Microsec E-szignó Üzleti Szolgáltatás

Hitelesítés-Szolgáltatási Szabályzat

Microsec Számítástechnikai Fejlesztő Kft.
1022 Budapest, Marczibányi tér 9.

A Szolgáltatási Szabályzat verziószáma: *1.0*
A szolgáltatási szabályzat azonosítója: *http://www.e-szigno.hu/adatok/HSZSZ_v1.0*
HIF regisztrációs szám: *A nyilvántartásba vétel még nem történt meg.*
Kibocsátás dátuma: *2002. április 30.*
Hatályba lépés dátuma: *A HIF nyilvántartásba vételének napja, illetve ennek hiányában a nyilvántartásba vétel iránti kérelem beadásának napjától számított 30. nap, amennyiben a HIF a nyilvántartásba vételt nem tagadja meg.*

A LEGFONTOSABB HSZSZ JOGOK ÉS KÖTELEZETTSÉGEK RÖVID ÖSSZEFOGLALÁSA

TOVÁBBI RÉSZLETEK TEKINTETÉBEN OLVASSA EL A SZABÁLYZATOT. EZ AZ ÖSSZEFOGLALÁS NEM TELJES. TÖBB MÁS FONTOS KÉRDÉST A HSZSZ TÁRGYAL.

1. A Hitelesítés Szolgáltatási Szabályzat (*lásd* definíciók) a Microsec E-SZIGNÓ Hitelesítés-Szolgáltató Hitelesítés-szolgáltatásának (*lásd* definíciók) működtetését és alkalmazását – beleértve a hitelesítési kérelmezést (*lásd* definíciók) [4], a kérelem jóváhagyását [5], tanúsítvány kibocsátását [6], elfogadását [7], használatát [8], felfüggesztését és visszavonását [9] – szabályozza.
2. Ön (a felhasználó) tudomásul veszi, hogy (i) a hitelesítési kérelem benyújtását megelőzően ajánlott a nyilvános kulcsok használatáról szóló megfelelő gyakorlaton és képzésen való részvétel, ill. (ii) a digitális aláírással, tanúsítványokkal, nyilvános kulcs infrastruktúrával (NYKI) és a hitelesítései-szolgáltatással (HSZ) kapcsolatos dokumentumok ismerete, az oktatási és képzési lehetőségek igénybevétele. Az (i)-(ii) pontokkal kapcsolatos tájékoztatás a Microsec E-SZIGNÓ ügyfélszolgálati irodáján beszerezhetőek. [16.]
3. A Microsec E-SZIGNÓ különböző hitelesítési szintű tanúsítványokat kínál [2.2]. Önnek kell döntenie arról, hogy milyen szintű tanúsítvány felel meg igényeinek.
4. A hitelesítési kérelem benyújtása előtt [4.2] Önnek létre kell hoznia egy kulcspárt [2.4.3, 4.1]. A kulcspár titkos kulcsát [4.1] biztonsági okokból (*lásd* definíciók), hitelt érdemlő (*lásd* definíciók) módon kell kezelnie [4.1.1]. Az Ön szoftver rendszerének erre a feladatra alkalmasnak kell lennie.
5. Mielőtt a tanúsítványt közzétenné, vagy más módon előidézné annak használatát, el kell fogadnia (*lásd* definíciók) az abban foglaltakat. Tisztában kell lennie azzal, hogy a tanúsítvány elfogadásával (*lásd* definíciók) fontos kötelezettségeket vállal.
6. Ha Ön tanúsítvánnyal rendelkező digitális aláírással ellátott dokumentum fogadója, akkor saját felelőssége bízni a tanúsítvány hitelességében. Ezért ajánlott az Ön számára, hogy a Microsec E-SZIGNÓ adattárának (*lásd* definíciók) segítségével ellenőrizze, és ezáltal igazolja (*lásd* definíciók), hogy a tanúsítvány érvényes (*lásd* definíciók), nem vonták vissza (*lásd* definíciók), vagy függesztették fel (*lásd* definíciók). Az ellenőrzést követően a tanúsítvány már alkalmas az Ön számára annak megerősítésére [8.1.], hogy a digitális aláírást (*lásd* definíciók) a tanúsítvány érvényes időszaka alatt a tanúsítványban (*lásd* definíciók) szereplő nyilvános kulcsnak (*lásd* definíciók) megfelelő titkos kulccsal (*lásd* definíciók) hozták létre, és a digitális aláírással (*lásd* definíciók) ellátott üzenetet (*lásd* definíciók) nem másították meg.
7. Ön kötelezettséget vállal arra [12.10.], hogy a titkos kulcs (*lásd* definíciók) veszélyeztetése (*lásd* definíciók) esetén haladéktalanul értesíti az illetékes tanúsítvány-kibocsátó irodát (*lásd* definíciók).
8. A Hitelesítés Szolgáltatási Szabályzat szerint (lásd definíciók) a Microsec E-SZIGNÓ, illetve a különböző Hitelesítés-Szolgáltatók szavatosságokat biztosítanak [11.3.] az Ön részére. A Microsec E-SZIGNÓ ezen kívül visszatérítési politikával is rendelkezik [11.1.]. A Hitelesítés Szolgáltatási Szabályzatban rögzített esetektől eltekintve a Microsec E-SZIGNÓ és a Hitelesítés-Szolgáltatók korlátolt felelősséggel rendelkeznek, és elállnak a szavatolástól.

További információért keresse meg a http://www.e-szigno.hu *Microsec E-SZIGNÓ Web oldalt, vagy lépjen kapcsolatba az ügyfélszolgálattal a* ugyfelszolgalat@e-szigno.hu *e-mail címen.*

Tartalomjegyzék

1 ÁTTEKINTÉS

A fejezet bemutatja a Microsec E-SZIGNÓ Hitelesítés-Szolgáltató Hitelesítés Szolgáltatási Szabályzatát (HSZSZ), struktúráját és a szabályzat alapjául szolgáló konvenciókat. A fejezet végén [1. táblázat] a HSZSZ-ben használt mozaikszavak és rövidítések találhatóak.

1.1 A szolgáltató adatai

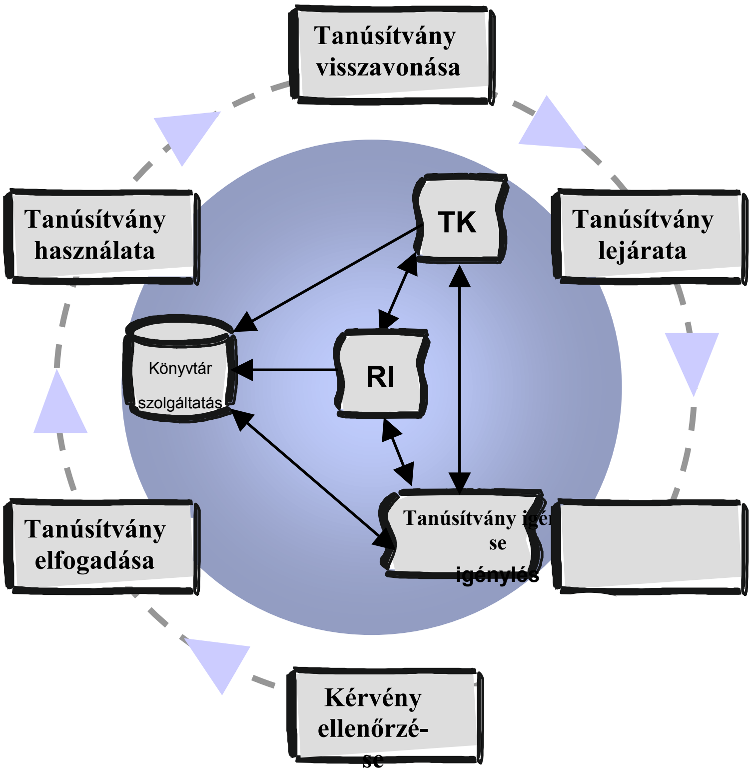
Név:	Microsec Számítástechnikai Fejlesztő Kft.
Cégjegyzék szám:	01-09-078353 a Fővárosi Bíróság mint Cégbíróság
Székhely, telephely:	1022 Budapest, Marczibányi tér 9.
Telefonszám:	438-6310
Telefax szám:	438-6320
A szolgáltatással kapcsolatos információk elérése:	http://www.e-szigno.hu
Központi e-mail cím:	info@e-szigno.hu
Ügyfélszolgálati iroda:	Microsec Számítástechnikai Fejlesztő Kft. 1022 Budapest, Marczibányi tér 9.
Panaszok bejelentésének helye:	Microsec Számítástechnikai Fejlesztő Kft. 1022 Budapest, Marczibányi tér 9.
Minősítések:	ISO 9001: 2000
HIF nyilvántartásba vétel napja:	A nyilvántartásba vétel még nem történt meg
Illetékes fogyasztóvédelmi felügyelőség:	Fogyasztóvédelmi Felügyelőség 1088 Budapest, József Krt. 6. Levélcím: 1428 Budapest Pf. 20. Telefon: 36-1 459-4800

1.2 A Szolgáltatási Szabályzat adatai

A Szolgáltatási Szabályzat verziószáma:	1.0
A szolgáltatási szabályzat azonosítója:	http://www.e-szigno.hu/adatok/HSZSZ_v1.0
HIF regisztrációs szám:	A nyilvántartásba vétel még nem történt meg.
Hatályba lépés dátuma:	A HIF nyilvántartásba vételének napja, illetve ennek hiányában a nyilvántartásba vétel iránti kérelem beadásának napjától számított 30. nap, amennyiben a HIF a nyilvántartásba vételt nem tagadja meg.
Hatályának megszűnése:	Visszavonáskor

1.3 A HSZSZ struktúrája

A hitelesítési folyamatot a hitelesítés-szolgáltatás életciklus modelljén keresztül [1. ábra] mutatjuk be. A hitelesítés-szolgáltatás a tanúsítvány-kibocsátó irodák (a továbbiakban: TK) létrehozásával és a folyamatok elindításával kezdődik [HSZSZ 3]. Ezt követi az általános TK feladatok megvalósítása; bejegyzés; tanúsítványok használata; tanúsítványok felfüggesztése, visszavonása; lejárata; megújítása; archiválása. Ennek a megközelítésnek előnyös tulajdonsága, hogy az eseményeket kronologikus sorrendben mutatja be, és összeegyeztethető a magán- és közszféra már létező végrehajtási szabályzataival. .



Tanúsítvány igénylése [HSZSZ 4.]

Kérvény ellenőrzése, tanúsítvány készítése [HSZSZ.5.]

Tanúsítvány elfogadása, bejegyzése és kibocsátása [HSZSZ 6.]

Tanúsítvány használata [HSZSZ 8.]

Tanúsítvány felfüggesztése és visszavonása [HSZSZ 9.]

Tanúsítvány lejárata és megújítása [HSZSZ 10.]

Tanúsítvány archiválása

1. ábra

1.4 Hivatkozás a HSZSZ-re

Más dokumentumokban a következő módokon kell hivatkozni a jelen Hitelesítés-Szolgáltatási Szabályzatra: „Microsec E-szignó HSZSZ”, vagy „Microsec E-szignó Hitelesítés-Szolgáltatási Szabályzat”. A szabályzaton belül pedig a következő módokon: „HSZSZ”, vagy „HSZSZ….”, illetve a függelékre: „13. …. Függelék”. A HSZSZ-t időszakosan frissítik. A HSZSZ változatait a „HSZSZ” után található változatszám jelzi. (pl. „1.2 változat”, vagy „HSZSZ 1.2”)

1.5 Közzététel

A jelen HSZSZ-t közzéteszik:

(i) A Microsec E-SZIGNÓ adattáron belül elektronikus formában a http://www.e-szigno.hu/adatok/HSZSZ_v1.0 címen,

(ii) Elektronikus formában e-mailen keresztül a HSZSZ-igeny@e-szigno.hu címen, és

(iii) Nyomtatva a következő címen: Microsec E-szignó Hitelesítés-szolgáltató 1022 Budapest, Marcibányi tér 9.

- A hivatkozott Microsec E-SZIGNÓ 'World Wide Web' URL-ek mindegyike a 'Secure Sockets Layer' (SSL) biztonsági protokoll alkalmazásával hívja le a HTTP-t, hogy elősegítse a „biztonságos módban” történő adatvisszanyerést (browser támogatott SSL használata esetén). A dokumentumok mindegyike elérhető „nem biztonságos módban” is, a https:// http://-vel történő behelyettesítésével. A biztonságos mód alkalmazásával lehet elérni az összes Web-en található dokumentum hivatalos változatát a Microsec E-SZIGNÓ adattáron belül.
- A HSZSZ-ben található néhány URL könyvtárakat és e-mail címeket jelöl. A HSZSZ-ben szereplő legtöbb Microsec E-SZIGNÓ URL hivatkozás elektronikus és papír alapú dokumentumként is elérhető a ugyfelszolgalat@e-szigno.hu e-mail címen.

1.6 Ügyfélszolgálat, képzés és tréning

A HSZSZ feltételezi, hogy az olvasó ismeri a digitális aláírást, a Nyilvános Kulcs Infrastruktúrát (NYKI), és a Microsec E-SZIGNÓ Hitelesítés-Szolgáltatását. Ha nem – mielőtt a hitelesítést kérelmezné –, javasoljuk a nyilvános kulcs módszereinek használatát ismertető gyakorlatokon való részvételt. További segítséget a Microsec E-SZIGNÓ felhatalmazott Hitelesítés-Szolgáltatójának ügyfélszolgálati irodájától kaphat (ugyfelszolgalat@e-szigno.hu).

MINDEN **HITELESÍTÉS-SZOLGÁLTATÁST** KÉRELMEZŐ ÉS ALÁÍRÓ ELISMERI, HOGY FELHÍVTÁK FIGYELMÉT ARRA, HOGY (i) A HITELESÍTÉSI KÉRELEM BENYÚJTÁSA ELŐTT AJÁNLOTT EGY MEGFELELŐ, A NYILVÁNOS KULCS MÓDSZEREIT ISMERTETŐ TRÉNINGEN VALÓ RÉSZVÉTEL, VALAMINT TUDOMÁSUL VESZI, HOGY (ii) A DIGITÁLIS ALÁÍRÁSSAL, TANÚSÍTVÁNYOKKAL, **NYILVÁNOS KULCS INFRASTRUKTÚRÁVAL**, ÉS A **HITELESÍTÉS-SZOLGÁLTATÁSSAL** KAPCSOLATOS DOKUMENTUMOK, TRÉNINGEK ÉS KÉPZÉSEK A MICROSEC E-SZIGNÓNÁL ELÉRHETŐEK.

1.7 Mozaikszavak és rövidítések jegyzéke

BET	Biztonságos Elektronikus Tranzakció
EAA	Ellenőrizetlen aláírói adatok
BE	Biztonsági Eljárások
FTP	FTP
GMT	Greenwichi középidő
HK	Hitelesítési kérelem
HSZ	Hitelesítési-szolgáltató
HSZSZ	Hitelesítés-Szolgáltatási Szabályzat
http	Hypertex átviteli protokoll
HTTPS	Biztonságos Hypertext átviteli protokoll
KK	közös kulcs
MT	Módosítás tervezet
n/r	Nem áll rendelkezésre
NISZ	Nemzeti Információfeldolgozási Szabványok
PIN	Személyazonosító szám
PKCS	Nyilvános kulcsú rejtjelezési szabvány
NYKI	Nyilvános-kulcs Infrastruktúra
RI	Regisztrációs Iroda
RMN	Relatívan Megkülönböztetett Név
RSA	Egy kriptografikus rendszer
S/MIME	Biztonságos többcélú e-mail kiterjesztés
SSL	Biztonságos Csatlakozó Felület
TK	Tanúsítvány-kibocsátó Iroda
VTL	Visszavont Tanúsítványok Listája
VPN	Virtuális magánhálózat
WWW	Világháló
X.509	Nemzetközi Telekommunikációs tanúsítvány

1. táblázat

2 MICROSEC E-SZIGNÓ HITELESÍTÉSI INFRASTRUKTÚRA

A fejezet ismerteti a Microsec E-SZIGNÓ hitelesítés-szolgáltatás alapjául szolgáló szerkezeti felépítést, úgymint a hitelesítési osztályokat, tanúsítványbővítéseket, időpecsételést és a Microsec E-SZIGNÓ adattárat.

2.1 Bizalmi infrastruktúra

A Microsec E-SZIGNÓ Hitelesítés-Szolgáltatót a Microsec Kft. azért hozza létre, hogy:

(i) megteremtse az elektronikus (köz)okiratok hiteles kibocsátásának lehetőségét,

(ii) elősegítse az elektronikus aláírással rendelkező iratok nem peres eljárásokban, így a cégeljárásban történő alkalmazhatóságát,

(iii) biztosítsa az ügyfél-barát elektronikus ügyvitel megvalósításához szükséges igazságügyi infrastruktúrát,

(iv) támogassa a biztonságos elektronikus kereskedelmet, és

(v) kielégítse ügyfeleinek szakmai, üzleti és személyes digitális aláírás iránti igényeit.

A Microsec E-SZIGNÓ hitelesítés-szolgáltatásának vezetési és adminisztratív feladatait úgy alakította ki, hogy az:

(i) kielégítse a különböző kommunikációs és információbiztonsági igényű felhasználókat, és

(ii) biztosítsa a felhasználókat arról, hogy a Microsec E-SZIGNÓ hitelesítés-szolgáltatások lényegében egységesek, továbbá a HSZSZ tartalmazza a Microsec E-SZIGNÓ hitelesítés-szolgáltatásának integritását biztosító általános vezetési, kezelési és végrehajtási szabályzatát.

Ennek eredményeként a Microsec E-SZIGNÓ hitelesítés-szolgáltatása a területileg elkülönült csoport igényeit is kielégíti, növelve ezzel a felhasználók szolgáltatásba vetett bizalmát. *A hitelesítés-szolgáltatási rendszer megvalósításának különböző logikai egységeit a HSZSZ 2.5. mutatja be.*

2.1.1 A tanúsítvány kibocsátás és kezelés általános bemutatása

A Microsec E-SZIGNÓ harmadik bizalmi félként igazolja a nyilvános kulcs és egy egyedi névvel (*ld.* „elnevezés” meghatározását) azonosított adathalmaz (törvényes név, állandó tartózkodási hely, születési dátum stb.) között fennálló kapcsolatot. Ezt a kapcsolatot kizárólag egy tanúsítvány – a Microsec E-SZIGNÓ által kiadott, digitálisan aláírt üzenet – bizonyítja. A tanúsítási folyamat magas szintű ügyvitelébe tartozik a regisztráció, az egyedi elnevezés és a megfelelő kérelmezői hitelesítés, a kiadás, a visszavonás és felfüggesztés. Az elnevezést elsősorban a Microsec E-SZIGNÓ hajthatja végre. A Microsec E-SZIGNÓ jelenleg három különböző szintű hitelesítés-szolgáltatást kínál. A tanúsítványok minden egyes szintje, vagy osztálya sajátos funkcionális és biztonsági jellemzőkkel rendelkezik. A hitelesítést kérelmezők az igényeiknek megfelelő szolgáltatások közül választhatnak; meg kell határozniuk, hogy melyik hitelesítési osztály felel meg igényeiknek. A választott hitelesítési osztálytól függően, a hitelesítést kérelmező elektronikus vagy postai úton jelentkezhet a Microsec E-SZIGNÓ-nál, vagy személyesen veszi fel a kapcsolatot a Microsec E-SZIGNÓ-val. A Microsec E-SZIGNÓ által kiadott minden egyes tanúsítvány a hitelesítés-szolgáltatás egy meghatározott bizalmi szintjének felel meg.

A hitelesítési kérelem benyújtása után a tanúsítványt vagy annak tervezetét a Microsec E-SZIGNÓ adja ki, vagy küldi el a hitelesítést kérelmezőnek. A hitelesítést kérelmezőnek meg kell ismernie a tanúsítványt vagy annak tervezetét, és meg kell állapítania, hogy a tanúsítvány vagy annak tervezete megfelel-e céljainak. Megfelelés esetén a hitelesítést kérelmező a hitelesítési regisztrációs eljárás útján elfogadja a tanúsítványt, továbbá elismeri a HSZSZ-ben meghatározott kötelezettségeket.

A tanúsítvány kezelése magában foglalja a tanúsítványok és a megfelelő titkos kulcsok dezaktiválását is a tanúsítványok visszavonásának és felfüggesztésének folyamatán keresztül.

2.1.2 Biztonsági szolgáltatás

A Microsec E-SZIGNÓ hitelesítés-szolgáltatása különböző, a kommunikációs és információs tőke védelmét szolgáló biztonsági mechanizmust (SSL, S/MIME, VPN stb.) támogat. A tanúsítvány önmagában nem mechanizmus. A hitelesítés-szolgáltatás olyan keretet biztosít, amelyen belül a kommunikációs felek tanúsítvány alapú biztonsági szolgáltatásokat vehetnek igénybe. A digitális aláírás használata és azok HSZ megerősítése elősegíti a nyílt információs hálózatokon keresztüli kommunikáció és elektronikus kereskedelem védelmét.

A tanúsítvány alapú biztonsági szolgáltatások felhasználói környezetben alkalmasak a biztonsági fenyegetésekkel szembeni védelemre. Ahhoz, hogy a felhasználók megfelelően védjék kommunikációs környezetüket a behatolókkal szemben, maguk választják ki a várható kockázati szintnek megfelelő biztonsági mechanizmust, biztonsági technológiát, biztonsági szolgáltatási szerződést.

A Microsec E-SZIGNÓ jelenleg az RSA nyilvános kulcsú rendszert alkalmazza minden hitelesítéssel kapcsolatos ügyben. A Microsec E-SZIGNÓ azonban kötelezettséget vállal más digitális aláírási standardok alkalmazására is, amennyiben a piaci igények más alternatívákat követelnek.

