Az Európai Unió
Tanácsa

Brüsszel, 2019. március 14.
(OR. en)

7510/19
ADD 3

TRANS 199
DELACT 68

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Jordi AYET PUIGARNAU igazgató
Címzett:	Jeppe TRANHOLM-MIKKELSEN, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	C(2019) 1789 final - Annex 3
Tárgy:	MELLÉKLET a következőhöz: A Bizottság felhatalmazáson alapuló rendelete a 2010/40/EU európai parlamenti és tanácsi irányelvnek a kooperatív intelligens közlekedési rendszer kiépítése és gyakorlati használata tekintetében történő kiegészítéséről

Mellékelten továbbítjuk a delegációknak a C(2019) 1789 final számú dokumentum III. mellékletét.

Melléklet: C(2019) 1789 final - Annex 3

EURÓPAI
BIZOTTSÁG

Brüsszel, 2019.3.13.
C(2019) 1789 final

ANNEX 3

MELLÉKLET

a következőhöz:

A Bizottság felhatalmazáson alapuló rendelete

a 2010/40/EU európai parlamenti és tanácsi irányelvnek a kooperatív intelligens közlekedési rendszer kiépítése és gyakorlati használata tekintetében történő kiegészítéséről

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

TARTALOMJEGYZÉK

III. MELLÉKLET

1. BEVEZETÉS

1.1. A házirend áttekintése és alkalmazási köre

E hitelesítési házirend (vagy más néven hitelesítési rend) az európai C-ITS-megbízhatósági modellt a nyilvános kulcsú infrastruktúra (PKI) alapján határozza meg az általános uniós C-ITS-biztonsági hitelesítéskezelő rendszer (EU CCMS) keretén belül. Követelményeket állapít meg a C-ITS-alkalmazásokkal összefüggő nyilvános kulcsú tanúsítványok kezelésére – mind a tanúsítványkiadók, mind azoknak a végfelhasználók általi európai igénybevétele vonatkozásában. Legmagasabb szinten a PKI egy sor gyökérszintű hitelesítésszolgáltatóból (gyökérszintűCA) áll, amelyeket a bizalmi lista kezelője (TLM) úgy engedélyez, hogy a hitelesítésszolgáltató tanúsítványait beilleszti az európai tanúsítványok megbízhatósági listájába (ECTL), melyet a bizalmi listát kezelő központi szervezet bocsátja ki és teszi közzé (lásd az 1.2. és 1.3. szakaszt).

Ez a házirend az európai bizalmas C-ITS rendszerben részt vevő valamennyi jogalany számára kötelező érvényű. A házirend segít annak felmérésében, hogy a PKI adott végfelhasználói tanúsítványával hitelesített üzenetnek a fogadója a kapott információ tekintetében milyen bizalmi szintet állapíthat meg. Az EU CCMS által megadott tanúsítványok iránti bizalom felmérésének lehetővé tétele érdekében a házirend egy sor kötelező érvényű követelményt határoz meg a bizalmi listát kezelő központi szervezet működésére és az európai tanúsítványok megbízhatósági listájának összeállítására és kezelésére vonatkozóan. Következésképpen ez a dokumentum az európai tanúsítványok megbízhatósági listájának alábbi vonatkozásait szabályozza:

- a PKI-szerepet kapó megbízók azonosítása és hitelesítése a bizalmi lista kezelője számára, ideértve az egyes szerepekkel járó kiváltságokról szóló nyilatkozatokat;
- a bizalmi lista kezelőjére vonatkozó minimumkövetelmények a helyi biztonsági gyakorlatok tekintetében, ideértve a fizikai, személyzeti és eljárásbeli ellenőrzéseket;
- a bizalmi lista kezelőjére vonatkozó minimumkövetelmények a műszaki biztonsági gyakorlatok tekintetében , ideértve a számítógépek biztonságát, a hálózati biztonságot és a kriptográfiai modul műszaki ellenőrzését;
- a bizalmi lista kezelőjére vonatkozó minimumkövetelmények a működési gyakorlatok tekintetében , ideértve az új gyökérszintű tanúsítványkiadó tanúsítványainak regisztrációját, a már meglévő és nyilvántartásba vett gyökérszintű tanúsítványkiadók ideiglenes vagy végleges törlését a nyilvántartásból, és az európai tanúsítványok megbízhatósági listája frissítéseinek közzétételét és terjesztését;
- az ECTL-profil (ideértve az ECTL valamennyi kötelező és opcionális adatmezőjét, a felhasználandó kriptográfiai algoritmusokat, a pontos ECTL-formátumot és az ECTL feldolgozásával kapcsolatos ajánlásokat);
- az ECTL-tanúsítvány teljes életciklusra kiterjedő kezelése, ideértve az ECTL-tanúsítványok terjesztését, aktiválását, lejártát és visszavonását;

- szükség szerint a gyökérszintű CA-k bizalommegvonási eljárásának lebonyolítása.

Mivel az ECTL megbízhatósága nem kizárólagosan magától az ECTL-től függ, hanem nagymértékben a PKI-ből és az alacsonyabb szintű CA-kból álló gyökérszintű CA-któl is, e hitelesítési házirend az összes részt vevő CA-ra (így a gyökérszintű CA-kra és az alacsonyabb szintű CA-kra) kötelező érvényű minimumkövetelményeket is meghatároz. A követelmények szerinti területek a következők:

- a PKI-szerepeket kapó megbízók azonosítása és hitelesítése (pl. biztonsági tisztviselő, adatvédelmi tisztviselő, biztonsági adminisztrátor, könyvtár-adminisztrátor és végfelhasználó), ideértve az egyes szerepekhez kapcsolódó feladatokról, felelősségi körökről, kötelezettségekről és kiváltságokról szóló nyilatkozatot;
- kulcskezelés, ideértve az elfogadható és kötelező tanúsítvány-aláíró és adataláíró algoritmusokat, és a tanúsítványok érvényességi idejét;
- a helyi biztonsági gyakorlatokra vonatkozó minimumkövetelmények, ideértve a fizikai, személyzeti és eljárásbeli ellenőrzéseket;
- a műszaki biztonsági gyakorlatokra vonatkozó minimumkövetelmények, így például a számítógépek biztonsága, a hálózati biztonság és a kriptográfiai modul műszaki ellenőrzése;
- a CA, EA és AA, valamint a végfelhasználók működési gyakorlatára vonatkozó minimumkövetelmények, ideértve a regisztrációt, a nyilvántartásból való törlést, a visszavonást, a kulcs titkosságának sérülését, az indokolt elutasítást, a tanúsítványfrissítést, az ellenőrzési gyakorlatot és a magán jellegű információk bizalmas kezelését;
- tanúsítvány és CRL-profil, ideértve a formátumot, az elfogadható algoritmusokat, a kötelező és opcionális adatmezőket és azok érvényes értéktartományát, illetve annak módját, hogy a hitelesítést végzők hogyan dolgozzák fel a tanúsítványokat;
- a C-ITS megbízhatósági modell szervezeteinek rendszeres ellenőrzése, riasztása, feladatköreinek visszaállítása, illetve a szervezetekről jelentések készítése annak érdekében, hogy így garantálják a biztonságos működést (többek között kötelességszegés esetén).

A fenti minimumkövetelményeken kívül a legfelső szintű és alacsonyabb szintű CA-kat működtető szervezetek további követelményeket is meghatározhatnak a megfelelő tanúsítványalkalmazási nyilatkozatukban (CPS), feltéve hogy azok nem mondanak ellent a hitelesítési házirend előírásainak. A CP-k auditálsáról és közzétételéről az 1.5. szakasz tartalmaz további részleteket.

A hitelesítési házirend (CP) ugyancsak meghatározza, hogy milyen célokra használhatók a gyökérszintű (legfelső szintű) CA-k és az alacsonyabb szintű CA-k, valamint az azok által kiadott tanúsítványok. Meghatározza, hogy milyen kötelezettségei vannak:

- a bizalmi lista kezelőjének (TLM);
- azon gyökérszintű CA-knak, amelyek tanúsítványai az ECTL-ben (európai tanúsítványok megbízhatósági listája) szerepelnek;

- a gyökérszintű CA alacsonyabb szintű CA-inak (EA és AA);
- a C-ITS megbízhatósági modell valamely szervezetéért felelős vagy azt működtető személynek, illetve szervezetnek.

A hitelesítési házirend (CP) az alábbiakra nézve kötelezettségeket is megszab:

- a bizalmi lista kezelője (TLM);
- azon gyökérszintű CA-knak, amelyek tanúsítványai az ECTL-ben (európai tanúsítványok megbízhatósági listája) szerepelnek;
- a gyökérszintű CA által tanúsított alacsonyabb szintű CA-k;
- a végfelhasználók;
- a C-ITS megbízhatósági modell valamely szervezetéért felelős vagy azt működtető személy, illetve szervezet.

Végül pedig a hitelesítési házirend (CP) követelményeket állapít meg arra vonatkozóan, hogy miként dokumentálják a tanúsítványalkalmazási nyilatkozatban (CPS) azon gyökérszintű hitelesítésszolgáltatók (CA-k) kötelezettségeinek korlátozásait, amelyek tanúsítványai az ECTL-ben szerepelnek.

Ez a hitelesítési házirend (CP) összhangban van a hitelesítési házirendnek és a hitelesítési gyakorlatnak az Internet-mérnöki Munkacsoport (IETF) [3] által elfogadott keretrendszerével.

1.2. Fogalommeghatározások és rövidítések

E melléklet alkalmazásában a [2], [3] és [4] fogalommeghatározásai érvényesek.

AA	engedélyezési hatóság
AT	engedélyezési jegy
CA	hitelesítésszolgáltató
CP	hitelesítési házirend
CPA	A C-ITS hitelesítési házirendjének hatósága
CPOC	C-ITS kapcsolattartási pont
CPS	tanúsítványalkalmazási nyilatkozat
CRL	tanúsítvány-visszavonási lista
EA	nyilvántartásba vételi hatóság
EC	nyilvántartásba vételi hitelesítő adatok
ECIES	elliptikus görbéjű, integrált titkosítási séma
EE	végfelhasználó (azaz C-ITS állomás)

ECTL	Európai tanúsítványok megbízhatósági listája
EU CCMS	EU C-ITS biztonsági hitelesítéskezelő rendszer
GDPR	Az általános adatvédelmi rendelet
HSM	biztonsági hardvermodul
PKI	nyilvános kulcsú infrastruktúra
RA	regisztrációs hatóság
sub-CA	EA és AA
TLM	bizalmi lista kezelője

Glosszárium

igénylő	Tanúsítványt (vagy annak megújítását) kérelmező természetes vagy jogi személy. A kezdeti tanúsítvány létrehozása után (inicializálás), a kérelmezőre a szöveg előfizetőként hivatkozik. A végfelhasználók számára kiállított tanúsítványok esetében az előfizető (tanúsítványigénylő) azon végfelhasználó ellenőrzéséért vagy működtetéséért/fenntartásáért felelős jogalany, amely a tanúsítvány címzettje – még akkor is, ha az aktuális tanúsítványkérelmet maga a végfelhasználó nyújtja be.
engedélyezési hatóság	Ebben a dokumentumban az „engedélyezési hatóság” (AA) kifejezés nemcsak az AA konkrét funkciójára utal, hanem az azt működtető jogi és/vagy operatív szervezetre is.
hitelesítésszolgáltató	A gyökérszintű hitelesítésszolgáltatóra, a nyilvántartásba vételi hatóságra és engedélyezési hatóságra együttesen hitelesítésszolgáltatókként (CA) hivatkozik a szöveg.
C-ITS megbízhatósági modell	A C-ITS megbízhatósági modell felel a C-ITS állomások közötti bizalmi kapcsolat kiépítéséért. Utóbbinak eszközéül egy gyökérszintű CA-kból, a CPOC-ből, TLM-ből, EA-kból és AA-kból és egy biztonságos hálózatból álló PKI szolgál.
kriptoagilitás	A C-ITS megbízhatósági modell szervezeteinek felkészültsége arra, hogy a hitelesítési házirendet (CP) a változó környezeti és az új jövőbeni igényekhez igazítsák (pl. a kriptografikus algoritmusok és a kulcshosszok időközbeni módosításával)
Kriptográfiai modul	Olyan biztonságos, hardveralapú elem, amelyben kulcsok generálhatók és/vagy tárolhatók, véletlenszerű számok generálhatók, és adatok kerülnek aláírásra, illetve titkosításra.
nyilvántartásba vételi hatóság	Ebben a dokumentumban a „nyilvántartásba vételi hatóság” (EA) kifejezés nemcsak az EA konkrét funkciójára utal, hanem az azt működtető jogi és/vagy operatív szervezetre is.
PKI-résztvevők	A C-ITS megbízhatósági modell szervezetei – így a TLM, a gyökérszintű CA-k, az EA-k, AA-k és a C-ITS állomások.
kulcsmegújítás	Ez az alkomponens olyan elemek a [3] dokumentumban meghatározottak szerinti leírására szolgál, amelyek új kulcspárt generáló vagy az új nyilvános kulcsot hitelesítő új tanúsítvány kiállítását kérelmező előfizetőhöz, illetve más ilyen résztvevőhöz kapcsolódnak.
adattár	A tanúsítványok és a C-ITS megbízhatósági modellhez tartozó szervezetek által megadott tanúsítványokra vonatkozó adatoknak a 2.3. szakaszban meghatározottak szerinti tárolására szolgáló adattár.
gyökérszintű hitelesítésszolgáltató	Ebben a dokumentumban a „gyökérszintű hitelesítésszolgáltató” (gyökérszintű CA) kifejezés nemcsak a CA konkrét funkciójára utal, hanem az azt működtető jogi és/vagy operatív szervezetre is.
alany	Adott tanúsítványban alanyként azonosított természetes személy, eszköz, rendszer, egység vagy jogi személy (azaz vagy az előfizető vagy az előfizető által ellenőrzött, illetve működtetett eszköz).
előfizető	Azon természetes vagy jogi személy, aki számára tanúsítványt állítanak ki, és akit adott előfizetői megállapodás, illetve annak használati feltételei jogilag kötnek.
előfizetői megállapodás	A CA és az igénylő/előfizető közötti megállapodás, amely meghatározza a felek jogait és kötelezettségeit.

1.3. PKI-résztvevők

1.3.1. Bevezetés

A PKI-résztvevők a PKI-ben a jelen házirendben meghatározott szerepet töltenek be. Hacsak azt kifejezetten meg nem tiltják, adott résztvevő egyidejűleg több szerepet is vállalhat. Egyes szerepek egyidejű vállalása azonban megtiltható, hogy azzal elejét vegyék az érdekellentéteknek és biztosítsák a feladatok elkülönülését.

A résztvevők feladatuk egy részét adott szolgáltatási szerződés részeként további szervezetekre is átruházhatják. Például, amikor a visszavonási állapotra vonatkozó információt tanúsítvány-visszavonási listákon (CRL) keresztül nyújtják be, a CA a tanúsítvány-visszavonási lista kiállítója is, azonban a lista kiállítási felelősségét egy másik szervezetre is átruházhatja.

A PKI-szerepek a következőkből állnak:

- hatósági szerepek, azaz minden egyes szerep egyedileg kerül példányosításra;
- operatív szerepek, azaz a szerepek egy vagy több szervezetnél is példányosíthatók.

Például, gyökérszintű CA lehet egy kereskedelmi szervezet, közérdekvédelmi csoport, nemzeti szervezet és/vagy uniós szervezet.

Az 1. ábra a C-ITS megbízhatósági modell architektúráját mutatja a [2] alapján. Az architektúra rövid leírása itt is megtalálható, de a fő elemek részletes ismertetését az 1.3.2–1.3.6. szakasz tartalmazza

A C-ITS CPA jelöli ki a bizalmi lista kezelőjét (TML), amely így valamennyi PKI-résztvevő számára megbízható szervezet. A CPA jóváhagyja a gyökérszintű CA működését, és megerősíti, hogy a bizalmi lista kezelője megbízhat a gyökérszintű CA-(k)ban. A bizalmi lista kezelője (TML) kiállítja az európai tanúsítványok megbízhatósági listáját (ECTL), amely alapján valamennyi PKI-résztvevő felé tanúsítja, hogy a jóváhagyott gyökérszintű CA-k megbízhatók. A gyökérszintű CA tanúsítványokat állít ki a nyilvántartásba vételi hatóság (EA) és az engedélyezési hatóság (AA) számára, így tanúsítva a működésükbe vetett bizalmat. A nyilvántartásba vételi hatóság regisztrációs tanúsítványt állít ki a küldő és átjátszó C-ITS-állomásoknak (mint végfelhasználóknak), így tanúsítva a működésükbe vetett bizalmat. Az engedélyezési hatóság engedélyezési jegyeket (AT) állít ki a C-ITS-állomások számára a nyilvántartásba vételi hatóság iránti bizalom alapján.

A fogadó és átjátszó C-ITS-állomás (mint átjátszó fél) más C-ITS állomásokban is megbízhat, mivel az engedélyezési jegyeket egy olyan engedélyezési hatóság állítja ki, amelyben adott, a bizalmi listát kezelő és a C-ITS CPA-jának bizalmát élvező gyökérszintű CA megbízik.

