

5.5.1 Az archivált adatok típusai

a) A Hitelesítés Szolgáltató gondoskodik arról, hogy típusonként archiválásra kerüljön az összes regisztrációs információ, beleértve az alábbiakat is:

- a kérelmező által a regisztráció támogatása céljából benyújtott dokumentumokat,
- az azonosító dokumentumok egyedi azonosító adatai (például a kérelmező személyi igazolvány száma),
- a kérelmező és azonosító dokumentumok (beleértve az aláírt, előfizetővel kötött megállapodást (lásd 4.1.2 c) pontja)
- az előfizetővel kötött megállapodás esetleges egyedi választásai (például a tanúsítvány közzétételéhez történő hozzájárulás);
- a kérelmet elfogadó regisztrációs ügyintéző azonosítója;
- az azonosító dokumentumok ellenőrzéséhez használt módszer és adatbázis;
- a Hitelesítés Szolgáltató és a tanúsítványkiadó rendszer neve (cn).

5.5.2 Az archívum megőrzési időtartama

a) A Hitelesítés Szolgáltató a tanúsítványokkal kapcsolatos elektronikus információkat - beleértve az azok előállításával összefüggőket is - és az ahhoz kapcsolódó személyes adatokat legalább a tanúsítvány érvényességének lejártától számított 10 évig, illetőleg az elektronikus aláírással, illetve az azzal aláírt elektronikus dokumentummal kapcsolatban felmerült jogvita jogerős lezárásáig őrzi meg.

b) Az a) pontban meghatározott adatokon kívüli naplózott adatokat a keletkezésüktől, a jelen szabályzat és annak módosításait pedig hatályon kívül helyezésétől számított 10 évig őrizni meg.

c) a megfelelő hitelesítési rend ([9], [9a]) meghatározásain túlmenően egyéb naplóbejegyzéseket a Hitelesítés Szolgáltató nem őriz meg.

5.5.3 Az archívum védelme

a) A Szolgáltató az archivált adatállomány minden bejegyzését védi a jogosulatlan módosítástól, törléstől. Az archivált adatállományt a megsemmisítésétől, és a jogosulatlanul hozzáféréstől a Hitelesítés Szolgáltató adminisztratív szabályozása védi.

5.5.4 Az archívum mentési folyamatai

Az archivum mentése naponta 2 példányban történik egyszer írható CD adathordozóra. Ezen kívül heti, havi mentésekre és hosszú távú archiválásokra kerül sor. Az archivált adatok adathordozóit a Hitelesítés Szolgáltató biztonságos környezetben tárolja, külön helyen.

5.5.5 Az adatok időbélyegzésére vonatkozó követelmények

Az archivált adatokhoz a HItelesítés Szolgáltató egy hiteles időbélyeget kapcsol.

5.5.6 Az archívum gyűjtési rendszere (belső vagy külső)

A külső regisztrációs pontokon keletkezett iratokat a regisztrációt végző munkatársak (RO, XRO) bizalmasan tárolják és őrzik. Az elektronikus másolati példányban létező iratok elektronikus üzenet formájában kerülnek a Hitelesítés Szolgáltató központi adattárba.

5.5.7 Archív információk hozzáférését és ellenőrzését végző eljárások

A Hitelesítés Szolgáltató biztosítja az archív információhoz történő hozzáférést és ellenőrzést, az alábbiak szerint:

a) Az archívumhoz Hitelesítés Szolgáltató ügyfélszolgálatán keresztül biztosít hozzáférést.

b) A jogosultságot és a hozzáférést a Hitelesítés Szolgáltató minden esetben ellenőrzi és nyilvántartja.

c) A Hitelesítés Szolgáltató biztosítja az archivált adatok megjelenítéséhez és elolvasásához szükséges eszközöket.

5.6 Kulcscsere

A Hitelesítés Szolgáltató által nem támogatott!

5.7 Felülhitelesítés

A Hitelesítés Szolgáltató hitelesítés szolgáltatását, a magyar Közigazgatási Gyökér Hitelesítés-szolgáltató (ld. a 1.3.5 pontban) felülhitelesíti.

A Közigazgatási Gyökér Hitelesítés-szolgáltató a felülhitelesítéssel (egy tanúsítvány kiadásával) igazolja, hogy, a Szolgáltató az elektronikus aláírásról szóló 2001. évi XXXV. törvény 6. § (1) bekezdés a) pontja szerinti szolgáltatást olyan módon nyújtja, hogy az általa kibocsátott tanúsítványok megfelelnek a 194/2005 (IX. 22.) Korm. rendelet 6-7. §, illetve 8-10. § szerinti közigazgatási követelményeknek és teljesítik a 11. § (9) bekezdés felhatalmazása alapján kiadott, és a 11. § (1) bekezdés alapján hatósági nyilvántartásba vett miniszteri ajánlások, valamint a KGyHSz Hitelesítési Rendjének előírásait.

5.8 Kompromittálódást és katasztrófát követő helyreállítás

A Hitelesítés Szolgáltató a megfelelő hitelesítési rend ([9], [9a]) előírásai szerint gondoskodik arról, hogy katasztrófa esetén, beleértve a saját szolgáltatói magánkulcsának kompromittálódását, illetve kritikus szoftver/hardver komponenseinek meghibásodását is, az üzemeltetés a lehető legrövidebb időn belül helyreálljon.

5.8.1 Váratlan esemény és kompromittálódás kezelési eljárások

a) A Hitelesítés Szolgáltató a rendkívüli üzemeltetési helyzetek esetére (különösen a kompromittálódás és a katasztrófa bekövetkezésére) olyan eljárást alkalmaz, amely lehetővé teszi a megbízható szolgáltatás mielőbbi helyreállítását.

5.8.2 Meghibásodott számítási erőforrások, szoftverek és/vagy adatok

a) A Hitelesítés Szolgáltató a biztonsági események és hibás működések által okozott kárt eseményjelentés és eseménykezelési gyakorlati eljárások használatán keresztül minimalizálja.

5.8.3 Magánkulcs kompromittálódása esetén követendő eljárások

a) Saját magánkulcsának kompromittálódása esetén a Hitelesítés Szolgáltató az alábbiakat vállalja:

   - A kompromittálódásról tájékoztatja az összes aláírót, előfizetőt, érintett felet és egyéb olyan más hitelesítés-szolgáltatót, amellyel kapcsolata van.

   - Jelzi, hogy az adott szolgáltatói kulcs felhasználásával kiadott tanúsítványok és visszavonási állapot információk már nem érvényesek.

   - Szükség esetén új kulccsal látja el az ügyfeleket és a szolgáltatói egységet, továbbá az ügyfélek számára új tanúsítványt bocsát ki.

   - Megteszi a szükséges lépéseket a kompromittálódás megismétlődése ellen.

b) Az aláíró illetve az előfizető számára kibocsátott tanúsítványhoz tartozó magánkulcs kompromittálódása esetén a Hitelesítés Szolgáltató az alábbiakat vállalja::

1. A kompromittálódásról (a visszavonás kezelés, illetve visszavonás állapot szolgáltatásokon keresztül) tájékoztatja az összes érintettet.