2.2 Hitelesítési szintek

A Microsec E-SZIGNÓ jelenleg három különböző hitelesítési szintnek megfelelő hitelesítési osztályt biztosít a hitelesítés-szolgáltatásban. Minden egyes szint egy kijelölt bizalmi fokozatnak megfelelő hitelesítési osztályt jelöl. A következő alfejezetek bemutatják az egyes hitelesítési szinteknek megfelelő hitelesítési osztályokat. További információ található a 2. táblázatban (Bizalmat befolyásoló tanúsítványjellemzők).

AZ EGYES HITELESÍTÉSI OSZTÁLYOK LEÍRÁSAI (LD. 2. TÁBLÁZAT) A FELHASZNÁLÓK ÁLTAL KIVITELEZETT ALKALMAZÁSRA ÉS KOMMUNIKÁCIÓS RENDSZERRE UTALNAK. NEM KÉPVISELNEK HSZ JÓVÁHAGYÁST, VAGY BÁRMILYEN KONKRÉT FELHASZNÁLÁSRA VONATKOZÓ JAVASLATOT. A FELHASZNÁLÓNAK EGYÉNILEG KELL FELMÉRNIE ÉS MEGHATÁROZNIA, HOGY AZ EGYES HITELESÍTÉSI OSZTÁLYOK MENNYIRE FELELNEK MEG A KÖVETELMÉNYEKNEK.

2.2.1 1. szintű hitelesítési osztály

Leírás: A 1. szintű hitelesítési osztály tanúsítványait kizárólag egyének számára adják ki. A 1. szintű hitelesítési osztály tanúsítványai igazolják, hogy a felhasználó neve (vagy álneve) és e-mail címe egyértelmű nevet alkotnak a Microsec E-SZIGNÓ adattárában. A 1. szintű hitelesítési osztály tanúsítványai elektronikus úton jutnak el az aláíróhoz, és a tanúsítvány elektronikus úton adódik hozzá az aláíró már meglévő tanúsítványaihoz. Elsősorban Web böngészés és e-mail küldés esetén alkalmazható, hogy mérsékelt mértékben növelje ezen környezetek biztonságosságát. Ezek a tanúsítványok még a kommunikáció folytonosságának biztosítására is alkalmazhatók (biztosítva, hogy a második közlemény is ugyanattól a küldőtől származik). A 1. szintű hitelesítési osztály tanúsítványai támogathatják harmadik szolgáltató felek – például Web honlap fenntartók – egyedi szolgáltatásait is abban az esetben, ha a hitelesítést kérelmező saját elhatározásából bizonyos „demográfiai adatokat" (ország, irányító szám, kor, és nem) nyújt be a hitelesítési kérelemmel együtt a bejegyzés során, és ezeket az információkat a harmadik szolgáltató fél felé elérhetővé teszik a tanúsítvánnyal

Biztosíték szintje: A 1. szintű hitelesítési osztály tanúsítványai nem teszik lehetővé az aláíró személyének hitelesítését. Pusztán egyszerű ellenőrzést biztosít az alany nevének egyértelműségéről a Microsec E-SZIGNÓ adattárán belül, és korlátozott mértékben megerősíti az e-mail címet. A 1. szintű hitelesítési osztály tanúsítványában lévő aláíró rendes neve (és a demográfiai adatai, ha elküldték) ellenőrizetlen aláírói adatoknak (EAA) minősülnek. EZ A TANÚSÍTVÁNY BIZTOSÍTJA AZ ÖSSZES MICROSEC E-SZIGNÓ TANÚSÍTVÁNY KÖZÜL A LEGALACSONYABB SZINTŰ GARANCIÁKAT. NEM ALKALMAZHATÓ OLYAN ELJÁRÁSOKBAN, ILLETVE ÜGYMENETEKBEN AHOL A SZEMÉLYAZONOSSÁG BIZONYÍTÁSA SZÜKSÉGES.

2.2.2 2. hitelesítési osztály

Leírás: A 2. szintű hitelesítési osztály tanúsítványait jelenleg kizárólag egyének számára adják ki. A 2. szintű hitelesítési osztály tanúsítványai igazolják, hogy az aláíró által közölt jelentkezési adatok nem mondanak ellent az elfogadott ügyféladatbázisban található adatoknak. A 2. szintű hitelesítési osztály tanúsítványokat elsősorban szervezeten belüli és szervezetek közötti e-mail; kis, illetve alacsony kockázatú tranzakciók; személyes/egyéni e-mail; jelszócsere; szoftver érvényességének igazolása; és online szolgáltatás előfizetése esetén használják. A Microsec E-SZIGNÓ különböző típusú 2. szintű hitelesítési osztályba tartozó tanúsítványokat kínál speciális használatra (például 'online' céginformáció igénybevételére). A 2. szintű hitelesítési osztályba tartozó tanúsítványok támogathatják harmadik szolgáltató felek – például Web honlap fenntartók – egyedi szolgáltatásait is abban az esetben, ha a hitelesítést kérelmező saját elhatározásából bizonyos „demográfiai adatokat" (ország, irányító szám, kor, és nem) nyújt be a hitelesítési kérelemmel együtt a bejegyzés során, és ezeket az információkat a harmadik szolgáltató fél felé elérhetővé teszik a tanúsítvánnyal.

A 2. szintű hitelesítési osztályba tartozó tanúsítványok aláírói szerződéseiket online küldik a Microsec E-SZIGNÓ 2. szintű hitelesítési osztálynak megfelelő helyi regisztrációs irodába (HRI), a hitelesítési kérelem adatait pedig harmadik fél közreműködésével igazolják. Ezt az igazolást alapul véve, a HRI vagy elfogadja, vagy elutasítja a kérelmet (*ld.* HSZSZ 5. Hitelesítési Kérelmek érvényesítése). Jóváhagyás után, a TK postai címigazolási eljárást hajt végre (*ld.* HSZSZ5.1.4.), kivéve, ha a Microsec E-SZIGNÓ HRI-ja számára adta ki a tanúsítványt.

Biztosíték szintje: A 2. szintű hitelesítési osztályba tartozó tanúsítvány elfogadható, de nem teljes mértékben biztos garanciákat nyújt az aláíró azonosságát illetően. A bejegyzési eljárás olyan automatizált online folyamaton alapul, amely a kérelmező nevét, címét és más személyes – a tanúsítványon szereplő – adatát összehasonlítja egyéb információs adatbázisból kinyert adatokkal. Az igazolási eljárásban a Microsec E-SZIGNÓ szembeállítja a harmadik fél adatbázisából kinyert adatokat a kérelemben található adatokkal, és az összehasonlítás eredményét alapul véve, vagy elfogadja, vagy elutasítja a kérelmet.

BÁR A 2. SZINTŰ HITELESÍTÉSI OSZTÁLY ONLINE AZONOSÍTÁSI ELJÁRÁSA A HITELESÍTÉST KÉRELMEZŐ HITELESÍTÉSÉNEK JELENTŐSEN AUTOMATIZÁLT MÓDJA, NEM KÍVÁNJA MEG A KÉRELMEZŐ SZEMÉLYES MEGJELENÉSÉT EGY BIZALMI FÉL (PL. HELYI REGISZTRÁCIÓS SZERV VAGY KÖZJEGYZŐ) ELŐTT. KÖVETKEZÉSKÉPPEN A 2. SZINTŰ HITELESÍTÉSI OSZTÁLYBA TARTOZÓ TANÚSÍTVÁNY MEGSZERZÉSEKOR, HASZNÁLATAKOR, ILLETVE A RÁ VALÓ HAGYATKOZÁSKOR FIGYELEMBE KELL VENNI RELATÍV HASZNÁT ÉS KORLÁTAIT, ÉS A TANÚSÍTVÁNYT ENNEK MEGFELELŐEN KELL HASZNÁLNI. TOVÁBBI INFORMÁCIÓ EZZEL AZ ONLINE HITELESÍTÉSI ELJÁRÁSSAL KAPCSOLATBAN ELÉRHETŐ A MICROSEC E-SZIGNÓ ADATTÁRBAN, A HTTP://WWW.E-SZIGNO.HU CÍMEN.

A 2. szintű hitelesítési osztályba tartozó tanúsítványban szereplő demográfiai adatok, ha azt benyújtották, EAA-nak minősülnek.

2.2.3 3. szintű hitelesítési osztály

Leírás: A 3. szintű tanúsítványt egyének és szervezetek számára adják ki.

- **Egyének esetén** – A 3. szintű tanúsítvány fontos biztosítékokkal szolgál az egyéni aláíró személyazonosságát illetően azáltal, hogy megköveteli a személyes (fizikai) megjelenést egy 3. szintű helyi regisztrációs irodában (HRI), vagy annak meghatalmazottja (pl. közjegyző) előtt. A Microsec E-SZIGNÓ vagy felhatalmazottja 3. szintű helyi regisztrációs irodájában, a hitelesítési kérelemben feltüntetett adatokat és tényeket a bemutatott okmányok alapján ellenőrzi.

- **Szervezetek esetén:** A 3. szintű tanúsítvány biztosítékokkal szolgál különböző köz- és magánszférába tartozó szervezet (pl. igazságszolgáltatási intézmények, állami intézmények, gazdasági társaságok és szervezetek) és képviselőjének létezéséről és nevéről. A Microsec E-SZIGNÓ vagy meghatalmazottja 3. szintű helyi regisztrációs irodájába (HRI), a hitelesítési kérelemben feltüntetett adatokat és tényeket a bemutatott iratok alapján igazolja.

Biztosíték szintje: Az egyéni 3. szintű tanúsítási folyamat különböző eljárásokkal szerzi meg az egyéni aláíró személyazonosságának vizsgálati bizonyítékait. Ez az érvényesítési eljárás erősebb biztosítékokkal szolgál a kérelmező személyazonosságáról, mint a 2. szintű tanúsítvány. A 3. szintű tanúsítvány gyakorlati használatát és megbízhatóságát közjegyző hitelesítése támogathatja (létező, fontos, és törvényesen elismert hitelesítési folyamat). Üzleti entitások számára kiadott a 3. szintű tanúsítvány esetén az üzleti szervezettel történő azonnali kommunikáció és az üzleti entitás adatainak harmadik fél (pl.: céginformációs szolgáltató) közreműködésével való megerősítése a megbízhatóság további biztosítékait szolgáltatja.

2.3 Tanúsítványtípusok

Az 1-es és 2-es, illetve 3-as osztályokban a következő tanúsítványtípusok kiadását végzi a Szolgáltató:

2.3.1 Személyes aláíró és titkosító tanúsítványok

Személyes tanúsítványokat természetes személy igényelhet a saját nevében.

2.3.2 Meghatalmazásos aláíró és titkosító tanúsítványok

Meghatalmazásos (névjegykártyás) tanúsítványokat természetes személy igényelhet egy adott szervezet tagjaként. A szervezet - többek között - lehet gazdálkodó szervezet, hivatal, önkormányzat, egyesület, alapítvány. A tanúsítványban szerepel a személy szervezetben betöltött funkciója is.

2.3.3 Szervezet aláíró és titkosító tanúsítványok

Szervezet tanúsítványokat szervezet vagy annak szervezeti egysége igényelhet saját nevében. A szervezet - többek között - lehet gazdálkodó szervezet, hivatal, önkormányzat, egyesület, alapítvány.

2.3.4 Szerver tanúsítvány

Szerver tanúsítványt Internet címmel (ún. host névvel) rendelkező, szervert üzemeltető természetes személy vagy szervezet igényelhet.

2.3.5 VPN tanúsítvány

VPN tanúsítványt VPN eszközt üzemeltető természetes személy vagy szervezet igényelhet.

2.3.6 Láncolt Hitelesítés Szolgáltató tanúsítvány

Egy adott szervezet számára, a szervezet alkalmazottai számára történő tanúsítvány-kibocsátást lehetővé tevő tanúsítvány.

2.4 Hitelesítési osztályok jellemzői

A 2. táblázat bemutatja az egyes hitelesítési osztályok jellemzőit. A táblázat fejléceit az alábbiakban ismertetjük.

	Az aláíró azonosságának igazolása	**Microsec E-SZIGNÓ titkos kulcsának védelme**	**Hitelesítést aláíró (és kérelmező) titkos kulcsának védelme**	***Kivitelezett vagy tervezett felhasználói alkalmazások. Ld. HSZSZ 2.2. Működés ellenőrzése 2.3.5.***
1. szint	Automatizált egyértelmű elnevezés és email címkutatás	hitelt érdemlő hardver	Kódoló szoftver (PIN védelem) ajánlott, de nem követelmény	Web böngészés és bizonyos email használat
2. szint	ua. mint az 1. szint, plusz automatizált bejegyzési adatellenőrzés és automatizált címellenőrzés	hitelt érdemlő hardware	Kódoló szoftver (PIN védelem) követelmény	egyéni, vállalaton belüli és vállalatok közötti email, online előfizetés, jelszócsere, és szoftver érvényesítése
3. szint	ua. mint 1 szint, plusz személyes jelenlét és személyazonosító dokumentumok, plusz 2. szintű automatizált személyazonosság ellenőrzés egyének esetén; plusz 3. szintű üzleti adatok (vagy akták) ellenőrzése szervezetek esetén	hitelt érdemlő hardware	Kódoló szoftver (PIN védelem) kötelező; hardver token ajánlott, de nem követelmény	személyes bankszolgáltatás, tagsági alapú online szolgáltatások, tartalom integritásszolgáltatások, szoftverérvényesítés,

2. táblázat

A hitelesítési osztályokat a következő tulajdonságok különböző szintjei jellemzik:

- azonosság igazolása (személyes jelenléttel vagy vizsgálattal),
- Microsec E-SZIGNÓ nyilvános kulcs védelme (megfelelő használat biztosítása),
- hitelesítést kérelmező és aláíró nyilvános kulcsának védelme, és működésének ellenőrzése.

Bár a hitelesítési osztályok sok más egyéb tulajdonsággal is rendelkeznek, a 2. táblázatban leírtak keretet biztosítanak a relatív megbízhatóságra hatással lévő néhány szempont megkülönböztetéséhez.

2.4.1 Az aláíró azonosságának igazolása

Azokra a tevékenységekre utal, amelyeket a bejelentkezési folyamat során a kérelmezők által nyújtott információk alapján a hitelesítést kérelmező azonosságának igazolása érdekében a Microsec E-SZIGNÓ végez. Az igazolás típusa, területe, és kiterjedése a hitelesítés osztályától, a kérelmező típusától (egyén, szervezet) és más tényezőktől függ. Az egyes igazolási módszerek és azok szigorúsága a hitelesítési osztálytól függnek.

2.4.2 A Microsec E-SZIGNÓ iroda titkos kulcsának védelme

A Microsec E-SZIGNÓ titkos kulcsát hitelt érdemlő hardver termékekkel kell biztosítani a veszélyeztetés ellen

2.4.3 Hitelesítést aláíró (és kérelmező) titkos kulcsának védelme

A hitelesítést aláíró (Microsec E-SZIGNÓ) (és kérelmező) titkos kulcsának titkosságát kódoló szoftverek és hardverek (pl. smart kártya) HSZSZ-ben meghatározott alkalmazásával kell biztosítani.

A MICROSEC E-SZIGNÓ NEM GENERÁLJA, ÉS NEM BIRTOKOLJA A HITELESÍTÉST KÉRELMEZŐ TITKOS KULCSÁT. TOVÁBBÁ A MICROSEC E-SZIGNÓ IRODA NEM ÁLLAPÍTHATJA MEG VAGY ÉRVÉNYESÍTHETI SEMMILYEN HITELESÍTÉST KÉRELMEZŐ NYILVÁNOS KULCSÁNAK VÉDELMI KÖVETELMÉNYEIT.

2.5 Általános Kiegészítések és bővített elnevezés

2.5.1 Kiegészítő mechanizmusok és a hitelesítési keret

A hitelesítés-szolgáltatás az X.509 v1, v2 és v3 tanúsítványok használatát támogatja. Az X.509 v3 tanúsítvány több lehetőséggel rendelkezik, mint a v1 és a v2 tanúsítvány, lehetővé teszi a tanúsítvány kiegészítését. Ez a lehetőség a Microsec E-SZIGNÓ hitelesítés-szolgáltatás általános eleme, kibővíti az általános hitelesítési szolgáltatási keretet.

2.5.2 Általános és szolgáltatás-specifikus kiegészítések

Az ISO/IEC 9594-8:1995 (X.509) 1. módosítása számos bővítést tartalmaz. Ez szélesebb körű vezetési és végrehajtási ellenőrzést tesz lehetővé a hitelesítési eljárásban. A Microsec E-SZIGNÓ hitelesítés-szolgáltatás számos ilyen ellenőrzési folyamatot hajt végre az X.509 céljainak megfelelően. (Megjegyzés: az X.509-nek megfelelő felhasználó szoftver feltételezhetően eleget tesz a HSZSZ-ben meghatározott érvényesítési követelményeknek. A Microsec E-

SZIGNÓ nem garantálja, hogy ezek a szoftverek támogatják és végrehajtják ezeket az ellenőrzéseket.)

A HSZSZ ezen kívül lehetővé teszi a felhasználók számára, hogy további „saját” kiegészítéseket határozzanak meg az alkalmazási környezetnek megfelelő sajátos céljaikra és használati eljárásaikra. A hitelesítési kérelmezésben, jóváhagyásban és kiadásban a szolgáltatásorientált kiegészítések kezelését a biztonsági eljárás (BE) keretében írják elő. A hitelesítés-szolgáltatás keretében, szolgáltatási célokból alkalmazott saját kiterjesztés például a Microsoft Windows® szoftver által alkalmazott szoftver érvényességet igazoló rendszer és az SSL biztonsági technológiának megfelelő Netscape Communications Corporation rendszere.

Ld. **http://microsoft.com/security**, és **hhtp://home.netscape.com/newsref/ref/netscape-security.html.**

2.5.3 Meghatározott kiegészítések azonosítása és kritikussága

Minden egyes kiegészítés célját a standard CÉLAZONOSÍTÓ érték jelöli (*ld.* X.509 meghatározása). Ezen túlmenően a tanúsítványok kiegészítései egy „kritikussági” valós/hamis értékkel is rendelkeznek. Ezt az értéket a Microsec E-SZIGNÓ állapítja meg, a hitelesítési kérelemben a kérelmező által közölt adatok alapján. Az értéknek meg kell felelnie a kiegészítés meghatározásáért felelős szervezet által megállapított kötöttségeknek.

Egy meghatározott kiegészítésben szereplő *valós* kritikussági érték megkívánja a tanúsítvány érvényességét igazoló személyektől, hogy a tanúsítványt tekintsék érvénytelennek, ha nem ismerik bármely meghatározott *valós* kritikussági értékű kiegészítés céljait és kezelési követelményeit. Ha a kiegészítés kritikussági értéke *hamis*, minden személynek át kell dolgoznia a kiegészítést a vonatkozó meghatározásnak megfelelően, amikor igazolják az érvényességet, egyébként figyelmen kívül kell hagyniuk a kiegészítést.

2.5.4 Bővített elnevezés és Microsec E-SZIGNÓ kiegészítések

Minden végső felhasználó aláírói tanúsítványában, kivéve bizonyos S/MIME v1 tanúsítványokat, kiegészítő „Szervezeti Egység” rovat található – X.509 sajátosság –, amely rövid ismertetést tartalmaz a felelősséget illetően, és hivatkozások segítségével felöleli a teljes HSZSZ-t, pl. „**OU=http://www.e-szigno.hu/adatok/HSZSZ**”.

Ez a szervezeti egység rovat a HSZSZ elsődleges címére (URL) hivatkozik, és azt jelöli, hogy a felelősség korlátolt és szerzői jogi védelmet is tartalmaz. Megjegyzés: A Szervezeti Egység rovat tartalma rövidített, mivel az X509 terjedelmét 64 byte-ra korlátozták. A Szervezeti Egység rovat használata megszűnik, amennyiben az X.509 v3 kiegészítéseinek funkcionális és következetes használata általánossá válik.

Ha a digitális aláírás érvényességét igazoló szoftverek és hardverek (együttesen „megerősítő szoftver”) támogatják a v3 tanúsítvány kiegészítéseinek elfogadását és használatát, akkor a megerősítő szoftverek bemutatják a HSZSZ-al való összefüggést és azokat a kiegészítéseket, amelyek annak fontos részeit határozzák meg.

Ha a megerősítő szoftver csak korlátozott számú, vagy egyénileg meghatározott v3 kiegészítéseket támogat, a megerősítő szoftver hasznosíthatja a kérelem-specifikus kiegészítéseket, hogy ekvivalens módon felfedjen bizonyos kritikus, végrehajtási szabályzattal összefüggő részeket. A 2. ábra illusztrálja, hogy a Microsec E-SZIGNÓ a v3 tanúsítványok esetében hogyan alkalmazza ezt az eljárást. Az ábra kulcsfontosságú elemeit a későbbiekben ismertetjük.

X.509 v3 TANÚSÍTVÁNY

Verzió (3)
Sorozat szám
Aláírási algoritmus ID
Kibocsátó neve
Aktív időszak:
Alany neve (bővített elnevezéssel OU=)
Alany nyilvános kulcs adatai:
Kibocsátó egyedi azonosítója
Alany egyedi azonosítója

Standard Kiegészítések	
	Microsec E-SZIGNÓ Adattár
„Módosított" Hitelesítési Politika	
▪ HSZSZ URL	HSZSZ;CRL;Digitális ID;"hivatalos oldalak"
▪ Ügyviteli hivatkozások	Fontos HSZSZ részletek
▪ Megjegyzés ID	Felhasználói határfelület „Figyelem!"
Egyéb kiegészítések, beleértve a:	
▪ A kérelem által meghatározott kiegészítéseket	PL. Netscape SSL Protocol
▪ A Microsec E-SZIGNÓ által meghatározott szabályozást	Kulcskezelési ügyvitel
▪ X.509 kiegészítéseket	Biztonsági terület kezelése

2. ábra

2.5.4.1 Egyesítés hivatkozással

A kiegészítéseket és bővített elnevezéseket vagy teljes egészében, de legalább részben tartalmazza a tanúsítvány. Az utóbbi esetben a többi részt egy külső, a tanúsítvánnyal hivatkozott egyesített dokumentum tartalmazza (*ld.* **EGYESÍTÉS HIVATKOZÁSSAL**).