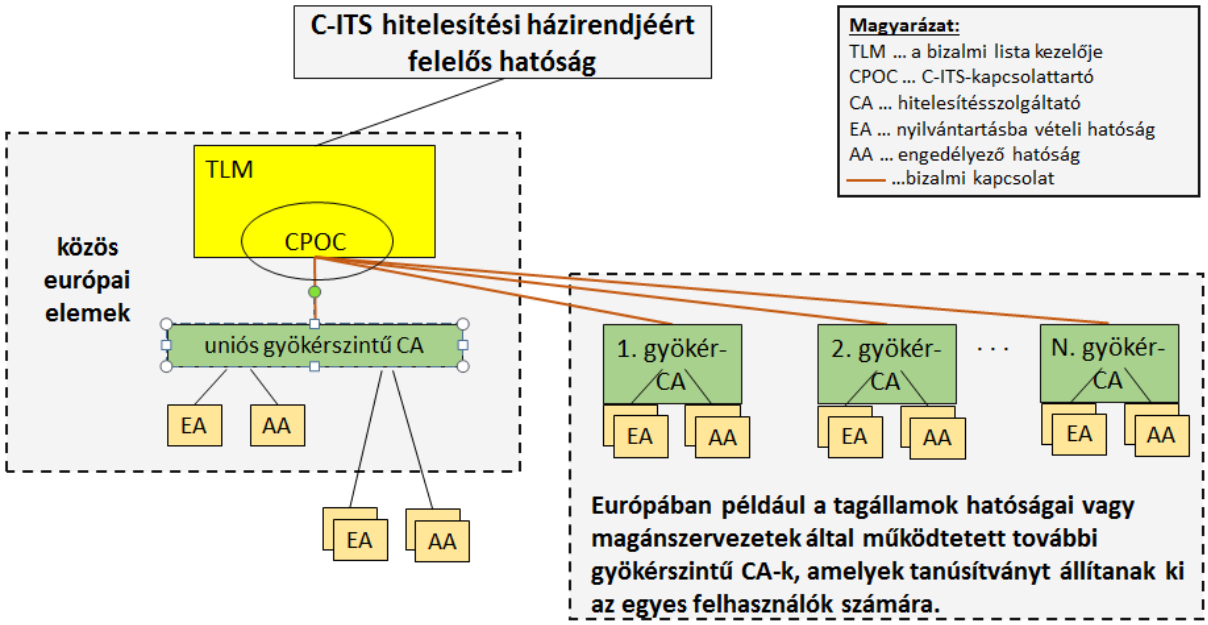
Vegye figyelembe, hogy az 1. ábra kizárólag a C-ITS megbízhatósági modell gyökérszintű CA-szintjét mutatja be. Az alacsonyabb szintek részleteit e hitelesítési házirend később részletezi, illetve az egyes gyökérszintű CA-k tanúsítványalkalmazási nyilatkozatai (CPS) taglalják.

A 2. ábra a PKI-résztvevők közötti információáramlás áttekintését mutatja. A zöld pontok a gépek közötti kommunikációt igénylő lépéseket mutatják. A piros színnel jelölt információáramlások meghatározott biztonsági követelményeket vonnak maguk után.

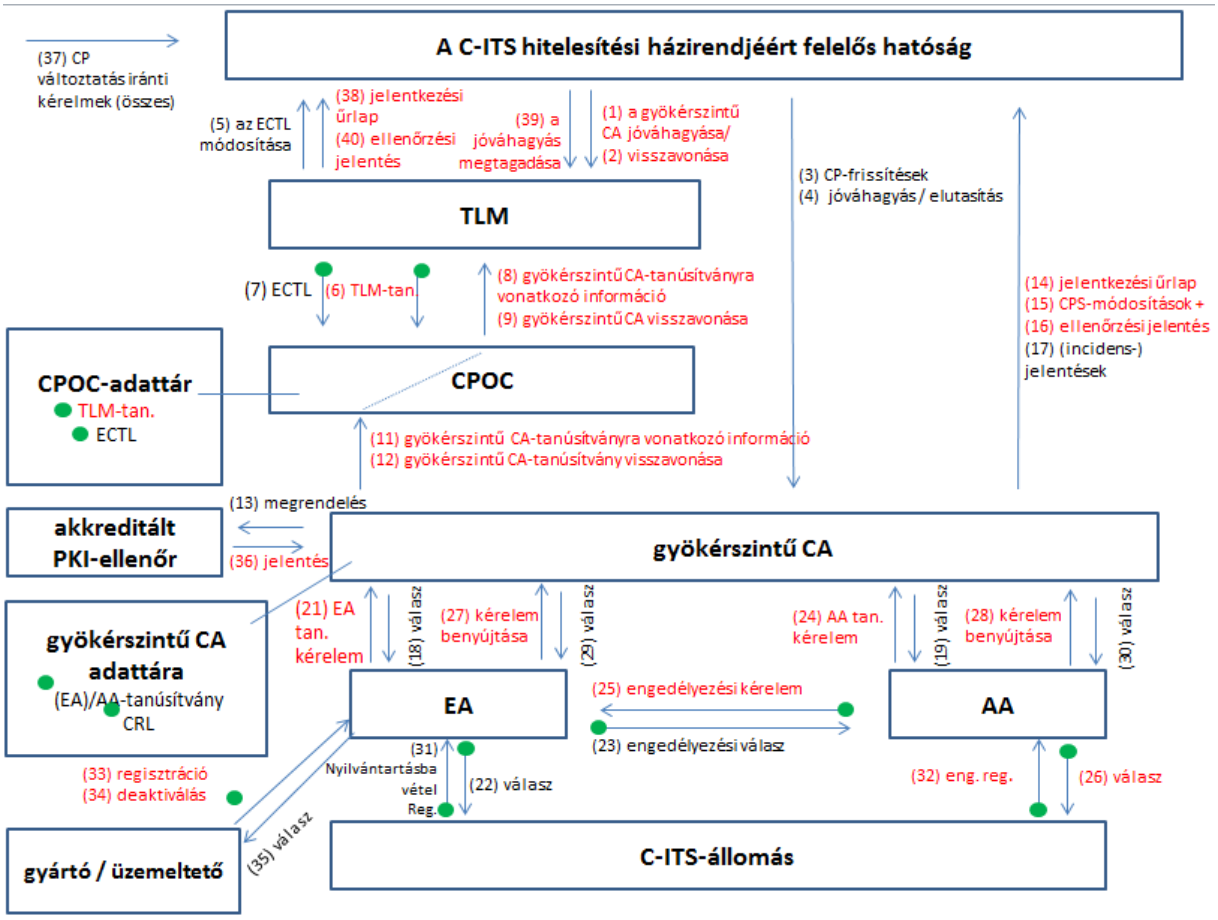
A C-ITS megbízhatósági modell egy többszörös gyökérszintű CA-architektúrára épül, ahol a gyökérszintű CA tanúsítványait (az alább meghatározottak szerinti) rendszeres időközönként egy központi kapcsolattartási pontra (CPOC) továbbítják egy, a CPOC által meghatározott biztonsági protokollon (pl. hivatkozási tanúsítványok) keresztül.

Adott gyökérszintű CA-t működtetheti egy kormány- vagy magánszervezet. A C-ITS megbízhatósági modell architektúrájának legalább egy gyökérszintű CA (a többi gyökérszintű CA-val azonos szintű uniós gyökérszintű CA) a részét képezi. Az uniós gyökérszintű CA-t a C-ITS megbízhatósági modellben részt vevő, de saját gyökérszintű CA-t létrehozni nem kívánó szereplők delegálják. A CPOC a megkapott gyökérszintű CA-tanúsítványokat a TLM-hez továbbítja, amely a gyökérszintű CA-k által kiállított tanúsítványok beszedéséért és jegyzékének aláírásáért felel, illetve azért, hogy azokat visszaküldje a CPOC-hez, amely a tanúsítványokat (lásd alább) mindenki számára nyilvánosan elérhetővé teszi.

A C-ITS megbízhatósági modellben érintett szervezetek közötti bizalmi kapcsolatot a következő ábrák, táblázatok és szakaszok mutatják be.



1. ábra: A C-ITS megbízhatósági modell architektúrája



2. ábra: A C-ITS megbízhatósági modellen belüli információáramlások

Lépés azonosítószáma	Forrás	Cél	Tartalom	Hivatkozás
(1).	CPA	TLM	a gyökérszintű CA kérelmezésének jóváhagyása	8
(2).	CPA	TLM	a gyökérszintű CA visszavonásának részletei	8.5
(3).	CPA	gyökérszintű CA	a hitelesítési házirend frissítései	1.5
(4).	CPA	gyökérszintű CA	a gyökérszintű CA kérelmezési formanyomtatványának elfogadása/elutasítása, illetve a CPS-kérelem módosításainak vagy az ellenőrzési folyamatnak az elfogadása/elutasítása	8.5, 8.6
(5).	TLM	CPA	értesítés az ECTL változásairól	4, 5.8.1
(6).	TLM	CPOC	TLM-tanúsítvány	4.4.2
(7).	TLM	CPOC	ECTL	4.4.2
(8).	CPOC	TLM	a gyökérszintű CA tanúsítványának adatai	4.3.1.1
(9).	CPOC	TLM	a gyökérszintű CA tanúsítványának visszavonása	7.3
(10).	CPOC	az összes végfelhasználó	TLM-tanúsítvány	4.4.2
(11).	gyökérszintű CA	CPOC	a gyökérszintű CA tanúsítványának adatai	4.3.1.1
(12).	gyökérszintű CA	CPOC	a gyökérszintű CA tanúsítványának visszavonása	7.3
(13).	gyökérszintű CA	ellenőr	ellenőrzési rend	8
(14).	gyökérszintű CA	CPA	a gyökérszintű CA kérelmezési formanyomtatványa – kezdeti kérelem	4.1.2.1
(15).	gyökérszintű CA	CPA	a gyökérszintű CA kérelmezési formanyomtatványa – a CPS változásai	1.5.1
(16).	gyökérszintű CA	CPA	a gyökérszintű CA kérelmezési formanyomtatványa – auditjelentés	8.6
(17).	gyökérszintű CA	CPA	a gyökérszintű CA incidensjelentései, ideértve adott, alacsonyabb szintű CA (EA, AA) visszavonását	III. melléklet, 7.3.1
(18).	gyökérszintű CA	EA	EA-tanúsítvány – válasz	4.2.2.3
(19).	gyökérszintű CA	AA	AA-tanúsítvány – válasz	4.2.2.3
(20).	gyökérszintű CA	az összes	EA/AA-tanúsítvány, CRL	4.4.2
(21).	EA	gyökérszintű CA	EA-tanúsítványkérelem	4.2.2.3

(22).	EA	C-ITS-állomás	nyilvántartásba vételi hitelesítő adatok – válasz	4.3.1.4
(23).	EA	AA	engedélyezési válasz	4.2.2.5
(24).	AA	gyökérszintű CA	AA-tanúsítványkérelem	4.2.2.3
(25).	AA	EA	engedélyezési kérelem	4.2.2.5
(26).	AA	C-ITS-állomás	engedélyezési jegy – válasz	4.3.1.5
(27).	EA	gyökérszintű CA	kérelem benyújtása	4.1.2.3
(28).	AA	gyökérszintű CA	kérelem benyújtása	4.1.2.3
(29).	gyökérszintű CA	EA	válasz	4.12 és 4.2.1
(30).	gyökérszintű CA	AA	válasz	4.12 és 4.2.1
(31).	C-ITS-állomás	EA	nyilvántartásba vételi hitelesítő adatokra irányuló kérelem	4.2.2.4
(32).	C-ITS-állomás	AA	engedélyezési jegy – válasz	4.2.2.5
(33).	gyártó/üzemeltető	EA	regisztráció	4.2.1.4
(34).	gyártó/üzemeltető	EA	deaktiválás	7.3
(35).	EA	gyártó/üzemeltető	válasz	4.2.1.4
(36).	ellenőr	gyökérszintű CA	jelentés	8.1
(37).	az összes	CPA	CP-módosítási kérelmek	1,5
(38).	TLM	CPA	kérelmezési formanyomtatvány	4.1.2.2
(39).	CPA	TLM	jóváhagyás/elutasítás	4.1.2.2
(40).	TLM	CPA	audit jelentés	4.1.2.2

1. táblázat: A C-ITS megbízhatósági modellen belüli információáramlások részletes leírása

1.3.2. A C-ITS hitelesítési házirendjének hatósága

(1) A C-ITS tanúsítványpolitikai hatósága (CPA) a C-ITS megbízhatósági modellben részt vevő állami és magánszektorbeli érdekelt felek képviselőiből áll (pl. tagállamok, gépjárműgyártók stb.). A CPA két alszerepért felel:

(1) hitelesítési házirend irányítása, ideértve a következőket:

- az aktuális hitelesítési házirend (CP), valamint hitelesítési házirend jövőbeni módosítási kérelmeinek jóváhagyása;

- döntéshozatal az egyéb PKI-résztvevők és -szervezetek által benyújtott,a hitelesítési házirendre módosítására irányuló kérelmek, illetve ajánlások felülvizsgálatáról;
- döntéshozatal az új CP-változatok kiadásáról;

(2) PKI-engedélyezéskezelés, ideértve a következőket:

- a CPS-ek jóváhagyási és a CA-k ellenőrzési eljárásainak (együttesen: „CA-jóváhagyási eljárások”) meghatározása, az azokkal kapcsolatos döntéshozatal, és nyilvánosságra hozataluk;
- a CPOC működési és rendszeres jelentéstételi engedélyének megadása;
- a TLM működési és rendszeres jelentéstételi engedélyének megadása;
- a gyökérszintű CA-k CPS-einek jóváhagyása, amennyiben azok megfelelnek az egységes és hatályos CP-knek;
- az akkreditált PKI-ellenőr auditjelentéseinek alapos vizsgálata valamennyi gyökérszintű CA esetében;
- a bizalmi lista kezelőjének értesítése a jóváhagyott és nem jóváhagyott gyökérszintű CA-k listájáról és tanúsítványaikról, a gyökérszintű CA-k beérkezett jóváhagyási jelentései és a rendszeres működési jelentések alapján.

(2) A CPA-k meghatalmazott képviselője felel a TLM meghatalmazott képviselőjének hitelesítéséért és a TLM felvételkérelmezési formanyomtatványának jóváhagyásáért. A CPA felel a TLM – e részben említett – működési engedélyezéséért.

1.3.3. A bizalmi lista kezelője

(3) A bizalmi lista kezelője (TLM) a CPA által kijelölt egyetlen szervezet.

(4) A TLM a következőkért felel:

- az ECTL-nek az egységes, hatályos hitelesítési házirendnek megfelelő működtetése, és a C-ITS megbízhatósági modell általános biztonságos működéséről rendszeres tevékenységi jelentéstétel a CPA-hoz;
- gyökérszintűCA-tanúsítványok fogadása a CPOC-től;
- ideértve/kivéve az ECTL-ben szereplő gyökérszintűCA-tanúsítványokat, a CPA-tól kapott értesítés esetén;
- az ECTL aláírása;
- az ECTL rendszeres és időszerű továbbítása a CPOC-hoz.

1.3.4. Akkreditált PKI-ellenőr

(5) Az akkreditált PKI-ellenőr a következőkért felel:

- gyökérszintű CA-k, TLM-ek és alacsonyabb szintű CA-k ellenőrzésének lebonyolítása vagy megszervezése;
- az auditjelentés (a kezdeti vagy az időszakos auditálásról) eljuttatása a CPA-nak a 8. szakaszban meghatározott feltételek szerint. Az auditjelentésnek az akkreditált PKI-ellenőr ajánlásait is tartalmaznia kell;

- az alacsonyabb szintű CA-k kezdeti vagy időszakos ellenőrzésének eredményes, illetve eredménytelen végrehajtását rögzítő gyökérszintű CA-t kezelő szervezet értesítése;
- annak felmérése, hogy a CPS összhangban van-e a CP-vel.

1.3.5. C-ITS kapcsolattartási pont (CPOC)

(6) A CPOC a C-ITS CPA által kijelölt egyetlen szervezet. A CPA meghatalmazott képviselője felel a CPOC meghatalmazott képviselőjének hitelesítéséért és a CPOC nyilvántartásba vétel kérelmezésére szolgáló formanyomtatványának jóváhagyásáért. A CPA felel a CPOC e szakasz szerinti működési engedélyezéséért.

(7) A CPOC a következőkért felel:

- a C-ITS megbízhatósági modell szereplői közötti biztonságos kommunikáció hatékony és gyors kialakítása és támogatása;
- a megbízhatósági modell többi résztvevője (pl. gyökérszintű CA-k) által benyújtott eljárásmódosítási kérelmek és ajánlások felülvizsgálata;
- a gyökérszintű CA-k tanúsítványainak továbbítása a TLM-hez;
- a nyilvános forráskulcs (bizalmi horgony) közzététele (aktuális nyilvános kulcs és a TLM hivatkozási tanúsítványa);
- az ECTL közzététele.

Az ETCL teljes leírása a 7. szakaszban olvasható.