5.8.4 Működés folyamatosságának biztosítása katasztrófát követően

Természeti vagy más katasztrófát követően, illetve a Hitelesítés Szolgáltató berendezéseinek meghibásodása esetén Szolgáltató a következő szolgáltatások legfeljebb 3 munkanapon belüli elindítását vállalja:

- visszavonáskezelés-szolgáltatás,
- visszavonási állapot közzététele szolgáltatás.

Minden egyéb szolgáltatás elindítását Hitelesítés Szolgáltató 5 munkanapon belül vállalja.

5.9 Hitelesítés szolgáltató vagy regisztrációs szervezet leállítása

A Hitelesítés Szolgáltató a jogszabályokban előírtaknak megfelelően gondoskodik a szolgáltatásainak megszüntetéséből származó, az aláírókat, előfizetőket és az érintett feleket érintő potenciális zavar minimalizálásáról, továbbá a jogi eljárásokhoz szükséges tanúsítvány-nyilvántartások fenntartásáról.

A Hitelesítés Szolgáltató általános tevékenységével kapcsolatosan:

a) Mielőtt a Szolgáltató leállítja szolgáltatásait, legalább az alábbi eljárásokat hajtja végre:

1. A Hitelesítés Szolgáltató legalább 60 nappal a leállítás előtt értesíti az általa kibocsátott és még vissza nem vont tanúsítványokban aláíróként megjelölt személyeket és az Eat. [1] által kijelölt Hatóságot. Az értesítés tartalmazza annak a vele azonos besorolású hitelesítés szolgáltató megjelölését, amely átveszi a tanúsítvány visszavonási listákat, a visszavonási állapot nyilvántartásokat (felfüggesztés és visszavonás információkat), a visszavont tanúsítványokkal kapcsolatos minden adatot (naplófájlokat, megőrzési időket), továbbá a visszavont tanúsítványokhoz kapcsolódó személyes adatokat, a nyilvános szabályozási dokumentumokat, valamint az aláírás ellenőrző adatokat,

2. Amennyiben a Hitelesítés Szolgáltató az értesítésben nem jelölne meg egy hitelesítés szolgáltatót (a fenti 1. pont szerint), a Hatóság jelöli ki azt.

3. Az értesítés időpontjától kezdve a hitelesítés-szolgáltató nem bocsát ki új tanúsítványt.

4. A Hitelesítés Szolgáltató legalább 20 nappal a leállítás előtt visszavonja az általa kibocsátott és még vissza nem vont tanúsítványokat, de nyilvánosságra hozatali kötelezettségének (ld. 2.3 pontot) egészen a leállításig továbbra is eleget tesz.

5. A Hitelesítés Szolgáltató a fenti 1. pontban megjelöltek szerint átadja a szolgáltatás biztosításához szükséges adatokat, a vele szerződésben álló hitelesítés szolgáltatónak.

6. A Hitelesítés Szolgáltató megszűnteti a tanúsítványok kibocsátási folyamatában a hitelesítés-szolgáltató nevében eljáró alvállalkozások összes felhatalmazását.

7. A Hitelesítés Szolgáltató magánkulcsait meg kell semmisítenie, illetve vissza kell vonni a használatból a (6.2.10) alatt meghatározottak szerint.

b) A Hitelesítés Szolgáltató tevékenysége befejezésekor az informatikai rendszerében foglalt adatairól teljes körű, időbélyegzővel (időjelzéssel) ellátott mentést készít. A mentett adatállományokat a Hitelesítés Szolgáltató védi a jogosulatlan módosítástól, illetve biztosítja azt, hogy az adatállomány tartalmához jogosulatlan személyek ne férhessenek hozzá. Biztosítja továbbá, hogy az adatok a megőrzési időn belül az arra jogosult személyek számára hozzáférhetőek és értelmezhetőek legyenek.

c) Ha a Hitelesítés Szolgáltató ellen felszámolási vagy végelszámolási eljárás indult, haladéktalanul tájékoztatja a Hatóságot e tényről, megnevezve az eljárást lefolytató szervezetet.

6. Műszaki biztonsági intézkedések

A Szolgáltató módosítás ellen védett, megbízható rendszereket és termékeket használ.

A Hitelesítés Szolgáltató által fenntartott regisztrációs (RA) informatikai infrastruktúra, és a Tanúsítványkiadó (ld. 5. c) pont) által üzemeltetett tanúsítványkiadói (CA) informatikai infrastruktúra külön telephelyen üzemel. A Tanúsítványkiadó által használt fizikai infrastruktúra (helyiségek és berendezések mint beléptető-rendszer, klíma, szünetmentes tápellátás, egyéb védelemi célú eszközök) megfelelnek a minősített hitelesítés szolgáltatási követelményeknek. A telephelyek közötti biztonságos kommunikáció megoldott.

A tervezés és az üzembe helyezés során, valamint a működtetés és menedzselés során a Hitelesítés Szolgáltató a jogszabályok, valamint a saját kockázatelemzése alapján érvényesíti a megbízható termékekhez kiadott gyári, továbbá – ha rendelkezésre áll – a termékhez tartozó független tanúsító szervezet által kibocsátott tanúsítvány dokumentációjában szereplő biztonsági feltételeket.

A Hitelesítés Szolgáltató által igénybe vett CA/RA rendszer a Hunguard Kft. által tanúsított elektronikus aláírás termékre épül. A termék megnevezése: Trust&CA, regisztrációs száma: HUNG-T-036-2007. A Hitelesítés Szolgáltató és a Tanúsítványkiadó megvizsgálta a tanúsítványhoz csatolt biztonságos alkalmazási feltételeket, és a szabályozást a Hitelesítés Szolgáltató, az informatikai rendszert a Tanúsítványkiadó eszerint hozta létre.

6.1 Kulcspár előállítása és telepítése

A Szolgáltató valamennyi általa (saját maga, címtárak, regisztrációs szervezetek, illetve alanyok számára) előállított magánkulcsát biztonságos és az ipari szabványoknak, valamint a hatályos jogszabályi előírásoknak megfelelően hozza létre. (Felelős: kulcsmenedzser)

6.1.1 Kulcspár előállítás

A Hitelesítés Szolgáltató saját kulcspárjának előállítása:

a) A szolgáltatói magánkulcs előállítását fizikailag védett környezetben (lásd 5.1 pont), legalább két bizalmi munkakörben dolgozó, erre feljogosított személy (például kulcsmenedzser és a hitelesítés szolgáltatásért általánosan felelős vezető; ld. bizalmi munkakörök az 5.2.1 pont szerint) együttes részvételével, más személyek jelenlétét kizárva végzik el.

b) A Hitelesítés Szolgáltató a saját kulcsainak előállítását egy nChipher gyártmányú, nShield 500 F3 típusú, a FIPS 140 [2] 3 követelményeknek megfelelő kriptográfiai eszközzel hajtja végre.

c) A kriptográfiai eszközzel az RSA kulcspár előállítása az [1] 18.§ szerint kiadott NHH határozatban [20] szereplő, RSA kulcspár előállításra alkalmasnak elismert algoritmussal történik.