A bővített Szervezeti Egység rovat adatai megtalálhatóak a **hitelesítési politika** kiegészítésben is, ha a tanúsítvány azt tartalmazza. A jelen HSZSZ az ISO/IEC 9594-8:1995 (X.509) 1. módosítása szerint alakítja ki a „hitelesítési politikát".

A Microsec E-SZIGNÓ, mint hitelesítési politika alakítója, kijelölt egy célazonosító értéket a HSZSZ számára, amelyet a **hitelesítési politika** kiegészítése tartalmaz. A „hitelesítési politika" meghatározása szükségessé teszi a politikamódosító tényezők igénybevételét, melyek a Microsec E-SZIGNÓ meghatározása szerint lehetnek mutató értékek, felszólítások, felelősség korlátozása és szavatosság megtagadása a 3. táblázatban leírtak, illetve az alábbiak szerint.

2.5.4.2 HSZSZ mutatók

Számítógépes mutatókat (URL vagy más azonosítók és mechanizmusok), és magyar vagy angol (olvasható) szöveget vagy mutatót alkalmazhatnak, így a tanúsítvány használói könnyen megtalálhatják és elérhetik a HSZSZ-t vagy más kapcsolódó információt.

2.5.4.3 Felszólítások, felelősség korlátozások, és szavatosság megtagadása

Minden egyes tanúsítvány tartalmaz egy rövid leírást, amely részletezi a felelősség korlátozását és a szavatosság megtagadását, illetve utal a HSZSZ-ben található felszólításokkal, korlátozásokkal és megtagadással kapcsolatos teljes szövegre.

Másik lehetőségként ezek az információk a tanúsítványmegtekintő funkció segítségével megjeleníthetőek, és a felhasználó vagy képviselő számára hypertext hivatkozás (URL) segítségével hozzáférhetőek.

Az információ közlésének (megjelenítés a felhasználónál) módjai a következők lehetnek: bővített elnevezésű szervezeti egység, Microsec E-SZIGNÓ standard módosítása a Microsec E-SZIGNÓ-nál jegyzett hitelesítési politika szerint (standard v3 kiegészítés alkalmazásával), és más eladónál regisztrált kiegészítések (pl. Netscape-nél regisztrált „Megjegyzés" kiegészítés).

A „bővített" szervezeti egység „**OU=http://www.e-szigno.hu/adatok/HSZSZ**", vagy ehhez hasonló kikötéseket tartalmazhat.

2.5.5 Microsec E-SZIGNÓ Adattár

A Microsec E-SZIGNÓ adattár a nyilvánosság számára is elérhető, a tanúsítvány tárolását, visszakeresését lehetővé tevő adatbázis, amely más, a tanúsítvánnyal kapcsolatos információkat is tartalmaz.

A Microsec E-SZIGNÓ adattár tartalmazza:

(i) a tanúsítványokat,

(ii) a Tanúsítvány-Visszavonási Listát (TVL), és

(iii) más felfüggesztési és visszavonási információkat,

(iv) a Microsec E-SZIGNÓ HSZSZ jelenlegi és korábbi változatait,

(v) és esetenként más, a Microsec E-SZIGNÓ által előírt információkat.

Microsec E-SZIGNÓ adattár változatlanul közli a tanúsítványokat, a tanúsítványok felfüggesztéséről vagy visszavonásáról szóló feljegyzést és egyéb információkat.

2.5.6 Közreadás a Microsec E-SZIGNÓ Adattárán keresztül

A Microsec E-SZIGNÓ adattár haladéktalanul közreadja a tanúsítványokat, a HSZSZ módosításait, a tanúsítványok felfüggesztéséről vagy visszavonásáról szóló feljegyzéseket, és egyéb információkat a jelen HSZSZ-nek és az alkalmazandó jogszabályoknak megfelelően. A Microsec E-SZIGNÓ adattár elérhető a ldap://www.e-szigno.hu címen, vagy más kommunikációs módon, amelyet a Microsec E-SZIGNÓ időnként kijelöl.

A Microsec E-SZIGNÓ az aláírói tanúsítványokat és a TVL bejegyzéseivel kapcsolatos adatokat a Microsec E-SZIGNÓ adattártól függetlenül másképpen is közreadhatja. A jelen HSZSZ tiltja bármilyen, a HSZSZ és/vagy a Microsec E-SZIGNÓ adattár által bizalmasnak nyilvánított adattári adathoz (vagy egy tanúsítvány-kibocsátó iroda által másképp nyilvántartott adathoz) való hozzáférést, ha arra a Microsec E-SZIGNÓ nem jogosít fel.

3 HITELESÍTÉSI TEVÉKENYSÉG KIALAKÍTÁSA

MEGJEGYZÉS: A HITELESÍTÉSI KÉRELMEZÉS ÜGYMENETÉT A HSZSZ 4. MUTATJA BE.

3.1 A Microsec E-SZIGNÓ joga a veszélyeztetések kivizsgálására

A Microsec E-SZIGNÓ vizsgálatot indíthat, de nem kötelező érvénnyel, a veszélyeztetések kivizsgálására a jogszabályok keretein belül. A hitelesítési kérelem (*ld.* HSZSZ 4.) benyújtásával minden kérelmező aláveti magát ezen vizsgálatoknak. Beleegyezik (közreműködik) abba, hogy elősegíti a HSZSZ által elvárt, illetve a Microsec E-SZIGNÓ által szükségesnek tartott tények, körülmények és más vonatkozó információk ellenőrzését, feltéve, hogy ezek a vizsgálatok megfelelnek a titkossági és adatvédelmi jogszabályoknak. A hitelesítést kérelmezők és aláírók vizsgálata tartalmazhat interjúkat és a megfelelő dokumentációk bekérését és értékelését.

3.2 Alkalmazkodás a HSZSZ-hez

A Microsec E-SZIGNÓ adattárnak feladatai ellátása során alkalmazkodnia kell a HSZSZ-hez.

3.3 Megbízhatóság

A Microsec E-SZIGNÓ adattár kizárólag hitelt érdemlő, megbízható rendszereket alkalmazhat feladatai ellátásához.

3.4 Pénzügyi felelősség

A Microsec E-SZIGNÓ-nak elegendő pénzügyi forrással kell rendelkeznie működésének fenntartásához és feladatának ellátásához, és azon aláírók, tanúsítvány elfogadók és más személyekért való felelősség kockázatának viseléséhez, akik az általa kiadott tanúsítványokra és időpecsétekre hagyatkoztak. A Microsec E-SZIGNÓ-nak a hibák következményei pénzügyi fedezetével is rendelkeznie kell.

3.5 Nyilvántartások megfelelőssége

A Microsec E-SZIGNÓ-nak hitelt érdemlő módon kell nyilvántartásokat vezetnie, beleértve:

(i) az összes hitelesítési kérelem, és az összes általa kiadott tanúsítvány létrehozása, kiadása, használata, felfüggesztése, visszavonása, lejárata, megújítása vagy újrajegyzése szempontjából lényeges intézkedések és információk dokumentációját. Ezen nyilvántartásoknak a Microsec E-SZIGNÓ birtokában lévő minden vonatkozó bizonyítékot tartalmazniuk kell, tekintettel:

  - a tanúsítványban megnevezett aláíró azonosságára (kivéve az 1.szintű tanúsítványokat, melyek esetén csak az aláíró megkülönböztetett nevét tartalmazó irat szükséges),
  - a tanúsítvány felfüggesztését vagy visszavonását kérő személy azonosságára (kivéve az 1.szintű tanúsítványokat, melyek esetén csak az aláíró megkülönböztetett nevét tartalmazó irat szükséges),
  - más, a tanúsítványban szereplő adatokra, és az
  - időpecsétre.

(ii) Bizonyos előre látható, a tanúsítvány kibocsátásával kapcsolatos lényeges konkrétumokat.

Az iratok elektronikus üzenetek formájában vagy papír alapú dokumentumok formájában tárolhatók, a nyilvántartás, tárolás, megóvás és reprodukció pontossága és teljessége mellett. A Microsec E-SZIGNÓ az aláírótól vagy képviselőjétől kérheti a dokumentumok benyújtását, annak érdekében, hogy eleget tegyen a követelményeknek.

3.6 Adatmegőrzési terv

A Microsec E-SZIGNÓ-nak a tanúsítvány visszavonásának, vagy lejáratának időpontjától számítva minimum öt (5) évig meg kell őriznie hitelt érdemlő módon az 1. és 2. szintű tanúsítványokat, illetve minimum harminc (30) évig a 3. szintű tanúsítványokat. Ezen iratok akár visszaalakítható elektronikus üzenet formájában, akár papír alapú dokumentumként is megőrizhetőek.

3.7 Bizalmas információk

A Microsec E-SZIGNÓ köteles az alábbi információkat bizalmasan kezelni:

- aláírói szerződéssel kapcsolatos iratok (kivéve a HSZSZ szerint a tanúsítványon szereplő és az adattárban lévő adatokat),
- kereskedelmi ügylettel kapcsolatos iratok (a teljes dokumentáció és az ügylettel kapcsolatos ellenőrzési útvonal),
- a Microsec E-SZIGNÓ által létrehozott vagy megőrzött iratok,
- A Microsec E-SZIGNÓ hardver és szoftver működését, hitelesítés-szolgáltatás és a kijelölt bejegyzési szolgáltatás irányítását szabályozó biztonsági intézkedések leírása.

A Microsec E-SZIGNÓ nem fedheti fel, vagy adhatja el a kérelmezők nevét vagy más személyazonosító információt, és nem oszthatja meg ezeket az információkat másokkal, kivéve, ha azt a HSZSZ másképp nem szabályozza.

Bizalmas információk önkéntes felfedése.

A Microsec E-SZIGNÓ nem fedhet fel bizalmas információkat, és nem kötelezhető azok felfedésére, anélkül, hogy:

(i) egy olyan személy, akinek a Microsec E-SZIGNÓ ilyen információk bizalmas kezelésével tartozik, a felfedést megelőzően hitelesített módon kifejezetten azt kérné, vagy

(ii) ügyészi, illetve bírósági határozat utasítaná.

A Microsec E-SZIGNÓ megkívánhatja, hogy a folyamodó személy vagy szervezet díjat fizessen, mielőtt felfednék ezeket az információkat.

3.8 Személyzeti igazgatás és szabályok

A Microsec E-SZIGNÓ olyan személyzeti és irányítási szabályokat alakít ki és követ, amelyek biztosítják a végrehajtás megbízhatóságát és kompetenciáját. Ezeknek a szabályoknak összhangban kell lenniük a HSZSZ-al.

3.8.1 Bizalmi pozíció

Minden olyan Microsec E-SZIGNÓ alkalmazott, vállalkozó és szakértő (együttesen „személyzet”), aki olyan kriptografikus művelethez fér hozzá, vagy azt irányítja, amely jelentős hatást gyakorolhat a Microsec E-SZIGNÓ tanúsítvány kiadására, használatára, felfüggesztésére vagy visszavonására – beleértve a Microsec E-SZIGNÓ adattár szűkebb körű műveleteit is –, jelen HSZSZ értelmében bizalmi pozícióban tevékenykedő személynek tekintendő. A személyzetbe beleértendő – de nem kizárólagosan – az ügyfélszolgálati személyzet, rendszeradminisztrátorok, kijelölt szakemberek, és olyan felelős vezetők, akiket a Microsec E-SZIGNÓ hitelt érdemlő rendszerének ellenőrzésére jelöltek ki.

3.8.2 Kivizsgálás és teljesítés

A Microsec E-SZIGNÓ köteles vizsgálatot végrehajtani minden bizalmi pozícióban levő személyre vonatkozóan, hogy megállapítsa megbízhatóságukat és hozzáértésüket. A Microsec E-SZIGNÓ köteles időszakosan vizsgálni minden bizalmi pozícióban tevékenykedő munkatársat, hogy folyamatosan ellenőrizze megbízhatóságukat és kompetenciájukat a Microsec E-SZIGNÓ személyzeti szabályzata szerint.

3.8.3 Bizalmi pozícióban lévő személyek eltávolítása

Minden olyan munkatárs, aki nem felel meg a kiinduló vagy időszakos vizsgálatoknak, nem tevékenykedhet bizalmi pozícióban.

3.9 Microsec E-SZIGNÓ kulcs generálása

A Microsec E-SZIGNÓ köteles biztonságosan generálni és megóvni saját titkos kulcsát, hitelt érdemlő rendszer alkalmazásával, és megtenni a szükséges elővigyázatossági intézkedéseket annak érdekében, hogy az megóvja a titkos kulcsot az elvesztéstől, megsemmisítéstől, módosítástól és jogosulatlan használattól.

4 HITELESÍTÉSI KÉRELMEZÉS FOLYAMATA

Az alábbi fejezet bemutatja a hitelesítési kérelmezés folyamatát. Tartalmazza a kulcspár generálásának és védelmének követelményeit és felsorolja az egyes hitelesítési osztályok kívánalmait.

Minden olyan személy, aki tanúsítványt kíván megszerezni, köteles az alábbi általános követelményeket teljesíteni minden egyes hitelesítési kérelem esetén:

- kulcspár generálása, majd a Microsec E-SZIGNÓ felé annak igazolása, hogy az egy működő kulcspár,
- a titkos kulcs (a kulcspár egyike) veszélyeztetéssel szembeni védelme,
- a tervezett megkülönböztetett név meghatározása, és
- a hitelesítési kérelem (aláírói szerződés) benyújtása, beleértve a kulcspár nyilvános kulcsát, a Microsec E-SZIGNÓ-nak.

4.1 Kulcsgenerálás és védelem

Az alábbi folyamat alkalmazandó minden, a jelen HSZSZ-ben meghatározottak szerinti, kulcsot generáló entitás esetén.

4.1.1 A birtoklás kizárólagossága; a titkos kulcs elérhetőségének felügyelete

Ha a jelen HSZSZ másképpen nem szabályozza, minden hitelesítési kérelmező köteles biztonságban kialakítani saját titkos kulcsát, hitelt érdemlő rendszer alkalmazásával. Köteles szükséges intézkedéseket tenni a veszélyeztetés, veszteség, felfedés, módosítás és illetéktelen használat megelőzésére.

A felek megállapodnak arra nézve is, hogy az aláíró (és hitelesítést kérelmező) többnyire olyan termékeket használnak, amelyek megfelelő védelmet biztosítanak a kulcsoknak.

MINDEN EGYES HITELESÍTÉST KÉRELMEZŐ (ÉS MEGÁLLAPODÁS SZERINT MINDEN ALÁÍRÓ) ELISMERI, HOGY Ő (ÉS NEM A MICROSEC E-SZIGNÓ) A KIZÁRÓLAGOS FELELŐS A TITKOS KULCS VESZÉLYEZTETÉS, VESZTESÉG, FELFEDÉS, MÓDOSÍTÁS VAGY JOGOSULATLAN HASZNÁLAT ELLENI VÉDELEMÉRT.

4.1.2 A titkos kulcs felelősségének átruházása

Az átruházás, ha felmerül, nem menti fel az átruházó személyt a generálással, a használattal, a megtartással, vagy a titkos kulcs megfelelő megsemmisítésével kapcsolatos felelősség és kötelezettség alól.

4.2 A hitelesítési kérelem adatai és az adatok közlése

A hitelesítési kérelem adatai tartalmazzák az alábbi 4. táblázatban felsorolt adatokat. *A tanúsítvány ezek közül nem tartalmaz minden adatot* (*ld.* 3. Ábra). *Megjegyzés:* A tanúsítványban nem szereplő adatokat, információkat a Microsec E-SZIGNÓ bizalmasan kezeli (*ld.* HSZSZ 3.13.).

HITELESÍTÉSI OSZTÁLY	HITELESÍTÉSI KÉRELEM ADATAI
1. SZINT	**Személyek:** ***Kötelező adatok*** (a) Felhasználó név (vagy álnév) (b) Az alany nyilvános kulcsa (c) e-mail cím (d) aláírt aláírói szerződés (e) Hitelkártyára vonatkozó információk (ha felmerül) (f) igazoló formula (az aláíró hitelesítésére a Microsec E-SZIGNÓ felé a későbbiek folyamán) (g) Microsec E-SZIGNÓ által meghatározott egyéb információk ***Választható*** (g) demográfiai adatok ***A kérelem ügyintézésének módja:*** a Microsec E-SZIGNÓ megküldi a tanúsítvány prototípusát (nem aláírt) és az aláírói szerződést a hitelesítést kérelmezőnek. Miután az Online párbeszéd biztonságos Web csatornán keresztül valósul meg, a hitelesítést kérelmező megerősíti, hogy (i) a hitelesítési kérelem információi pontosak és (ii) elolvasta, megértette és elfogadja az aláírói szerződés feltételeit. Meghatározott hitelesítési eljárások végrehajtását követően a Microsec E-SZIGNÓ e-mailt küld a hitelesítési eljárásban, a hitelesítést kérelmező által meghatározott e-mail címre. Ez az e-mail üzenet tartalmaz egy PIN kódot (és tetszés szerint, a tanúsítvány információtartalmának tervezetét), amely felhatalmazza a hitelesítési kérelmezőt, hogy tanúsítványt kapjon a Microsec E-SZIGNÓ -tól. **Üzleti entitások:** az 1. szintű tanúsítványokat csak egyének számára bocsátják ki.

3. táblázat

2. SZINT	**Személyek:** ***Szükséges információk*** (a) Törvényes név (felhasználói név formájában) (b) tervezett megkülönböztetett név (c) állandó tartózkodási hely címe: utca, város, állam, postai irányítószám, ország (d) vezetékes telefon száma (állandó tartózkodási hely) (e) e-mail cím (f) alany nyilvános kulcsa (g) Hitelkártyára vonatkozó információk (h) házastárs kereszt neve (ha felmerül) (i) társadalombiztosítási szám (j) születési dátum (k) munkáltató (ha felmerül) (l) igazoló formula (az aláíró hitelesítésére a Microsec E-SZIGNÓ felé a későbbiek folyamán) (m) aláírt aláírói szerződés (n) előző cím (ha az elmúl két évben megváltozott) (o) vezetői engedélyre vonatkozó információk (ha felmerül) (p) a „szoftver forgalmazói kötelezettség” (csak egyéni szoftver forgalmazói hitelesítési kérelmezők esetén –*ld.* HSZSZ 4.3.) (q) a Microsec E-SZIGNÓ által meghatározott egyéb információk ***Választható*** (r) demográfiai adatok ***A kérelem ügyintézésének módja:*** *ugyanaz, mint az 1. szint esetén* ***Ügynökök/felhatalmazott képviselők**:* n/r **Üzleti entitások:** a 2. szintű tanúsítványokat csak egyének számára bocsátják ki.

4. táblázat

3. SZINT	**Személyek:** ***Szükséges információk*** *– ugyanaz mint a 2. szint esetén, plusz* (a) a hitelesítési kérelmező három (3) fajta személyazonosítása alapján (a „személyes jelenlét” követelményének eleget téve) közjegyző vagy a Microsec E-SZIGNÓ által hitelesített aláírói szerződés. ***Választható*** (b) előző munkáltató ***Ügynökök/felhatalmazott képviselők****:* A 3. szint engedélyezi a vállalkozások (nem egyének) számára, hogy ügynök kérelmezze a hitelesítést, megnevezve a megbízót (vállalkozás) mint aláírót. ***A kérelem ügyintézésének módja:*** *ugyanaz, mint az 1. szint esetén* **Üzleti entitások:** ***Szükséges információk*** (a) területi név (b) szervezet (c) szervezeti egység (ha felmerül) (d) szakmai és számlázási kontaktszemély (e) cím: utca, város, állam, postai irányítószám (f) névhasználat igazolása (harmadik fél adatbázisa általi ellenőrzés és haladéktalan megerősítés) (g) szervezeti pozíció igazolása (mint a társasági szerződés, ha van, vagy más hasonló bizonyíték) (h) az ügynök felhatalmazásának igazolása (i) a „szoftver forgalmazói kötelezettség” (j) a szerver sorozatszáma ***Választható-*** (k) cégjegyzékszám ***Ügynökök/felhatalmazott képviselők:*** *ld. fent* ***A kérelem ügyintézésének módja:*** *ugyanaz, mint az 1. szint esetén*

5. táblázat

5 HITELESÍTÉSI KÉRELEM ÉRVÉNYESÍTÉSE

Az alábbi fejezet bemutatja az illetékes TK vagy egy felhatalmazott helyi regisztrációs szerv kötelességeit a hitelesítési kérelem érvényesítése során. Továbbá bemutatja az ellenőrzés során nem megfelelt kérelmekkel kapcsolatos eljárásokat is.

5.1 Hitelesítési kérelmek érvényesítésének feltételei

A hitelesítési kérelem átvétele után (HSZSZ 4. – Hitelesítési kérelmezés folyamata szerint) a Microsec E-SZIGNÓ a tanúsítvány kibocsátásának előfeltételeként köteles minden szükséges igazolási eljárást elvégezni (HSZSZ 6. – Tanúsítványok a következőket) az alábbiak szerint. A Microsec E-SZIGNÓ köteles igazolni, hogy

(a) a hitelesítést kérelmező személye megegyezik a kérelemben azonosított személlyel (a hitelesítési osztály követelményeivel összhangban, *ld.* HSZSZ 2., és a továbbiakban leírtak szerint),

(b) a hitelesítés kérelmezője jogosan birtokolja a tanúsítványban szereplő nyilvános kulcsnak megfelelő titkos kulcsot (e feltétel teljesítéséhez elegendő a hitelesítési kérelmező nyilatkozata is)

(c) a tanúsítványban szereplő adatok pontosak, kivéve az ellenőrizhetetlen aláírói adatokat, és

(d) a hitelesítési kérelmező nyilvános kulcsát tartalmazó tanúsítványt igénylő képviselő (kizárólag 3. szintű hitelesítés esetén az üzleti entitások számra lehetséges) jogosult a kérelmezésre.