1.3.6. Operatív szerepkör

(8) Az alábbi, [2]-ben meghatározott szervezetek rendelkeznek az RFC 3647 szabvány szerinti operatív szerepkörrel:

Funkcionális elem	PKI szerepkör ([3] és [4])	Részletes szerepkör ([2])
gyökérszintű hitelesítésszolgáltató	CA/RA (regisztrációs hatóság)	Az EA és AA számára igazolja, hogy azok kiállíthatnak EC-ket, illetve AT-ket
nyilvántartásba vételi hatóság	gyökérszintű CA előfizetője / EA-tanúsítvány alanya CA/RA	adott C-ITS-állomást hitelesíti és hozzáférést ad az ITS kommunikációjához
engedélyezési hatóság	gyökérszintű CA előfizetője / AA-tanúsítvány alanya CA/RA	Adott C-ITS-állomás számára hatóságilag igazolja, hogy az bizonyos ITS-szolgáltatásokat igénybe vehet
küldő C-ITS-állomás	a végfelhasználói (EE) tanúsítvány (EC) alanya	Az EA-tól jogot szerez az ITS kommunikációjához való hozzáféréshez Az AA-tól egyeztetés útján jogot szerez ITS-szolgáltatások indítására Egyugrásos és átjátszott (továbbított) szórási üzeneteket küld
átjátszó (továbbító) C-ITS állomás	átjátszó fél/az EE-tanúsítvány alanya	A C-ITS-állomástól szórási üzeneteket fogad és – ha szükséges – azokat továbbítja a fogadó C-ITS állomáshoz
fogadó C-ITS-állomás	átjátszó fél	Szórási üzeneteket fogad a küldő, illetve átjátszó C-ITS-állomástól
gyártó	az EA előfizetője	a biztonságirányításhoz szükséges információkat a gyártásnál beépíti a C-ITS-állomásba
üzemeltető	az EA/AA előfizetője	a biztonságirányításhoz szükséges információkat a működés során beépíti a C-ITS-állomásba, és frissíti is azokat

2. táblázat: Operatív szerepkör

Megjegyzés: A [4] alapján ez a hitelesítési házirend más terminológiát használ az előfizetőre (amely a tanúsítványok kiállítása céljából szerződik a CA-val) és az alanyra (azaz arra, akire a tanúsítvány vonatkozik). Előfizető minden olyan jogalany, amely szerződéses jogviszonyban áll valamely CA-val. Az alanyok olyan jogalanyok, amelyekre a tanúsítványok vonatkoznak. Az EA-k/AA-k egyszerre előfizetők és a gyökérszintű CA alanyai; és EA/AA-tanúsítványt igényelhetnek. A C-ITS állomások alanyok, és végfelhasználói tanúsítványt igényelhetnek.

(9) Nyilvántartási hatóságok:

Az EA feladata a végfelhasználók tekintetében a regisztrációs hatóság szerepének ellátása. Kizárólag hitelesített és engedélyezett előfizető regisztrálhat új végfelhasználót (C-ITS-állomást) az EA-nál. A megfelelő gyökérszintű CA-k feladata az EA-k és AA-k tekintetében a nyilvántartási hatóságok szerepének ellátása.

1.4. Tanúsítványhasználat

1.4.1. Alkalmazható felhasználási területek

(10) A jelen hitelesítés házirend szerint kiállított tanúsítványokat arra a célra használhatók fel, hogy azokkal validálják az együttműködő ITS-

kommunikációs kontextusában a digitális aláírásokat, a [2] referencia architektúrájának megfelelően.

(11) Az [5] szerinti tanúsítványprofilok meghatározzák, hogy a tanúsítványokat a bizalmi lista kezelője, a gyökérszintű CA-k, a nyilvántartásba vételi hatóságok, az engedélyezési hatóságok és a végfelhasználók szempontjából hogyan lehet felhasználni.

1.4.2. Felelősségkorlátozások

(12) A tanúsítványok nem használandók és nem használhatók fel az alábbi esetekben:

- olyan körülmények, amelyek vonatkozó jogszabályt, rendeletet (pl. általános adatvédelmi rendelet), határozatot vagy kormányrendeletet sértik vagy azzal ellentétesek;
- olyan körülmények, amelyek mások jogait sértik vagy azokkal ütköznek;
- e hitelesítési házirend, illetve a vonatkozó előfizetői megállapodás megsértése;
- bármely olyan körülmény, ahol a tanúsítványok felhasználása közvetlenül halált okozhat vagy személyi sérüléshez, illetve súlyos környezeti kárhoz vezethet (pl. a nukleáris létesítmények működésében, a repülőgépek irányításában vagy kommunikációjában, illetve a fegyvervezérlő rendszerekben bekövetkezett meghibásodások révén);
- olyan körülmények, amelyek ellentétesek a jobb közúti közlekedésbiztonság és a hatékonyabb közúti közlekedés általános európai célkitűzéseivel.

1.5. A hitelesítési házirend adminisztrációja

1.5.1. Az európai tanúsítványok megbízhatósági listáján szereplő hitelesítésszolgáltatók tanúsítványalkalmazási nyilatkozatainak aktualizálása

(13) Az európai tanúsítványok megbízhatósági listáján (ECTL) szereplő valamennyi gyökérszintű CA köteles közzétenni saját tanúsítványalkalmazási nyilatkozatát, amelynek meg kell felelnie a jelen hitelesítési házirendnek. A gyökérszintű CA-k további követelményeket is megállapíthatnak, de gondoskodniuk kell arról, hogy a jelen hitelesítési házirend követelményei mindvégig teljesüljenek.

(14) Az európai tanúsítványok megbízhatósági listáján szereplő valamennyi gyökérszintű CA-nak egy megfelelő módosítási eljárást is ki kell dolgoznia saját tanúsítványalkalmazási nyilatkozatára. A módosítási eljárás főbb jellemzőit a tanúsítványalkalmazási nyilatkozat nyilvános részében kell dokumentálni.

(15) A módosítási eljárással biztosítani kell, hogy a hitelesítési házirendet érintő változásokat körültekintően megvizsgálták, és amennyiben az a módosított hitelesítési házirendnek való megfelelőséghez szükséges, úgy a tanúsítványalkalmazási nyilatkozatot a hitelesítési házirendet érintő módosítási eljárás végrehajtási lépésében meghatározott időkereten belül frissítik. A módosítás eljárás különösen azon sürgősségi módosítási eljárásokat érinti, amelyekkel a hitelesítési házirend biztonsági szempontból fontos változtatásainak időszerű végrehajtása biztosított.

(16) A módosítási eljárásnak ki kell terjednie azon intézkedésekre is, amelyek a tanúsítványalkalmazási nyilatkozatot érintő változtatásoknak a hitelesítési házirendnek való megfelelőségét vizsgálják. A tanúsítványalkalmazási nyilatkozat módosításait egyértelműen és világosan kell dokumentálni. A tanúsítványalkalmazási nyilatkozat újabb változatának bevezetése előtt egy akkreditált PKI-ellenőrnek meg kell erősítenie, hogy az megfelel a hitelesítési házirendnek.

(17) A gyökérszintű CA köteles a CPA-t értesíteni minden, a tanúsítványalkalmazási nyilatkozatot érintő változtatásról; ehhez legalább az alábbi információkat meg kell adnia:

- a változtatás pontos leírása;
- a változtatás indoklása;
- az akkreditált PKI-ellenőr jelentése a hitelesítési házirendnek való megfelelőség megerősítéséről;
- a tanúsítványalkalmazási nyilatkozatért felelős személy kapcsolattartási adatai;
- a bevezetés tervezett időtartama.

1.5.2. A tanúsítványalkalmazási nyilatkozat jóváhagyási eljárása

(18) Működésének megkezdése előtt a leendő gyökérszintű CA köteles tanúsítványalkalmazási nyilatkozatát a megfelelőségi audit elrendelésének (13. lépés) részeként egy akkreditált PKI-ellenőr elé terjeszteni, és a nyilatkozatát a CPA-hoz is be kell nyújtania jóváhagyásra (15. lépés).

(19) A gyökérszintű CA a tanúsítványalkalmazási nyilatkozat módosításait köteles a megfelelőségi audit elrendelésének (13. lépés) részeként egy akkreditált PKI-ellenőr elé terjeszteni, és azt a CPA-hoz is be kell nyújtania jóváhagyás céljából (15. lépés) még a módosítások hatályba lépése előtt.

(20) Adott nyilvántartásba vételi/engedélyezési hatóságnak a saját tanúsítványalkalmazási nyilatkozatát, illetve az azt érintő változtatásokat a gyökérszintű CA-val ismertetnie kell. A gyökérszintű CA a nyilvántartásba vételi hatóság/engedélyezési hatóság jóváhagyásáért felelős állami vagy magánszervezettől a – 4.1.2. és a 8. szakaszban meghatározottaknak megfelelően – megfelelőségi tanúsítványt kérhet.

(21) Az akkreditált PKI-ellenőr a 8. szakasznak megfelelően értékeli a CPS-t.

(22) Az akkreditált PKI-ellenőr a 8.1. szakasznak megfelelően az auditjelentés részeként közli a CPS értékelésének eredményét. A CPS elfogadására vagy elutasítására az auditjelentés 8.5. és 8.6. szakaszban említett elfogadásának részeként kerül sor.

2. KÖZZÉTÉTELI ÉS ADATTÁRRAL KAPCSOLATOS FELELŐSSÉGI KÖRÖK

2.1. A tanúsítványadatok közzétételének módjai

(23) A tanúsítványadatok a 2.5. szakasz értelmében a következő esetekben tehetők közzé:

- rendszeresen, illetve rendszeres időközönként; vagy

- válaszul valamely részt vevő jogalany kérésére.

Mindkét esetben a közzététel sürgőssége eltérő mértékű, így az ütemezés is más, azonban a jogalanyoknak készen kell állniuk mindkét intézkedéstípusra.

(24) A tanúsítványadatok rendszeres közzététele lehetővé teszi azon legtávolabbi határidő meghatározását, ameddig a tanúsítványadatokat a C-ITS-hálózat valamennyi csomópontján aktualizálják. Az összes tanúsítványadat közzétételének gyakoriságát a 2.2. szakasz határozza meg.

(25) A C-ITS-hálózatban részt vevő szervezetek kérésére, bármely résztvevő bármikor megkezdheti a tanúsítványadatok közzétételét, és állapotuktól függően az aktuális tanúsítványadatokat is kikérheti, hogy így a C-ITS-hálózat teljes körű, megbízható „csomópontjává" válhasson. Az effajta közzététel célja főként az, hogy a szervezeteket naprakész információkkal lássák el a tanúsítványadatok jelenlegi, hálózaton belüli állapotáról, és lehetővé tegyék számukra az információk következő rendszeres közzétételéig a bizalmi alapú kommunikációt.

(26) Adott egyetlen gyökérszintű CA szintén bármikor kezdeményezheti a tanúsítványadatok közzétételét: ehhez az aktualizált tanúsítványokat el kell küldenie a C-ITS-hálózat „előfizetői tagjainak", akik az ilyen információk rendszeres címzettjei. Ez a CA-k működését is támogatja, és lehetővé teszi, hogy a tanúsítványok rendszeres és tervezett kiadása között a CA elérjék a tagokat.

(27) A 2.5. szakasz a gyökérszintű CA-k tanúsítványainak közzétételére és az ECTL-re vonatkozó eljárásokat és mechanizmust határoz meg.

(28) A CPOC köteles közzétenni a gyökérszintű CA-k (az ECTL-ben foglalt és nyilvános felhasználásra szánt) tanúsítványait, a TLM-tanúsítványokat és az általa kiadott ECTL-t.

(29) A gyökérszintű CA-k kötelesek közzétenni az EA/AA-tanúsítványokat és a tanúsítvány-visszavonási listákat, és felkészültnek kell lenniük az itt említett mindhárom mechanizmus támogatására annak érdekében, hogy a tanúsítványok az előfizető tagok és az érintett felek számára közzétételre kerüljenek, ennek kapcsán pedig minden szükséges lépést meg kell tenni annak érdekében, hogy a 4. szakaszban említett biztonságos továbbítás garantált legyen.

2.2. A közzététel ideje, illetve gyakorisága

(30) A tanúsítványok és a tanúsítvány-visszavonási listák közzétételének ütemezésére vonatkozó követelményeket az egyedi C-ITS-csomópontok különböző korlátozó tényezőinek függvényében kell meghatározni – egy „megbízhatósági hálózat" működtetésének és a frissítéseknek az összes érintett C-ITS-állomás számára történő minél hamarabbi közzétételének általános céljával.

- A frissített tanúsítványadatok (pl. az ECTL vagy a CRL összetételének változásai) rendszeres közzététele esetében legfeljebb három hónapra van szükség ahhoz, hogy a C-ITS-hálózat biztonságosan tudjon működni.
- A gyökérszintű CA-k kötelesek a kiadás után minél hamarabb közzétenni a CA-tanúsítványaikat és a tanúsítvány-visszavonási listákat.

- A tanúsítvány-visszavonási lista közzétételéhez a gyökérszintű CA adattárát kell felhasználni.

Ezenkívül minden egyes CA tanúsítványalkalmazási nyilatkozatában meg kell adni azt az időtartamot, amelyen belül a tanúsítványt – azt követően, hogy azt a CA kiállította – közzéteszik.

Ez a szakasz kizárólag a rendszeres közzététel idejét és gyakoriságát határozza meg. E dokumentum előírásainak megfelelően biztosítani kell az összekapcsolhatóságot annak érdekében, hogy a-C-ITS állomásokat a közzététel előtt egy héttel az ECTL-lel és CRL-ekkel frissítsék (normál működési feltételek mellett, pl. celluláris lefedettség, ténylegesen működő jármű).

2.3. Adattár

(31) Az adattár szerkezete tekintetében annak követelményei, hogy hogyan tárolják a tanúsítványokat és a C-ITS-hálózat szervezetei milyen információkat adjanak meg – az egységes szervezetek esetében – a következőképpen alakulnak:

- általánosságban véve, minden gyökérszintű CA-nak a saját, mindenkor érvényes EA/AA tanúsítványadatainak és CRL-jének adattárát kell felhasználnia a többi PKI-résztvevő (pl. LDAP-alapú könyvtárszerviz) tanúsítványának közzétételéhez. Az egyes gyökérszintű CA-k adattárának támogatnia kell minden a C-ITS-sel kapcsolatos információk terjesztési módjai szempontjából szükséges hozzáférés-ellenőrzést (2.4. szakasz) és továbbítási időt (2.2. szakasz);
- a TLM adattárának (amely például a CPOC által kiadott ECTL- és TLM-tanúsítványokat tárolja) egy olyan közzétételi mechanizmuson kell alapulnia, amely minden terjesztési mód esetében biztosítani tudja a 2.2. szakaszban meghatározott továbbítási időket.

Nem kerülnek meghatározásra az AA-ra vonatkozó követelmények, azonban azoknak a többi szervezettel azonos biztonsági szintet kell biztosítaniuk, és erről a CPS-ben is nyilatkozni kell.

2.4. Az adattárak hozzáférés-ellenőrzései

(32) A tanúsítványadatok adattárához való hozzáférés ellenőrzési követelményeinek legalább az ISO/IEC/27001 szabványban felvázolt általános biztonságos információkezelési előírásoknak és a 4. szakasz szerinti követelményeknek meg kell felelniük. Emellett tükrözniük kell a tanúsítványadatok közzététele során alkalmazandó egységes eljárás lépései vonatkozásában megállapítandó eljárásbiztonsági igényeket.

- Ez magában foglalja a TLM-tanúsítványok és a TLM/CPOC ECTL-adattárának kialakítását. Minden egyes CA, illetve adattárkezelő köteles a C-ITS-szervezetekkel és a külső felekkel összefüggésben a hozzáférést legalább három szinten ellenőrizni (pl. nyilvános, a C-ITS-szervezetekre korlátozott, gyökérszintű CA szint), hogy így elejét vegyék annak, hogy illetéktelen szervezetek kiegészítsék, módosítsák vagy töröljék az adattár bejegyzéseit.
- Az egyetlen szervezet pontos hozzáférés-ellenőrzési mechanizmusai a vonatkozó CPS részét kell, hogy képezzék.

- Az egyes gyökérszintű CA-k esetében fontos, hogy a nyilvántartásba vételi hatóság és az engedélyezési hatóság adattárai a hozzáférés-ellenőrzési eljárások tekintetében azonos követelményeknek tegyenek eleget – az adattárat kezelő szolgáltató helyétől vagy szerződés szerinti elérhetőségétől függetlenül.

A hozzáférés-ellenőrzési szintek kiindulási pontjaként az egyes CA-knak, illetve adattár-kezelőknek legalább három szintről kell gondoskodniuk (pl. nyilvános, a C-ITS szervezetekre korlátozódó, gyökérszintű CA-szint).

2.5. A tanúsítványadatok közzététele

2.5.1. A tanúsítványadatok TLM általi közzététele

(33) A közös európai C-ITS megbízhatósági területen a TLM-nek a CPOC-n keresztül az alábbi információkat kell közzétennie:

- a következő működési időszakra jelenleg érvényes összes TLM-tanúsítvány (aktuális és hivatkozási tanúsítvány, ha van ilyen);
- hozzáférési ponttal kapcsolatos információk a CPOC adattára tekintetében, a gyökérszintű CA aláírt listájának (ECTL) biztosítása érdekében;
- általános tájékoztatási pont az ECTL és a C-ITS kiépítése kapcsán.

2.5.2. A tanúsítványadatok CA-k általi közzététele

(34) A közös európai C-ITS megbízhatósági területen a gyökérszintű CA-k kötelesek az alábbi információkat közzétenni:

- a 2.3. szakaszban említett adattárban szereplő, kiadott (jelenleg érvényes) gyökérszintű CA-tanúsítványok (aktuális és a megfelelő újrakódoláson átesett tanúsítványok, ideértve a hivatkozási tanúsítványt);
- valamennyi érvényes EA és AA szervezet, működési azonosítójukkal és tervezett működési idejükkel;
- a 2.3. szakaszban említett adattárban tárolt, kiadott CA-tanúsítványok;
- a visszavont CA-tanúsítványokra vonatkozó tanúsítvány-visszavonási listák, az alacsonyabb szintű nyilvántartásba vételi és engedélyezési hatóságokra is kitérve;
- információ arról, hogy a gyökérszintű CA hogyan fér hozzá a CRL-lel és CA-val kapcsolatos információkhoz (hozzáférési pont).