A Szolgáltató által más felek számára előállított kulcspár előállítása:

d) A Hitelesítés Szolgáltató által más felek (pl. bizalmi munkakört betöltő saját munkatársai) számára szolgáló kulcsok előállítását fizikailag védett környezetben végzi a megfelelő hitelesítési rendben ([9], [9a]) előírtak alapján.

e) A Hitelesítés Szolgáltató más alanyok számára az 1.1.7 pont szerint generál kulcspárokat.

f) A Hitelesítés Szolgáltató által saját részére (pl. bizalmi munkakört betöltő saját munkatársai) és az alanyok számára előállított kulcsokat olyan algoritmussal állítja elő, melyet az [1] 18.§-a szerint kiadott NHH határozat [20] erre a felhasználásra alkalmasnak ismer el.

6.1.2 Magánkulcs eljuttatása az ügyfélhez

a) A Szolgáltató nem tárol és nem szállít az ügyfelek számára magánkulcsokat. (Továbbiakat ld. 1.1.7 pontban)

6.1.3 A nyilvános kulcs eljuttatása a tanúsítvány kibocsátóhoz

a) A Hitelesítés Szolgáltató regisztrációs eljárás során (a kriptográfiai hardver eszközön) generált kulcspár nyilvános kulcs részét olyan módon juttatja el a tanúsítvány létrehozását végző Tanúsítványkiadóhoz, ami biztosítja a továbbított adat sértetlenségét, valamint a feladó azonosítását.

6.1.4 A hitelesítés szolgáltató nyilvános kulcsának közzététele az érintett felek számára

a) A Hitelesítés Szolgáltató, a saját szolgáltatói nyilvános kulcsát tartalmazó tanúsítványt a fenti 2.3 pont szerinti web-címen teszi elérhetővé az érintett felek számára.

6.1.5 Kulcsméretek

A Hitelesítés Szolgáltató saját kulcsának mérete:

a) A Hitelesítés Szolgáltató RSA szolgáltatói kulcsa legalább 2048 bites.

A Hitelesítés Szolgáltató által más felek számára előállított kulcsok mérete:

b) a Hitelesítés Szolgáltató által más felek (címtárak, regisztrációs szervezetek és alanyok) számára előállított RSA kulcsok hossza legalább 1024 bites.

6.1.6 Nyilvános kulcs paraméterek előállítása, a paraméterek ellenőrzése

A nyilvános kulcs paraméterek megfelelnek a magyar előírásoknak, és előállításuk során a megfelelő szabványok, algoritmusok kerültek alkalmazásra – az Eat. [1] 18. § és az NHH határozata [20] alapján.

6.1.7 A kulcs használat célja (az X.509 v3 kulcshasználati mező tartalmának megfelelően)

a) A Hitelesítés Szolgáltató a kulcshasználati tartalmat a megfelelő hitelesítési rend szerint ([9], [9a]) határozza meg.

b) A Hitelesítés Szolgáltató természetes személyek számára fokozott biztonságú aláírásra használható aláíró tanúsítványokat bocsáthat ki, melyekre teljesülnek az alábbiak:

   - az aláíró tanúsítvány kulcshasználati mezője kritikus, és a mezőben a "NonRepudiation" bit van „true” értékre beállítva, s ezen kívül legfeljebb a "DigitalSignature” bit lehet még "true” értékre beállítva.

6.2 A szolgáltatói magánkulcsok védelme és a kriptográfiai modulokkal kapcsolatos műszaki előírások

A megfelelő hitelesítési rendben ([9], [9a]) meghatározottak szerint,

A Szolgáltató gondoskodik saját és ügyfelei magánkulcsainak titkosságáról és sértetlenségéről.

A Szolgáltató a saját magánkulcsát egy biztonságos kriptográfiai hardver eszközben tartja, illetve olyan eszközzel használja, amely megfelel a hitelesítési rendekben meghatározott követelményeknek, emellett az NHH nyilvántartásában szereplő tanúsított elektronikus aláírási termék.

6.2.1 Kriptográfiai modulra vonatkozó szabványok

A Szolgáltató magánkulcsát egy biztonságos, FIPS 140 [2] 3 követelményeknek megfelelő kriptográfiai hardver eszközben tartja. Továbbiakat ld. a fenti 6.1.1 b) pontban.

6.2.2 Magánkulcs többszereplős ("n-ből m") használata

a) A Hitelesítés Szolgáltató a kulcsok védelme érdekében biztosítja a magánkulcs többszereplős védelmét. A titokmegosztás kriptográfiai eszközök felhasználásával valósul meg.

b) A Hitelesítés Szolgáltató a magánkulcsait legalább 3 erre feljogosított munkatárs közül legalább 2 (kulcsmenedzserek, hitelesítés szolgáltatásért általánosan felelős vezető -- bizalmi munkakört betöltő személyek) jelenléte mellett és felügyelete mellett, a Szolgáltató belső (kulcs- és kártyamenedzsment) szabályozása szerint állíthatják vissza, védett környezetben (lásd 5.1 pont). A szabályozásban megjelölt személyeken kívül más személyek ezen

eljárásból ki vannak zárva.

c) Az eljárás lefolytatásáról jegyzőkönyv készül. A jegyzőkönyvet minden jelenlevő aláírásával hitelesíti.

6.2.3 Magánkulcs letétbe helyezése

a) A Hitelesítés Szolgáltató a magánkulcsát nem helyezi letétbe.

6.2.4 Magánkulcs mentése

a) Mentési célból (például a kriptográfiai egység klónozásához szükséges módon) a Hitelesítés Szolgáltató a magánkulcsait csak védett környezetben (5.1), legalább két kulcsmenedzser (bizalmi munkakört betöltő személy) együttes részvételével, más személyek jelenlétét kizárva másolja le.

b) A Hitelesítés Szolgáltató magánkulcsainak mentett másolatait a Hitelesítés Szolgáltató belső szabályzatában rögzített biztonsági eljárásai hozzák létre.

6.2.5 Magánkulcs archiválása

b) A Hitelesítés Szolgáltató a magánkulcsát nem archiválja.

6.2.6 Magánkulcs bejuttatása kriptográfiai modulba, vagy onnan történő exportja

a) A Hitelesítés Szolgáltató magánkulcsai a kriptográfiai modulban jönnek létre.

b) A szolgáltatói magánkulcsok kriptográfiai modulba kívülről történő bejuttatására egyedül a magánkulcs véletlen megsérülése, megsemmisülése esetén lehet szükség. Az ilyen esetekre a 6.2.2 pont elvárása vonatkozik.

c) A szolgáltatói magánkulcsok kriptográfiai modulból történő exportálására kizárólag mentési célból kerülhet sor. Az ilyen esetekre a 6.2.4 pont elvárásai vonatkoznak.