A tanúsítvány kibocsátását követően a Microsec E-SZIGNÓ csak akkor ellenőrzi és vizsgálja a tanúsítványban szereplő adatok pontosságát, ha a Microsec E-SZIGNÓ-t a jelen HSZSZ-nek megfelelően értesítik a tanúsítvány veszélyeztetéséről. A 6. táblázat Hitelesítési kérelmek érvényesítésének feltételei az egyes hitelesítési osztályok érvényesítési feltételei között fennálló különbségeket mutatja be. A Microsec E-SZIGNÓ az érvényesítési eljárások változtatásának jogát fenntartja az érvényesítési folyamat fejlesztésének érdekében. Az érvényesítéssel kapcsolatos további részleteket az alábbiak mutatják be. A módosított érvényesítési eljárások (ha történt változtatás) megtalálhatóak a Microsec E-SZIGNÓ adattárban a http://www.e-szigno/adatok/HSSZ.mod címen, és beszerezhető a Microsec E-SZIGNÓ ügyfélszolgálatán.

ÉRVÉNYESÍTÉSI FELTÉTELEK	1. SZINT	2. SZINT	3. SZINT
SZEMÉLYES JELENLÉT	Nem	Nem	Igen – Személyek: közjegyző vagy Microsec E-SZIGNÓ. Szervezetek: Opcionális
SZEMÉLYES KIVIZSGÁLÁS (EGYÉNEK ESETÉN)	Nem	Nem	Igen – Egyének: közjegyzőnél, a hitelesítési kérelem közjegyzői hitelesítésével együtt
SZEMÉLYES (EGYÉNI) ADATOK HARMADIK FÉL ÁLTAL TÖRTÉNŐ AUTOMATIZÁLT IGAZOLÁSA	Nem	Igen	Igen (*lásd* alábbiak)
ÜZLETI ENTITÁSOK HARMADIK FÉL ÁLTAL TÖRTÉNŐ IGAZOLÁSA	-	-	Igen (*lásd* alábbiak)
POSTAI IRÁNYÍTÓSZÁM IGAZOLÁSA	-	Igen (*ld.* alábbiak)	-
INTERNIC DOMAIN NÉV IGAZOLÁSA	-	-	Igen (*lásd* alábbiak)

6. táblázat Hitelesítési kérelmek érvényesítésének feltételei

5.1.1 Személyes jelenlét

Az kérelmező és a kérelmező nyilvános kulcsa közötti megfelelő kapcsolat létrehozása érdekében a 3. szintű hitelesítési osztályba tartozó tanúsítványt igénylő egyének, illetve képviselők személyes jelenlétükkel kötelesek igazolni személyazonosságukat egy bizalmi entitás előtt (pl. közjegyző, cégbíróság vagy Microsec E-SZIGNÓ). A személyes jelenlét követelményének számos módon megfelelhetnek (a tanúsítvány hitelesítési szintjétől és típusától függően), beleértve meghatározott személyazonosító okmányok bemutatását is.

5.1.2 Személyes adatok ellenőrzése harmadik fél közreműködésével

Ha szükséges, a hitelesítést igénylő által közölt személyes adatokat harmadik fél, saját adatbázisával összehasonlítva igazolhatja Az adatok hitelesek, ha a hitelesítést igénylő adatai a Microsec E-SZIGNÓ ügyfélkör illesztési algoritmus vagy más megfelelő meghatározó eljárás szerint megegyeznek az adatbázis adataival.

Az online kivizsgálás, amely az igénylő egyéni adatait közhiteles adatbázisok adataival hasonlítja össze, biztosítékkal szolgál a személyazonosságról. Ilyen adatbázisok segítségével igazolhatják az igénylő címét is. Azonban az online kivizsgálás alkalmazási körét az egyes országok adatvédelmi törvénye szabályozza.

5.1.3 Üzleti entitások adatainak ellenőrzése harmadik fél közreműködésével

Ha szükséges, a hitelesítést igénylő által közölt üzleti entitások adatait harmadik fél saját adatbázisával összehasonlítva igazolhatja. A Microsec E-SZIGNÓ megfelelő cégbíróságnál, kormányzati szervnél informálódva, és ezen a módon is igazolhatja az üzleti entitás nevét, címét, és egyéb regisztrációs adatait.

A vállalatok, bankok és megbízottjaik adatainak igazolásához bizonyos egyedi (lehetőleg lokalizált), meghatározott üzleti kritériumokra összpontosító eljárásokra van szükség. A harmadik fél telefonszámokat is biztosíthat, hogy az üzleti entitások adatait telefonon keresztül ellenőrizzék (például egy megbízott pozíciójának ellenőrzése az üzleti entitáson belüli, vagy annak igazolása, hogy a kérelemben szereplő egyén ténylegesen az igénylő). Ha az adatbázis nem tartalmazza az összes szükséges információt, a Microsec E-SZIGNÓ kérésére a harmadik fél közhiteles adatbázisok adatait felhasználva vizsgálatot végezhet, vagy a hitelesítés kérelmezőjétől további információkat és bizonyítékokat kérhet.

5.1.4 Postai irányítószám ellenőrzése

2. szintű (ideiglenes) hitelesítési osztályba tartozó tanúsítvány kibocsátását követően a Microsec E-SZIGNÓ köteles a hitelesítési kérelemben benyújtott, és ellenőrzött (harmadik fél adatbázisával igazolt – *lásd* HSZSZ 5.1.2.) postai címre visszaigazoló levelet (tértivevényes) küldeni. Ez a visszaigazolási eljárás további biztosítékot nyújt arról, hogy az aláíró címe megegyezik a hitelesítési kérelemben szereplő címmel, és az aláíró személye megegyezik a kérelemben szereplővel.

A visszaigazoló levél tartalmaz egy személyazonosító számot (PIN), amely célja a tanúsítványt igénylő hitelesítésének biztosítására szolgál.

5.1.5 InterNIC domain név igazolása és tanúsítványsorszám kijelölése

A Microsec E-SZIGNÓ hatáskörében tartozó névadó hatóság saját belátása szerint dönt a Relatív Megkülönböztetett Nevek (RMN) és az általa kiadott tanúsítványon szereplő tanúsítványsorszám kijelöléséről. A Microsec E-SZIGNÓ, ha szükséges az InterNIC-et használhatják az RMN feloldására. Az InterNIC eljárást és biztosítékokat érintő további információ megtalálható a http://ds.internic.net/ds/admin.html címen.

5.2 1-2. szintű hitelesítési osztályba tartozó hitelesítési kérelmek jóváhagyása

Az 1. vagy 2. szintű hitelesítési osztályba tartozó hitelesítési kérelmek szükséges megerősítésének sikeres teljesítését követően (a HSZSZ 5.1), a Microsec E-SZIGNÓ köteles a kérelmet jóváhagyni. A jóváhagyást a HSZSZ 6. (Tanúsítványok kiadása) szerint a normál tanúsítvány kiadása demonstrálja

5.3 3. szintű hitelesítési osztályba tartozó hitelesítési kérelmek jóváhagyása

A 3. szintű hitelesítési osztályokba tartozó hitelesítési kérelmek szükséges megerősítésének sikeres teljesítését követően (a HSZSZ 5.1) a Microsec E-SZIGNÓ köteles ideiglenesen jóváhagyni a hitelesítési kérelmet. A jóváhagyást az ideiglenes tanúsítvány kiadása biztosítja a HSZSZ 6.2 (Ideiglenes tanúsítvány) szerint.

5.4 Hitelesítési kérelem elutasítása

Ha a megerősítés nem jár sikerrel, az illetékes a Microsec E-SZIGNÓ köteles elutasítani a hitelesítési kérelmet, haladéktalanul értesítve a hitelesítés kérelmezőjét a megerősítés sikertelenségéről a sikertelenségi ok kódjának (kivéve, ha törvény tiltja) megjelölésével. Ha a megerősítés sikertelensége harmadik fél adatbázis-adatai összehasonlításának következménye, a Microsec E-SZIGNÓ köteles a hitelesítés igénylő számára elérhetővé tenni a harmadik fél kapcsolatfelvételi információit a kivizsgálás és a vita eldöntésének érdekében. Az ilyen értesítéseket ugyanolyan módon kell eljuttatni a hitelesítés igénylőjéhez, mint amilyen módon a hitelesítési kérelmet juttatták el a tanúsítvány-kibocsátó irodához.

Azon személy, akinek a hitelesítési kérelmét elutasították, a későbbiekben újra igényelheti a hitelesítést.

6 TANÚSÍTVÁNYOK KIBOCSÁTÁSA

A fejezet bemutatja a tanúsítványok kiadásának követelményeit, és felsorolja azokat a nyilatkozatokat, amelyeket a tanúsítvány-kibocsátó irodák tesznek a tanúsítvány kibocsátása után.

6.1 Normál tanúsítvány

A hitelesítési kérelem jóváhagyását követően (HSZSZ 5. szerint) a Microsec E-SZIGNÓ kiadja a tanúsítványt. A normál tanúsítvány kiadása a hitelesítési kérelem teljes és végleges Microsec E-SZIGNÓ jóváhagyását jelzi. A normál tanúsítvány a hitelesítés kérelmezőjének elfogadása után érvényes tanúsítványnak számít (*lásd* HSZSZ 7., elfogadás).

6.2 Ideiglenes tanúsítvány

Az ideiglenes tanúsítványt, bizonyos hitelesítési osztályokon belül (jelenleg 2. szintű hitelesítési osztály), az aláíró postai levelező címének megerősítése során adják ki. Az ideiglenes tanúsítvány normál tanúsítvánnyá válik az ideiglenes időszak végén, feltéve, ha nem vonták vissza *(Lásd* 6. táblázat Hitelesítési kérelmek érvényesítésének feltételei).

6.3 Az aláíró hozzájárulása a tanúsítvány kibocsátásához

A Microsec E-SZIGNÓ a hitelesítés igénylőjének hozzájárulása nélkül tanúsítványt nem adhat ki. Az igénylő által benyújtott kérelem feltételezi a kiadáshoz való hozzájárulást jóllehet, a tanúsítványt még nem fogadták el.

6.4 A tanúsítvány kiadásának megtagadása

A Microsec E-SZIGNÓ saját belátása szerint kötelezettség nélkül visszautasíthatja a tanúsítvány kiadását, és nem felel a visszautasításból eredő bármely károkért vagy költségekért. A tanúsítvány kiadásának megtagadását követően a Microsec E-SZIGNÓ köteles haladéktalanul visszatéríteni a hitelesítés kérelmezőjének a kifizetett hitelesítési bejegyzési díjat, kivéve, ha a hitelesítés kérelmezője csalárd vagy hamis információkat juttatott el a tanúsítvány-kibocsátó irodához.

6.5 Tanúsítvány kiadását követő Microsec E-SZIGNÓ nyilatkozatok

6.5.1 Microsec E-SZIGNÓ nyilatkozat az aláíró felé

(i) Ha a HSZSZ másképp nem rendelkezik, vagy a hitelesített iratban a Microsec E-SZIGNÓ és az aláíró kölcsönösen másképp nem állapodott meg, a Microsec E-SZIGNÓ vállalja a tanúsítványban megnevezett aláíróval szemben, hogy

  a. a Microsec E-SZIGNÓ által ismert, vagy a Microsec E-SZIGNÓ -tól származó adatok a valóságnak megfelelően szerepelnek a tanúsítványban,

  b. a tanúsítvány kialakítása során a Microsec E-SZIGNÓ és a hitelesítés kérelmezője közötti adatközvetítés során a Microsec E-SZIGNÓ az adatátvitelt szakszerűen teljesített.

(ii) Ha a HSZSZ másképp nem rendelkezik, vagy hitelesített iratban a Microsec E-SZIGNÓ és az aláíró kölcsönösen másképp nem állapodott meg, a Microsec E-SZIGNÓ vállalja, hogy mindent megtesz a jelen HSZSZ rendelkezéseivel összhangban annak érdekében, hogy

  a. a HSZSZ 9. rendelkezéseinek megfelelően haladéktalanul visszavonja vagy felfüggessze a tanúsítványokat, és

  b. értesítse az aláírót bármely olyan tudomására jutott tényről, amely jelentős mértékben befolyásolja az aláíró számára kibocsátott tanúsítvány érvényességét és megbízhatóságát.

(iii) A HSZSZ 6.5.1. (i) és (ii) kötelezettségei és kijelentései kizárólag az aláíró érdekeit szolgálják, nem érvényesíthető semmilyen másik fél esetén. A Microsec E-SZIGNÓ a HSZSZ 6.5.1 . (ii) bekezdésének megfelelően, a jelen HSZSZ rendelkezéseinek és a hatályos jogszabályoknak megfelelő intézkedéseket tesz.

6.5.2 Microsec E-SZIGNÓ kijelentése bizalmi fél felé

A tanúsítvány kiadásával a Microsec E-SZIGNÓ mindenki számára kinyilvánítja, aki a HSZSZ-nek megfelelő tanúsítványban szereplő nyilvános kulccsal hitelesíthető digitális aláírásban bízik, hogy:

(i) a tanúsítványban szereplő minden adat, vagy hivatkozás pontos, kivéve a ellenőrizhetetlen aláírói adatokat (EAA), és

(ii) a tanúsítvány kibocsátása során teljes mértékben eleget tesz a jelen HSZSZ követelményeinek.

6.6 Közzététel utáni kijelentés

A tanúsítvány közreadásával (*ld* HSZSZ 7.5 .) a Microsec E-SZIGNÓ igazolja a Microsec E-SZIGNÓ adattár és mindazok számára, akik a tanúsítvány által tartalmazott adatokra hagyatkoznak, hogy tanúsítványt adott ki az aláíró számára és azt az aláíró a HSZSZ 7.1 pontban meghatározottak szerint elfogadta.

6.7 A tanúsítvány kibocsátásának ideje

A Microsec E-SZIGNÓ köteles megtenni mindent annak érdekében, hogy az alábbi időtartamokon belül igazolja a hitelesítési kérelem adatait és végső felhasználó aláírói tanúsítványt adjon ki:

	1. SZINT	**2.SZINT**	**3.SZINT**
IDŐSZAK	1 órán belül	1 munkanapon belül	1-5 munkanap

A Microsec E-SZIGNÓ akkor képes betartani a határidőket, ha a hitelesítés igénylője időben eljuttatta a szükséges adatokat, és eleget tesz a Microsec E-SZIGNÓ bármilyen ügyintézéssel kapcsolatos kérésének.

6.8 A tanúsítvány érvényessége és az aktív időszak

Minden tanúsítvány érvényesnek tekintendő, ha a Microsec E-SZIGNÓ kiadta, és az aláírói elfogadta (*lásd* HSZSZ 7.). Ha felfüggesztés vagy visszavonás során nem szüntették meg az aktív időszakot, a szokásos aktív időszakok az egyes hitelesítési osztályokban az alábbiak szerint alakulnak.

TANÚSÍTVÁNY KIADÁSA:		**1. SZINT**	**2. SZINT**	**3. SZINT**
KI	**KINEK**			
MICROSEC E-SZIGNÓ	**VÉGSŐ FELHASZNÁLÓ/ALÁÍRÓ**	1 év	1 év	1 év

A tanúsítványok aktív időszaka a kibocsátás időpontjában kezdődik, kivéve, ha a tanúsítványban egy későbbi időpontot (maximum hatvan (60) nappal a kibocsátás után) határoztak meg. Az aktív időszak akkor is megkezdődik ebben az időpontban, ha a tanúsítványt még nem fogadták el.

6.9 A kiadott de nem elfogadott tanúsítványokra vonatkozó korlátozás

Az aláíró a tanúsítványban szereplő nyilvános kulcsnak megfelelő titkos kulccsal nem állíthat elő digitális aláírást (más módon sem használhatja), ha az előidézheti az érvénytelen (még nem elfogadott) tanúsítványban vetett bizalom kialakulását.

7 A TANÚSÍTVÁNY ALÁÍRÓI ELFOGADÁSA

A következő fejezet tartalmazza a tanúsítvány aláírói elfogadásának feltételeit, azokat a kijelentéseket, amelyeket az aláíró a tanúsítvány elfogadása után tesz, az aláíró titkos kulcsának védelmével kapcsolatos kötelezettségeket, és a tanúsítvány közreadásának folyamatát.

7.1 A tanúsítvány elfogadása

Az aláíró akkor fogadja el a tanúsítványt, ha a hitelesítési kérelem benyújtását (HSZSZ 4.2. pontja szerint) követően az elfogadást a 7. táblázatban leírtak szerint ki nyilvánítja.

HITELESÍTÉSI OSZTÁLY	AZ ELFOGADÁS ESZKÖZEI
1. SZINT	**Személyek:** **online(web-en keresztül):** A hitelesítés kérelmezője a tanúsítvány megszerzéséhez és az elfogadásához beírja a PIN kódját. Megjegyzés: A hitelesítést igénylő köteles a Microsec E-SZIGNÓ-t a tanúsítvány bármilyen pontatlansága vagy hiányossága esetén haladéktalanul értesíteni a tanúsítvány átvételét, közzétételét, vagy korábbi, a tanúsítvány adattartalmára vonatkozó értesítést követően. **E-mail (S/MIME):** A hitelesítés kérelmezője a tanúsítvány elfogadásakor hitelesítési kérelmet (HK) küld el a tanúsítvány-kibocsátó iroda részére. Meghatározott érvényesítési eljárások után, a Microsec E-SZIGNÓ elküldi a tanúsítványt arra az e-mail címre, ahonnan a HK-t kapta. Megjegyzés: A hitelesítést igénylő köteles a Microsec E-SZIGNÓ-t irodát a tanúsítvány bármilyen pontatlansága vagy hiányossága esetén haladéktalanul értesíteni a tanúsítvány átvételét, közzétételét, vagy korábbi, a tanúsítvány adattartalmára vonatkozó értesítést követően. **Üzleti entitások**: n/r
2. SZINT	**Személyek:** **online(web-en keresztül):** *ld. 1. Szint online* Továbbá miután a hitelesítés kérelmezője megkapta a visszaigazoló levelet a tanúsítvány-kibocsátó irodától, a hitelesítés igénylője köteles a levél tartalmát áttekinteni, és a tanúsítvány-kibocsátó irodával kapcsolatba lépni, ha a levél hibát tartalmaz, a HSZSZ (Postai irányítószám igazolása) pontjának megfelelően. **E-mail (S/MIME):** *ld. 1. Szint e-mail* **Üzleti entitások:** n/r
3. SZINT	**Személyek:** **Online (web-en keresztül):** *ld. 1. Szint on-line* **E-mail (S/MIME):** *ld. 1. Szint e-mail* **Üzleti entitások:** **online(web-en keresztül):** *ld. 1. Szint on-line* **E-mail (S/MIME):** *ld. 1. Szint e-mail*

7. táblázat

7.2 Elfogadás utáni aláírói kijelentés

A Microsec E-SZIGNÓ által kiadott tanúsítvány elfogadásával az aláíró szerződést köt a Microsec E-SZIGNÓ-val és igazolja a Microsec E-SZIGNÓ irodának és minden olyan személynek, aki megbízik a tanúsítvány adataiban, hogy az elfogadás időpontjától kezdődően a tanúsítvány aktív időszakán keresztül, ha az aláíró mást nem jelent be:

(i) minden, a tanúsítványban szereplő nyilvános kulcsnak megfelelő titkos kulcs alkalmazásával előállított digitális aláírás az aláíró digitális aláírása, a tanúsítványt elfogadták, és a digitális aláírás kialakításának időpontjában a tanúsítvány aktív (nem járt le, nem függesztették fel, és nem vonták vissza),

(ii) felhatalmazás nélkül senki sem férhet hozzá a titkos kulcshoz,

(iii) az aláíró minden, a tanúsítvány tartalmára vonatkozó, és a Microsec E-SZIGNÓ -hoz eljuttatott állítása igaz,

(iv) az aláíró tudása és ismerete szerint a tanúsítványban szereplő minden információ igaz, ezért nem értesíti haladéktalanul a Microsec E-SZIGNÓ irodát ezen információk bármilyen lényeges pontatlansága miatt (*ld.* HSZSZ 6.),

(v) a tanúsítványt, a jelen HSZSZ rendelkezéseinek megfelelően, kizárólag csak engedélyezett és törvényes célokra lehet használni, és

(vi) az aláíró végső felhasználó aláíró és nem Microsec E-SZIGNÓ iroda, így nem használhatja a tanúsítványban szereplő nyilvános kulcsnak megfelelő titkos kulcsot tanúsítvány (vagy bármilyen más hitelesített nyilvános kulcs), vagy VTL szignálására, mint egy tanúsítvány-kibocsátó iroda, kivéve, ha az aláíró és a Microsec E-SZIGNÓ erről írásban másképpen nem állapodott meg.

A TANÚSÍTVÁNY ELFOGADÁSÁVAL, AZ ALÁÍRÓ TUDOMÁSUL VESZI, HOGY MEG KELL FELELNIE A HSZSZ RENDELKEZÉSEINEK ÉS FELTÉTELEINEK ÉS AZ ALÁÍRÓI SZERZŐDÉSNEK.

7.3 A titkos kulcs felfedését megelőző aláírói kötelezettségek

A tanúsítvány elfogadásával, az aláíró kötelezettséget vállal az aláíró titkos kulcsának felügyeletére, hitelt érdemlő rendszer használatára, és a veszteségek, felfedés, módosítás és illetéktelen használat megelőzésére.