A tanúsítványadatokat három titkossági szint szerint kell csoportosítani, és a nyilvánosságnak szóló dokumentumokat pedig korlátozás nélkül nyilvánosan elérhetővé kell tenni.

3. AZONOSÍTÁS ÉS HITELESÍTÉS

3.1. Elnevezés

3.1.1. Elnevezés típusa

3.1.1.1. A TLM, gyökérszintű CA, EA-k és AA-k elnevezései

(35) A TLM-tanúsítványban szereplő névnek egyetlen „subject_name” attribútumból kell állnia, a következő fenntartott értékkel: „EU_TLM”.

(36) A gyökérszintű CA-k esetében a névnek egyetlen „subject_name” attribútumból kell állnia, a CPA által allokált értékkel. A nevek egyedisége a CPA kizárólagos felelőssége. A CPA értesítése alapján a TLM köteles nyilvántartást vezetni a gyökérszintű CA neveiről (a gyökérszintű CA jóváhagyása, visszavonása/törlése). A „subject_name” elnevezések a tanúsítványban 32 bájtra korlátozódnak. Az egyes gyökérszintű CA-k tervezett nevüket a kérelmezési formanyomtatványon keresztül (14. lépés) terjesztik a CPA elé. A CPA felel a nevek egyediségének ellenőrzéséért. Amennyiben a név nem egyedi, úgy a kérelmezési formanyomtatványt elutasítják (4. lépés).

(37) Az egyes EA/AA-tanúsítványokban szereplő elnevezésnek egyetlen „subject_name” attribútumból kell állnia, a tanúsítvány kiadója által generált értékkel. Az elnevezések egyedisége a kiállító gyökérszintű CA kizárólagos felelőssége.

(38) Az EA- és AA-tanúsítványokban használt elnevezések nem lehetnek 32 bájtnál nagyobbak, hiszen a „subject_name” a tanúsítványokban 32 bájtra korlátozódik.

(39) Az engedélyezési jegyekben (AT) nem szerepelhet név.

3.1.1.2. Végfelhasználók elnevezései

(40) Az egyes C-ITS-állomásokhoz két fajta egyedi azonosítót kell hozzárendelni:

- egy kanonikus azonosítót, amelyet a gyártó felelőssége mellett a C-ITS-állomás kezdeti nyilvántartásában tárolnak. Ennek tartalmaznia kell egy, a gyártót, illetve üzemeltetőt azonosító olyan karakterláncrészt, amely biztosítja az azonosító egyediségét;
- valamint egy „subject_name” nevet, amely az EA felelőssége mellett a C-ITS-állomás EC-jének részét képezheti.

3.1.1.3. Tanúsítványok azonosítása

(41) Az [5] szerinti formátumnak megfelelő tanúsítványok az ott meghatározott módon kiszámított HashedId8-érték alapján azonosíthatók.

3.1.2. Az elnevezések érthetőségének szükségessége

Nincs kikötés.

3.1.3. A végfelhasználók anonimitása és álnév-használata

(42) Az engedélyezési hatóság (AA) gondoskodik a C-ITS-állomás álnév-használatáról: ehhez a C-ITS-állomás számára egy olyan engedélyezési jegyet ad, amely nem tartalmaz semmilyen olyan elnevezést vagy információt, amely az alanyt a valós személyazonosságával összeköthetné.

3.1.4. A különböző elnevezési formák értelmezési szabályai

Nincs kikötés.

3.1.5. Az elnevezések egyedisége

(43) A bizalmi lista kezelőjének (TLM), a gyökérszintű CA-knak, a nyilvántartásba vételi (EA) és engedélyezési hatóságoknak (AA), valamint a C-ITS állomásoknak egyedi elnevezéssel, illetve egyedi kanonikus azonosítóval kell rendelkezniük.

(44) A TLM köteles gondoskodni arról, hogy adott gyökérszintű CA-nak az ECTL-ben való regisztrációja során a tanúsítványazonosító (HashedId8) egyedi legyen. A gyökérszintű CA pedig arról gondoskodik a kiállítás során, hogy az alárendelt CA-k tanúsítványazonosítója (HashedId8) legyen egyedi.

(45) A kiállító CA-n belül a nyilvántartásba vételi hitelesítő adatok (EC) HashedId8-jének egyedinek kell lennie. Egy adott engedélyezési jegy HashedId8-jének nem kell egyedinek lennie.

3.2. Kezdeti azonosság-ellenőrzés

3.2.1. A titkos kulcs birtoklásának igazolási módja

(46) A gyökérszintű CA-nak igazolnia kell, hogy az önaláírt tanúsítvány nyilvános kulcsának megfelelő titkos kulcs jogszerűen van a birtokában. Ennek igazolását a CPOC ellenőrzi.

(47) A nyilvántartásba vételi/engedélyezési hatóságnak igazolnia kell, hogy a tanúsítványban szerepeltetendő nyilvános kulcsnak megfelelő titkos kulcs jogszerűen van a birtokában. Ennek igazolását a gyökérszintű CA ellenőrzi.

(48) Kulcsmegújítás esetén az új titkos kulcs birtoklását igazolni kell: ehhez az új titkos kulccsal kell aláírni a kérelmet (belső aláírás), amely után az aláírt kérelem külső aláírását a jelenleg érvényes titkos kulcs segítségével hozzák létre (a kérelem hitelességének garantálása érdekében). Az igénylőnek az aláírt tanúsítványkérelmét a kiállító CA-hoz egy biztonságos kommunikációs csatornán keresztül kell benyújtania. A kiállító CA-nak meg kell győződnie arról, hogy az igénylőnek a kérelmezési üzenetben szereplő digitális aláírása a tanúsítványkérelemhez csatolt nyilvános kulcsnak megfelelő titkos kulccsal készült. A gyökérszintű CA-nak meg kell határoznia, hogy a tanúsítványalkalmazási nyilatkozata (CPS) a tanúsítványokkal összefüggésben mely kéréseket és válaszokat támogatja.

3.2.2. A szervezeti azonosság hitelesítése

3.2.2.1. A gyökérszintű CA-k szervezeti azonosságának hitelesítése

(49) A CPA-nak címzett kérelmezési formanyomtatványon (azaz 14. lépés) a gyökérszintű CA-nak meg kell adnia a szervezet azonosító adatait és a regisztrációhoz szükséges információkat, amelyek a következők:

- szervezet neve;
- postai cím;
- e-mail-cím;
- a szervezet kapcsolattartó személyének neve;

- telefonszám;
- a gyökérszintű CA tanúsítványának digitális ujjlenyomata (azaz a SHA 256 hash érték) nyomtatott formában;
- a gyökérszintű CA tanúsítványában szereplő kriptografikus információk (azaz kriptografikus algoritmusok, kulcshosszok);
- az összes olyan engedély, amelyet a gyökérszintű CA felhasználhat és az alacsonyabb szintű CA-knak továbbadhat.

(50) A CPA köteles meggyőződni a szervezet azonosságáról és adott gyökérszintű CA-tanúsítványnak az ECTL-be való felvétele céljából a tanúsítványigénylő által megadott egyéb regisztrációs adatok valódiságáról.

(51) A CPA-nak vagy közvetlen bizonyítékot kell bekérnie vagy – megfelelő és engedélyezett forrástól származó – igazolást kell beszereznie a tanúsítvány címzettjeiül szolgáló alanyok személyazonosságáról (pl. név), és adott esetben azok bizonyos attribútumairól. A bizonyítékot papírformátumban vagy elektronikus dokumentum formájában lehet benyújtani.

(52) Az alany személyazonosságát a regisztrációkor a megfelelő eszközökkel és a jelenlegi hitelesítési házirenddel összhangban ellenőrizni kell.

(53) Az egyes tanúsítványigénylésekkel egy időben a következőket kell igazolni:

- a szervezet teljes neve (magánszervezet, kormányzati szervezet vagy nem kereskedelmi célú szervezet);
- olyan, nemzeti szinten elfogadott regisztrációs vagy egyéb attribútumok, amelyek – amennyire csak lehetséges – felhasználhatók arra, hogy a szervezetet megkülönböztessék a többi, ugyanolyan nevű szervezettől.

A fenti szabályok a TS 102 042 [4] szabványon alapulnak: *A CA köteles gondoskodni arról, hogy az előfizető és az alany nevének és kapcsolódó adatainak azonosságát és pontosságát igazoló bizonyítékokat vagy a meghatározott szolgáltatás részeként vessék alapos vizsgálat alá, vagy – adott esetben – a megfelelő és engedélyezett forrásoktól származó igazolások vizsgálata révén ellenőrizzék. Biztosítania kell továbbá, hogy a tanúsítványkérelmek pontosak, engedélyezettek és hiánytalanok legyenek – a bekért bizonyítékoknak, illetve igazolásoknak megfelelően.*

3.2.2.2. A TLM szervezeti azonosságának hitelesítése

(54) A TLM-et működtető szervezetnek igazolnia kell a név és a kapcsolódó adatok valódiságát és pontosságát is ahhoz, hogy a TLM-tanúsítvány kezdeti létrehozásakor és kulcsmegújításakor elvégezhessék a megfelelő ellenőrzést.

(55) Az alany személyazonosságát a kezdeti létrehozáskor és újrakódoláskor a megfelelő módon és a jelenlegi tanúsítási házirenddel összhangban ellenőrizni kell.

(56) A szervezetnek a bizonyítékot a 3.2.2.1. szakaszban meghatározott módon kell benyújtani.

3.2.2.3. Az alacsonyabb szintű CA-k szervezeti azonosságának hitelesítése

(57) A gyökérszintű CA köteles meggyőződni a szervezet azonosságáról és a tanúsítványigénylők által az alacsonyabb szintű CA-k (EA/AA) tanúsítványaihoz benyújtott egyéb regisztrációs adatok valódiságáról.

(58) Minimumkövetelményként a gyökérszintű CA-nak:

- meg kell állapítania, hogy a szervezet létezik-e: ehhez legalább egy független személyazonosság-igazoló szolgáltatást vagy adatbázist igénybe kell vennie, vagy alternatív lehetőségként a megfelelő kormányügynökség által kiadott, illetve a szervezet létezését megerősítő illetékes hatóságnál nyilvántartott szervezeti dokumentációra kell támaszkodnia;
- postai levél vagy hasonló eljárás útján fel kell kérnie a tanúsítványigénylőt arra, hogy megerősítsen a szervezettel kapcsolatos bizonyos információkat, így például azt, hogy engedélyezte a tanúsítványigénylést és az igénylő nevében a kérelmet benyújtó személy erre meghatalmazást kapott. Amennyiben adott tanúsítvány adott egyén, mint a szervezet meghatalmazott képviselője nevét is tartalmazza, akkor azt is meg kell erősíteni, hogy az illető a szervezet alkalmazásában áll, és az egyén a szervezet nevében való eljárásra meghatalmazást kapott.

(59) A CA-tanúsítványok kibocsátására vonatkozó validálási eljárásokat a gyökérszintű CA adott tanúsítványalkalmazási nyilatkozatában (CPS) dokumentálni kell.

3.2.2.4. Végfelhasználók előfizetői szervezetének hitelesítése

(60) Még azt megelőzően, hogy a végfelhasználók (gyártó/üzemeltető) előfizetője adott megbízható nyilvántartásba vételi hatóságnál (EA) annak céljából regisztrálhat, hogy végfelhasználói az EC-tanúsítványra irányuló kérelmüket benyújthassák, az EA-nak:

- ellenőriznie kell az előfizető szervezet azonosságát és meg kell győződnie a tanúsítványigénylő által benyújtott további regisztrációs adatok valódiságáról is;
- ellenőriznie kell, hogy a C-ITS-állomás (azaz a C-ITS-állomás márkája, modellje és verziója szerinti konkrét termék) megfelel-e valamennyi megfelelőségértékelési kritériumnak.

(61) Minimumkövetelményként az EA-nak:

- meg kell állapítania, hogy a szervezet létezik-e: ehhez legalább egy független személyazonosság-igazoló szolgáltatást vagy adatbázist igénybe kell vennie, vagy alternatív lehetőségként a megfelelő kormányügynökség által kiadott, illetve a szervezet létezését megerősítő illetékes hatóságnál nyilvántartott szervezeti dokumentációra kell támaszkodnia;
- postai levél vagy hasonló eljárás útján fel kell kérnie a tanúsítványigénylőt arra, hogy megerősítsen a szervezettel kapcsolatos bizonyos információkat, így például azt, hogy engedélyezte a tanúsítványigénylést és az igénylő nevében a kérelmet benyújtó személy erre meghatalmazást kapott. Amennyiben adott tanúsítvány adott egyén, mint a szervezet meghatalmazott képviselője nevét is tartalmazza, akkor azt is meg kell erősíteni, hogy az illető a szervezet alkalmazásában áll, és az egyén a szervezet nevében való eljárásra meghatalmazást kapott.

(62) Az adott C-ITS-állomás előfizető általi regisztrációjára vonatkozó validálási eljárásokat a nyilvántartásba vételi hatóság tanúsítványalkalmazási nyilatkozatában (CPS) dokumentálni kell.

3.2.3. Egyedi szervezet hitelesítése

3.2.3.1. A TLM/CA egyedi szervezetének hitelesítése

(63) Adott jogi személlyel vagy szervezettel (pl. az előfizetővel) összefüggésben azonosított egyedi szervezet (fizikai személy) hitelesítése esetében igazolni kell:

- az alany teljes nevét (ideértve a vezetéknevét és a keresztnevét, a vonatkozó jogszabályokkal és a nemzeti személyazonosítási gyakorlattal összhangban);
- az előfizető születési helyét és idejét, vagy egy nemzeti szinten elfogadott személyazonossági okmány, illetve az előfizető olyan további attribútumainak meglétét, amelyekkel – amennyire csak lehet – meg tudják különböztetni az illetőt a többi, ugyanolyan nevű személytől;
- a kapcsolódó jogi személy vagy egyéb szervezet teljes nevét és jogi státuszát (pl. előfizető);
- a kapcsolódó jogi személlyel vagy egyéb szervezettel kapcsolatos releváns nyilvántartási adatokat (pl. cégbejegyzés);
- azt, hogy az alany a jogi személyhez vagy egyéb szervezethez kötődik.

A bizonyítékot papírformátumban vagy elektronikus dokumentum formájában lehet benyújtani.

(64) Személyazonosságának igazolására a gyökérszintű CA meghatalmazott képviselője, illetve adott nyilvántartásba vételi vagy engedélyezési hatóság meghatalmazott képviselője, illetve az előfizető köteles dokumentumokkal igazolni, hogy az adott szervezetnél dolgozik (meghatalmazási tanúsítvány). Hivatalos személyazonosító okmányát szintén be kell mutatnia.

(65) A kezdeti nyilvántartásba vételi eljáráshoz (31/32. lépés), az EA/AA képviselője köteles a megfelelő gyökérszintű CA számára minden szükséges információt rendelkezésre bocsátani (lásd: 4.1.2. szakasz).

(66) A gyökérszintű CA munkatársainak meg kell győződniük a tanúsítványigénylő képviselőjének személyazonosságáról és a kapcsolódó dokumentumok valódiságáról; ehhez az 5.2.1. szakasz szerinti megbízható személyzetre vonatkozó követelményeket kell alapul venniük. (A kérelmezési adatok validálásáért és a tanúsítvány gyökérszintű CA általi létrehozásáért a gyökérszintű CA-nál működő „megbízható személyek” felelnek, akik tevékenységeiket – tekintettel arra, hogy azok az 5.2.2. szakasz értelmében kockázatos műveleteknek minősülnek – legalább kettős felügyelet alatt végzik.)

3.2.3.2. A C-ITS-állomások előfizetői személyazonosságának hitelesítése

(67) Az előfizetőket a szervezeten belül olyan meghatalmazott végfelhasználók képviselik, akik a kibocsátó EA és AA nyilvántartásában szerepelnek. Ezeknek a szervezetek (gyártók vagy üzemeltetők) által kijelölt végfelhasználóknak

személyazonosságukat és hitelességüket még azt megelőzően igazolniuk kell, hogy:

- a végfelhasználót a megfelelő nyilvántartásba vételi hatóságnál regisztrálják (ideértve a kanonikus nyilvános kulcsot, a kanonikus személyazonosítót [egyedi azonosító] és a végfelhasználónak megfelelő engedélyeket);
- az engedélyezési hatóságnál regisztrálnak és gondoskodnak az előfizetői megállapodás EA-hoz benyújtható igazolásáról.

3.2.3.3. A C-ITS-állomások azonosságának hitelesítése

(68) A nyilvántartásba vételi hitelesítő adatok végfelhasználói alanyai kötelesek a nyilvántartásba vételi hitelesítő adatok (EC) igénylésekor saját személyazonosságukat igazolni (31. lépés), amelynek során a kezdeti hitelesítéshez a kanonikus titkos kulcsukat kell használniuk. Az EA köteles a végfelhasználóknak megfelelő kanonikus nyilvános kulccsal ellenőrizni a hitelesítést. A végfelhasználók kanonikus nyilvános kulcsát még a kezdeti kérelem előtt az EA-nak bemutatják; ehhez egy a C-ITS állomás gyártója, illetve üzemeltetője és az EA közötti biztonságos csatornát használnak (33. lépés).