6.2.7 Magánkulcs tárolása kriptográfiai modulban

a) A Hitelesítés Szolgáltató a magánkulcsait üzem közben és üzemen kívül kriptográfiai modulban tárolja. A Hitelesítés Szolgáltató a kriptográfiai hardver biztonsági funkcióinak és az adminisztratív intézkedéseinek ellenőrzött alkalmazásával megfelelő hozzáférés-ellenőrzéseket végez annak biztosítása érdekében, hogy a magánkulcsok a kriptográfiai modulon kívül ne legyenek hozzáférhetők.

6.2.8 A magánkulcs aktiválásának módja

A Hitelesítés Szolgáltató által igénybevett kriptográfiai modul csak a felhasználót engedélyező módban teszi elérhetővé a szolgáltató magánkulcsait. Ehhez a felhasználónak az azonosító és hitelesítő adatait kell megadnia.

6.2.9 A magánkulcs deaktiválásának módja

Ha a kriptográfiai modul (szabályos vagy szabálytalan módon) kikerül az aktív állapotból -- például a hozzá tartozó szerviz leállása miatt -- a kulcs addig nem hozzáférhető, amíg a felhasználó az azonosító és hitelesítő adatait újra meg nem adja.

6.2.10 A magánkulcs megsemmisítésének módja

a) A magánkulcs megsemmisítését a hardver kriptográfiai moduljához rendelt kulccsal lehet elvégezni. Ez a kulcs hardver és adminisztratív biztonsági eszközökkel van védve.

b) A Szolgáltató a megsemmisítést legalább két, bizalmi munkakört betöltő, erre feljogosított személy (például kulcsmenedzser és a hitelesítés szolgáltatásért általánosan felelős vezető; ld. bizalmi munkakörök az 5.2.1 pont szerint) együttes részvételével végzi.

6.2.11 A kriptográfiai modulok értékelése

a) A Hitelesítés Szolgáltató által használt kriptográfiai modul megfelel legalább a FIPS 140-2 3-as szintnek.

b) A Hitelesítés Szolgáltató tanúsítványok előállításához csak olyan kriptográfiai modult használ, amely rendelkezik az NHH által nyilvántartásba vett, tanúsításra jogosult szervezetek által erre a célra kiállított (az a) pontban szereplő értékelési eredményeken alapuló), vagy azzal egyenértékű igazolással is.

6.3 A kulcspár kezelésének egyéb szempontjai

6.3.1 Nyilvános kulcs archiválása

A Hitelesítés Szolgáltató a nyilvános kulcsait archiválja.

6.3.2 A tanúsítványok és kulcspárok használatának periódusa

a) A Hitelesítés Szolgáltató magánkulcsainak használati periódusa nem haladja meg azok érvényességi idejét.

b) A Hitelesítés Szolgáltató által az ügyfelek számára kibocsátott tanúsítványok használati

periódusa (érvényességi időtartama) 1 év.

6.4 Aktivizáló adatok (PIN-kód)

6.4.1 Aktivizáló adatok előállítása és telepítése

A részletes szabályok az alanyok és a Hitelesítés Szolgáltató érdekében nem nyilvánosak!

A Szolgáltató kriptográfiai hardver eszközének használatához (magánkulcs létrehozása, használat, mentés és visszaállítás, stb.) történő aktivizálásához - a kívánt müvelettől függően - legalább három, bizalmi tisztségviselőnek kiosztott, chipkártyán generált és őrzött kulcsokra, valamint egy-egy aktivizáló (PIN) kódra van szükség. (ld. továbbá 6.2.2 pontban)

Az aláírók számára átadott chipkártyák felhasználói aktivizáló (PIN) adatát a Szolgáltató az aláíró által hozatja létre.

6.4.2 Az aktivizáló adatok védelme

a) A Hitelesítés Szolgáltató a kriptográfiai hardver eszközhöz tartozó aktivizáló adatokat csak abból a célból rögzíti, hogy azt a szolgáltatást igénybe vevő személy számára – másolat megőrzése nélkül - átadhassa.

b) A Hitelesítés Szolgáltató a kriptográfiai hardver eszközhöz tartozó aktivizáló adatot a kriptográfiai hardver eszköztől elkülönítve osztja szét.

c) A Hitelesítés Szolgáltató a kriptográfiai hardver eszközt, valamint az ehhez tartozó aktivizáló adatokat biztonságosan osztja/szállítja ki.

6.4.3 Az aktivizáló adatok egyéb szempontjai

A pontos szabályok az alanyok és a Hitelesítés Szolgáltató érdekében nem nyilvánosak!

6.5 Informatikai biztonsági óvintézkedések

A Szolgáltató a vele szerződésben álló Tanúsítványkiadóval (ld. 5. c) pont) együttesen teremtik meg és tartják fent a hitelesítési rendekben ([9], [9a]) elvárt biztonsági feltételeket.

A hitelesítés szolgáltatási rendszer, valamint a szolgáltatás eljárásai dokumentáltak. Az alkalmazott eszközök és eljárások, a szolgáltatásban dolgozó munkatársak a Szolgáltató kockázatvállalásának megfelelően lettek kiválasztva.

A hitelesítés szolgáltatás biztosítása során a Hitelesítés Szolgáltató látja el az alábbi kritikus

szolgáltatásokat/tevékenységeket (ld. 1.1.4 pontot)

- kezdeti regisztrálás és személyazonosság megállapítása,
- tanúsítványkérelem feldolgozása,
- tanúsítvány megújítás és módosítás szolgáltatás,
- tanúsítvány visszavonás és felfüggesztés szolgáltatás,
- tanúsítvány állapot szolgáltatás,
- tanúsítványarchiválás,
- kulcsmenedzsment,
- egyedi névképzés,
- adattárolás,
- viszontazonosítás

adminisztratív eljárásait, valamint

- aláírás-létrehozó eszköz kibocsátás,
- kulcsmenedzsment,
- kulcsgenerálás az aláírás-létrehozó eszközön,
- a kulcshoz tartozó tanúsítvány elhelyezése az aláírás-létrehozó eszközön,
- adattárolás

adminisztratív eljárásait és informatikai (IT) támogatását.

Tanúsítványkiadó látja el

- tanúsítvány kibocsátás szolgáltatás,
- tanúsítvány elfogadás,
- tanúsítvány megújítás és módosítás szolgáltatás,
- tanúsítvány visszavonás és felfüggesztés szolgáltatás,
- tanúsítvány állapot szolgáltatás,
- tanúsítványarchiválás,
- kulcsmenedzsment,
- egyedi névképzés,
- adattárolás,
- viszontazonosítás,
- a kulcshoz tartozó tanúsítvány elhelyezése az aláírás-létrehozó eszközön,

informatikai (IT) támogatását.

A két szervezet közötti informatikai biztonsági szerepek és eljárások össze vannak hangolva, le vannak dokumentálva. A szolgáltatások vonatkozásában minden felelősség a Hitelesítés Szolgáltatót terheli.

6.5.1 Speciális informatikai biztonsági műszaki követelmények

A hitelesítés szolgáltatási rendszer ledokumentált, a működtetéshez rendelkezésre állnak a szükséges kézikönyvek. Az informatikai biztonsági szabályozás előírja, hogy milyen eljárásokat, milyen óvintézkedések mellett kell végrehajtani. Amikor egy műszaki intézkedés nem elég, megfelelő adminisztratív intézkedéssel van biztosítva a megfelelő védelem.