7.4 Aláírói biztosíték

A tanúsítvány elfogadásával az aláíró megállapodik abban, hogy kártalanítja és megóvja a Microsec E-SZIGNÓ-t, ügynökeit és vállalkozóit bármilyen tartozást, veszteséget, kárt, pert vagy költségeket eredményező tevékenységgel és mulasztással szemben. A költségek tartalmazzák az a Microsec E-SZIGNÓ, ügynökeik és vállalkozóik tanúsítványhasználatával és a közzététellel kapcsolatban felmerült ügyvédi költségeit, amely az alábbiakból ered:

(i) az aláíró (vagy olyan személy, amely az aláíró megbízottjának utasítására cselekszik) valótlan állítása és általa előidézett félrevezetés;

(ii) lényeges tény elhallgatása az aláíró hibájából, ha a félrevezetés vagy mulasztás hanyagság következménye, vagy az aláírónak a Microsec E-SZIGNÓ, vagy bármely, a tanúsítványban megbízó személy félrevezetése a célja.

(iii) az aláíró titkos kulcs védelmének és hitelt érdemlő rendszer használatának elmulasztása, vagy veszélyeztetést, veszteséget, felfedést, módosítást és a titkos kulcs jogosulatlan használatát megelőző intézkedések hiánya.

Ha a tanúsítványt az aláíró ügynökének kérelmére adják ki, az ügynöknek és az aláírónak együttesen és külön-külön kell a jelen alfejezetnek megfelelően kártalanítani a Microsec E-SZIGNÓ-t, ügynökeiket és vállalkozóikat. Az aláíró köteles értesíteni a kibocsátót, ha az ügynök nem valósághű tényeket közölt, vagy mulasztott.

7.5 Közzététel

Miután az aláíró elfogadta a tanúsítványt, a Microsec E-SZIGNÓ köteles, a Microsec E-SZIGNÓ határozata szerint, a tanúsítvány egy példányát a Microsec E-SZIGNÓ adattárban közzétenni. Az aláíró más adattárakban is közreadhatja a Microsec E-SZIGNÓ hitelesítési szolgáltatás tanúsítványát.

8 A TANÚSÍTVÁNYOK HASZNÁLATA

Az alábbi fejezet bemutatja azon entitások jogait és kötelezettségeit, amelyek jogait és kötelezettségeit a HSZSZ szabályozza (*lásd* “felek” meghatározása) a digitális aláírás használatával és a Microsec E-SZIGNÓ tanúsítványoknak megfelelő digitálisan szignált üzenetekkel kapcsolatosan.

A felek (Microsec E-SZIGNÓ és a tanúsítvány “használói”, pl. az aláíró és a bizalmi felek) ezennel kijelentik, hogy az alábbi előírások szabályozzák a felek jogait és egymással szembeni kötelezettségeit. A megállapodás

(i) Microsec E-SZIGNÓ esetében a jelen HSZSZ közreadásával;

(ii) Hitelesítés kérelmező, vagy aláíró esetében a hitelesítési kérelem elküldésével; és

a tanúsítvány fogadója vagy bizalmi fél esetén pedig a tanúsítványban és a tanúsítványban szereplő nyilvános kulccsal igazolható digitális aláírásban vetett bizalom kialakulásával lép érvénybe.

8.2 A végső felhasználó aláírói tanúsítvány érvényesítésének eredménye

A digitális aláírás kötelezettségeket jelent létrehozója számára, ha

(i) azt az érvényes tanúsítvány aktív időszaka alatt hozták létre,

(ii) a digitális aláírást a hitelesítési lánc segítségével megfelelően igazolni lehet,

(iii) a bizalmi félnek nincs tudomása arról, hogy az aláíró megszegte volna a HSZSZ rendelkezéseit, és

(iv) a bizalmi fél betartja a jelen HSZSZ rendelkezéseit.

A TANÚSÍTVÁNY HASZNÁLATA NEM HATALMAZZA FEL A FELHASZNÁLÓT ARRA, HOGY BÁRMELY SZEMÉLY NEVÉBEN CSELEKEDJEN, VAGY BÁRMILYEN TEVÉKENYSÉGET VÉGREHAJTSON. A DIGITÁLISAN ALÁÍRT ÜZENET ELLENŐRZŐI EGY SZEMÉLYBEN FELELŐSEK A GONDOS ÉS ÉSSZERŰ VÉLEMÉNY KIALAKÍTÁSÁÉRT, MIELŐTT A TANÚSÍTVÁNYOKRA ÉS DIGITÁLIS ALÁÍRÁSOKRA HAGYATKOZNÁNAK. A TANÚSÍTVÁNNYAL A MICROSEC E-SZIGNÓ NEM RUHÁZ ÁT SEMMILYEN JOGOT VAGY ELŐJOGOT, KIVÉVE, HA A JELEN HSZSZ ARRÓL MÁSKÉPP RENDELKEZIK.

8.3 A digitális aláírás megerősítésének sikertelenségét követő intézkedések

Az ellenőrizhetetlen digitális aláírásra hagyatkozó személy minden ezzel kapcsolatos kockázatot vállal, és a digitális aláírás nem tekinthető az aláíró aláírásának a HSZSZ 8.4-8.6 . pontjainak megfelelően.

8.4 Bizalom a digitális aláírásban

Az aláíró által digitálisan aláírt üzenet fogadója megbízhat a digitális aláírásban, és követeléseket támaszthat az aláíróval szemben, ha:

(i) a digitális aláírást az érvényes tanúsítvány aktív időszaka alatt hozták létre és az az érvényesített hitelesítési láncra hivatkozva ellenőrizhető,

(ii) a bizalom indokolt az adott körülmények között. Ha a körülmények további biztosítékokat kívánnak meg, a bizalmi fél köteles megszerezni a biztosítékokat az indokolt bizalom kialakításához.

A fentieken kívül ellenőrző személy köteles figyelembe venni a tanúsítvány hitelesítési osztályát és a tanúsítvány állapotát (normál, ideiglenes). Kizárólag az ellenőrző személy dönthet arról, hogy az ellenőrzött digitális aláírás bizalmat érdemel, vagy sem.

8.5 Írás

Érvényes tanúsítványban szereplő nyilvános kulccsal megerősített digitális aláírással ellátott üzenet ugyanolyan érvényes, eredményes és érvényesíthető, mintha az üzenetet papíron rögzítették és írták volna alá.

8.6 Aláírás

Ha a jogszabályok vagy az alkalmazandó gyakorlat aláírást tesz szükségessé, vagy az aláírás hiánya bizonyos következményekkel jár, az üzenetek esetén a jogszabálynak megfelel az aláíró digitális aláírása, amelyet utólagosan az érvényes tanúsítványban szereplő nyilvános kulcsra való hivatkozás erősít meg.

8.7 Biztonsági intézkedések

Bármely, Microsec E-SZIGNÓ által kiadott tanúsítványt és azzal összefüggő üzenetet a felhasználó, vagy arra hagyatkozó személy köteles az üzenetet biztonsági eszközökkel ellátni, biztosítva az üzenet hitelességét és, amennyiben szükséges, az adatok megbízhatóságát.

8.8 Tanúsítványok kiadása

Kizárólag a Microsec E-SZIGNÓ adhat ki tanúsítványt.

9 TANÚSÍTVÁNY FELFÜGGESZTÉSE ÉS VISSZAVONÁSA

A következő fejezet bemutatja, hogy mikor kerülhet sor a tanúsítványok felfüggesztésére vagy visszavonására. Továbbá részletezi a felfüggesztés, visszavonás és az újra érvénybehelyezés folyamatát.

9.1 A felfüggesztés és a visszavonás általános kiváltó okai

A tanúsítványt fel kell függeszteni, vagy visszavonni, ha

- a tanúsítvány alanyának titkos kulcsát ellopták, módosították, jogtalanul felfedték, vagy másképpen veszélyeztették,
- a tanúsítvány alanya (aláíró) a jelen HSZSZ-ben meghatározott kötelességének nem tett eleget, vagy
- a jelen HSZSZ-ben meghatározott kötelezettségek teljesítését késleltetik, vagy vis maior; természeti katasztrófa; számítástechnikai vagy kommunikációs hiba; törvények, jogszabályok változása; hivatalos kormányzati intézkedés, vagy más, a személyes hatáskörön kívüli okok, és más személy információinak jelentős fenyegetettsége és veszélyeztetettsége következtében meghiúsították.

9.2 Visszavonás aláírói kérésre

A Microsec E-SZIGNÓ köteles az aláíró kérésére visszavonni a tanúsítványt, ha megerősítik, hogy a tanúsítvány visszavonását kérő személy maga az aláíró.

9.3 Visszavonás hibás kibocsátás miatt

A Microsec E-SZIGNÓ köteles haladéktalanul visszavonni a tanúsítványt, ha bebizonyosodik, hogy azt nem a HSZSZ-nek megfelelő módon adták ki. A visszavonás okainak kivizsgálása alatt a tanúsítványt felfüggeszthetik.

9.4 A felfüggesztést és visszavonást követő értesítés és megerősítés

A tanúsítvány felfüggesztését vagy visszavonását követően a Microsec E-SZIGNÓ köteles a Microsec E-SZIGNÓ adattárban közzétenni a felfüggesztésről vagy visszavonásról szóló értesítést. A Microsec E-SZIGNÓ a következő dokumentumokat teheti közzé:

- Biztonságos csatornán elérhető visszavont (és felfüggesztett) tanúsítványok listája,
- Visszavont tanúsítványok listája (VTL) jelölve mind a visszavont, mind a felfüggesztett tanúsítványokat. A Microsec E-SZIGNÓ köteles legalább naponta közzétenni a visszavont tanúsítványok listáját. A Microsec E-SZIGNÓ döntése szerint a VTL-t sürgős esetekben azonnal is közreadhatják.

Kérésre, a szükséges díjak megfizetése mellett, a Microsec E-SZIGNÓ az alábbi felfüggesztési és visszavonási értesítéseket küldheti:

- A tanúsítvány visszavonásának vagy felfüggesztésének megerősítése, ha tanúsítvány alanyától származó digitális aláírással ellátott üzenetben azt kérték,
- Haladéktalan értesítés biztosítása, azaz az adott tanúsítvány felfüggesztését vagy visszavonását követő értesítés a Microsec E-SZIGNÓ részéről.

9.5 A felfüggesztés és a visszavonás következményei

9.5.1 Tanúsítványok

A felfüggesztés alatt, vagy az aláíró tanúsítványának visszavonását követően, a tanúsítvány aktív időszakát megszűntnek kell tekinteni.

9.5.2 Alapvető kötelezettségek

A tanúsítvány felfüggesztése vagy visszavonása nem befolyásolhatja a jelen HSZSZ-ben kialakított és közzétett szerződésbe foglalt kötelezettségeket.

9.5.3 A titkos kulcs védelme a felfüggesztést vagy visszavonást követően

A felfüggesztett vagy visszavont tanúsítványban szereplő nyilvános kulcsnak megfelelő titkos kulcsot, ha nem semmisült meg, köteles az aláíró hitelt érdemlő módon a felfüggesztés időtartama alatt, és a visszavonást követően az előírt visszatartási időszakban megvédeni.

10 TANÚSÍTVÁNY LEJÁRATA

A fejezet leírja a felek tanúsítvány lejáratával kapcsolatos kötelezettségeit. A tanúsítvány lejárata nem egyezik meg a tanúsítvány felfüggesztésével és visszavonásával (*lásd* HSZSZ 9.). A tanúsítvány érvényességét és aktív időszakát a HSZSZ 6.9. pontja tárgyalja.

10.1 A lejáratot megelőző értesítés

A Microsec E-SZIGNÓ mindent megtesz annak érdekében, hogy e-mailen keresztül értesítse az aláírókat a tanúsítvány közeli lejáratáról. Ez az értesítés kizárólag az aláíró kényelmét szolgálja az újrajegyzési vagy megújítási folyamat során.

10.2 A tanúsítvány lejáratának alapvető kötelezettségekre gyakorolt hatása

A tanúsítvány lejárata nem befolyásolhatja a jelen HSZSZ-ben kialakított és közzétett szerződésbe foglalt kötelezettségeket.

10.3 Újrajegyzés és aláírói megújítás

Az aláírói újrajegyzést és megújítást a következő módokon lehet kezdeményezni:

1. SZINT	2. SZINT	3. SZINT
A kezdő kérelmezési folyamattal megegyező teljes folyamat	A kezdő kérelmezési folyamattal megegyező teljes folyamat. A hitelesítést igénylő csak az új vagy megváltozott adatokat köteles elküldeni.	A kezdő kérelmezési folyamattal megegyező teljes folyamat. A hitelesítést igénylő csak az új vagy megváltozott adatokat köteles elküldeni.

8. táblázat

A megújítás és az újrajegyzés követelményeit a Microsec E-SZIGNÓ belátása szerint megváltoztathatja. Az újrajegyzéssel és megújítással kapcsolatos legfrissebb információk elérhetőek a Microsec E-SZIGNÓ adattárban a http://www.e-szigno.hu címen.

11 A MICROSEC E-SZIGNÓ KÖTELEZETTSÉGEI ÉS KORLÁTOZÁSAI

A következő fejezet összefoglalja a Microsec E-SZIGNÓ visszatérítési politikáját Microsec E-SZIGNÓ szavatosságait, ezen kötelezettségek megtagadását és korlátozását.

11.1 Visszatérítési politika

A Microsec E-SZIGNÓ betartja a hitelesítési tevékenység és a tanúsítványok kibocsátásának szabályait. Mindazonáltal, ha az aláíró bármilyen okból nem elégedett a számára kiadott tanúsítvánnyal, a kibocsátástól számított harminc (30) napon belül az aláíró kérheti a Microsec E-SZIGNÓ-tól a tanúsítvány visszavonását. Az első harminc (30) napot követően az aláíró kezdeményezheti a Microsec E-SZIGNÓ-nál a tanúsítvány visszavonását, és kártérítést igényelhet, ha a Microsec E-SZIGNÓ megsértette az aláíróval vagy az aláírói tanúsítvánnyal kapcsolatos, a jelen HSZSZ-ben rögzítetteket. Miután a Microsec E-SZIGNÓ visszavonta az aláíró tanúsítványát, a Microsec E-SZIGNÓ visszafizeti az aláírónak a tanúsítványért fizetett díj teljes összegét.

11.2 Korlátozott szavatosság és más kötelezettségek

A Microsec E-SZIGNÓ, a jelen HSZSZ vonatkozó fejezeteinek értelmében

- biztosítja az infrastruktúrát és a hitelesítési szolgáltatást, beleértve a Microsec E-SZIGNÓ adattár létrehozását és működtetését, a HSZSZ 2. (Microsec E-SZIGNÓ hitelesítési infrastruktúra) fejezetében leírtak szerint,
- ellátja a Microsec E-SZIGNÓ NYKI felügyeletét és alapítását, beleértve a Microsec E-SZIGNÓ kulcsgenerálást, kulcsvédelmet,
- elvégzi az adott hitelesítési osztályban a hitelesítési kérelmek érvényesítését a HSZSZ 5. (Hitelesítési kérelem érvényesítése) fejezetében leírtak szerint,
- a HSZSZ 6. fejezetének megfelelően tanúsítványokat ad ki, és tiszteletben tartja az aláírók és bizalmi felek felé a HSZSZ 6.5. pontjában leírt kijelentéseket (Tanúsítvány kiadását követő Microsec E-SZIGNÓ kijelentések)
- a HSZSZ 6.6. (Közzététel utáni kijelentés) és a HSZSZ 7.5. (Közzététel) pontjainak megfelelően közzéteszi az elfogadott tanúsítványokat,
- teljesíti a Microsec E-SZIGNÓ kötelezettségeit és támogatja a tanúsítványt használó aláírók és bizalmi felek jogait a HSZSZ 8. (A tanúsítványok használata) fejezetének megfelelően,
- a HSZSZ 9. (Tanúsítvány felfüggesztése és visszavonása) fejezetének rendelkezései szerint tanúsítványokat függeszt fel és von vissza,
- intézkedik a tanúsítványok lejáratával, újrajegyzésével és megújításával kapcsolatban a HSZSZ 10. (Tanúsítvány lejárata) fejezetében leírtak szerint,
- megfelel a HSZSZ 12. (Egyéb Rendelkezések) fejezetében található rendelkezéseknek.

Továbbá a Microsec E-SZIGNÓ garantálja, hogy saját titkos kulcsaikat semmi nem veszélyezteti, kivéve, ha ennek ellenkezőjéről nem értesítik a feleket a Microsec E-SZIGNÓ adattáron keresztül.

A MICROSEC E-SZIGNÓ A JELEN HSZSZ-BEN FOGLALTAKAT MEGHALADÓAN ÉS NEM VÁLLAL TOVÁBBI KÖTELEZETTSÉGEKET.

11.3 A Microsec E-SZIGNÓ kötelezettségeinek korlátozása és megtagadása

A FENTIEKBEN (HSZSZ 11.3.) FELSOROLTAKON KÍVÜL A MICROSEC E-SZIGNÓ MEGTAGAD MINDENNEMŰ SZAVATOSSÁGOT ÉS KÖTELEZETTSÉGET.

Ha a fentiek (HSZSZ 11.3) azt kifejezetten nem tartalmazzák, a Microsec E-SZIGNÓ

- nem garantálja a tanúsítványban szereplő, közzétett, vagy terjesztett adatok pontosságát, hitelességét, megbízhatóságát, teljességét, aktualitását, piacképességét, vagy alkalmasságát,
- nem tartozik felelősséggel a tanúsítványban szereplő adatokért, feltéve, ha a tanúsítvány tartalma lényegében megfelel a jelen HSZSZ rendelkezéseinek,
- nem garantálja a tanúsítvány vagy üzenet letagadhatatlanságát (mivel a "letagadhatatlanságot" kizárólag jogszabály és vita eldöntő mechanizmus határozhatja meg), és
- nem garantál semmilyen szoftvert.

11.4 Bizonyos kárelemek kizárása

A Microsec E-SZIGNÓ nem vállalt felelősséget bármilyen indirekt, egyedi, eseti vagy következményes kárért, illetve bármilyen pénzveszteségért, adatveszteségért, vagy egyéb indirekt, következményes, vagy büntetésből adódó kárért, mely a tanúsítványok, digitális aláírások, vagy egyéb, a jelen HSZSZ-ban ajánlott és szabályozott üzletkötés vagy szolgáltatás alkalmazásával, eladásával, licence-ével, teljesítésével, vagy nem teljesítésével kapcsolatban merül fel.

11.5 Kár- és veszteségkorlátozás

A Microsec E-SZIGNÓ, kártérítési felelőssége minden egyéb fél felé (beleértve az összes aláírót, igénylőt, fogadót, vagy bizalmi felet) semmilyen körülmények között nem haladhatja meg a tanúsítvány esetében a 12. táblázat szerint meghatározott kártérítési összeget.

A Microsec E-SZIGNÓ egyesített kártérítési felelőssége minden, egy bizonyos tanúsítvánnyal kapcsolatos személy felé, nem haladhatja meg a tanúsítvánnyal összefüggő digitális aláírás és üzletkötés alábbi költségeit.

	KÁRTÉRÍTÉSI ÖSSZEGEK
1. SZINT	10 000 HUF
2. SZINT	25 000 HUF
3. SZINT	100 000 HUF

9. táblázat

A kártérítés korlátozása érvényes a veszteségek és károk minden típusára, beleértve, de nem kizárólagosan a közvetlen, kompenzációs, közvetett, egyedi, következményes, eseti és a kár összegét meghaladó kártérítést, amelyet bármely személy, beleértve az aláírót, igénylőt, fogadót, vagy megbízható felet, köteles fizetni, és amely a Microsec E-SZIGNÓ által kiadott, kezelt, használt, felfüggesztett, vagy visszavont tanúsítvány, illetve lejárt tanúsítvány használatából ered. A kártérítés korlátozása alkalmazandó bármely kártérítési szerződés, kárt okozó cselekmény, és bármely egyéb kártérítési követelés esetén. A kártérítési összegnek minden tanúsítvány esetében meg kell egyeznie, függetlenül a digitális aláírások, üzletkötések, vagy a tanúsítvánnyal kapcsolatos követelések számától. Ha a kifizetendő kártérítés meghaladja az igényelt kártérítési összeget, először a legelső kártérítési igényt kell kielégíteni, kivéve, ha az illetékes bíróság másképp rendelkezik. Semmilyen körülmények között nem köteles a Microsec E-SZIGNÓ az egyes tanúsítványok esetén a lehetséges kártérítési összegnél nagyobb kártérítést fizetni, függetlenül a kártérítési összeg, a kártérítést igénylők közötti felosztásának módszerétől.

11.6 Aláírói felelősség a bizalmi felek felé

Más, a jelen HSZSZ-ben meghatározott aláírói kötelezettség korlátozása nélkül, az aláírók felelősek a tanúsítvány tartalmának minden hibájáért, hiányosságáért minden olyan harmadikféllel szemben, akik egy vagy több digitális aláírást igazolva a tanúsítvánnyal, megbíztak a tanúsítványban szereplő adatokban.

11.7 Bizalmon kívül alapuló kapcsolat

Az Microsec E-SZIGNÓ az aláíróknak és a bizalmi feleknek nem ügynöke, bizalmi személye, vagy más képviselője. A Microsec E-SZIGNÓ és az aláírók, illetve a Microsec E-SZIGNÓ és a bizalmi felek között fennálló viszony nem ügynök – megbízó viszony. Az aláírók, és a bizalmi felek nincsenek felhatalmazva arra, hogy a Microsec E-SZIGNÓT bármire kötelezzék. Kockázatos tevékenységek

A Microsec E-SZIGNÓ hitelesítési szolgáltatás nem jogosult és nem alkalmas arra, hogy kockázatos körülmények között, mint ellenőrző eszközt alkalmazzák, illetve újra eladják, vagy üzembiztonságot igénylő körülmények között, mint például nukleáris eszközök működtetésénél, légi irányítás vagy kommunikáció esetén, légi forgalom, vagy fegyverkezés irányítási rendszere esetén használják, ahol egy hiba közvetlen halálesetet, személyi sérülést, vagy komoly környezeti károkat okozhat.

12 EGYÉB RENDELKEZÉSEK

A következő fejezet olyan rendelkezéseket és feltételeket tartalmaz, amelyek nem találhatóak meg a jelen HSZSZ egyéb fejezeteiben.