(69) Az engedélyezési jegyek végfelhasználói alanyai kötelesek az engedélyezési jegyek igénylésekor saját személyazonosságukat igazolni (32. lépés), amihez az egyedi, nyilvántartásba vételi titkos kulcsukat kell használniuk. Az engedélyezési hatóságnak (AA) validálásra továbbítania kell az aláírást a nyilvántartásba vételi hatósághoz (EA) (25. lépés); majd az EA azt validálja és az eredményt megerősíti az AA felé (23. lépés).

3.2.4. Nem ellenőrzött előfizetői adatok

Nincs kikötés.

3.2.5. Hatóság validálása

3.2.5.1. A TLM, a gyökérszintű CA, az EA és AA validálása

(70) A tanúsítványalkalmazási nyilatkozatban minden szervezet köteles legalább egy olyan képviselőt (pl. biztonsági tisztviselő) megnevezni, aki az új tanúsítványok és megújítások igényléséért felel. A szervezetnek alkalmaznia kell a 3.2.3. szakaszban meghatározott elnevezési szabályokat.

3.2.5.2. A C-ITS-állomás előfizetőinek validálása

(71) A nyilvántartásba vételi hatóságnak legalább egy olyan fizikai személyről tudnia kell, aki a C-ITS-állomásoknak a nyilvántartásba vételi hatóságoknál történő regisztrációjáért felel (pl. biztonsági tisztviselő), és annak személyét az EA-nak jóvá kell hagynia (lásd: 3.2.3. szakasz).

3.2.5.3. A C-ITS-állomások validálása

(72) A C-ITS-állomás előfizetője akkor regisztrálhat C-ITS-állomásokat egy konkrét nyilvántartásba vételi hatóságnál (33. lépés), ha az előfizetőt annál a konkrét nyilvántartásba vételi hatóságnál hitelesítették.

Ha a C-ITS-állomást adott EA-nál egy egyedi kanonikus azonosítóval és kanonikus nyilvános kulccsal regisztrálják, akkor az állomás a korábban regisztrált kanonikus nyilvános kulcshoz kapcsolódó kanonikus titkos kulccsal

aláírt kérelem formájában nyilvántartásba vételi hitelesítő adatot (EC) is igényelhet.

3.2.6. Együttműködési kritériumok

(73) A C-ITS-állomások és az EA-k (illetve AA-k) közötti kommunikáció érdekében a C-ITS állomásnak az EA-kkal (illetve AA-kkal) biztonságosan kell tudnia kommunikálni (így alkalmasnak kell lennie az [1]-ben meghatározottak szerint az adatok hitelesítésével, bizalmas kezelésével és sértetlenségével összefüggő feladatok ellátására). Más protokollok is alkalmazhatók, amennyiben az [1] követelményei teljesülnek. Az EA-nak és az AA-nak támogatnia kell ezt a biztonságos kommunikációt.

(74) Az EA-nak és az AA-nak támogatnia kell az [1] szerinti tanúsítványkérelmeket és -válaszokat; mindez pedig egy olyan, az engedélyezési jeggyel összefüggő biztonságos kérés-válasz protokoll meglétét feltételezi, amely támogatja az igénylő AA-val szembeni anonimitását, és az AA és EA közötti feladatmegosztást. Más protokollok is alkalmazhatók, amennyiben az [1] követelményei teljesülnek. Annak megakadályozása érdekében, hogy a C-ITS-állomások hosszú távú azonosítója kiszivárogjon, gondoskodni kell arról, hogy az adott mobil C-ITS-állomás és az EA közötti kommunikáció titkos legyen (pl. a kommunikáció részleteit teljes körűen titkosítani kell).

(75) Az AA köteles engedélyezésvalidálási kérelmet benyújtani (25. lépés) minden olyan engedélyezési kérelemre, amely egy végfelhasználói tanúsítvány alanyától érkezik be hozzá. Az EA köteles e kérelmet az alábbiak szerint validálni:

- a végfelhasználó státusza az EA-nál;
- az aláírás érvényessége;
- a kért ITS-alkalmazásazonosítók (ITS-AID) és jogosultságok;
- az előfizető számára biztosított AA-szolgáltatások állapota.

3.3. A kulcsmegújítási kérelmek azonosítása és hitelesítése

3.3.1. A rutinszerű kulcsmegújítási kérelmek azonosítása és hitelesítése

3.3.1.1. TLM-tanúsítványok

(76) A TLM egy kulcspárt és két tanúsítványt hoz létre: a 7. szakasznak megfelelően egy önaláírt és egy hivatkozási tanúsítványt.

3.3.1.2. Gyökérszintű CA-k tanúsítványai

Nem alkalmazható.

3.3.1.3. EA/AA-tanúsítványok megújítása vagy újrakódolása

(77) Azt megelőzően, hogy az EA/AA-tanúsítvány lejárna, az EA/AA-nak új tanúsítványt kell igényelnie (21./24. lépés) a tanúsítványhasználat folytonosságának biztosítása érdekében. Az EA/AA-nak új kulcspárt kell generálnia a lejáró kulcspár felváltására, és az aktuálisan érvényes titkos kulccsal alá kell írnia az új nyilvános kulcsot tartalmazó kulcsmegújítási kérelmet („kulcsmegújítás”). A nyilvántartásba vételi, illetve az engedélyezési hatóság új kulcspárt generál, és az új titkos kulccsal írja alá a kérelmet (belső aláírás), hogy így igazolja az új titkos kulcs birtoklását. A teljes kérelmet az

aktuálisan érvényes titkos kulccsal (külső aláírás) írják alá (aláírás felülírása), hogy így biztosítsák a kérelem sértetlenségét és hitelességét. Titkosító és visszafejtő kulcspár használata esetén az új titkos kulcs birtoklását igazolni kell (a kulcsmegújítás részletes leírását lásd a 4.7.3.3. szakaszban).

(78) A rutinszerű kulcsmegújítás azonosítási és hitelesítési módja megegyezik a kezdeti gyökérszintű CA-tanúsítvány validálásának kezdeti kiadásával, a 3.2.2. szakaszban foglaltaknak megfelelően.

3.3.1.4. Végfelhasználók nyilvántartásba vételi tanúsítványai

(79) Azt megelőzően, hogy az aktuális hitelesítő adatok érvényességüket vesztenék, a végfelhasználó köteles új tanúsítványt igényelni (31. lépés) a tanúsítványhasználat folytonosságának biztosítása érdekében. A végfelhasználó köteles új kulcspárt generálni a meglévő kulcspár felváltására, és egy az új nyilvános kulcsot tartalmazó új tanúsítványt kell igényelnie; a kérelmet az aktuálisan érvényes EC titkos kulccsal kell aláírni.

(80) A végfelhasználó a kérelmet az újonnan létrehozott titkos kulccsal is aláírhatja (belső aláírás) annak igazolására, hogy az új titkos kulcs a birtokában van. Majd az egész kérelmet az aktuálisan érvényes nyilvános kulccsal (külső aláírás) írják alá (aláírás felülírása) és az [1] szerinti fogadó EA számára titkosítják, hogy így biztosítsák a kérelem titkosságát, sértetlenségét és hitelességét. Más protokollok is alkalmazhatók, amennyiben az [1] követelményei teljesülnek.

3.3.1.5. Végfelhasználók engedélyezési jegyei

(81) Az engedélyezési jegyek (AT) tanúsítvány-kulcsmegújítása – az [1] szabványnak megfelelően –ugyanazt a folyamatot követi, mint a kezdeti engedélyezésé. Más protokollok is alkalmazhatók, amennyiben az [1] követelményei teljesülnek.

3.3.2. Visszavonás utáni kulcsmegújítási kérelmek azonosítása és hitelesítése

3.3.2.1. CA-tanúsítványok

(82) Adott CA-szervezet gyökérszintű CA-, EA- és AA-tanúsítvánnyal összefüggő, visszavonás utáni kulcsmegújításhoz szükséges hitelesítése ugyanazt a folyamatot követi, mint adott CA-tanúsítvány kezdeti kiadása (lásd a 3.2.2. szakaszt).

3.3.2.2. Végfelhasználók nyilvántartásba vételi tanúsítványai

(83) Adott végfelhasználó EC-tanúsítványának visszavonás utáni kulcsmegújítása esetén a hitelesítés ugyanazt a folyamatot követi, mint az EE-tanúsítványok kezdeti kiadása (lásd a 3.2.2. szakaszt).

3.3.2.3. Végfelhasználók engedélyezési kérelmei

Nem alkalmazható, mivel az engedélyezési jegyek nem kerülnek visszavonásra.

3.4. Visszavonási kérelemmel összefüggő azonosítás és hitelesítés

3.4.1. Gyökérszintű CA/EA/AA-tanúsítványok

(84) Adott CA-tanúsítványnak az ECTL-ből történő törlésére irányuló kéréseket a gyökérszintű CA-nak a TLM felé hitelesítenie kell (12. és 9. lépés). Adott EA/AA-tanúsítvány visszavonási kérelmét a megfelelő gyökérszintű CA-nak és alacsonyabb szintű CA-nak magának kell hitelesítenie.

(85) Adott előfizető visszavonási kérelmének hitelesítésére – egyebek mellett – az alábbi eljárások fogadhatók el:

- az előfizető céges levélpapírra írt, aláírt üzenete a visszavonás kérelmezéséről, hivatkozással a visszavonandó tanúsítványra;
- az előfizetővel folytatott kommunikáció, amely észszerű biztosítékot szolgáltat arra, hogy a visszavonást kérelmező személy, illetve szervezet tulajdonképpen maga az előfizető. A körülményektől függően, a fenti kommunikáció az alábbiak közül egy vagy akár több formában is megvalósulhat: e-mail, postai levél vagy futárszolgálat.

3.4.2. A C-ITS-állomás nyilvántartásba vételi hitelesítő adatai

(86) A C-ITS-állomás előfizetője visszavonhatja az adott nyilvántartásba EA-nál korábban már regisztrált C-ITS-állomás nyilvántartásba vételi hitelesítő adatait (EC) (34. lépés). A kérelmező előfizetőnek ehhez kérelmet kell benyújtania adott C-ITS-állomás, illetve adott C-ITS állomások listájának visszavonására. A nyilvántartásba vételi hatóságnak – még annak feldolgozása előtt – hitelesítenie kell a visszavonási kérelmet, és meg kell erősítenie a C-ITS-állomások és azok nyilvántartásba vételi hitelesítői adatainak visszavonását.

(87) Az EA adott C-ITS-állomás nyilvántartásba vételi hitelesítő adatait a 7.3. szakasz szerint vonhatja vissza.

3.4.3. A C-ITS-állomás engedélyezési jegyei

(88) Mivel az engedélyezési jegyek nem kerülnek visszavonásra, azok érvényessége adott időszakra korlátozódik. A jelen hitelesítési házirend szerint elfogadható érvényességi időtartamokat a 7. szakasz ismerteti.

4. A TANÚSÍTVÁNYOK ÉLETCIKLUSÁRA VONATKOZÓ MŰVELETI KÖVETELMÉNYEK

4.1. Tanúsítványigénylés

(89) E szakasz a tanúsítványkibocsátás kezdeti igénylésére vonatkozó követelményeket határozza meg.

(90) A „tanúsítványigénylés” kifejezés a következő eljárásokra utal:

- regisztráció, valamint a TLM és a CPA közötti bizalmi kapcsolat kiépítése;
- regisztráció, valamint a gyökérszintű CA, a CPA és TLM közötti bizalmi kapcsolat kiépítése, ideértve az első gyökérszintű CA-tanúsítványnak az ECTL-be történő beemelését;
- regisztráció, valamint az EA/AA és a gyökérszintű CA közötti bizalmi kapcsolat kiépítése, ideértve egy új EA/AA-tanúsítvány kiállítását;
- a C-ITS-állomás gyártó/üzemeltető általi regisztrációja az EA-nál;
- a C-ITS-állomás nyilvántartásba vételi hitelesítő adatok (EC)/engedélyezési jegy (AT) iránti kérelme.

4.1.1. A tanúsítványigénylések benyújtására jogosultak listája

4.1.1.1. Gyökérszintű CA-k

(91) A gyökérszintű CA-k maguk generálják a saját kulcspárjaikat és maguk állítják ki a gyökértanúsítványukat. Adott gyökérszintű CA kijelölt képviselőjén keresztül nyújthat be tanúsítványigénylést (14. lépés).

4.1.1.2. *TLM*

(92) A TLM maga generálja a saját kulcspárjait és maga állítja ki a tanúsítványát. A TLM-tanúsítvány kezdeti létrehozását a TLM egy szervezeti képviselője végzi el, a CPA ellenőrzése mellett.

4.1.1.3. EA és AA

(93) Az EA, illetve AA meghatalmazott képviselője az alacsonyabb szintű CA (EA és/vagy AA) tanúsítványkérelmi igényét a megfelelő gyökérszintű CA meghatalmazott képviselőjéhez is benyújthatja (27./28. lépés).

4.1.1.4. C-ITS állomás

(94) Az előfizetőknek minden egyes C-ITS-állomást regisztrálniuk kell az EA-nál a 3.2.5.3. szakasznak megfelelően.

(95) Az EA-nál regisztrált valamennyi C-ITS-állomás benyújthat EC-kérelmet (31. lépés).

(96) Az C-ITS-állomások anélkül is benyújthatnak AT-kérelmet (32. lépés), hogy az előfizető részéről bármilyen interakciót igényelnének. Adott engedélyezési jegy (AT) kérelmezése előtt a C-ITS-állomásnak rendelkeznie kell már EC-vel.

4.1.2. Nyilvántartásba vételi folyamat és felelősségi körök

(97) Kizárólag azon tagállamok adhatnak engedélyt arra, hogy a legfelső vagy alacsonyabb szintű CA-k tanúsítványt állítsanak ki különleges (kormányzati) célokra (pl. különleges mobil és telepített C-ITS-állomások), amelyekben ezen szervezetek működnek.

4.1.2.1. Gyökérszintű CA-k

(98) Ellenőrzésüket követően (13. és 36. lépés, 8. szakasz), a gyökérszintű CA-k a CPA-nál kérelmezhetik a tanúsítvány(aik)nak az ECTL-be történő beemelését (14. lépés). A nyilvántartásba vételi folyamat egy aláírt manuális kérelmezési formanyomtatványra épül, amelyet a gyökérszintű CA meghatalmazott képviselőjének a CPA-hoz személyesen kell eljuttatnia, és amely legalább a 3.2.2.1, 3.2.3 és 3.2.5.1. szakaszok szerinti információkat tartalmazza.

(99) A gyökérszintű CA kérelmezési formanyomtatványát annak meghatalmazott képviselője alá kell hogy írja.

(100) A kérelmezési formanyomtatvány mellett a gyökérszintű CA meghatalmazott képviselőjének a gyökérszintű CA tanúsítványalkalmazási nyilatkozatának egy példányát (15. lépés) és az auditjelentést is be kell nyújtania a CPA-hoz jóváhagyásra (16. lépés). Pozitív elbírálás esetén a CPA megfelelőségi tanúsítványt készít és azt elküldi a CPOC-nek/TLM-nek, illetve a megfelelő gyökérszintű CA-nak.

(101) Ezt követően a gyökérszintű CAk meghatalmazott képviselője az önaláírt tanúsítvány ujjlenyomatát tartalmazó kérelmezési formanyomtatványt, a

hivatalos személyazonosítót és az engedélyezés igazolását eljuttatja a CPOC-hez/TLM-hez. Az önaláírt tanúsítványt elektronikus úton kell eljuttatni a CPOC-hez/TLM-hez. A CPOC-nek/TLM-nek az összes dokumentumot ellenőriznie kell, az önaláírt tanúsítvánnyal együtt.

(102) Pozitív elbírálás esetén a TLM – a CPA értesítése alapján – a gyökérszintű CA tanúsítványát beemeli az ECTL-be (1. és 2. lépés). A részletes folyamatot a TLM tanúsítványalkalmazási nyilatkozata ismerteti.

(103) Biztosítani kell azon további eljárás lehetőségét, hogy a gyökérszintű CA-k tanúsítványalkalmazási nyilatkozatát és auditjelentését bizonyos országokban egy tetszőleges nemzeti szerv hagyja jóvá.

4.1.2.2. *TLM*

(104) Ellenőrzését követően a TLM kérheti nyilvántartásba vételét a CPA-nál. A nyilvántartásba vételi folyamat egy aláírt manuális kérelmezési formanyomtatványra épül, amelyet a TLM meghatalmazott képviselőjének a CPA-hoz nyomtatott formában kell eljuttatnia (38. lépés), és amely legalább a 3.2.2.2. és 3.2.3. szakaszok szerinti információkat tartalmazza.

(105) A TLM kérelmezési formanyomtatványát az előbbi meghatalmazott képviselőjének alá kell írnia.

(106) A TLM először létrehozza saját önaláírt tanúsítványát, majd azt biztonságosan továbbítja a CPA-hoz. Ezután a TLM (az önaláírt tanúsítvány ujjlenyomatát tartalmazó) kérelmezési formanyomtatványt, a tanúsítványalkalmazási nyilatkozatának egy példányát, a hivatalos személyazonosítót, az engedélyezés igazolását és az auditjelentést eljuttatja a CPA-hoz (40. lépés). A CPA-nak az összes dokumentumot ellenőriznie kell, az önaláírt tanúsítvánnyal együtt. Amennyiben valamennyi dokumentum, az önaláírt tanúsítvány és az ujjlenyomat is mind pozitív elbírálást kap, a CPA-nak meg kell erősítenie a nyilvántartásba vételi folyamatot: ennek keretében jóváhagyását a TLM-hez és CPOC-hoz el kell juttatnia (39. lépés). A CPA-nak el kell tárolnia a TLM által megküldött kérelmezési adatokat. Majd ezután a CPOC-n keresztül kiállításra kerül a TLM-tanúsítvány.