A Szolgáltató gondoskodik arról, hogy az informatikai rendszeréhez való hozzáférés kellően felhatalmazott egyénekre legyen korlátozva. Különösképpen:

a) A Szolgáltató rendszerei védettek, az információinak sértetlensége biztosított, a vírusok, káros és engedély nélküli szoftverek tekintetében.

b) Az adathordozó eszközök kezelése biztonságosan történik azok sérülése, ellopása és jogosulatlan hozzáférése elleni védelme érdekében.

c) A Szolgáltató szerepkörök szerint korlátozza a rendszerek használatát.

d) A Szolgáltató gondoskodik a logikai és fizikai hozzáférések hatékony nyilvántartásáról, beleértve a sikeres és sikertelen (támadási célú) kapcsolatfelvételeket is.

e) A Szolgáltató naplózási rendszere rögzíti a kritikus rendszerállapotokat, a kritikus eszközöknél a jogosult és jogosulatlan használatot (ld. 5.4.1 pontot). A Szolgáltató azonosítja és hitelesíti a tanúsítványkezeléssel kapcsolatos kritikus alkalmazások igénybe vevőit. Az RA műveletek (pl. regisztráció, visszavonás) esetében, valamint a kritikus CA műveleteknél az azonosítás PKI tanúsítvány-alapon történik. Az egyéb helyeken a bejelentkezés adminisztratív eljárásokhoz , illetve felhasználó/jelszó megadásához kötött.

f) A védelme biztosított (ld. 5.4.4), a naplózás mentése és archiválása (ld. 5.4.5) biztonságos körülmények között történik.

g) A szolgáltatási rendszer fizikailag is és logikailag is osztott, területenként önálló biztonsági megoldásokkal üzemel (ld. továbbá a 6. pontot).

h) A Hitelesítés Szolgáltató és a Tanúsítványkiadó feladatai és felelősségei szabályozva vannak, a szabályozás érvényesítésére az eszközök és a személyzet biztosított. A nem várt eseményekre, vagy a szolgáltatás biztonságát veszélyeztető helyzetekre riasztási megoldások vannak kialakítva. Emellett a Hitelesítés Szolgáltató SO-ja figyeli a felügyelő rendszer jelentéseit is.

i) Kár megelőzési szándékkal, az esetleges hibák és fel nem fedett támadások felderítése céljából a Hitelesítés Szolgáltató biztonsági felelőse (SO) eseti és rendszeres (havi, féléves) ellenőrzéseket végez a Tanúsítványkiadónál, ahol egyeztet az ott dolgozó SO-val.

j) Az érzékeny adatokat a Hitelesítés Szolgáltató elkülönített rendszerelemekkel és védelmi megoldásokkal kezeli. Ide tartoznak a kulcsok, valamint a személyes adatok.

6.5.2 Az informatikai biztonság értékelése

A Szolgáltató – az adott feladatnak megfelelő, a jogszabályokban, vagy ajánlásokban megjelölt garanciákkal rendelkező – megbízható rendszereket és termékeket használ.

Az informatika biztonság értékelését a Szolgáltató a hitelesítés szolgáltatásra vonatkozóan az MSZ ISO/IEC 17799 szerint tervezte és hajtja végre.

6.6 Életciklusra vonatkozó műszaki előírások

6.6.1 Rendszerfejlesztési előírások

a) A jelen szabályzatban érintett szolgáltatásokat – biztonsági okokból – el kell különíteni az egyéb szolgáltatásoktól.

b) Az új rendszerelemeket külön próbának kell alávetni. A próba nem történhet a működő rendszeren, nem veszélyeztetheti a szolgáltatás rendelkezésre állását.

c) A Szolgáltató változtatás kezelési eljárásokat alkalmaz valamennyi működő rendszerelem esetében a kibocsátásokra/leszállításra, a módosításokra és amennyiben értelmezhető a szoftver javításokra vonatkozóan.

d) A szolgáltatási rendszer, vagy ennek meghatározott (CA, HSM, naplózási rendszer, mentési rendszer, RA, chipkártya-megszemélyesítés, rendszervizsgálói munkahely, működés felügyelő rendszer, ügyfélszolgálati munkahely) részeinek a beüzemelését egy erre a feladatra megbízott, az NHH által nyilvántartásba vett, elektronikus aláírás szolgáltatási szakértő felügyeli.

e) A szolgáltatás beüzemelése egy, a Szolgáltató által (a hitelesítés szolgáltatásért általánosan felelős vezető által ellenjegyzett,) elfogadott teszt-terv alapján történik.

6.6.2 Biztonságkezelési előírások

A Szolgáltató a rendszerterv alapján elkészítette az eszközök adat-centrikus biztonsági besorolását.

A rendszerterv és a besorolás alapján, továbbá a kapcsolódó dokumentáció és tesztek figyelembe vételével a Szolgáltató kockázatelemzést végzett. Ennek alapján megállapította az üzleti kockázatvállalás mértékét, a biztonsági elvárások és eljárások megfelelőségét, meghatározta a jobbító tevékenységeket.

A hitelesítés-szolgáltató – a kártya- és kulcsmenedzsment szabályzata alapján – gondoskodik a kriptográfiai hardver biztonságáról annak teljes élettartama alatt.

6.6.3 Életciklusra vonatkozó biztonsági előírások

A rendszerterv és a biztonsági értékelés során a Szolgáltató kezeli a kritikus életciklus-információkat.

6.7 Hálózatbiztonsági előírások

A Szolgáltató gondoskodik arról, hogy informatikai rendszerében megfelelő hálózat biztonsági ellenőrzésekre kerüljön sor.

A hálózati rendszerelemek elkülönített fizikai helyen (a regisztráció külön RA helyiségben, a

rendszervizsgáló külön munkahelyen, az archiválási rendszer külön munkahelyen, a VPN pontok, védett helyeken, minden más, a CA tevékenységhez tartozó rendszerelem a Tanúsítványkiadó biztonsági területein) van elhelyezve.

A Szolgáltató tűzfalakat és behatolásjelzőt is üzemeltet.

A rendszerterv tartalmazza azokat a megoldásokat, amelyekkel a szolgáltatói rendszer védhető az illetéktelen behatolás és hamisítás ellen. Különösen kiemelt védelmet kell biztosítani az RA helyiség számára, valamint a Hitelesítés Szolgáltató és a Tanúsítványkiadó kommunikációjára.

6.8 Időbélyegzés

A Szolgáltató megbízható rendszereinek belső órája a MÁV informatika Zrt. időforrásához van szinkronizálva. A pontosság 1 másodpercnél jobb.

A Szolgáltató a csatlakoztatott MÁV informatika Zrt. által (ntp-vel) küldött időadatok sérthetetlenségét, illetve módosíthatatlanságát biztosítja.

7. Tanúsítvány-, és tanúsítvány visszavonási lista

7.1 Tanúsítványprofilok

A Hitelesítés Szolgáltató a megfelelő hitelesítési rend ([9], [9a]) elvárásait teljesíti.