12.1 Ellentmondó rendelkezések

Ellentmondó rendelkezések esetén az aláíró köteles a jelen HSZSZ rendelkezései alá vetni magát, kivéve, ha (i) a HSZSZ első kiadását megelőzően létrejött a szerződés, vagy (ii) a szerződés helyettesíti a jelen Hitelesítés Szolgáltatási Szabályzatot.

12.2 Irányadó jog

A Magyar Köztársaság jogrendszere szabályozza a jelen HSZSZ alkalmazhatóságát, felépítését, értelmezését, és érvényességét. Ezeket a jogszabályokat azért hozták létre, hogy biztosítsák az egységes eljárásokat és értelmezést minden felhasználó esetében, függetlenül attól, hogy hol tartózkodik és használja-e a tanúsítványát.

12.3 Vita eldöntése, fórum választása, és vélelem

12.3.1 Vita bejelentése a felek között

Mielőtt igénybe vennék a vita eldöntő mechanizmust (beleértve javaslatot vagy egyeztető eljárást, az alábbiakban részletezett módon), a jelen HSZSZ szempontjaival vagy a Microsec E-SZIGNÓ által kiadott tanúsítvánnyal kapcsolatos vitának eldöntésére, a kezdeményező fél köteles értesíteni a Microsec E-SZIGNÓ-t, és minden vitarésztvevő felet, akik maguk között megoldást keresnek.

12.3.2 NYKI Szakértői Bizottság

Ha a vitát nem döntik el a HSZSZ 12.4.1 pontjának megfelelő értesítés elküldését követő tíz (10) napon belül, a felek továbbíthatják a vitatott problémát írott vagy elektronikus formában a Microsec E-SZIGNÓ-hoz, hogy az NYKI Szakértői Bizottságától (NYKI SZB) kérjenek elbírálást. Ezt követően a Microsec E-SZIGNÓ összehívja a három NYKI szakértőből álló NYKI SZB-t, hogy összegyűjtsék a vita megoldását elősegítő tényeket. A kifogást benyújtó fél köteles a beadvány egy-egy példányát minden érintett fél részére eljuttatni. Bármely nem kezdeményező fél egy (1) héten belül megfelelő információkat biztosíthat a NYKI SZB számára. Az NYKI SZB köteles a benyújtástól számított három (3) héten belül döntést hozni, és azt közölni a felekkel, (kivéve, ha a felek kölcsönösen megegyeznek az időszak határozott idejű meghosszabbításában). Az NYKI SZB általában e-mailen, telefonon, és futár-, illetve hagyományos postai úton tevékenykedik. Az NYKI SZB javaslatai nem kötelező érvényűek a felekre nézve.

12.3.3 Vita hivatalos eldöntése

Miután az NYKI SZB meghozta és közölte javaslatait, de a NYKI SZB nem tudott megfelelő döntést hozni és azt közölni (a HSZSZ 12.4.2. pontjával összhangban), a az alábbiak szerint igénybe vehető a vitát eldöntő mechanizmus. A HSZSZ 12.4 pontja nem tilthatja meg a Microsec E-SZIGNÓ-nak, hogy állítólagos veszélyeztetés vagy állítólagos szabályszegés esetén az irányadó jogszabályoknak és a jelen HSZSZ-nek megfelelően méltányos (beleértve az elrendelést) enyhítéseket keressen.

(i) **Minden vitázó fél belföldi illetékességű személy, vagy belföldön székelő szervezet.** Ha a vitázó felek nem egyeznek meg egy alternatív vitaeldöntő mechanizmusban (pl. választott bírói eljárás), minden, a jelen HSZSZ rendelkezéseit érvényesítő, a jelen HSZSZ-al kapcsolatos, vagy a felek közötti üzleti kapcsolatot érintő pert kötelesek az illetékes megyei vagy a Fővárosi bíróság elé vinni. Ha a felek alternatív módszert választanak a vita eldöntésére, a magyar jog szabályozza az egyeztető eljárást.

(ii) **Egy vagy több vitázó fél külföldi illetékességű személy, vagy külföldön székelő szervezet.** A HSZSZ-al kapcsolatban felmerülő minden vitás ügyben a Nemzetközi Kereskedelmi Kamara (ICC) a HSZSZ rendelkezéseinek megfelelően egy vagy több választott bíró által módosított Békéltetési és Egyeztetési Szabályzata a döntő. A választott bírói eljárásnak Budapesten magyar nyelven kell lezajlania. Egy választott bíró esetén a választott bíró személyéről a felek kötelesek kölcsönösen megegyezni. Ha tizenöt (15) napon belül nem egyeznek meg a felek a választott bíró személyében, az ICC köteles választott bírót választani, aki jártas a számítástechnikai szoftver jogban, adatbiztonságban, és kriptográfiában, vagy más képesítéssel rendelkezik e területen.

12.4 Jogutódok és jogosítottak

A jelen HSZSZ a jogutódokra, végrehajtókra, örökösökre, képviselőkre, ügyintézőkre és jogosítottakra nézve kötelező érvényű, és azok érdekeit szolgálja. A jelen HSZSZ-ben meghatározott jogokat és kötelezettségeket a felek, vagy a törvény (fúzió, vagy szavazati jogot biztosító értékpapírok többségi részesedésének átruházása) átruházhatja, feltéve, hogy az átruházás nem újítja meg az átruházás időpontjában az átruházó fél más felekkel szemben fennálló egyéb tartozásait vagy kötelezettségeit.

12.5 Fúzió

A jelen HSZSZ egyetlen kikötése és rendelkezése sincs hatással a Microsec E-SZIGNÓ vagy bármelyik tanúsítvány-kibocsátó iroda jogaira és kötelezettségeire, amelyet szóban módosítottak, lemondtak róla, kiegészítettek, módosítottak, vagy megszüntettek, kivéve az érintett fél hitelesített üzenete vagy dokumentuma által, kivéve, ha a HSZSZ másképp nem rendelkezik.

12.6 Elkülöníthetőség

Ha a HSZSZ bármely rendelkezése, vagy annak alkalmazása, bármilyen okból és bármilyen mértékben érvénytelennek vagy végrehajthatatlannak minősül, a HSZSZ fennmaradó részét (és az érvénytelen és végrehajthatatlan rendelkezések más személyekre és körülményekre való ráillesztését) úgy kell értelmezni, hogy az legjobban megfeleljen a felek szándékainak. A FELEK MEGÁLLAPODNAK ARRA NÉZVE, HOGY A JELEN HSZSZ MINDEN OLYAN RENDELKEZÉSE, AMELY A FELELŐSSÉG KORLÁTOZÁSÁRÓL, BÁRMILYEN SZAVATOSSÁG VAGY KÖTELEZETTSÉG KORLÁTOZÁSÁRÓL VAGY MEGTAGADÁSÁRÓL, VAGY A KÁRTÉRÍTÉS KIZÁRÁSÁRÓL RENDELKEZIK, ELKÜLÖNÍTHETŐ ÉS FÜGGETLEN MINDEN MÁS RENDELKEZÉSTŐL ÉS ENNEK MEGFELELŐEN KELL VÉGREHAJTANI.

12.7 Értelmezés és fordítás

Ha másképpen nem rendelkeztek, a jelen Hitelesítés Szolgáltatási Szabályzatot kereskedelmi szempontból a legmegfelelőbb módon kell értelmezni az adott körülmények között. A HSZSZ értelmezésekor figyelembe kell venni a nemzetközi lehetőségeket és alkalmazást, az alkalmazás egységesítésének érdekét, és a jóhiszeműség megtartását.

A jelen HSZSZ a magyar nyelven kívül más nyelveken is megtalálható az adattárban. Ha a magyar és a másik nyelven közölt változat eltér egymástól, értelmezéskor a magyar változat az irányadó.

12.8 Elállás korlátozása

Ha a jelen HSZSZ bármely rendelkezését valamely személy nem hajtotta végre, nem jelenti az adott, vagy más rendelkezés végrehajtásától való elállást.

12.9 Értesítés

Ha bármely személy a továbbiakban értesítést, követelést, vagy kérelmet kíván vagy köteles a jelen HSZSZ-sel kapcsolatban elküldeni, azt a jelen HSZSZ követelményeinek megfelelő digitálisan aláírt üzenet formájában, vagy írásban teheti meg. Az elektronikus kommunikáció eredményes, ha a feladó a fogadótól érvényes, digitálisan aláírt elismervényt kap a fogadásról.

Az ilyen elismervényeket öt (5) napon belül meg kell kapni. Írásos értesítést is lehet alkalmazni. Az írásos értesítést futárszolgálattal, amely írásban, vagy ajánlott levélben igazolja a kézbesítést, előre készpénzzel bérmentesítve, visszaigazolási kérelemmel kell eljuttatni az alábbi címre:

Microsec Számítástechnikai Fejlesztő kft
1022 Budapest, Márcibányi tér 9.

A Microsec E-SZIGNÓ-tól egy másik személy részére:

A Microsec E-SZIGNÓ –nál nyilvántartott iraton található legújabb cím.

12.10 A jelen HSZSZ fejezetcímei és függelékei

A jelen HSZSZ-ben található fejezet- és alfejezet címek és egyéb jelzések csupán a kényelem és hivatkozás célját szolgálják, és nem használhatóak a HSZSZ rendelkezéseinek magyarázatakor, értelmezésekor, vagy végrehajtásakor. A függelék, beleértve a jelen HSZSZ meghatározásait, minden esetben a HSZSZ szerves és kötelező érvényű része.

12.11 Az TK nyilvántartásában lévő aláírói adatok változtatása

12.11.1 A Microsec E-SZIGNÓ által kezelt aláírói adatok megváltoztatása

Bármely aláíró megváltoztathat a Microsec E-SZIGNÓ által tárolt bizonyos adatokat saját magával kapcsolatban, amelyeket nem tartalmaz a tanúsítvány (jellemzően, az aláírói szerződésben vagy a hitelesítési kérelemben szereplő adatokat), a HSZSZ 12.10. (Értesítés) pontjának megfelelően harminc (30) napos értesítéssel. Az ilyen adatváltozás harminc (30) nap után lép érvénybe.

12.11.2 A HSZSZ módosításai

12.11.2.1 Általános módosítások

A Microsec E-SZIGNÓ jogosult a jelen HSZSZ időszakos módosítására (a jövőre vonatkozóan és nem visszamenőleg). A Microsec E-SZIGNÓ jogosult a módosítások elhelyezésére a Microsec E-SZIGNÓ adattárban, vagy a HSZSZ módosított változatának közzétételével, vagy a Microsec E-SZIGNÓ adattár Frissített Szabályok és Értesítések (Practices Updates and Notices) szekciójában.

12.11.2.2 Frissített Szabályok és Értesítések

A Microsec E-SZIGNÓ adattár Frissített Szabályok és Értesítések szekciójában közzétett HSZSZ módosítások (*lásd* **http://www.e-szigno.hu/adatok/mod**) módosítják magát a HSZSZ-t. Ezek a módosítások helyettesítik a hivatkozott HSZSZ változatának kijelölt, ellentmondó rendelkezéseit.

12.11.2.3 Lényegbevágó módosítások

A HSZSZ lényegbevágó módosításai tizenöt (15) nappal azt követően lépnek érvénybe, hogy a Microsec E-SZIGNÓ közzétette a módosításokat a Microsec E-SZIGNÓ adattárban a HSZSZ 12.12.2.1 pontjának megfelelően, kivéve, ha a Microsec E-SZIGNÓ a módosítás visszavonásáról értesítést tesz közzé az adattárban a tizenöt (15) napos időtartamon belül.

12.11.2.4 Lényegbevágó módosítások kifogásolása

A HSZSZ 12.12.2.3 pontjával ellentétben, ha a Microsec E-SZIGNÓ a HSZSZ lényegbevágó módosítását a HSZSZ 12.12.2.1. pontjának megfelelően közzéteszi, a Microsec E-SZIGNÓ adattárban közzétett adatok, a közzétételt követően haladéktalanul érvénybe lépnek, ha a módosítás elmulasztása a Microsec E-SZIGNÓ, vagy bármely részének veszélyeztetését vonja maga után.

12.11.2.5 Nem lényegbevágó módosítások

A HSZSZ nem lényegbevágó módosításai haladéktalanul érvénybe lépnek a Microsec E-SZIGNÓ adattárban. Egy módosítást saját belátása szerint kizárólag csak a Microsec E-SZIGNÓ nyilváníthat nem lényegbevágónak.

12.11.2.6 Hozzájárulás a módosításokhoz

Ha a hitelesítést igénylő és az aláíró nem kéri tanúsítványának visszavonását a módosítás közzétételétől számított tizenöt (15) napon belül, az a módosítás elfogadását jelenti.

Lásd a Microsec E-SZIGNÓ adattárának Frissített Szabályok és Értesítések szekcióját a **http://www.e-szigo.hu/adatok/mod** címen.

12.12 Vagyoni érdekeltség a biztonsági eszközökben

Ha másképpen nem egyeztek meg, a vagyoni érdekeltség az alábbi biztonsággal kapcsolatos információs eszközök és adatok esetén az alábbiak szerint oszlik meg a felek között:

- **Tanúsítványok:** A tanúsítványok az illetékes tanúsítvány-kibocsátó iroda tulajdonát képezik. A Microsec E-SZIGNÓ által kiadott tanúsítványok szerzői jogvédelemmel van ellátva: "Copyright ©2000 E-SZIGNÓ HSZH, Minden jog fenntartva", vagy "©2000" a Microsec E-SZIGNÓ-val kapcsolatban. Lehetőség van a tanúsítványok nem kizárólagos, szerzői jogdíj mentes többszörözésére és elosztására, ha teljes terjedelmükben készítenek másolatot osztják el azokat, kivéve, ha a tanúsítványt nem tehetik közzé nyilvánosság számára elérhető adattárakban vagy könyvtárakban a Microsec E-SZIGNÓ írásos engedélye nélkül. A megszorítás célja, részben, az aláírói titok védelme a tanúsítványok illetéktelen újrakiadásával szemben. A szerzői jogvédelemmel kapcsolatos kérdéseiket feltehetik a HSZSZ 12.10 (Értesítés) pontjában felsorolt címeken, vagy a jogi.informatika**@e-szigno.hu** e-mail címen.
- **HSZSZ:** A jelen HSZSZ a Microsec kft. tulajdonát képezi.
- **Megkülönböztetett nevek:** A megkülönböztetett nevek a nevezett személy (vagy munkáltatója, vagy felettese) tulajdonát képezi.
- **Titkos kulcs:** A titkos kulcs az aláíró személyes tulajdona, aki (vagy munkáltatója, vagy felettese) a titkos kulcs teljes jogú használója, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.
- **Nyilvános kulcs:** A titkos kulcs az aláíró személyes tulajdona, tekintet nélkül arra a fizikai közegre, amely tárolja és védi a kulcsokat.
- **Microsec E-SZIGNÓ nyilvános kulcsok:** A Microsec E-SZIGNÓ gyökér nyilvános kulcsa, a Microsec kft. tulajdona. A Microsec E-SZIGNÓ csak hitelt érdemlő hardware vagy szoftver termékekkel kapcsolatban engedélyezi a felek számára a kulcsok használatát,

amely során a gyökér nyilvános kulcsát a Microsec E-SZIGNÓ meghatalmazásával osztják szét.

12.13 Visszaélés és egyéb károkozás

A hitelesítést igénylők (és elfogadást követően aláírók) kijelentik és szavatolják, hogy a beadvány. (Microsec E-SZIGNÓ-hoz), és a domain és megkülönböztetett nevének használata (és más hitelesítési kérelem információ) nem sérti, és nem ütközik harmadik fél jogaiba, tekintettel a védjegyre, szolgáltatás jelzésére, márka névre, vállalat nevére, vagy bármilyen más szellemi tulajdoni jogra. Az igénylők ezen kívül nem használja a domain és megkülönböztetett nevet törvénytelen célokból, ideértve, korlátozás nélkül, a szerződés vétkes megszegését, vagy jogellenes üzleti haszonszerzést, tisztességtelen versenyt, más hírnevének megsértését, természetes vagy jogi személy megzavarását vagy félrevezetését. A hitelesítés igénylője (az elfogadás után az aláíró) köteles megvédeni, kártéríteni, és biztosítani a Microsec E-SZIGNÓ sértetlenségét minden, a fentiekben említett akadályozásból és jogsértésből eredő kár és veszteség esetén.

A Microsec E-SZIGNÓ nem vállal felelősséget a ellenőrizhetetlen aláírói adatokért (EAA), amelyeket a Microsec E-SZIGNÓ-hoz, a Microsec E-SZIGNÓ adattárhoz, vagy másképpen juttattak el, hogy szerepeljenek a tanúsítványban. Gyakorlatilag az aláírók kizárólagosan felelősek a jelen HSZSZ-nek megfelelően kiadott tanúsítványok számára szolgáltatott adatok törvényességéért minden olyan területen, ahol a tanúsítvány tartalmát felhasználják, vagy megtekintik. Mivel az adattovábbítást és elérhetőséget érintő jogszabályok folyamatosan változnak a hitelesítést igénylő személy és aláíró felelősségét nem csupán a tanúsítvány kiadásának időpontjában hatályos jogszabály határozza meg, hanem minden olyan jogszabály is, amely a kibocsátás után lép hatályba. A hitelesítést igénylő személynek és az aláírónak figyelemmel kell lennie arra, hogy több törvény szabályozza az adatok, különösen a kódolt, vagy kódoló algoritmust tartalmazó adatok, továbbítását, és ezek a törvények jelentős mértékben eltérhetnek az egyes államok és országok között. Továbbá, általában nem lehetséges, hogy az Interneten, vagy más, a felhasználó/néző helyzetén alapuló egyéb hálózatokon keresztül történő tartalomtovábbítást korlátozzák, és ez megkívánja a hitelesítés igénylőjétől és az aláírótól, hogy minden területen megfeleljen a jogszabályoknak, ahol a tartalmat felhasználhatják, vagy megtekinthetik.

A hitelesítés igénylője és az aláíró nem juttathat el a Microsec E-SZIGNÓ-hoz, vagy a Microsec E-SZIGNÓ adattárhoz (i) rágalmazó, becsületsértő, obszcén, pornográf, sértegető, fanatikus, gyűlöletkeltő, vagy rasszista üzenetet, (ii) olyan üzenetet, amely illegális tevékenységre buzdít, vagy az elkövetés szándékával részletezi azokat, vagy (iii) bármilyen törvénybe ütközik.

12.14 Díjak

A Microsec a szolgáltatások igénybevételért díjat számít fel az aláíróknak. Az érvényes díjszabás a Microsec E-SZIGNÓ adattárban megtalálható a **http://www.e-szigno.hu/adatok/dijak** címen. A Microsec kft. az árváltoztatás jogát fenntartja.

12.15 A kriptográfiai eljárások kiválasztása

Valamennyi megbízó tudomásul veszi, hogy kizárólagosan felelős a biztonsági szoftver, hardware, és kódoló/digitális aláírás algoritmus, beleértve a paraméterek, eljárások és módszerek kiválasztásáért, amelyet saját döntésük alapján hozták. E tekintetben a Microsec E SZIGNÓ semmilyen felelősség sem terheli.

12.16 Hatályosság

A HSZSZ 3.8. (Bizalmas Információk), a HSZSZ 11. (A Microsec E-SZIGNÓ kötelezettségei és korlátozásai), és a HSZSZ 12. (Egyéb Rendelkezések) fejezeteiben szereplő kötelezettségek érvényben maradnak a jelen HSZSZ elévülését követően is.

12.17 Vis maior

A tanúsítvány-kibocsátó irodák és a Microsec E-SZIGNÓ nem felelős a szavatosság megsértésért, késésért, vagy a jelen HSZSZ követelményeinek nem teljesítéséért, ha vis maior áll elő.

13 FÜGGELÉK

13.1 Meghatározások

1., 2., VAGY 3., SZINTŰ HITELESÍTÉSI OSZTÁLYBA TARTOZÓ TANÚSÍTVÁNY

Meghatározott bizalmi szintű tanúsítvány. (ld. HSZSZ 2.2)

ADAT

Számítógépen tárolt, számítógéppel továbbított, vagy feldolgozott programok, fájlok és más információk.

ADATBÁZIS

Komputerizált vezetői információs rendszer által előállított, tárolt és befolyásolt egymással összefüggő információk rendszere.

ADAT INTEGRITÁSA

Az adatot nem változtatták vagy semmisítették meg illetéktelen módon. (ld. **FENYEGETÉS; VESZÉLYEZTETÉS)**

ADATTÁR

Tanúsítványok és más kapcsolódó információk online módon elérhető adatbázisa.

AKTÍV TANÚSÍTVÁNY

Olyan tanúsítvány, amely a jelen pillanatban, vagy a tanúsítványban meghatározott időponttól kezdődően aktív időszakában van, azaz érvényes.

AKTÍV IDŐSZAK

Olyan periódus, amely a tanúsítvány kiadásával (vagy a tanúsítványban meghatározott későbbi időponttal) kezdődik, és a tanúsítvány lejártával, vagy azt megelőzően a tanúsítvány felfüggesztésével vagy visszavonásával véget ér.

ALSÓBB SZINTŰ HSZ

Az Nemzeti NYKI hierarchiában minden hitelesítés-szolgáltató, akár HSZH, MHSZ, HSZ vagy “alsóbb szintű HSZ”, az NHSZH alsóbb szintű Hitelesítés-Szolgáltatója. A HSZH beosztott szerve lehet MHSZ vagy HSZ. Egy MHSZ vagy HSZ alacsonyabb szintű beosztott szerve lehet egy másik alacsonyabb szintű HSZ. (ld. **MAGASABB SZINTŰ HSZ**)

ALÁÍRÁS

Olyan eljárás, amelyet a dokumentum létrehozója alkalmaz saját maga igazolására, és amelyet az átvevő elfogad, vagy használata az adott körülmények között elfogadott. (ld. **DIGITÁLIS ALÁÍRÁS**)

ALÁÍRÓ

A tanúsítványban szereplő nyilvános kulcsnak megfelelő titkos kulcs használatára feljogosított személy, a kiadott tanúsítvány alanya.