4.1.2.3. EA és AA

(107) A nyilvántartásba vételi folyamat során az EA-nak/AA-nak a megfelelő dokumentumokat (pl. tanúsítványalkalmazási nyilatkozat és auditjelentés) jóváhagyásra be kell nyújtania a megfelelő gyökérszintű CA-hoz (27/28. lépés). A dokumentumok pozitív elbírálása esetén a gyökérszintű CA a jóváhagyást elküldi a megfelelő, alacsonyabb szintű CA-knak (29/30. lépés). Ezt követően az alacsonyabb szintű CA (EA vagy AA) aláírt kérelmét elektronikus úton továbbítja, és (a 3.2.2.1. szakasszal összhangban) kérelmezési formanyomtatványát személyesen benyújtja – az engedélyezés igazolásával és a személyazonosító dokumentummal együtt – a megfelelő gyökérszintű CA-hoz. A gyökérszintű CA ellenőrzi a kérelmet és a beérkezett dokumentumokat – így az ujjlenyomatot [azaz az alacsonyabb szintű CA kérelmének SHA 256 hash értékét] tartalmazó kérelmezési formanyomtatványt, az engedélyezés igazolását és a személyazonosító dokumentumot. Pozitív elbírálás esetén a gyökérszintű CA kiállítja a megfelelő alacsonyabb szintű CA tanúsítványát. A kezdeti kérelem folyamatának részleteit az adott CPS ismerteti.

(108) Az alacsonyabb szintű CA-k kérelmezési formanyomtatványa mellett az alacsonyabb szintű CA-k meghatalmazott képviselőjének a gyökérszintű CA számára a tanúsítványalkalmazási nyilatkozat másolatát is csatolnia kell.

(109) Az ellenőrzésről a 8. szakasznak megfelelően tájékoztatni kell egy akkreditált PKI-ellenőrt.

(110) Amennyiben valamely alacsonyabb szintű CA egy olyan jogalany tulajdonában áll, amely eltér a gyökérszintű CA-t tulajdonló szervezetektől, úgy még azt megelőzően, hogy az alacsonyabb szintű CA tanúsítványkérelmét kiállítanák, az alacsonyabb szintű CA szervezetének szerződést kell kötnie a gyökérszintű CA szolgáltatására.

4.1.2.4. C-ITS-állomás

(111) A végfelhasználói alanyok (C-ITS-állomások) az EA-nál történő kezdeti regisztrációját a felelős előfizetőnek (gyártó/üzemeltető) kell elvégeznie (33. és 35. lépés) azt követően, hogy a 3.2.2.4 és 3.2.5.2. szakasszal összhangban az előfizető szervezetének és egy képviselőjének hitelesítése eredményesen lezárult.

(112) A C-ITS-állomás EC-kulcspárt (lásd a 6.1. szakaszt) és aláírt EC-kérelmet is létrehozhat az [1] alapján. Más protokollok is alkalmazhatók, amennyiben az [1] követelményei teljesülnek.

(113) Hagyományos C-ITS-állomás regisztrációja esetén (a különleges mobil, illetve telepített C-ITS-állomás regisztrációjától eltérően), az EA-nak ellenőriznie kell, hogy a kezdeti kérelem szerinti engedélyek nem kormányzati használatra szólnak-e. A kormányzati használatra szóló engedélyeket az illetékes tagállamok határozzák meg. A regisztrációs eljárás és a gyártó/üzemeltető számára küldött EA-válaszüzenet (33. és 35. lépés) részletes leírását az EA megfelelő tanúsítványalkalmazási nyilatkozatában kell szerepeltetni.

(114) A C-ITS-állomás EA-nál történő nyilvántartásba vételéhez (3.2.5.3. szakasz) – az [1] szabvánnyal összhangban – be kell nyújtani annak kezdeti EC-kérelmét.

(115) Miután egy hitelesített előfizető képviselője révén a kezdeti regisztráció megvalósult, az EA megerősíti, hogy a végfelhasználói alany (azaz a C-ITS-állomás) mely engedélyezési jegyeket (AT) kaphatja meg. Ezenkívül minden végfelhasználóhoz egy olyan bizalomgarantálási szintet is hozzárendelnek, amely – a 6.1.5.2. szakaszban felsoroltak közül valamely védelmi profil alapján – a végfelhasználó tanúsítványához kapcsolódik.

(116) A hagyományos járművek kizárólag egy, egyetlen EA-nál regisztrált C-ITS-állomással rendelkezhetnek. A különleges célú járművek (úgymint rendőrautók és további, egyedi jogokkal bíró, különleges célú járművek) egy további EA-nál is regisztrálhatók, illetve az engedélyezésekhez egy további C-ITS-állomással is rendelkezhetnek – a különleges cél határain belül. A fenti mentességeket élvező járműveket a felelős tagállamoknak kell meghatározniuk. Különleges mobil és telepített C-ITS-állomásokra vonatkozó engedélyeket kizárólag a felelős tagállamok adhatnak ki. Az említett tagállamokban ilyen járművekre tanúsítványt kiállító legfelső, illetve alacsonyabb szintű CA-k tanúsítványalkalmazási nyilatkozatában meg kell határozni, hogy a tanúsítási folyamat hogyan alkalmazandó ezen járművek esetében.

(117) Amennyiben az előfizető egy C-ITS-állomást valamely EA-tól egy másik EA-hoz visz át, úgy a C-ITS-állomás két (hasonló) EA-nál is regisztrálásra kerülhet.

(118) A C-ITS-állomás egy AT-kulcspárt (lásd a 6.1. szakaszt) és egy AT-kérelmet is létrehoz, az [1] szabványnak megfelelően. Más protokollok is alkalmazhatók, amennyiben az [1] végre lett hajtva.

(119) A C-ITS-állomások az engedélyezési hatóság URL-jére engedélyezési kérelmet küldenek (32. és 26. lépés): ennek keretében megadják legalább a 3.2.3.3. szakaszban említett szükséges adatokat. Az AA és EA minden egyes kérelem esetében, a 3.2.6 és a 4.2.2.5. szakaszokkal összhangban validálja az engedélyezést.

4.2. Tanúsítványigénylés feldolgozása

4.2.1. Azonosítási és hitelesítési feladatok ellátása

4.2.1.1. A gyökérszintű CA-k azonosítása és hitelesítése

(120) A CPA meghatalmazott képviselője felel a gyökérszintű CA meghatalmazott képviselőjének hitelesítéséért és a nyilvántartásba vételi folyamat 3. szakasznak megfelelő jóváhagyásáért.

4.2.1.2. A bizalmi lista kezelőjének (TLM) azonosítása és hitelesítése

(121) A CPA meghatalmazott képviselője felel a TLM meghatalmazott képviselőjének hitelesítéséért és a felvételkérelmezési formanyomtatvány jóváhagyásáért a 3. szakasznak megfelelően.

4.2.1.3. A nyilvántartásba vételi hatóság (EA) és az engedélyezési hatóság (AA) azonosítása és hitelesítése

(122) A megfelelő gyökérszintű CA felel az EA/AA meghatalmazott képviselőjének hitelesítéséért és a nyilvántartásba vételt kérelmező formanyomtatványának jóváhagyásáért a 3. szakasznak megfelelően.

(123) A gyökérszintű CA köteles a kérelmezési formanyomtatványok pozitív validálási eredményét az EA/AA felé megerősíteni. Az EA/AA ezt követően tanúsítványkérelmet nyújthat be a gyökérszintű CA-hoz (21/24. lépés), amely a megfelelő EA/AA felé kiállítja a tanúsítványokat (18/19. lépés).

4.2.1.4. A végfelhasználói (EE) előfizető azonosítása és hitelesítése

(124) Még mielőtt valamely C-ITS-állomás egy EC-tanúsítványra kérelmet nyújthatna be, az EE-előfizetőnek biztonságos úton el kell juttatnia az EA-hoz a C-ITS állomás azonosító adatait (33. lépés). Az EA ezután megvizsgálja a kérelmet, és pozitív elbírálás esetén a C-ITS-állomás adatait az adatbázisában rögzíti, és ezt az EE előfizető felé is megerősíti (35. lépés). Ezt a műveletet a gyártó, illetve üzemeltető minden egyes C-ITS-állomás esetében csak egyszer végzi el. Amint a C-ITS-állomást valamely EA regisztrálta, az a szükséges EC-tanúsítványra kérelmet nyújthat be – de egyszerre csak egyet (31. lépés). Az EA hitelesíti és megerősíti, hogy az EC-tanúsítványkérelemben szereplő információk a C-ITS-állomások szempontjából valóban helytállóak.

4.2.1.5. Engedélyezési jegyek

(125) Az engedélyezési kérelmek során (32. lépés), az [1] szabvánnyal összhangban, az AA-nak hitelesítenie kell azt az EA-t, amelytől a C-ITS-állomás az EC-t

kapta. Más protokollok is alkalmazhatók, amennyiben az [1] követelményei teljesülnek. Amennyiben az eAA nem tudja hitelesíteni az EA-t, úgy a kérelem elutasításra kerül (26. lépés). Előírás továbbá, hogy az AA az EA hitelesítéséhez és a válasz ellenőrzéséhez rendelkezzen a szükséges EA-tanúsítvánnyal (25. és 23. lépés, 3.2.5.3. szakasz).

(126) Az engedélyezési jegyet (AT) kérelmező C-ITS-állomás hitelesítéséhez azEA ellenőrzi az állomás nyilvántartásba vételi hitelesítő adatait (EC) (25. és 23. lépés).

4.2.2. A tanúsítványigénylések elfogadása, illetve elutasítása

4.2.2.1. A gyökérszintű CA-k tanúsítványainak elfogadása, illetve elutasítása

(127) A TLM – a CPA jóváhagyása alapján – a gyökérszintű CA tanúsítványait beemeli az ECTL-be, illetve onnan törli (1/2. lépés).

(128) Miután megkapta a CPA jóváhagyását, a TLM-nek ellenőriznie kell a gyökérszintű CA tanúsítványainak aláírását, adatait és kódolását (1. lépés). Pozitív elbírálás és a CPA jóváhagyása esetén a TLM felveszi a megfelelő gyökértanúsítványt az ECTL-be és arról értesíti a CPA-t (5. lépés).

4.2.2.2. A TLM-tanúsítványok jóváhagyása és elutasítása

(129) A CPA felel a TLM-tanúsítványok jóváhagyásáért, illetve elutasításáért.

4.2.2.3. Az EA- és AA-tanúsítványok jóváhagyása vagy elutasítása

(130) A gyökérszintű CA ellenőrzi az alacsonyabb szintű CA-k tanúsítványkérelmeit (21./24. lépés) és azon vonatkozó (az akkreditált PKI-ellenőr által kiállított) jelentéseket, amelyek igazolják, hogy a kérelmek a gyökérszintű CA megfelelő alacsonyabb szintű CA-jától érkeztek (36. lépés, 8. szakasz). Amennyiben a kérelem ellenőrzése pozitív eredménnyel zárul, úgy a megfelelő gyökérszintű CA a kérelmező EA/AA számára tanúsítványt állít ki (18./19. lépés); ellenkező esetben a kérelmet elutasítják, és nem állítanak ki tanúsítványt az EA/AA számára.

4.2.2.4. Az EC jóváhagyása, illetve elutasítása

(131) Az EA a 3.2.3.2. és a 3.2.5.3. szakasz szerint ellenőrzi és validálja az EC-kérelmeket.

(132) Amennyiben az [1] szerinti tanúsítványkérelem helyes és érvényes, úgy az EA elkészíti a kért tanúsítványt.

(133) Amennyiben a tanúsítványkérelem nem érvényes, úgy az EA azt elutasítja, és az [1] értelmében a megküldött válaszában meghatározza az elutasítás okát. Ha adott C-ITS-állomás továbbra is igényt tart egy EC-re, úgy új tanúsítványkérelmet kell benyújtania. Más protokollok is alkalmazhatók, amennyiben az [1] követelményei teljesülnek.

4.2.2.5. Az AT jóváhagyása, illetve elutasítása

(134) A tanúsítványkérelmet az EA ellenőrzi. A kérelem validálása ügyében az AA az EA-val kommunikációt folytat (25. lépés). Az EA hitelesíti a kérelmező C-ITS-állomást és ellenőrzi, hogy az a hitelesítési házirend alapján jogosult-e a kért engedélyezési jegyre (pl. ellenőrzi a visszavonási állapotot, validálja a tanúsítvány időbeli és területi érvényességét, akárcsak az engedélyeket és a biztosítási szintet stb.). Az EA köteles a validálásról válaszüzenetet küldeni

(23. lépés), és ha annak tartalma pozitív, úgy az AA-nak a kért tanúsítványt ki kell állítania és azt továbbítania kell a C-ITS-állomáshoz. Ha az AT-kérelem nem helytálló vagy a nyilvántartásba vételi hatóság (EA) validálási válaszüzenete negatív, az AA elutasítja a kérelmet. Ha a C-ITS továbbra is igényt tart egy AT-re, úgy új engedélyezési kérelmet kell benyújtania.

4.2.3. A tanúsítványigénylés feldolgozási ideje

4.2.3.1. A gyökérszintű CA-k tanúsítványigénylése

(135) A tanúsítványigénylés azonosítási és hitelesítési folyamata a munkanapokra korlátozódik, és maximális határidejét a gyökérszintű CA tanúsítványalkalmazási nyilatkozat (CPS) határozza meg.

4.2.3.2. *TLM-tanúsítvány igénylése*

(136) A TLM-tanúsítványigénylés feldolgozására a TLM tanúsítványalkalmazási nyilatkozatában meghatározott maximális határidő vonatkozik.

4.2.3.3. *EA- és AA-tanúsítvány igénylése*

(137) A tanúsítványigénylés azonosítási és hitelesítési folyamata a munkanapokra korlátozódik a tagállamok/magánszervezetek gyökérszintű CA-ja és alacsonyabb szintű CA-ja között létrejött megállapodás és szerződés értelmében. Az alacsonyabb szintű CA-k tanúsítványigényléseinek feldolgozási idejére az alacsonyabb szintű CA-k tanúsítványalkalmazási nyilatkozatában meghatározott maximális határidő vonatkozik.

4.2.3.4. *EC igénylése*

(138) Az EC-igénylések feldolgozására az EA tanúsítványalkalmazási nyilatkozatában meghatározott maximális határidő az irányadó.

4.2.3.5. *AT igénylése*

(139) Az AT-igénylések feldolgozására az AA tanúsítványalkalmazási nyilatkozatában meghatározott maximális határidő az irányadó.

4.3. Tanúsítványkibocsátás

4.3.1. CA-tevékenységek a tanúsítványok kiállítása során

4.3.1.1. Gyökérszintű CA tanúsítványának kiállítása

(140) A gyökérszintű CA-k saját önaláírt gyökérszintű CA-tanúsítványaikat, hivatkozási tanúsítványaikat, alacsonyabb szintű CA-tanúsítványaikat és a tanúsítványalkalmazási nyilatkozatokat maguk állítják ki.

(141) A CPA jóváhagyása után (4. lépés), a gyökérszintű CA a tanúsítványát a CPOC-n keresztül elküldi a TLM-hez, hogy azt beemeljék az ECTL-e (11. és 8. lépés) (lásd a 4.1.2.1. szakaszt). A TLM ellenőrzi, hogy a CPA jóváhagyta-e a tanúsítványt (1. lépés).

4.3.1.2. *TLM-tanúsítvány kiállítása*

(142) A TLM saját önaláírt TLM- és hivatkozási tanúsítványát maga állítja ki, és azt elküldi a CPOC-nek (6. lépés).

4.3.1.3. EA- és AA-tanúsítvány kiállítása

(143) Az alacsonyabb szintű CA-k aláírt tanúsítványkérelmet hoznak létre és azt továbbítják a megfelelő gyökérszintű CA-hoz (21. és 24. lépés). A

gyökérszintű CA ellenőrzi a kérelmet és az [5] szerint tanúsítványt állít ki a kérelmező alacsonyabb szintű CA számára; utóbbit a rendes működési gyakorlatokról szóló tanúsítványalkalmazási nyilatkozatban meghatározottak szerint minél hamarabb, de legkésőbb a kérelem beérkeztétől számított öt munkanapon belül végre kell hajtani.

(144) A gyökérszintű CA köteles frissíteni az alacsonyabb szintű CA-k tanúsítványait tartalmazó adattárat.

4.3.1.4. EC kiállítása

(145) A C-ITS-állomás az [1] szerint EC-kérelmet nyújt be az EA-hoz. Az EA hitelesíti és ellenőrzi, hogy a tanúsítványkérelemben szereplő adatok a C-ITS-állomások szempontjából helytállóak-e. Más protokollok is alkalmazhatók, amennyiben az [1] végre lett hajtva.

(146) Pozitív elbírálás esetén az EA a C-ITS-állomás regisztrációja alapján (lásd: 4.2.1.4. szakasz) tanúsítványt állít ki, és azt az [1] szerint EC-válaszüzenet formájában elküldi a C-ITS-állomásnak. Más protokollok is alkalmazhatók, amennyiben az [1] végre lett hajtva.