A közigazgatási célra kibocsátott tanúsítványok követik "Az Informatikai és Hírközlési Minisztérium ajánlása a közigazgatásban alkalmazható végfelhasználói tanúsítványok szerkezetének és adattartalmának műszaki specifikációjára" dokumentum előírásait.

7.1.1 Verzió szám(ok)

A Hitelesítés Szolgáltató X.509 v3 (értékszám: 2), illetve az RFC 3280 [14] előírásainak megfelelő tanúsítványokat bocsát ki.

További információk találhatók a Hitelesítés Szolgáltató elektronikus aláíráshoz kapcsolódó hitelesítés szolgáltatásának tanúsítvány-profilja [8] dokumentumban.

7.1.2 Az algoritmus objektum azonosítója

A Hitelesítés Szolgáltató az alábbi objektumazonosítót használja a tanúsítványok és a visszavonási listák (CRL) aláíró algoritmusának algoritmus meghatározásához:

> sha-lWithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha-1(5)

7.1.3 Névformák és névhasználati megkötöttségek

A Hitelesítés Szolgáltató az általa kibocsátott tanúsítványok alanyaként egy egyedi nevet (DN-t) foglal be a tanúsítványba. Továbbiakat ld. 3.1.1 pontban.

7.1.4 A hitelesítési rend objektum azonosítója

A Hitelesítés Szolgáltató által kibocsátott minden tanúsítványban szerepel a megfelelő Hitelesítési Rend (ld. 1.1 pontban) objektumazonosítója.

7.1.5 Tanúsítvány kiterjesztések

A Szolgáltató az X.509 szabvány 3. változatának megfelelő tanúsítvány kiterjesztéseket támogatja.

A kiterjesztési mezők feldolgozásáért az Előfizető és Érintett fél alkalmazása és eljárása felelős. A Szolgáltató semmilyen körülmények között nem hibáztatható a kiterjesztés, vagy a szabályzatokban foglaltak figyelmen kívül hagyása, téves értelmezése miatt.

7.1.6 Az aláíró számára kibocsátott tanúsítványok szerkezete

Mező/Attribútum	**Adattartalom**
tbs certificate (tanúsítványadatok)	**a jellemző adatokat ld. a következő pontban, a tanúsítvány egyéb adatait a tanúsítvány-profil dokumentum** [8] részletesen ismerteti
signature algorithm (a szolgáltató által alkalmazott aláírási algoritmus)	SHA1withRSA
signature value (a szolgáltató aláírása)	az aláírás értéke

7. táblázat A tanúsítvány szerkezete

7.1.7 Az aláíró számára kibocsátott tanúsítványok jellemző adatai

Mező/Attribútum	**Adattartalom**
country (országkód)	„HU” (ld. a 3.1.1 pontban)
organization (a kibocsátó megnevezése)	**„**Educatio Társadalmi Szolgáltató Kht” (ld. a 3.1.1 pontban)
common name (a szolgáltatás azonosítója)	„EDUCA-2” (ld. a 3.1.1 pontban)

8. táblázat A kibocsátó adatai

Mező/Attribútum	Adattartalom
country (országkód)	„HU” (ld. a 3.1.1 pontban)
organization (szervezet), organization-unit (szervezeti egység)	szervezet, szervezeti egység megjelölése, ha megadandó
common name (az aláíró neve)	az aláíró neve (ld. a 3.1.1 pontban)
subject public key info algorithm (aláírás algoritmus info)	RSA, legalább 2048 bites kulcsokkal
extensions (tanúsítvány-kiterjesztések)	standard és Internet kiterjesztések
basic constraints cA (CA tanúsítvány)	FALSE (nem)
key usage (kulcshasználat)	ld. 6.1.7 pontban
certificate policies (hitelesítési rendek)	OID azonosítók (ld. az 1.1 pontban)
subject alt name, rfc822 name (az aláíró levelezési címe)	e-mail cím (ld. 3.1.1 pontban)
policy qualifier id qualifier (hitelesítési rend érvényesítése)	CPS , OID: 1.3.6.1.5.5.7.2.1, http://educa2.educatio.hu/szabalyzatok/EducatioHSZSZ.pdf user notice – ld. 1.4.1.1 pontban
CRL distribution points (visszavonási lista helye)	ld. 2.3 pontban
authority Information access, access method, access location (CA tanúsítványának a helye, valamint az OCSP responder elérése)	ld. 2.3 pontban

9. táblázat Az aláíró adatai

7.2 Tanúsítvány visszavonási lista profil

A Hitelesítés Szolgáltató a megfelelő hitelesítési rend ([9], [9a]) elvárásait teljesíti.

További információk találhatók a Hitelesítés Szolgáltató elektronikus aláíráshoz kapcsolódó hitelesítés szolgáltatásának tanúsítvány-profilja [8] dokumentumban.

7.2.1 Verzió szám(ok)

A Hitelesítés Szolgáltató X.509 v2 (értékszám: 1), illetve az RFC 3280 [14] előírásainak megfelelő visszavonási listákat (CRL) bocsát ki.

További információk találhatók a Hitelesítés Szolgáltató elektronikus aláíráshoz kapcsolódó hitelesítés szolgáltatásának tanúsítvány-profilja [8] dokumentumban.

7.2.2 Egyéb információk

A Hitelesítés Szolgáltató a visszavonási listelemekben szerepelteti azt, ha azok felfüggesztési eljárás miatt kerültek be a CRL-be.

A kiterjesztési mezők feldolgozásáért az Előfizető és Érintett fél alkalmazása és eljárása felelős. A Szolgáltató semmilyen körülmények között nem hibáztatható a kiterjesztés, vagy a szabályzatokban foglaltak figyelmen kívül hagyása, téves értelmezése miatt.

7.3 OCSP profil

Az OCSP válaszadó (responder) tanúsítványát az EDUCA-2 adja ki. Az aláíró kulcsok felhasználójának a megnevezése a tanúsítványban: „EDUCA-2 OCSP responder”, szervezet: „Educatio Társadalmi Szolgáltató Kht.”, ország: „HU”. A kulcsfelhasználás megjelölése (KeyUsage): "digitalSignature", "nonRepudiation" (kritikus); (Extended Key Usage:) "OCSPSigning" (OID: 1.3.6.1.5.5.7.3.9).

További információk találhatók a Hitelesítés Szolgáltató elektronikus aláíráshoz kapcsolódó hitelesítés szolgáltatásának tanúsítvány-profilja [8] dokumentumban, melynek vonatkozó része az RFC 2560 [21] felhasználásával készült.

8. Megfelelőségi audit és egyéb ellenőrzések

A Hitelesítés Szolgáltató a szolgáltatás kialakítása során, a megfelelőség biztosítása érdekében egy, az NHH által nyilvántartásba vett elektronikus aláírás szolgáltatási szakértőt alkalmazott.

A Hitelesítés Szolgáltató – a jogszabályok alapján – egy független, az NHH által nyilvántartásba vett elektronikus aláírási szolgáltatási szakértő szakvéleményét elkészítette, ezt a szakvéleményt a nyilvántartásba vételi kérelem mellékleteként szerepeltette.