ALÁÍRÓI ADATOK

A hitelesítési kérelemmel, a hitelesítési szolgáltatóhoz eljuttatott adat. (ld. **HITELESÍTÉSI KÉRELEM**)

ALÁÍRÓI SZERZŐDÉS

Az aláíró és a hitelesítési szolgáltató között, a HSZSZ-nek megfelelően létrejött megállapodás a kijelölt hitelesítési szolgáltatások ellátásáról.

ALANY

A nyilvános kulcsnak megfelelő titkos kulcs tulajdonosa. Az “alany” fogalma utalhat arra az eszközre, amely birtokolja a titkos kulcsot, és arra az egyénre is, ha létezik, aki ellenőrzi ezt az eszközt. Az alany egyértelműen meghatározott nevet kap, amely az alany tanúsítványában szereplő nyilvános kulccsal függ össze.

ALANY NEVE

A tanúsítvány “alany neve” rovatában szereplő egyértelmű érték, amely összefügg a nyilvános kulccsal.

ALIAS

Álnév.

ARCHÍVÁLÁS

A nyilvántartások és szakmai anyagok meghatározott ideig tartó tárolása biztonsági, szakmai és felülvizsgálati okokból.

AZONOSÍTÁS

Egy személy azonosságának igazolása. A nyilvános kulcs rejtjelezésének azonosítását a tanúsítvány könnyíti meg.

AZONOSSÁG

Olyan egyedi információ, amely egy területen belül egy bizonyos entitást jelöl. Ezek az információk csak egy bizonyos területen belül egyediek.

BEJEGYZÉS

A hitelesítést kérelmező hitelesítés igénylési folyamata.

BIZALOM

Általában az a feltételezés, hogy egy entitás lényegében úgy viselkedik, ahogy azt elvárják. A bizalom csak bizonyos funkciókra vonatkozik. A hitelesítés keretein belül a fogalom kulcsfontosságú szerepe az entitás és a Microsec E-SZIGNÓ között fennálló kapcsolat leírása. A hitelesítő entitásnak bizonyosnak kell lennie abban, hogy a Microsec E-SZIGNÓ kizárólag érvényes és megbízható tanúsítványokat állít ki, és a tanúsítványok felhasználói megbízhatnak a hitelesítő entitás bizalmában.

BIZALMI GYÖKÉR

Nyilvános kulcs, amely kapcsolatát a Microsec E-SZIGNÓ-val egy felhasználó, vagy rendszer adminisztrátor igazolta. A szoftver és hardver rendszer hitelesítése nyilvános kriptográfiára és tanúsítványokra támaszkodik, feltételezve, hogy a kulcshoz korrekt módon jutottak hozzá. Ezt egy bizalmi rendszeradattár által folyamatosan megerősítik, amelyet csak egy azonosított és bizalmi ügyintéző módosíthat.

BIZALMI HARMADIK FÉL

Általában egy független, elfogulatlan harmadik fél, aki közreműködik a legbiztonságosabb és hitelt érdemlő elektronikus adattovábbításban. A bizalmi harmadik fél nem feltételez megbízói – bizalmi személy, vagy más bizalmi – kapcsolat létét. (ld. **BIZALOM**)

BIZALMI POZÍCIÓ

Egy Hiteleítési szolgáltatás keretein belül betöltött pozíció a kriptográfiai tevékenységek feletti ellenőrzés és hozzáférés ellátására, amely jelentősen befolyásolja a tanúsítványok kiadását, használatát, felfüggesztését, vagy visszavonását, beleértve azon a tevékenységek ellátását is, amelyek korlátozzák az adattárhoz való hozzáférést.

BIZALMI SZEMÉLY

Olyan személy, aki bizalmi pozícióban tevékenykedik, és a jelen HSZSZ-vel összhangban alkalmas a feladat elvégzésére.

BIZTONSÁG

Jogosulatlan használat és ellenőrizhetetlen kár vagy következmény elleni védelem. A gyakorlatban lehetetlen megvalósítani a teljes biztonságot, és egy adott biztonsági rendszer minősége viszonylagos. Egy adott biztonsági rendszeren belül, a biztonság egy bizonyos “állapot”, amelyet meg kell őrizni a tevékenységek során.

BIZTONSÁGI SZOLGÁLTATÁS

Bizonyos biztonsági mechanizmusok által, biztonsági keretek között működtetett szolgáltatás. Ezek a szolgáltatások magukba foglalják (nem kizárólagosan) a hozzáférés ellenőrzését, adatok titkosságát és teljességét.

BIZTONSÁGOS CSATORNA

Rejtjelezéssel megerősített kommunikációs út, amely megvédi az üzeneteket a felismert biztonsági fenyegetésekkel szemben.

BIZTONSÁGPOLITIKA

A hitelesítési szolgáltatás támogatásával, egy hitelt érdemlő védelmi rendszer által kapcsolatos kívánalmakat és gyakorlatokat tartalmazó dokumentum.

BIZTOSÍTÉK

Olyan kimutatás vagy intézkedés, amely a tanúsítvány-kibocsátó iroda által meghatározott szolgáltatások biztosításának és fenntartásának jóhiszemű szándékát közvetíti. A “biztosíték” nem garantálja szükségszerűen, hogy a szolgáltatás teljes és kielégítő. A biztosíték nem egyezik meg a biztosítással, kötelezettséggel, garanciával és jótállással, ha ezt másképpen nem jelezték.

BŐVÍTETT

Az X.509 v3 tanúsítvány kibővített szervezetrovatának használata.

DEMOGRÁFIAI ADATOK

Egyes tanúsítványokban, lakhelyre (ország, irányítószám), korra, és nemre vonatkozó opcionális (Aláíró által választhatóan szereplő) adatok.

DEMO TANÚSÍTVÁNY

A Microsec E-SZIGNÓ által kiadott tanúsítvány, melyet kizárólag demonstrációs és prezentációs célokra használhatnak, más biztonsági vagy titkos kommunikációra nem. A demó tanúsítványokat csak felhatalmazott személy használhatja.

DIGITAL ID^{SM}

A Microsec E-SZIGNÓ szolgáltatás hitelesítési védjegye és márkaneve. (ld. **TANÚSÍTÁS)**

DIGITÁLIS ALÁÍRÁS

Egy üzenet átalakítása aszimmetrikus rejtjelezéssel úgy, hogy az a személy, aki birtokában van az eredeti üzenetnek és az aláíró nyilvános kulcsának, pontosan meg tudja határozni, hogy az átalakítás az aláíró nyilvános kulcsának megfelelő titkos kulccsal történt-e, és az átalakítás óta megváltoztatták-e az üzenetet.

DOKUMENTUM

Kézzelfogható közvetítőeszközre, papírra és nem számítógépes adathordozóra, feljegyzett információ. (ld. **ÜZENET; NYILVÁNTARTÁS)**

ENTITÁS (LD. SZEMÉLY) – ENTITY

EGYÉNI SZOFTVER FORGALMAZÓI TANÚSÍTVÁNY

2. szintű hitelesítési osztályba tartozó tanúsítvány, melyet csak egyének számára adnak ki és a szoftver érvényességének igazolására használják. (ld. **KERESKEDELMI SOFTWARE FORGALMAZÓI TANÚSÍTVÁNY; SOFTWARE ÉRVÉNYESSÉGÉNEK IGAZOLÁSA)**

EGYÉRTELMŰ NÉV (LD. MEGKÜLÖNBÖZTETETT NÉV)

EGYESÍTÉS HIVATKOZÁSSAL

Egy üzenet egyesítése egy másikkal úgy, hogy az egyesítendő üzenetet olyan információkkal azonosítjuk, amelyek képessé teszik a fogadó felet a hozzáférésre és az egyesítendő üzenet hiánytalan megszerzésére, azzal a kifejezett szándékkal, hogy az része legyen az egyesülő üzenetnek. Az ilyen egyesített üzenet ugyanazzal a kihatással rendelkezik, mintha azt a törvényes kereteken belül teljes mértékben meghatározták volna az üzenetben.

ELÉRHETŐSÉG

Információk, vagy eljárások ésszerű hozzáférhetőségének és felhasználhatóságának mértéke az igényeknek megfelelően egy felhatalmazott entitás által, és a felhatalmazott számára a forrásokhoz és sürgős tevékenységek időszerű teljesítéséhez való hozzáférés engedélyezése.

(TANÚSÍTVÁNY) ELFOGADÁSA

A tanúsítvány jóváhagyása a hitelesítést kérelmező által annak tartalmának ismeretében, a HSZSZ–szel összhangban.

ELLENŐRZÉS

A folyamat integritását és minőségét biztosító intézkedések.

ELNEVEZÉS

Az elnevezés, meghatározott kibocsátási eljárásokat követően, egyéni típusokat leíró azonosítók kijelölése egy hatóság által, amely kezeli az azonosított regisztrációs eljárásnak megfelelő egyedi iratokat. (ld. **NÉVADÓ HATÓSÁG; Microsec E-SZIGNÓ NÉVADÓ HATÓSÁG**)

NEMZETI HITELESÍTÉSI SZOLGÁLTATÓ HATÓSÁG

Olyan hatóság, amely a Magyar Köztársaság területére alkalmazandó hitelesítés-szolgáltatói gyakorlatot kialakítja a hitelesítési hatóságok, a hitelesítés-szolgáltatók és a felhasználók számára.

E-MAIL

Számítógépes kommunikációs rendszeren keresztül digitális formában küldött, fogadott, vagy továbbított üzenet.

ÉRTESÍTÉS

A HSZSZ-nek megfelelően elküldött értesítés. (ld. HSZSZ 12.10)

ÉRVÉNYES TANÚSÍTVÁNY

A Microsec E-SZIGNÓ által kibocsátott, és a tanúsítványon szereplő aláíró által elfogadott tanúsítvány.

ÉRVÉNYESÍTÉS (HITELESÍTÉSI KÉRELEMÉ)

A Microsec E-SZIGNÓ által végzett, hitelesítési kérelmet követő tevékenység, amely a kérelem jóváhagyásának és a tanúsítvány kiadásának előfeltétele.

ÉRVÉNYESÍTÉS (SZOFTVER-É) (LD. SPFTWARE ÉRVÉNYESSÉGÉNEK IGAZOLÁSA)

FELEK

Azon entitások, amelyek jogait és kötelezettségeit a jelen HSZSZ szabályozza. Ide értendők a hitelesítés kérelmezők, a Microsec E-SZIGNÓ, az aláírók, és a bizalmi felek.

FELHASZNÁLÓ

Felhatalmazott entitás, aki mint kérelmező, aláíró, fogadó vagy megbízható fél a tanúsítvány felhasználója, kivéve a tanúsítvány-kibocsátó irodát. (ld. **HITELESÍTÉS KÉRELMEZŐ; ENTITÁS; SZEMÉLY; ALÁÍRÓ**)

FELHATALMAZÁS – AUTHORIZATION

Jogok adományozása, beleértve meghatározott információkhoz és forrásokhoz való hozzáférés jogát.

FELÜLVIZSGÁLAT

Olyan eljárás, amely igazolja, hogy az ellenőrzés helyénvaló és céljának megfelel. Magában foglalja az információs rendszerbe történő behatolások és visszaélések felderítését célzó intézkedések nyilvántartását és elemzését. A felülvizsgálat során felmerült hiányosságokat az illetékes vezetőnek jelentik.

FENYEGETÉS

Potenciálisan a rendszer rongálását okozó körülmény vagy esemény, beleértve a rendszer megsemmisítését, jogosulatlan használatát, az adatok módosítását, és/vagy a szolgáltatás elutasítását.

FOGADÓ (DIGITÁLIS ALÁÍRÁST)

Az a személy, aki digitális aláírást fogad, és aki megbízik benne, függetlenül attól, hogy megbízhat-e benne. (ld. **MEGBÍZHATÓ FÉL**)

FTP (FILE TRANSFER PROTOCOL)

Alkalmazási protokoll, amely fájlrendszerekhez való hozzáférést tesz lehetővé hálózati szolgáltatás segítségével.

ELSŐDLEGES HITELESÍTÉS-SZOLGÁLTATÓ

Az a HSZ, amely a hitelesítési láncban az első tanúsítványt adja ki. Az elsődleges szolgáltató nyilvános kulcsát a tanúsítvány felhasználójának előzetesen ismernie kell, hogy a hitelesítési láncot érvényesíthesse. A gyökér nyilvános kulcsát hitelt érdemlően hozzák létre néhány mechanizmus segítségével, mint például biztonsági fizikai elosztással, amely nem egyezik meg a hitelesítéssel.

HASH (HASH FUNKCIÓ)

Olyan algoritmus, amely feltérképezi, vagy átalakítja a bitek egységét más (általában kisebb) egységgé úgy, hogy

(i) Az üzenet ugyanazt eredményezi minden esetben, amikor az algoritmus ugyanazt az üzenetet kapja bemenetként.

(ii) A számítás nem teszi lehetővé, hogy az üzenetet visszaszármaztassák, vagy visszaalakítsák az algoritmus segítségével kapott eredményből.

(iii) A számítás nem teszi lehetővé, hogy két különböző üzenet ugyanazt az algoritmust használva ugyanazt a hash eredményt adja.

HITELESÍT (LD. HITELESÍTÉS)

HITELESÍTÉS

Olyan folyamat, amely igazolja egy személy azonosságát, vagy egy bizonyos információ valódiságát. A tanúsítás üzenete magában foglalja a forrás megnevezését és igazolja, hogy a továbbítás során az üzenetet nem módosították, és nem helyettesítették. (ld. **MEGERŐSÍT (DIGITÁLIS ALÁÍRÁST)**)

HITELESÍTÉSI SZOLGÁLTATÁSI SZABÁLYZAT (HSZSZ)

A jelen dokumentum, melyet időről időre felülvizsgálnak (a Microsec E-SZIGNÓ azon gyakorlatait tartalmazza, amelyeket a tanúsítvány kibocsátása során alkalmaz).

HITELESÍTÉSI BEADVÁNY (HB)

A hitelesítési kérelem számítógép által olvasható formája. (ld. **HITELESÍTÉSI KÉRELEM**)

HITELESÍTÉSI KÉRELEM

A hitelesítést kérelmező (vagy felhatalmazott képviselője) által a tanúsítvány-kibocsátó irodához benyújtott kérelem a nyilvános kulcs tanúsítása iránt. (ld. **HITELESÍTÉST KÉRELMEZŐ; HB**)

HITELESÍTÉSI LÁNC

A tanúsítványok rendezett sorrendje, amely tartalmaz egy végső felhasználó aláírói tanúsítványt és Microsec E-SZIGNÓ tanúsítványt. (ld. **ÉRVÉNYES TANÚSÍTVÁNY**)

HITELESÍTÉSI LÁNC ÉRVÉNYESÍTÉSE

A lánc minden egyes tanúsítványa esetében, a fogadó vagy megbízható fél által végzett tevékenység, amely során igazolják a nyilvános kulcsot (minden tanúsítvány esetén), igazolják, hogy minden tanúsítvány érvényes, a Microsec E-SZIGNÓ tanúsítvány aktív időszakában adták ki, és minden fél (Microsec E-SZIGNÓ, végső felhasználó aláíró, fogadó, és megbízható fél) a HSZSZ-nek és a láncban található tanúsítványoknak megfelelően működik.

HITELESÍTÉSI LÁNC RATIFIKÁLÁSA

A hitelesítési lánc jóváhagyásának folyamata, és azt követően a végső felhasználó aláírói tanúsítvány jóváhagyása.

HITELESÍTÉSI SZOLGÁLTATÁS (HSZ) (LD. MICROSEC E-SZIGNÓ HITELESÍTÉSI SZOLGÁLTATÁS)

HITELESÍTŐ KULCS (LD. MICROSOFT AUTHENTICODE^{TM}; SZOFTVER ÉRVÉNYESÍTÉSE)

HITELESÍTETTEK NYILVÁNTARTÁSA

A tanúsítást igazoló, megfelelő biztosítékkal, vagy egy megbízható fél által, digitálisan aláírt, érvényes 3. szintű hitelesítési osztályba tartozó tanúsítvánnyal igazolt, üzenettel ellátott dokumentum. A felfüggesztést és visszavonást bejelentő üzenet digitális aláírását a nyilvános kulcsnak megfelelő titkos kulccsal kell létrehozni, melyet az alkalmazható tanúsítványkategóriáról szóló igazolás tartalmaz.

HITELESÍTÉST KÉRELMEZŐ

Olyan személy, vagy felhatalmazott képviselő, aki a Microsec E-SZIGNÓ nyilvános kulcs tanúsítására nyújt be kérelmet. (ld. **HSZ KÉRELMEZŐ; ALÁÍRÓ)**

HITELESÍTŐ (LD. TANÚSÍTVÁNY KIBOCSÁTÓ IRODA (TK))

HITELESÍTŐ SZOLGÁLTATÓ (HSZ)

Tanúsítvány kibocsátására feljogosított személy (ld. **SZEMÉLY** definíciója). A Microsec E-SZIGNÓ hitelesítési szolgáltatásának keretén belül működő HSZH az NHSZH alatt helyezkedik el a hierarchiában. (ld. **REGISZTRÁCIÓS HATÓSÁG; BIZALMI HARMADIK FÉL**)

HITELT ÉRDEMLŐ RENDSZER

Olyan komputer hardverek, szoftverek és eljárások, amelyek a feltörések és visszaélésekkel szemben meglehetősen biztonságosak; magas szintű elérhetőséget, megbízhatóságot és megfelelő működést biztosítanak; alkalmasak feladataik elvégzésére; és végrehajtják az alkalmazandó biztonságpolitikát. A hitelt érdemlő rendszer nem szükségszerűen "bizalmi rendszer", ahogy az a bizalmas kormányzati nómenklatúrában szerepel.

HOZZÁFÉRÉS

A bejelentkező és a kommunikációs vagy információs források között létrejövő speciális kapcsolat, amely információáramlást, szabályozást, vagy egy folyamat elindítását eredményezheti.

IDEIGLENES TANÚSÍTVÁNY

2. szintű hitelesítési osztályba tartozó tanúsítvány az aktív időszak első 21 napjában, melyet tekintettel a 2. szintű hitelesítési kérelemre (HSZSZ 5.1-val összhangban), az összes előírt belső Microsec E-SZIGNÓ érvényesítési eljárás teljesítése után adnak ki. Az ideiglenes állapot jelzi, hogy a hitelesítési kérelemben szereplő aláírói adatok azonosságának igazolása postai címellenőrzés "tértivevény" útján történik. (ld. CPS 5.1.4 ; **TANÚSÍTÁS**)

IDŐPECSÉT – TIMESTAMP

Olyan megjelölés, amely (legalább) jelzi egy tevékenység pontos dátumát és időpontját, és az időpecsétet küldő, vagy fogadó személy vagy eszköz azonosságát.

IGAZOLÁS

Tisztázás megfelelő kivizsgálással. (ld. **FELJOGOSÍTÁS; DIGITÁLIS ALÁÍRÁS MEGERŐSÍTÉSE)**

IGAZOLÓ FORMULA

A hitelesítést kérelmező által kiválasztott szám- vagy betűsorozat, amelyet a hitelesítési kérelemmel együtt elküldött a Microsec E-SZIGNÓ részére, és amellyel a Microsec E-SZIGNÓ feljogosítja az aláírót a HSZSZ-ben meghatározott különböző céloknak megfelelően. A formulával a titkos rész tulajdonosa is igazolhatja magát a titkos rész kibocsátója felé.

INGYENES TANÚSÍTVÁNY

Microsec E-SZIGNÓ által kiadott tanúsítvány, melyért nem számol fel az aláírónak díjat, vagy más egyéb térítést.

ÍRÁS

Egy irat hozzáférhető és későbbi referenciaként alkalmazható információtartalma.

IRAT

Kézzelfogható közvetítőeszközre feljegyzett (dokumentum), vagy elektronikus formában, vagy más eszközzel tárolt információ, amely érzékelhető formájúvá alakítható vissza. Az “irat” fogalma két részből tevődik össze, a “dokumentum” és “üzenet” fogalmából. (ld. **DOKUMENTUM; ÜZENET**)

JEGYZŐ

Egy végrehajtó kormányhivatal által felhatalmazott természetes személy jegyzői tevékenységek, úgymint közjegyzői tanúsítvány, eskü vagy jóváhagyás ügyintézésének ellátására, tanúsító vagy hitelesítő aláírásra, forgatható értékpapírok megóvatolására. A Magyar Köztársaságban a természetes személyt az igazságügy miniszter nevezi ki és hatalmazza fel a Közjegyzői Törvényben meghatározott feladatok ellátására.

JOGOSULTSÁG IGAZOLÁSA

A törvényhozás egy feljogosított tisztviselője által kiadott dokumentum, mely tartalmaz közjegyzői tanúsítványt, úgymint a közjegyzőnek a Magyar Köztársaság miniszteri feljogosítását.

JÓ VISZONYBAN LÉVŐ ALKALMAZOTT

Nem próbaidős alkalmazott, akit nem bocsátottak el, nincs felfüggesztve, és munkáltatója nem folytat ellene fegyelmi eljárást.

JÓVÁHAGY/JÓVÁHAGYÁS

Olyan intézkedés, amely megállapítja, vagy jelzi, hogy az adatok korrektek és az információk megfelelnek a valóságnak.

CSATOLÁS

A tanúsítvány kibocsátójának (Microsec E-SZIGNÓ) igazolása a nevezett entitás és a nyilvános kulcs közötti kapcsolatról.