(147) Regisztráció hiányában az EA egy hibakódot hoz létre és azt az [1] szerinti EC-válaszüzenet formájában elküldi a C-ITS-állomásnak. Más protokollok is alkalmazhatók, amennyiben az [1] követelményei teljesülnek.

(148) Az EC-kérelmeket és EC-válaszokat titkosítani kell a bizalmas adatkezelés érdekében, és alá is kell írni a hitelesség és sértetlenség biztosítása céljából.

4.3.1.5. AT kiállítása

(149) A C-ITS-állomás az [1] szerinti AT-kérelemre irányuló üzenetet küld az AA-nak. Az AA az [1] szerinti AT-validálási kérelmet küld az EA-hoz. Az EA az AT validálásáról válaszüzenetet küld az AA-nak. Pozitív válasz esetén az AA létrehoz egy engedélyezési jegyet (AT) és azt az [1] szerinti AT-válaszüzenet formájában elküldi a C-ITS-állomásnak. Negatív válasz esetén az AA egy hibakódot hoz létre, és azt az [1] szerinti AT-válaszüzenet formájában elküldi a C-ITS-állomásnak. Más protokollok is alkalmazhatók, amennyiben az [1] követelményei teljesülnek.

(150) Az AT-kérelmeket és AT-válaszokat (kizárólag a mobil C-ITS-állomásoknál szükségeseket) titkosítani kell a bizalmas adatkezelés érdekében, és alá is kell írni a hitelesség és sértetlenség biztosítása céljából.

4.3.2. Az előfizetőnek a hitelesítésszolgáltató általi értesítése a tanúsítványok kiállításáról.

Nem alkalmazható.

4.4. Tanúsítvány elfogadása

4.4.1. A tanúsítványelfogadás folyamata

4.4.1.1. Gyökérszintű CA

Nem alkalmazható.

4.4.1.2. *TLM*

Nem alkalmazható.

4.4.1.3. EA és AA

(151) Az EA/AA ellenőrzi a tanúsítvány típusát, illetve a megkapott tanúsítványban szereplő aláírást és adatokat. Az EA/AA minden olyan EA/AA-tanúsítványt elutasít, amelynek ellenőrzése nem megfelelő, és új kérelmet állít ki.

4.4.1.4. C-ITS-állomás

(152) A C-ITS-állomás az eredeti kérelemmel összevetve ellenőrzi az EA/AA-tól kapott EC/AT-választ, ideértve az aláírást és a tanúsítási láncot. Minden olyan EC/AT-választ elutasít, amelynek ellenőrzése nem megfelelő. Ilyen esetekben új EC/AT-kérelmet kell küldenie.

4.4.2. A tanúsítvány közzététele

(153) A TLM-tanúsítványokat és azok hivatkozási tanúsítványait a CPOC-n keresztül valamennyi résztvevő számára elérhetővé kell tenni.

(154) A gyökérszintű CA tanúsítványait a CPOC az ECTL-en keresztül teszi közzé, amelyet a TLM az aláírásával lát el.

(155) Az alacsonyabb szintű CA-k (EA-k és AA-k) tanúsítványait a gyökérszintű CA teszi közzé.

(156) Az EC-k és AT-k nem kerülnek közzétételre.

4.4.3. Értesítés tanúsítványkiállításról

Nincs kibocsátási értesítés.

4.5. Kulcspár- és tanúsítványhasználat

4.5.1. ***Titkos kulcs és tanúsítvány használata***

4.5.1.1. Titkoskulcs- és tanúsítványhasználat a TLM esetében

(157) A TLM a titkos kulcsaival írja alá saját (TLM- és hivatkozási) tanúsítványait és az ECTL-t.

(158) A TLM-tanúsítványt a PKI-résztvevők az ECTL ellenőrzésére és a TLM hitelesítésére használhatják fel.

4.5.1.2. Titkoskulcs- és tanúsítványhasználat a gyökérszintű CA-k esetében

(159) A gyökérszintű CA-k a titkos kulcsaikkal írják alá saját tanúsítványaikat, a CRL-t, a hivatkozási tanúsítványokat és az EA/AA-tanúsítványokat.

(160) A gyökérszintű CA-k tanúsítványait a PKI-résztvevők arra használják, hogy azokkal ellenőrizzék a kapcsolódó AA- és EA-tanúsítványokat, hivatkozási tanúsítványokat és a CRL-eket.

4.5.1.3. Titkoskulcs- és tanúsítványhasználat az EA-k és AA-k esetében

(161) Az EA a titkos kulcsaival írja alá az EC-ket és szintén saját titkos kulcsait használja a nyilvántartásba vételi kérelem visszafejtéséhez.

(162) Az EA-tanúsítványokat a kapcsolódó EC-k aláírásának ellenőrzésére, valamint az [1] szabványban meghatározottak szerint az EC- és AT-kérelmek végfelhasználói titkosításához használják fel.

(163) Az AA saját titkos kulcsaival írja alá az AT-ket és használja fel azokat az AT-kérelmek visszafejtéséhez.

(164) Az AA-tanúsítványokat a végfelhasználók a kapcsolódó AT-k ellenőrzésére, és az [1] szabványban meghatározottak szerint az AT-kérelem titkosításához használják fel.

4.5.1.4. Titkoskulcs- és tanúsítványhasználat a végfelhasználók esetében

(165) A végfelhasználónak (EE) az [1] szabványban meghatározottak szerint az adott érvényes EC-nek megfelelő titkos kulcsot kell használniuk új nyilvántartásba vételi kérelem aláírásához. A kérelem belső aláírását az új titkos kulccsal kell elkészíteni annak igazolására, hogy az új EC nyilvános kulcsnak megfelelő titkos kulcs birtokában vannak.

(166) A végfelhasználónak az [1] szabványban meghatározottak szerint az adott érvényes EC-nek megfelelő titkos kulcsot kell használnia engedélyezési kérelem aláírásához. A kérelem belső aláírását az új AT-nek megfelelő titkos kulccsal kell elkészíteni annak igazolására, hogy az új AT nyilvános kulcsnak megfelelő titkos kulcs birtokában vannak.

(167) A végfelhasználónak – az [5]-ben meghatározottak szerint – a megfelelő AT-nek megfelelő titkos kulccsal kell aláírnia a C-ITS-üzeneteket.

4.5.2. ***Érintett fél nyilvánoskulcs- és tanúsítványhasználata***

(168) Az érintett felek a megbízható tanúsítási utat és a kapcsolódó nyilvános kulcsokat a tanúsítványban meghatározott célokra és az EC-k, illetve AT-k megbízható közös identitásának hitelesítésére használják.

(169) Nem használhatók a gyökérszintű CA-, EA- és AA-tanúsítványok, illetve az EC-k és AT-k anélkül, hogy azokat valamely érintett fél előzetesen ellenőrizné.

4.6. Tanúsítvány megújítása

Nem megengedett.

4.7. Tanúsítvány kulcsának megújítása

4.7.1. Tanúsítvány-kulcsmegújítás feltételei

(170) Tanúsítvány kulcsának megújítására akkor kerül sor, ha a tanúsítvány az élettartamának végéhez ér, vagy ha a titkos kulcs operatív használata a végéhez ér, de a CA-val való bizalmi kapcsolat továbbra is fennáll. Minden esetben létre kell hozni egy új kulcspárt és ki kell adni annak megfelelő tanúsítványát.

4.7.2. Ki kérelmezhet kulcsmegújítást

4.7.2.1. Gyökérszintű CA

(171) A gyökérszintű CA nem kérelmez kulcsmegújítást. A kulcsmegújítás a gyökérszintű CA esetében egy belső eljárás, mivel a gyökérszintű CA tanúsítványa önaláírt. A gyökérszintű CA vagy a hivatkozási tanúsítványok vagy új kiállítás esetében fordul a kulcsmegújítás eszközéhez (lásd a 4.3.1.1. szakaszt).

4.7.2.2. *TLM*

(172) A bizalmi lista kezelője nem kérelmez kulcsmegújítást. A kulcsmegújítás a TLM esetében egy belső eljárás, mivel a TLM tanúsítványa önaláírt.

4.7.2.3. EA és AA

(173) Az alacsonyabb szintű CA-k tanúsítványkérelmeit kellő időben kell benyújtani annak biztosításához, hogy az alacsonyabb szintű CA új tanúsítványát és operatív kulcspárját még azt megelőzően megkapja, hogy a jelenlegi titkos (alacsonyabb szintű CA) kulcs lejárna. A benyújtási határidőnél ugyancsak figyelembe kell venni a jóváhagyáshoz szükséges időt.

4.7.2.4. C-ITS-állomás

Nem alkalmazható.

4.7.3. Kulcsmegújítás folyamata

4.7.3.1. TLM-tanúsítvány

(174) A gyökérszintű CA a kulcsmegújításról a 6.1. és 7.2. szakasz követelményei alapján dönt. A részletes leírást a tanúsítványalkalmazási nyilatkozatnak kell tartalmaznia.

(175) A TLM köteles kellő időben elvégezni a kulcsmegújítást annak lehetővé tétele érdekében, hogy az új TLM-tanúsítványt és hivatkozási tanúsítványt minden résztvevő megkapja még az előtt, hogy a jelenlegi TLM-tanúsítvány érvényességét vesztené.

(176) A TLM-nek a kulcsmegújításhoz és az új önaláírt tanúsítvány bizalmi kapcsolatának garantálásához hivatkozási tanúsítványokat kell használnia. Az újonnan létrehozott TLM- és hivatkozási tanúsítványt a CPOC-hez továbbítják.

4.7.3.2. Gyökérszintű CA tanúsítványa

(177) A gyökérszintű CA a kulcsmegújításról a 6.1.5. és 7.2. szakasz követelményei alapján dönt. A részletes leírást a tanúsítványalkalmazási nyilatkozatnak kell tartalmaznia.

(178) A gyökérszintű CA köteles kellő időben (még a gyökérszintű CA-tanúsítvány lejárta előtt) elvégezni a kulcsmegújítást annak lehetővé tétele érdekében, hogy az új tanúsítványt még az előtt beemeljék az ECTL-be, hogy a gyökértszintű CA-tanúsítvány érvénybe lépne (lásd az 5.6.2. szakaszt). A kulcsmegújítást vagy hivatkozási tanúsítványok segítségével vagy úgy kell végrehajtani, mintha kezdeti kérelemről lenne szó.

4.7.3.3. EA- és AA-tanúsítvány

(179) Az EA, illetve AA az alábbiak szerint kérelmezhet új tanúsítványt:

Lépés	**Jelzés**	**Kulcsmegújítási kérelem**
1	**Kulcspár létrehozása**	Az alacsonyabb szintű CA-k (EA-k és AA-k) a 6.1. szakasznak megfelelően új kulcspárokat hoznak létre.
2	**Tanúsítványkérelem és belső aláírás létrehozása**	Az alacsonyabb szintű CA az újonnan létrehozott nyilvános kulcsból – a 3. szakasz elnevezési mintájának (subject_info), az aláíró algoritmusnak, a szolgáltatásspecifikus jogosultságoknak (SSP-knek) és az opcionális kiegészítő paramétereknek a figyelembe vétele mellett – tanúsítványkérelmet generál, majd létrehozza a megfelelő új titkos kulccsal a belső aláírást. Amennyiben titkosító kulcsra van szükség, úgy az alacsonyabb szintű CA-nak igazolnia kell, hogy a birtokában van a megfelelő titkos visszafejtő kulcs.

3	**Külső aláírás generálása**	A teljes kérelmet az aktuálisan érvényes titkos kulccsal kell aláírni az aláírt kérelem hitelességének biztosítása érdekében.
4	**Kérelem küldése a gyökérszintű CA-hoz**	Az aláírt kérelmet a megfelelő gyökérszintű CA-hoz kell benyújtani.
5	**Kérelem ellenőrzése**	A megfelelő gyökérszintű CA ellenőrzi a kérelem sértetlenségét és hitelességét. Először a külső aláírást ellenőrzi le. Pozitív eredmény esetén a belső aláírt is megvizsgálja. Ha igazoló bizonyíték van a titkos visszafejtő kulcs birtoklására, úgy azt is ellenőrzi.
6	**Kérelem elfogadása vagy elutasítása**	Amennyiben az ellenőrzések kivétel nélkül pozitív eredménnyel zárulnak, a gyökérszintű CA elfogadja a kérelmet; ellenkező esetben pedig elutasítja azt.
7	**Tanúsítvány generálása és kiállítása**	A gyökérszintű CA új tanúsítványt generál és azt továbbítja a kérelmező alacsonyabb szintű tanúsítványkiadóhoz.
8	**Válasz küldése**	Az alacsonyabb szintű CA a gyökérszintű CA-nak állapotüzenetet küld (arról, hogy megérkezett-e a tanúsítvány).

3. táblázat: EA- és AA-hatóságok kulcsmegújítási eljárása

(180) Az alacsonyabb szintű CA-k automatikus kulcsmegújítása során a gyökérszintű CA gondoskodik arról, hogy a kérelmező valóban birtokában legyen a titkos kulcsának. A titkos visszafejtő kulcsok birtoklásának igazolására a megfelelő protokollokat kell alkalmazni, például az RFC 4210 és 4211 szabványban meghatározottak szerint. Titkos aláírókulcsok esetében a belső aláírást kell használni.

4.7.3.4. C-ITS-állomás tanúsítványai

Az AT esetében nem alkalmazandó.

4.8. Tanúsítvány módosítása

Nem megengedett.

4.9. Tanúsítvány visszavonása vagy felfüggesztése

Lásd a 7. szakaszt.

4.10. Tanúsítvány állapotával kapcsolatos szolgáltatások

4.10.1. Operatív jellemzők

Nem alkalmazható

4.10.2. Szolgáltatás elérhetősége

Nem alkalmazható

4.10.3. További lehetséges jellemzők

Nem alkalmazható

4.11. Előfizetés vége

Nem alkalmazható

4.12. Kulcs letétbe helyezése és visszaállítása

4.12.1. Előfizető

4.12.1.1. Letétbe helyezhető kulcspárok

Nem alkalmazható.

4.12.1.2. Visszaállítási kérelem benyújtására jogosultak

Nem alkalmazható.

4.12.1.3. Visszaállítási eljárás és felelősségi körök

Nem alkalmazható.

4.12.1.4. Azonosítás és hitelesítés

Nem alkalmazható.

4.12.1.5. Visszaállítási kérelmekjóváhagyása vagy elutasítása

Nem alkalmazható.

4.12.1.6. KEA és KRA-intézkedések a kulcspár visszaállítása során

Nem alkalmazható.

4.12.1.7. KEA és KRA elérhetősége

Nem alkalmazható.

4.12.2. Munkamenetkulcs-beágyazás, valamint helyreállítási politika és gyakorlatok

Nem alkalmazható.

5. LÉTESÍTMÉNY, IRÁNYÍTÁS ÉS OPERATÍV ELLENŐRZÉSEK

(181) A PKI a gyökérszintű CA-ból, az EA/AA-ból, a CPOC-ből és a TLM-ből áll, ideértve azok IKT-komponenseit (pl. hálózatok és szerverek).

(182) Ez a szakasz a PKI valamely eleméért felelős szervezetet maga az elem azonosítja. Más szóval, „az ellenőrzés végrehajtásáért felelős CA” megegyezik „a ... végrehajtásáért felelős CA-t irányító szervezettel vagy személlyel”.

(183) A „C-ITS megbízhatósági modell elemei” közé tartozik a gyökérszintű CA, a TLM, az EA/AA, a CPOC és a biztonságos hálózat.

5.1. Fizikai ellenőrzések

(184) A C-ITS megbízhatósági modell valamennyi műveletét olyan, fizikailag védett környezetben kell végrehajtani, amely megelőzi és megakadályozza a bizalmas információk és rendszerek jogosulatlan használatát, közzétételét és az azokhoz való jogosulatlan hozzáférést, illetve észleli az ilyen esetek előfordulását. A C-ITS megbízhatósági modell elemeinek az ISO 27001 és ISO 27005 szabványoknak megfelelően fizikai biztonsági ellenőrzéseket kell végezniük.

(185) A C-ITS megbízhatósági modell elemeit kezelő szervezeteknek saját tanúsítványalkalmazási nyilatkozatukban (CPS) ismertetniük kell a fizikai, eljárásbeli és személyzeti biztonsági ellenőrzéseket. A CPS-ben különösen a következőkkel kapcsolatos információknak kell szerepelniük: az épületek helymeghatározása és konstrukciója, valamint a C-ITS megbízhatósági modell szervezeteinek létesítményében használt helyiségekbe való ellenőrzött bejutást garantáló fizikai biztonsági ellenőrzések.

5.1.1. Helymeghatározás és konstrukció

5.1.1.1. Gyökérszintű CA, CPOC, TLM

(186) A gyökérszintű CA, a CPOC és a TLM berendezéseinek és adatainak (HMS, aktiválási adatok, kulcspár biztonsági másolata, számítógép, napló,

kulcsceremónia forgatókönyve, tanúsítványkérelem stb.) otthont adó létesítmény helyszínének és konstrukciójának meg kell egyeznie a nagy jelentőségű és bizalmas információknak otthont adó létesítményekével. A gyökérszintű CA-t a többi PKI-komponens fizikai területétől elhatárolt, erre a célra kijelölt fizikai környezetben kell működtetni.