8.1 A megfelelőség ellenőrzésének körülményei és gyakorisága

A Szolgáltató a jogszabályi és a szabályozási követelményeknek történő megfelelést, az eszközök megfelelőségének ellenőrzését legalább évente megvizsgálja. A vizsgálat lehet esetleges is, amikor egy szabályozás módosítása a cél, vagy egy eszköz használatba vételét megelőzően kerül rá sor.

A Hitelesítés Szolgáltató naponta ellenőrzi az előző nap, vagy napok eseménynaplóit és napló-fájlait. (Felelős: független rendszervizsgáló)

A Hitelesítés Szolgáltató legalább havonta ellenőrzi a Tanúsítványkiadó rendszerét, ebben a tanúsítványkiadót (CA), valamint a tanúsítványtár és ügyfélnyilvántartás működtetését, a tanúsítványállapot információk nyilvánossá tételét, tanúsítvány visszavonási lista információk biztosítását (CRL), valamint a viszontazonosítási szolgáltatás ellátását, továbbá a munkaidőn túli

felfüggesztési eljárás kezelését, emellett a kulcsmenedzsment infrastruktúrát, és az ügyfélnyilvántartási rendszert. Az ellenőrzés kiterjed a Hitelesítés Szolgáltató és a Tanúsítványkiadó között megkötött szolgáltatói szerződés és felelősségvállalási nyilatkozatok elvárásaiban meghatározott teljesítések ellenőrzésére is. (Felelős: üzleti kérdésekben a hitelesítés szolgáltatásért általánosan felelős vezető, biztonsági kérdésekben az SO)

8.2 Az auditor és szükséges képesítése

A külső és belső auditálást csak a megfelelő szakmai ismeretek birtokában lévő, tapasztalt szakemberek végezhetik. A hitelesítés szolgáltatás vonatkozásában a Szolgáltató csak elektronikus aláírás szolgáltatási szakértőt alkalmaz.

8.3 Az auditor és az auditált rendszerelem függetlensége

A külső és belső auditálást végző személyeknek függetlenek az összes általa vizsgált rendszerelemtől, ennek megfelelően a Szolgáltató üzemeltetését végző személyektől, termékektől, gyártóktól, szállítóktól és rendszerintegrátoroktól.

8.4 Az auditálás által lefedett területek

Az auditálás lefedni az alábbi területeket:

a) fizikai biztonság,
b) dokumentálás és folyamatok biztonsága,
c) a személyi állomány biztonsági ellenőrzése,
d) adatvédelem,
e) műszaki biztonság.

8.5 A hiányosságok kezelése

A szolgáltatásban résztvevő minden dolgozó köteles a hiányosságok felderítésére, a rendszervizsgálatok megfelelőségének a támogatására.

A biztonságot veszélyeztető hiányosságról tájékoztatni kell a hitelesítés szolgáltatásért általánosan felelős vezetőt, aki döntési helyzetben van hiányosság megítélésében. Adott esetben felül kell vizsgálni a szolgáltatás dokumentációit, a vonatkozó Hitelesítési rend és a Szolgáltatási szabályzat dokumentumokat is, segítséget kell kérnie egy elektronikus aláírás szolgáltatási szakértőtől.

A hiányosságok menedzselésénél figyelembe kell venni a kockázatokat, a szolgáltatás folytatásának, illetve szüneteltetésének, valamint leállításának következményeit is. Ebben a kérdésben felelős: a hitelesítés szolgáltatásért általánosan felelős vezető.

8.6 Az eredmények közzététele

A külső és belső auditálást végző személy csak a megbízójának adhat információt a szolgáltató tevékenységével kapcsolatban.

9. Egyéb üzleti és jogi kérdések

9.1 Díjak

A mindenkor érvényes szolgáltatások díjait a Hitelesítés Szolgáltató saját Internetes oldalán (web-lapján) közzéteszi. A web-lap elérése: http://www.educatio.hu

A díjfizetés tekintetében az Általános Szerződési Feltételek [10] 8. pontjában meghatározottak irányadók.

9.2 Anyagi felelősségvállalás

Az Általános Szerződési Feltételek [10] 7. pontja szerint. Lásd továbbá 9.9 pontot.

9.3 Az üzleti információk bizalmassága

A Szolgáltató a birtokába jutott adatokat a hatályos jogszabályi rendelkezések alapján biztonságosan tárolja és kezeli. A regisztráció során kitöltött regisztrációs adatlap adatait elektronikus formában, a jelen szabályzatban meghatározott azonosítási eljárások végrehajtása során fénymásolat formájában birtokába jutott adatokat papíron, illetve elektronikus formában tárolja.

Az ügyféladatok gyűjtésének célja a hitelesítés szolgáltatás i tevékenység regisztrációs feladatainak ellátása.

A Hitelesítés Szolgáltató az információkat a saját adatkezelési utasításai szerint kezeli. Ld. továbbá az Általános Szerződési Feltételek [10] 6.1.5. és 6.1.6 pontjait; adatkezelési és adatvédelmi szabályzat [12]. További felvilágosítást az ügyfélszolgálati munkatársak adnak.

9.3.1 Bizalmas információk

A Szolgáltató bizalmas információnak tekinti azokat az ügyféladatokat, amelyek egy kibocsátott tanúsítványban nem szerepelnek, valamint bizalmasnak nyilvánítja a Szolgáltató nem nyilvános tervdokumentumait (rendszertervet, szabályozási anyagokat, stb.) és működési dokumentumait, vizsgálati és tesztadatait.

9.3.2 Nem bizalmas információk

A Hitelesítés Szolgáltató nem bizalmas információnak tekinti azokat az ügyféladatokat, amelyek az ügyfél engedélye alapján nyilvánosként kezelhet, továbbá nyilvánosak a jogszabályok által meghatározott szabályzatok, valamint a Hitelesítés Szolgáltató által meghatározott egyéb szabályzatok, a visszavonási listák (CRL). A Hitelesítés Szolgáltató nyilvános információként kezeli a tanúsítványtárban elhelyezett azon tanúsítványokat, amelyek publikálását az ügyfél engedélyezte.

9.4 A személyes adatok védelme

a) A Szolgáltató az információkat a saját adatkezelési utasításai szerint kezeli. Ld. [12] További felvilágosítást az ügyfélszolgálati munkatársak adnak.

b) A Szolgáltató működése és szabályzatai megfelelnek a Személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi XLIII. törvény követelményeinek.

9.4.1 Információszolgáltatás hatósági szervek részére

Az elkövetett bűncselekmények felderítése vagy megelőzése céljából, illetőleg nemzetbiztonsági érdek alapján a Hitelesítés Szolgáltató adatokat továbbít a nyomozóhatóságnak és a nemzetbiztonsági szolgáltatóknak, az elektronikus aláírásról szóló 2001. évi XXXV. törvény [1] 11. § (2) és (4) bekezdése szerint.