KÉRELMEZŐ

(ld. **HSZ KÉRELMEZŐ**; **HITELESÍTÉST KÉRELMEZŐ**)

KERESKEDELMI ÉSSZERŰSÉG

Az elektronikus kereskedelemmel összefüggésben, technológia, ellenőrzés, igazgatási és operációs eljárások megvalósítása és alkalmazása, mely ésszerű keretek között biztosítja a rendszer és az üzenet megbízhatóságát, hitelességét.

KERESKEDELMI SZOFTVERFORGALMAZÓI TANÚSÍTVÁNY

3. szintű hitelesítési osztályba tartozó tanúsítvány, melyet csak szervezetek számára adnak ki és a szoftver érvényességének igazolására használják. (ld. **EGYÉNI SOFTWARE FORGALMAZÓI TANÚSÍTVÁNY; SOFTWARE ÉRVÉNYESÍTÉSE)**

KÖZREAD/KÖZREADÁS

Az adatok rögzítése és tárolása a Microsec E-SZIGNÓ gyűjteményben, vagy lehetőség szerint, minimum egy másik gyűjteményben, annak érdekében, hogy az ilyen adatokat nyilvánosságra hozzák a HSZSZ-szel és az alkalmazandó jogszabályokkal összhangban.

KIBOCSÁTÓ (LD. KIBOCSÁTÓ HATÓSÁG)

KIEGÉSZÍTÉS

Az X.509 v3 tanúsítvány kiegészítő rovatai. (ld. **X.509**)

KIKÖTÉS (LD. MICROSEC E-SZIGNÓ KIKÖTÉS)

KÓDOLÁS

Rejtjelezetlen adatok rejtjelezett formába (rejtjeles szöveg (ciphertext)) történő átalakítása úgy, hogy az adatokat vagy nem lehet visszaalakítani eredetivé (egyutas kódolás), vagy csak az ellentétes dekódoló folyamattal alakíthatóak vissza (kétutas kódolás).

KÖNYVTÁR (LD. ADATTÁR)

KÖTELEZETTSÉG (LD. SZOFTVER FORGALMAZÓI KÖTELEZETTSÉG)

KRIPTOGRÁFIA (LD. NYILVÁNOS KULCS KRIPTOGRÁFIA)

(i) A matematika alkalmazza az adatok titkosságának és valódiságának biztosítása érdekében úgy, hogy az adatokat helyettesítik egy átalakított változattal, amely csak a megfelelő kriptografikus algoritmus és kulcs birtokában alakítható vissza az eredeti adattá.

(ii) Olyan tudomány, mely tartalmazza az adatátalakítás fő elveit, eszközeit és módszereit, célja az információ elrejtése, a felderítetlen módosítások kivédése, és/vagy a jogosulatlan használat megelőzése.

KRIPTOGRAFIKUS ALGORITMUS

Egyértelműen meghatározott matematikai számítási folyamat; szabályok sorozata, mely előre megszabott eredményre vezet.

KRIPTOMODUL

Egy titkosító rendszer hitelt érdemlő megvalósítása, mely biztonságosan kódolja és dekódolja az adatokat.

KULCS GENERÁLÁSA

Titkos- és nyilvános kulcsok létrehozásának hitelt érdemlő folyamata. A nyilvános kulcsot a hitelesítési kérelmezés során eljuttatják a Microsec E-SZIGNÓ számára.

KULCSPÁR

Titkos kulcs és az annak megfelelő nyilvános része. A nyilvános kulcs igazolhatja a megfelelő titkos kulcs alkalmazásával létrehozott digitális aláírást. Ezen kívül, az alkalmazott algoritmustól függően, a kulcspár összetevői titkosítási célból kódolhatnak és dekódolhatnak információkat, ahol a titkos kulcs egyedül képes a megfelelő nyilvános kulccsal kódolt információ felfedésére.

KULCSPÁR GENERÁLÁSA

A hitelesítési kérelmezés során a titkos kulcs létrehozásának hitelt érdemlő folyamata, és a megfelelő nyilvános kulcs továbbítása a Microsec E-SZIGNÓ-nak olyan módon, hogy az jelezze a kérelmező titkos kulcshasználatának képességét.

LETAGADÁS

A teljes kommunikációban, vagy csak egy részében résztvevő személy letagadása, vagy letagadási kísérlete.

LETAGADHATATLANSÁG

Az adat eredetének és továbbításának bizonyítása annak érdekében, hogy megvédje a feladót attól, hogy a fogadó letagadja az adatokhoz való hozzájutást, vagy megvédje a fogadót attól, hogy a feladó letagadja az adatok elküldését. Megjegyzés: Csak vizsgáló szakértő (a vita eldöntésére felhatalmazott egyén) hozhat végső döntést. Például, a döntéshez bizonyítékul szolgálhat a HSZSZ-nek megfelelően megerősített digitális aláírás, de önmagában nem jelenti a letagadhatatlanságot.

LÉTREHOZÓ

Az a személy (vagy megbízottja), akinek szándékában áll egy üzenet létrehozása, tárolása, vagy továbbítása. A kifejezés nem foglalja magában a közvetítőként szerepet játszó személyt.

MEGBÍZHATÓ FÉL

A tanúsítványban és a digitális aláírásban megbízó fogadó. (ld. **FOGADÓ; MEGBÍZNI (TANÚSÍTVÁNY ÉS DIGITÁLIS ALÁÍRÁS)**

MEGBÍZNI (TANÚSÍTVÁNY ÉS DIGITÁLIS ALÁÍRÁS)

Digitális aláírás elfogadása és a használhatatlan digitális aláírásokkal szembeni fellépés. (ld. **MEGBÍZHATÓ FÉL; FOGADÓ**)

MEGERŐSÍT (DIGITÁLIS ALÁÍRÁST)

Adott digitális aláírással, üzenettel, és nyilvános kulccsal kapcsolatban megállapítják, hogy:

(i) a digitális aláírást, érvényes tanúsítvány aktív időszaka alatt, a tanúsítványban szereplő nyilvános kulcsnak megfelelő titkos kulccsal hozták létre, és

(ii) a kapcsolódó üzenetet nem változtatták meg a digitális aláírás létrehozása óta.

(ld. **TANÚSÍTÁS; IGAZOLÁS**)

MEGFELELÉS

Azonos kulcspárhoz való tartozás (ld. **NYILVÁNOS KULCS; TITKOS KULCS**)

ÉRTESÍTÉS

A HSZ és az alkalmazott jogszabályok által megkívánt egyedi információ közlése egy másik személlyel.

MEGKÜLÖNBÖZTETETT NÉV

Olyan adatok, melyek azonosítják a valós, létező személyt a számítógépes környezetben lévő személlyel. (pl.: országNév = HU, állam = Magyar, szervezetNév = E-szignó Inc. Név = Nagy János).

MEGÚJÍTÁS

Ugyanazon hitelesítési osztályba tartozó és ugyanolyan típusú, ugyanarra vonatkozó új tanúsítvány megszerzésének folyamata abban az esetben, ha a meglévő tanúsítvány lejárt.

ELLENŐRIZHETETLEN ALÁÍRÓI ADATOK (EAA)

Egy hitelesítést kérelmező által a Microsec E-SZIGNÓ -hoz eljuttatott, a tanúsítványban szereplő információ, amelyet a Microsec E-SZIGNÓ nem erősített meg, és amelyért a Microsec E-SZIGNÓ nem szolgál más biztosítékkal mint azzal, hogy az információt a hitelesítési kérelemmel együtt juttatták el hozzá. Tudományos fokozat, szakmai végzettség, meghatalmazás, demográfiai adatok EAA-nak minősülnek, ha azt másképp nem jelzik.

NÉV

Egy bizonyos típusú személyt leíró azonosító jelek sorozata.

NÉVADÓ HATÓSÁG

A névadó politikát és eljárásokat végrehajtó testület, amely ellenőrzést gyakorol az egyes hitelesítési osztályok egyszerű (alap) elnevezéseinek regisztrálása és kijelölése felett. (ld. **ELNEVEZÉS; Microsec E-SZIGNÓ NÉVADÓ HATÓSÁG**)

NORMÁL TANÚSÍTVÁNY (LD. TANÚSÍTVÁNY)

NYILVÁNOS KULCS

Nyilvánosság számára is elérhető kulcs, amely megerősíti a megfelelő titkos kulccsal együtt létrehozott aláírást. Az algoritmustól függően, a nyilvános kulcs alkalmas üzenetek és fájlok kódolására, amelyeket ezután a megfelelő titkos kulccsal lehet dekódolni. (ld. **NYILVÁNOS KULCS REJTJELEZÉSE; TITKOS KULCS**)

NYILVÁNOS KULCS INFRASTRUKTÚRA (NYKI)

Felépítés, szervezet, módszerek, gyakorlatok, eljárások, amelyek együttesen a tanúsításra alapozott nyilvános kulcs rejtjelezési rendszerének megvalósítását és működését segítik elő. A NYKI olyan rendszerekből áll, amelyek együttműködve biztosítják és megvalósítják a hitelesítési és más lehetséges kapcsolódó szolgáltatást.

NYILVÁNOS KULCS REJTJELEZÉSE

A kriptográfia egy típusa, amely matematikai kapcsolatban lévő kriptografikus kulcspárokat használ fel. A nyilvános kulcs elérhető mindenki számára, ha alkalmazni szeretné, és alkalmas adatok kódolására vagy digitális aláírás megerősítésére; a titkos kulcsot a tulajdonosa titkosan kezeli, amely képes adatok dekódolására és digitális aláírás létrehozására.

NYILVÁNOS/TITKOS KULCSPÁR (LD. NYILVÁNOS KULCS; TITKOS KULCS; KULCSPÁR)

NYILVÁNOS KULCS TANÚSÍTÁSA (LD. TANÚSÍTÁS) –

ON-LINE

Azonnali kapcsolatot biztosító kommunikáció a Microsec E-SZIGNÓ hitelesítési szolgáltatással.

OUTSOURCING

Hivatalos megállapodás harmadik féllel egy informatikai funkció ellátására a szervezet számára. Az outsourcing során a költségvetési szervezet teljesen felelős marad az érintett szolgáltatások biztosításáért és megtartja az ellenőrzést a menedzsment döntései felett, mialatt a másik, a szerződő szervezet üzemelteti a tevékenységet vagy teljesíti a szolgáltatást.

PASSWORD (JELSZÓ, PIN KÓD)

Titkos igazoló információ, általában a számítógéphez való hozzáférést biztosító karakterek sorozata.

NYKI HIERARCHIA

Hitelesítési szolgáltatók csoportja, amelyek feladatát a felhatalmazás fő elvei szerint határozták meg, és amelyek egymással alá- és fölérendeltségi viszonyban állnak.

REGISZTRÁLT KARAKTERSOROZAT

A regisztrációs és nyilvántartási eljárás tárgya, amely egyértelműen jelzi az értéket a regisztrációs hatóság nyilvántartásában. A nyilvántartott érték típusa karakterek sorozata.

RELATÍV MEGKÜLÖNBÖZTETETT NÉV (RMN)

Az entitás megkülönböztetett nevét magába foglaló jelsorozat, amely az adott területen belül megkülönbözteti az entitást a többi ugyanolyan típusú entitástól.

RSA

A Rivest, Shamir & Adelman által létrehozott nyilvános kulcsú rejtjelező rendszer.

SAJÁT SZIGNÁLÁSÚ NYILVÁNOS KULCS

A tanúsítvánnyal megegyező felépítésű adathalmaz, de aláírója az adathalmaz alanya. A tanúsítványtól eltérően, a saját szignálású nyilvános kulcsot nem használhatják hitelt érdemlően a nyilvános kulcs más felek felé történő igazolására.

SMART KÁRTYA

Hardware berendezés, amely magában foglal rejtjelezési feladatok végrehajtására egy vagy több integrált áramkört (IC), és amely hamisítással szembeni ellenállással rendelkezik.

S/MIME

MIME kiterjesztéssel rendelkező rejtjelezett üzenet szintaxist kihasználó E-mail biztonsági protokoll.

SORSZÁM (LD. TANÚSÍTVÁNY SORSZÁMA)

SZEMÉLY

Egy ember, vagy szervezet (vagy az ember vagy szervezet irányítása alá tartozó eszköz), amely képes egy üzenet aláírására vagy hitelesítésére, akár törvényesen, akár gyakorlati okokból. (Az **ENTITÁS** szinonimája)

SZEMÉLYES JELENLÉT

Megjelenés egy a Microsec E-SZIGNÓ, vagy az általa kijelölt hatóság előtt azonosságának igazolására (fizikailag és nem virtuálisan, vagy jelképesen), néhány esetben ez a tanúsítvány kiadásának előfeltétele.

SZERVER

Olyan számítógépes rendszer, amely válaszol a kliens rendszerek bejelentkezéseire.

SZERVEZET

Társult felhasználók egysége. Egy szervezet lehet felhasználó is.

SZIGNÁLÁS

Üzenet digitális aláírásának létrehozása, vagy dokumentum ellátása aláírással, a szövegkörnyezettől függően.

SZIGNÁLÓ

Az a személy, aki egy üzenetet digitális aláírással, vagy egy dokumentumot aláírással lát el.

SZOLGÁLTATÁS MEGTAGADÁSA (LD. ELÉRHETŐSÉG)

TANÚSÍTÁS

Microsec E-SZIGNÓ által kibocsátott tanúsítvány kiadásának folyamata.

TANÚSÍTVÁNY (NYILVÁNOS KULCS TANÚSÍTVÁNYA)

Egy üzenet (ld. **ÜZENET** definíciója), mely legalább egy nevet tartalmaz, vagy azonosítja a kibocsátó szolgáltatót, az aláírót, tartalmazza az aláíró nyilvános kulcsát, meghatározza a tanúsítvány lejárati idejét, tartalmazza a tanúsítvány sorszámát, és a kibocsátó szolgáltató digitális aláírását. Minden módosító jelző nélküli hivatkozás az "1., 2., vagy 3. szintű hitelesítési osztályban tartozó tanúsítványra", vagy "tanúsítványra", vonatkozik mind a "normál" mind az "ideiglenes" tanúsítványra, ha a szövegösszefüggés másképp nem kívánja. A tanúsítvány kizárólag egy kibocsátó szolgáltató által kibocsátott tanúsítványra vonatkozik. (Ld. **IDEIGLENES TANÚSÍTVÁNY)**

TANÚSÍTVÁNY BŐVÍTÉSE

A tanúsítvány olyan bővítése, mely további információkat tartalmaz a tanúsított nyilvános kulcsról, a tanúsított aláíróról, tanúsított kibocsátóról, és/vagy a tanúsítói folyamatról. Az alapvető bővítéseket az ISO/IEC 9594-8:1995 (X.509) 1. módosítása tartalmazza.

TANÚSÍTVÁNY ÉRVÉNYESÍTÉSE (PL. VÉGSŐ FELHASZNÁLÓI ALÁÍRÓ TANÚSÍTVÁNYA)

A fogadó vagy megbízható fél által végzett tevékenység, amely során igazolják, hogy a végső felhasználói aláíró tanúsítvány érvényes, és aktív volt a vonatkozó digitális aláírás létrehozásának időpontjában.

TANÚSÍTVÁNY FELFÜGGESZTÉSE

A tanúsítvány aktív időszakában az érvényesség időszakos felfüggesztése a tanúsítvány végleges visszavonása nélkül. A tanúsítvány felkerül a VTL listára, ahol jelölik a felfüggesztés okának kulcsát. (ld. **TANÚSÍTVÁNY VISSZAVONÁSA**)

TANÚSÍTVÁNY KEZELÉSE

A tanúsítvány kezelése magában foglalja a tanúsítvány nyilvántartását, terjesztését, közzétételét, visszavonását, de nem korlátozódik csupán ezekre a tevékenységekre. A Microsec E-SZIGNÓ tanúsítványkezelési tevékenységet végez, mint az aláírói tanúsítványok regisztrációs irodája. A Microsec E-SZIGNÓ a kibocsátott és elfogadott tanúsítványokat a közzététellel érvényesnek minősíti.

TANÚSÍTVÁNY KIADÁSA

Microsec E-SZIGNÓ által végzett tevékenység, melynek során a tanúsítványban szereplő hitelesítési kérelmezőt (feltételezett későbbi aláíró) tanúsítják és értesítik.

TANÚSÍTVÁNY LEJÁRATA

A tanúsítványban meghatározott azon időpont és dátum, amikor az operációs időszak véget ér, tekintet nélkül minden korábbi a felfüggesztésre vagy visszavonásra.

TANÚSÍTVÁNY SORSZÁMA

Olyan szám, amely egyértelműen azonosítja a Microsec E-SZIGNÓ által kibocsátott tanúsítványt.

TANÚSÍTVÁNY VISSZAVONÁSA

Egy tanúsítvány aktív időszakának végleges megszakítása egy meghatározott időponttól kezdve.

TÁRSULT SZEMÉLY

Olyan személy, aki tagja egy szervezetnek (i) mint igazgatótanácsi tag, igazgató, alkalmazott, társ, vállalkozó, gyakornok, vagy a szervezeten belül működő egyéb személy, vagy (ii) a szervezettel szerződéses viszonyban áll, és a szervezet olyan üzleti nyilvántartásokkal rendelkezik, amelyek garantálják az ilyen személy személyazonosságát. (ld. **TÁRSULT TANÚSÍTVÁNY**)

TÁRSULT TANÚSÍTVÁNY

Társult személy számára kibocsátott tanúsítvány. (ld. **TÁRSULT SZEMÉLY**)

TÍPUS (TANÚSÍTVÁNY)

Egy tanúsítvány meghatározó jellemzői, amelyek a típussal kizárólagosan összefüggő alkalmazási kategóriákra korlátozzák a tanúsítvány szándékolt célját.

TITKOS KULCS

Kódolt (titkosított) üzenetek és fájlok dekódolására használt (a tulajdonos által titkosan kezelt) matematikai kulcs. (ld. **NYILVÁNOS KULCS REJTJELEZÉSE, NYILVÁNOS KULCS**)

TITKOS RÉSZ

Néhány fizikai token közötti kriptográfiai titkos rész egy része.

TITKOS RÉSZ ELOSZTÁSA (LD. TITKOS RÉSZ)

A titkos kulcsok titkos részeinek szétosztása a titkos részek tulajdonosai között.

TITKOSSÁG

Bizalmas adatok olyan állapota, amely során azokat titokban tartják és csak az arra feljogosított felek férhetnek hozzá.

TOKEN

A hardware biztonsági token magában foglalja a felhasználó titkos kulcsát (kulcsait), a nyilvános kulcs tanúsítványát, és tetszés szerint más tanúsítványokat, beleértve a felhasználó hitelesítési láncában található összes tanúsítványt.

TOVÁBBÍTÁS

Üzleti információk elektronikus továbbítása, amely magában foglalja a világhálón történő kommunikálást támogató speciális folyamatokat.

URL

A World Wide Weben megtalálható bizonyos adatok és más források azonosítására és lokalizálására szolgáló szabványosított cím.

ÚJRAJEGYZÉS (LD, MEGÚJÍTÁS)

ÜZENET

Információ digitális formában történő megjelenítése; elektronikus irat, az **IRAT** részhalmaza. (ld. **IRAT**)

ÜZENET INTEGRITÁSA (LD. ADAT INTEGRITÁSA)

VÁLTOZATLAN TARTALOMSZOLGÁLTATÁS

A szolgáltatás tanúsítványt biztosít azon szoftverforgalmazók számára, akik szoftvereiket digitális aláírással szándékoznak ellátni, hogy elősegítsék ügyfeleik (végső felhasználók) számára a szoftver érvényességének igazolását.

INTEGRITÁS (LD. ADAT INTEGRITÁSA)

MICROSEC E-SZIGNÓ HITELESÍTÉSI SZOLGÁLTATÁS

A Microsec E-SZIGNÓ és bármely, a jelen HSZSZ-ben meghatározott E-SZIGNÓ felhatalmazású, biztosított hitelesítési rendszer.

MICROSEC E-SZIGNÓ KIKÖTÉS

A Microsec E-SZIGNÓ HSZSZ-t megszorító értékek ismertetését elősegítő adatszintaxis. A kikötési érték bővíti a kiegészítés típusára vonatkozó X.509 által meghatározott szabályoknak megfelelően, az összes tanúsítványban szereplő standard hitelesítési politika kiegészítését.

MICROSEC E-SZIGNÓ NÉVADÓ HATÓSÁG

Microsec E-SZIGNÓ regisztrációs hatósága, amely kialakítja és végrehajtja az ellenőrzés folyamatát, és döntéshozói hatáskörrel rendelkezik a tanúsítvány-kibocsátó irodák relatív megkülönböztetett nevének kibocsátását illetően (végső felhasználó aláírók esetén nem). (ld. **NÉVADÓ HATÓSÁG**)

VESZÉLYEZTETÉS

A biztonsági politika megsértése (vagy feltételezett megsértése), melynek során előfordulhat bizalmas információk jogtalan felfedése, vagy a felettük való ellenőrzés megszűnése. (ld. **ADAT INTEGRITÁSA**)

VILÁGHÁLÓ (WWW)

Kapcsolt szöveg (hypertext) alapú elterjedt információs rendszer, ahol a felhasználók kapcsolt dokumentumokat hozhatnak létre, szerkeszthetnek, vagy böngészhetnek. Grafikus dokumentum közreadó és visszavonó médiuma; az Interneten fellelhető kapcsolódó dokumentumok gyűjteménye.

VISSZAVONT TANÚSÍTVÁNYOK LISTÁJA (VTL)

Időszakosan (vagy rendhagyóan) kiadott, egy TK digitális aláírásával ellátott lista azokról a meghatározott tanúsítványokról, amelyeket a lejáratuk időpontja előtt felfüggesztettek vagy visszavontak. A lista rendszerint tartalmazza a VTL kibocsátójának nevét, a kibocsátás időpontját, a következő VTL tervezett kibocsátásának időpontját, a felfüggesztett vagy visszavont tanúsítványok sorszámát, és a felfüggesztés és visszavonás okát és időpontját.

X.509

Nemzetközi Telekommunikációs tanúsítvány (ITU-T International Telecommunications Union-T)