9.4.2 Információszolgáltatás polgári peres eljárás keretében

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény [1] 11. § (3) bekezdése szerint, a tanúsítvány érvényességét érintő polgári peres, illetve nem peres eljárás során a Hitelesítés Szolgáltató – az érintettség igazolása esetén - az aláíró személyazonosságát igazoló, valamint a 12. § (2) bekezdése alapján egyeztetett adatokat, átadhatja az ellenérdekű peres félnek vagy képviselőjének, illetőleg azt közölheti a megkereső bírósággal.

9.4.3 Egyéb információszolgáltatás

Az elektronikus aláírásról szóló 2001. évi XXXV. törvény [1] 16. § (2) és (3) bekezdése szerint, a Hitelesítés Szolgáltató tevékenységének befejezésekor más – vele azonos besorolású – szolgáltatónak átadja a törvényben megjelölt nyilvántartásokat, beleértve a visszavont tanúsítványokkal kapcsolatos minden adatot, ezek között a személyes adatokat is.

9.5 Szellemi tulajdonjogok

A szolgáltatási tevékenység során alkalmazott összes név, szabályzat, CRL a Hitelesítés Szolgáltató tulajdonát képezi. A szoftver, firmware és hardver komponensek részben a Hitelesítés Szolgáltató tulajdonát képezik, részben azokat jogszerűen használja/veszi igénybe.

9.6 Tevékenységért viselt felelősség és helytállás

9.6.1 A Szolgáltató felelőssége és helytállása

a) A Szolgáltató felelős a jelen szabályzat keretei között végzett szolgáltatói tevékenységekért, különösen az általa kibocsátott tanúsítványok szerkezetéért, tartalmáért és hitelességéért, az általa generált kulcspárok megfelelőségéért, az intelligens kártyák biztonsági beállításáért.

b) A Hitelesítés Szolgáltató a felelős az általa támogatott Hitelesítési Rendben és a jelen Szolgáltatási Szabályzatban leírt eljárásoknak való megfelelőségért, beleértve a Tanúsítványkiadó által ellátott szolgáltatásokat/tevékenységeket is (ld. 6.5 Informatikai biztonsági óvintézkedések pontot).

c) A felelősség korlátozását ld. az alábbi 9.8 pontban.

9.6.2 Az aláíró / előfizető felelőssége és helytállása

Az aláíró az aláírás létrehozó adatot kizárólag az aláírás létrehozására használhatja, beleértve a tanúsítványban jelölt esetleges egyéb korlátozásokat is.

Az aláíró felelőssége, hogy az aláírás létrehozó adatot a tőle elvárható legnagyobb gondossággal birtokolja.

9.6.3 Az érintett fél felelőssége

Ld. a 4.5.2 Az érintett felek nyilvános kulcs- és tanúsítvány használata pontot, ebben is különösen a c) alpontot, valamint az alábbi 9.8 pontot.

9.7 Helytállás érvénytelenségi köre

Hitelesítés Szolgáltató a tanúsítványt kizárólag Magyarország területére érvényesen, valamint 0 Ft kötelezettségvállalással bocsátja ki. Ezen korlátokat meghaladó ügyletekben kibocsátott és aláírt elektronikus dokumentumokból származó követelésekért, illetve az így okozott kárért a Hitelesítés Szolgáltató nem felel.

9.8 Felelősségi korlátozások

A Hitelesítés Szolgáltató kizárja felelősségét, ha az aláírás ellenőrzés lépései a Hitelesítési rendben ([9], [9a]) meghatározott módon bármi okból – beleértve a Hitelesítés Szolgáltatónál keletkező működtetési és menedzselési problémát is – nem hajthatóak végre az aláírás ellenőrzésének időpontjában, és az elektronikus aláírás, illetve az aláírással ellátott dokumentum az aláírás ellenőrzője által ennek ellenére elfogadásra kerül.

Szolgáltató nem felelős az olyan károkért, amelyek abból adódtak, hogy az Aláíró vagy az Érintett Fél a tanúsítványok ellenőrzése és felhasználása során nem a hatályos jogszabályoknak, illetve szolgáltatói szabályzatoknak megfelelően járt el, illetve nem tanúsította a tőle elvárható gondosságot.

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

9.9 Kártérítési kötelezettségek

Az Általános szerződési feltételekben [10] van meghatározva.

9.10 Érvényesség

Jelen szabályzat visszavonásig érvényes.

9.11 A felek közötti kommunikációra vonatkozó előírások

A Hitelesítés Szolgáltató köteles a szolgáltatás megkezdését követően a jelen szabályzat és az Általános szerződési feltételek [10] módosításait azok hatályba lépése előtt 30 nappal közzétenni.

Azok az előfizetők, akik a módosítást nem fogadják el, jogosultak a hatálybalépést követően 15 napon belül 15 napos felmondási idővel az Szolgáltatási Szerződést felmondani. A Szolgáltatási Szerződés felmondása egyben a kiadott tanúsítvány iránti visszavonási kérelemnek is tekinthető és a Hitelesítés Szolgáltató jogosult a tanúsítványt nyilvántartásából törölni.

9.12 Kiegészítések

Nincs kiegészítés.

9.13 Vitás kérdések megoldása

Az Általános szerződési feltételekben [10] van meghatározva.

9.14 Irányadó jog

Az Általános szerződési feltételekben [10] van meghatározva.

9.15 Az érvényben lévő jogszabályoknak való megfelelőség

A jelen dokumentumban megfogalmazott szabályzat az alábbi törvényeknek, rendeleteknek és irányelveknek való megfelelőséget tűzte célul:

a) Személyes adatok védelméről és a közhasznú adatok nyilvánosságáról szóló 1992 évi LXIII. törvény

b) Az elektronikus aláírásról szóló 2001. évi XXXV. törvény

c) 9/2005 (VII.21.) IHM rendelet az elektronikus aláírási termékek tanúsítását végző szervezetekről, illetve a kijelölésükre vonatkozó szabályokról

d) 45/2005 (III. 11.) Kormányrendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással kapcsolatos feladat- és hatásköréről, valamint eljárásának részletes szabályairól

e) 3/2005 (III. 18.) IHM rendelet az elektronikus aláírással kapcsolatos szolgáltatásokra és ezek szolgáltatóira vonatkozó részletes követelményekről

f) 4/2006 (IV. 19.) IHM rendelet a Nemzeti Hírközlési Hatóságnak az elektronikus aláírással összefüggő nyilvántartással kapcsolatos tevékenységéért fizetendő díjakról

g) 7/2002 (IV. 26.) MeHVM rendelet az elektronikus aláírással kapcsolatos szolgáltatási szakértő nyilvántartásba vételéről

h) Az Európai Parlament és a Tanács 1999/93/EK számú irányelve az elektronikus aláírással kapcsolatos közösségi keretrendszerről

i) A közigazgatási hatósági eljárás és szolgáltatás szabályairól szóló 2004. évi CXL. törvény és az elektronikus ügyintézéshez kapcsolódó végrehajtási rendeletek, azaz a 193/2005 (IX.22.), 194/2005 (IX.22.) és 195/2005 (IX.22.) számú kormányrendeletek.