(187) A gyökérszintű CA, a CPOC és a TLM köteles szabályzatokkal és eljárásokkal folyamatos magas szintű biztonságot biztosítani abban a fizikai környezetben, ahol a gyökérszintű CA berendezése telepítve van, valamint garantálni, hogy:

- a környezet a megbízhatósági modellen kívüli hálózatoktól el legyen határolva;
- a környezet több, (legalább kettő) fokozatosan egyre biztonságosabb fizikai biztonsági övezetre legyen felosztva;
- a bizalmas adatokat (HSM, kulcspár biztonsági másolata, aktiválási adatok stb.) egy erre a célra kijelölt széfben tárolják egy erre kijelölt fizikai helyen, többszörös belépés-ellenőrzés biztosítása mellett.

(188) Az alkalmazott biztonsági technikákat úgy kell kialakítani, hogy azok a nagy számú és a különböző támadási formák kombinációinak is ellenálljanak. Az alkalmazott mechanizmusoknak legalább az alábbiakra ki kell terjedniük:

- biztonsági övezet riasztói, zárt láncú televízió, megerősített falak és mozgásérzékelők;
- minden személy vagy jelvény esetében kéttényezős hitelesítés (pl. okoskártya és PIN) ahhoz, hogy a gyökérszintű CA létesítményeibe és a biztonságos, fizikailag védett területre beléphessenek vagy azt elhagyhassák.

(189) A gyökérszintű CA, a CPOC és a TLM meghatalmazott munkatársak segítségével gondoskodik a berendezésnek otthont adó létesítmény állandó és folyamatos ellenőrzéséről a nap minden órájában. Az operatív környezetet (pl. fizikai létesítmény) tilos felügyelet nélkül hagyni. Az operatív környezet munkatársai nem léphetnek be a gyökérszintű CA-k, illetve az alacsonyabb szintű CA-k biztonsági területére, kivéve ha erre engedélyt kapnak.

5.1.1.2. *EA/AA*

(190) Az 5.1.1.1. szakasz rendelkezései alkalmazandók.

5.1.2. Fizikai hozzáférés

5.1.2.1. Gyökérszintű CA, CPOC, TLM

(191) A berendezést és az adatokat (HSM, aktiválási adatok, a kulcspár biztonsági másolata, számítógép, napló, kulcsceremónia forgatókönyve, tanúsítványkérelem stb.) mindig védeni kell az illetéktelen hozzáférésektől. A berendezésekre irányuló fizikai biztonsági mechanizmusoknak legalább az alábbiakról gondoskodniuk kell:

- illetéktelen behatolás állandó figyelése – manuálisan vagy elektronikusan;
- annak biztosítása, hogy senki se tudjon jogosulatlanul hozzáférni a hardverhez és az aktiválási adatokhoz;
- annak biztosítása, hogy a bizalmas, nem titkosított („plain-text”) információkat tartalmazó cserélhető adathordozókat és iratokat egy biztonságos tárolóban tárolják;

- annak biztosítása, hogy ne maradjon a gyökér-CA-, a CPOC-, illetve a TLM- létesítmények meghatalmazott munkatársának felügyelete nélkül olyan személy, aki nem rendelkezik állandó belépési engedéllyel;
- annak biztosítása, hogy belépési naplót is vezessenek és azt rendszeres időközönként ellenőrizzék;
- legalább két szintű, fokozatosan egyre szigorodó biztonság (pl. biztonsági övezet, épület és műveleti helyiség szinten);
- két, megbízható szereppel rendelkező fizikai hozzáférés-ellenőrző igénylése a kriptográfiai HSM-hez és az aktiválási adatokhoz.

(192) A berendezésnek otthont adó létesítmény biztonsági ellenőrzése akkor szükséges, ha azt felügyelet nélkül hagyják. Az ellenőrzés során legalább az alábbiakról meg kell győződni:

- a berendezés az aktuális működési módnak megfelelő állapotban van;
- az offline összetevők szempontjából valamennyi berendezés le van állítva;
- a biztonsági tárolók (biztonsági tasak, széf stb.) megfelelően biztosítottak;
- a fizikai biztonsági rendszerek (pl. ajtózárak, szellőzőnyílások, elektromos hálózat) megfelelően működnek;
- a területet az illetéktelen behatolókkal szemben védik.

(193) A cserélhető kriptográfiai modulokat az eltárolás előtt deaktiválni kell. Használaton kívül az ilyen modulokat és az elérésükhöz és engedélyezésükhöz használt aktiválási adatokat egy széfben kell elhelyezni. Az aktiválási adatokat vagy memorizálni kell, vagy rögzítésükre és tárolásukra olyan módszert kell találni, amely illeszkedik a kriptográfiai modul számára nyújtott biztonsági szinthez. Az adatok tárolásához nem használható a kriptográfiai modul: így elejét veszik annak, hogy csak egyetlen személy férhessen hozzá a titkos kulcshoz.

(194) Egy megbízható szereppel rendelkező személyt vagy csoportot kifejezetten felelőssé kell tenni az ilyen ellenőrzések elvégzéséért. Ha emberek csoportja a felelős, úgy naplót kell vezetni, amelyben azonosítják az egyes ellenőrzéseket végző személyeket. Amennyiben a létesítményben nincsen állandóan személyzet, úgy a legutolsóként távozónak egy kijelentkező lapot is el kell látnia a kézjegyével, amelyen feltünteti a távozás dátumát és idejét, és megerősíti, hogy az összes szükséges fizikai védelmi mechanizmus működik és aktiválva van.

5.1.2.2. *EA/AA*

(195) Az 5.1.2.1. szakasz rendelkezései alkalmazandók.

5.1.3. Áramellátás és légkondicionálás

(196) A C-ITS megbízhatósági modell elemeinek (gyökérszintű CA, CPOC, TLM, EA és AA) biztonságos létesítményei számára biztosítani kell a szinte hibátlan működéshez elengedhetetlen megbízható áramellátást. Elsődleges és tartalék berendezésekre a külső áramellátás megszakadása esetén van szükség, míg

áramkimaradás esetén a C-ITS megbízhatósági modell berendezésének fokozatos leállítása szükségszerű. A C-ITS megbízhatósági modell létesítményeit hűtő-/fűtő-/légkondicionáló rendszerrel is fel kell szerelni ahhoz, hogy a C-ITS megbízhatósági modelljéhez tartozó berendezés hőmérsékletét és relatív páratartalmát a működési tartományon belül tartsák. A C-ITS megbízhatósági modell elemének tanúsítványalkalmazási nyilatkozata (CPS) részletesen ismerteti a fenti követelmények végrehajtására kidolgozott tervet és folyamatokat.

5.1.4. Víznek való kitettség

(197) A C-ITS megbízhatósági modell elemeinek (gyökérszintű CA, CPOC, TLM, EA és AA) biztonságos létesítményei számára olyan védelmet kell nyújtani, amivel minimálisra csökkentik a víz okozta károkat. Éppen ezért kerülni kell a vízvezetékeket és épületszennyvíz-főcsöveket. A C-ITS megbízhatósági modell elemének tanúsítványalkalmazási nyilatkozata (CPS) részletesen ismerteti a fenti követelmények végrehajtására kidolgozott tervet és folyamatokat.

5.1.5. Tűzmegelőzés és tűzvédelem

(198) A tűz-, illetve füstkár megelőzése érdekében a C-ITS megbízhatósági modell elemeihez (gyökérszintű CA, CPOC, TLM, EA és AA) tartozó biztonságos létesítményeket az előbbieket szem előtt tartva kell kiépíteni és felszerelni, és a tűzveszély kezelésére eljárásokat kell kidolgozni. Az adathordozókat megfelelő tárolókban kell védeni a tűzkár ellen.

(199) A C-ITS megbízhatósági modell elemeinek a kritikus rendszeradatokról, illetve az egyéb bizalmas információkról biztonsági másolatokat tartalmazó fizikai hordozókat védeniük kell a környezeti veszélyektől, valamint a jogosulatlan használattól, az illetéktelen hozzáféréstől és attól, hogy az ott tárolt adatok kiszivárogjanak. A C-ITS megbízhatósági modell elemének tanúsítványalkalmazási nyilatkozata (CPS) részletesen ismerteti a fenti követelmények végrehajtására kidolgozott tervet és folyamatokat.

5.1.6. Adathordozók kezelése

(200) A C-ITS megbízhatósági modell elemeinél (gyökérszintű CA, CPOC, TLM, EA és AA) használt adathordozókat biztonságos kezelésükkel védik a kárral, lopással és jogosulatlan hozzáféréssel szemben. Az adathordozók kezelésére irányuló eljárások célja az, hogy azon időszakban, amelyre vonatkozóan bejegyzéseiket meg kell őrizni, elejét vegyék az adathordozó erkölcsi kopásának és elhasználódásának.

(201) A bizalmas adatokat védeni kell az ellen, hogy azokhoz újrahasznált tárolási objektumok (pl. törölt fájlok) útján hozzáférhessenek, hiszen utóbbi révén a bizalmas adatok jogosulatlan felhasználók számára is hozzáférhetővé válhatnak.

(202) Nyilvántartást kell vezetni az információs eszközökről, és követelményeket kell megállapítani a kockázatelemzésben érintett eszközök védelmére. A C-ITS megbízhatósági modell elemének tanúsítványalkalmazási nyilatkozata (CPS) részletesen ismerteti a fenti követelmények végrehajtására kidolgozott tervet és folyamatokat.

5.1.7. Hulladékártalmatlanítás

(203) A C-ITS megbízhatósági modell elemeinek (gyökérszintű CA, CPOC, TLM, EA és AA) a hulladék (papír, adathordozók, illetve egyéb más hulladék) biztonságos és végleges eltávolítására különböző eljárásokat kell alkalmazniuk, amelyekkel megakadályozzák, hogy a bizalmas/magán jellegű információt tartalmazó hulladékhoz illetéktelenek hozzáférjenek, azt jogosulatlanul használják vagy közzétegyék. A bizalmas adatok tárolására használt adathordozókat (mint például kulcsok, aktiválási adatok, illetve fájlok) még eltávolításuk előtt meg kell semmisíteni. A C-ITS megbízhatósági modell elemének tanúsítványalkalmazási nyilatkozata (CPS) részletesen ismerteti a fenti követelmények végrehajtására kidolgozott tervet és folyamatokat.

5.1.8. Külső helyszíni biztonsági mentés

5.1.8.1. Gyökérszintű CA, CPOC és TLM

(204) A gyökérszintű CA, CPOC és TLM komponenseinek – a rendszermeghibásodás utáni helyreállításhoz elegendő – teljes biztonsági mentését offline kell elvégezni minden egyes új kulcspár létrehozása után, illetve azt követően, hogy a gyökérszintű CA-t, CPOC-t és TLM-et üzembe helyezték. A fontos üzleti információkról (kulcspár és CRL) és a szoftverekről rendszeresen készül biztonsági másolat. A biztonsági mentésekhez a megfelelő felszerelés is biztosított, amellyel garantálják vészhelyzet vagy adathordozó-hiba esetén a fontos üzleti információk és szoftverek helyreállíthatóságát. Az önálló rendszerek biztonsági műveleteit rendszeresen tesztelik annak biztosítása érdekében, hogy azok megfeleljenek az üzletfolytonossági terv követelményeinek. Legalább egy teljes biztonsági másolatot külső helyszínen kell tárolni (vészhelyreállítás). A biztonsági másolatot a működő PKI-rendszerével megegyező fizikai és eljárásbeli ellenőrzéssel biztosított helyszínen tárolják.

(205) A biztonsági mentési adatokra ugyanazon hozzáférési követelmények vonatkoznak, mint a működési adatokra. A biztonsági mentési adatokat titkosítani kell, és külső helyszínen kell tárolni. Teljes adatvesztés esetén a gyökérszintű CA, CPOC és TLM újbóli üzembe helyezéséhez szükséges információkat hiánytalanul vissza kell állítani a biztonsági mentési adatokból.

(206) A gyökérszintű CA, CPOC és TLM titkoskulcs-anyagának biztonsági mentéséhez nem standard biztonsági mentési mechanizmusokat kell használni, hanem a kriptográfiai modul biztonsági mentési funkcióját.

5.1.8.2. *EA/AA*

(207) Erre a szakaszra az 5.1.8.1. szakaszban meghatározott eljárások alkalmazandók.

5.2. Eljárásbeli ellenőrzések

Ez a szakasz a személyzet szerepeire, feladatköreire és azonosítására vonatkozó követelményeket határozza meg.

5.2.1. Megbízható szerepek

(208) Azon munkatársakat, alvállalkozókat és tanácsadókat, akik megbízható szerepet kaptak, „megbízható személyeknek” kell tekinteni. Azon személyeknek, akik megbízható pozíció elnyerésével kívánnak megbízható

személyekké válni, meg kell felelniük e tanúsítási házirend szűrési követelményeinek.

(209) A megbízható személyek hozzáférnek olyan hitelesítési és titkosítási műveletekhez, illetve az ellenőrzésük alatt tartanak olyan hitelesítési és titkosítási műveleteket, amelyek nagy mértékben befolyásolhatják a következőket:

- a tanúsítványigénylésekben szereplő információk validálása;
- a tanúsítványigénylések, visszavonási kérelmek és megújítási kérelmek elfogadása, elutasítása, illetve más feldolgozási aspektusa;
- a tanúsítványok kiállítása vagy visszavonása, ideértve az adattár korlátozott részeihez hozzáférő személyzetet, illetve az előfizetői adatok és kérelmek kezelését.

(210) A megbízható szerepek közé tartoznak – a teljesség igénye nélkül – a következők:

- ügyfélszolgálat;
- rendszeradminisztráció;
- célzott mérnöki munka;
- az infrastrukturális megbízhatóság gondozásával megbízott vezetők.

(211) A CA-nak a tanúsítványalkalmazási nyilatkozatában egyértelmű és világos leírást kell adnia minden megbízható szerepről.

5.2.2. Az egyes feladatokhoz szükséges személyek száma

(212) A C-ITS megbízhatósági modell elemei szigorú ellenőrzési eljárásokat hoznak létre, tartanak fenn és eszközölnek a feladatkörök megbízható szerepek szerinti elkülönítésének biztosítására és annak garantálására, hogy a bizalmas feladatok ellátásán több megbízható személy dolgozzon. A C-ITS megbízhatósági modell elemeinek (TLM, CPOC, gyökérszintű CA, EA és AA) meg kell felelniük a [4] követelményeinek és az alábbi bekezdésekben foglalt előírásoknak.

(213) Szabályozási és ellenőrzési eljárásokkal biztosítják a feladatoknak a munkaköri felelősség alapján történő elkülönítését. A legérzékenyebb feladatok (például a CA kriptográfiai hardveréhez (HSM) és a kapcsolódó kulcsanyaghoz való hozzáférés, illetve ezek kezelése) több megbízható személy engedélyezését igénylik.

(214) Ezeket a belső ellenőrzési eljárásokat úgy kell kialakítani, hogy az eszköz fizikai és logikai hozzáféréséhez legalább két megbízható személy igénybevételét biztosítsák. A CA kriptográfiai hardveréhez való hozzáférés korlátozásait a megbízható személyeknek a teljes életciklus alatt szigorúan be kell tartatniuk – a bejövő nyugtától kezdve egészen a végső logikai és/vagy fizikai megsemmisítésig. Amint egy modult a működési kulcsokkal aktiválnak, további hozzáférési ellenőrzéseket is elindítanak, hogy az eszközhöz való fizikai és logikai hozzáférés szintjén egyaránt biztosítsák az osztott ellenőrzést.

5.2.3. Azonosítás és hitelesítés az egyes szerepek szempontjából

(215) A hitelesítési házirendben meghatározottak szerint – minden olyan személyt, akihez szerepet rendeltek hozzá, azonosítani és hitelesíteni kell annak garantálására, hogy azok a szerep révén el tudják látni PKI-feladataikat.

(216) A C-ITS megbízhatósági modell elemeinek még azt megelőzően ellenőrizniük és igazolniuk kell a „megbízható személy” minősítésre törekvő munkatársak személyazonosságát és engedélyezését, hogy:

- számukra kiadnák a hozzáférési eszközöket és hozzáférést kapnának a szükséges berendezésekhez;
- megkapnák az elektronikus hitelesítő adataikat, amelyekkel a CA-rendszerekhez hozzáférhetnek és azokon bizonyos feladatokat végrehajthatnak.

(217) Az egyének azonosítására és hitelesítésére alkalmazott mechanizmusokat a CPS ismerteti.

5.2.4. A feladatkörök szétválasztását igénylő szerepek

(218) A feladatok szétválasztását igénylő szerepek közé tartozik (a teljesség igénye nélkül):

- a kérelmek befogadása, elutasítása és visszavonása, illetve a CA-tanúsítványigénylések egyéb feldolgozási aspektusa;
- a CA-tanúsítvány létrehozása, kiállítása és megsemmisítése.

(219) A feladatok elkülönítéséhez támaszkodhatnak a PKI-berendezésekre, különböző eljárásokra, vagy akár mindkettőre. Egyetlen személyhez sem rendelhető egynél több identitás, hacsak azt a gyökérszintű CA jóvá nem hagyja.

(220) A tanúsítványgenerálásban és a visszavonás lebonyolításában érintett CA (illetve a gyökérszintű CA ezen funkciókban érintett része) számára előírás, hogy a szolgáltatások létrehozásával, biztosításával, fenntartásával és felfüggesztésével kapcsolatos döntéseit – a hatályos hitelesítési házirenddel összhangban – más szervezetektől függetlenül kell hozza meg. Különösen a felső vezetőire, vezetői munkatársaira és megbízható szerepet betöltő munkatársaira igaz az, hogy nem engedhetnek semmilyen olyan kereskedelmi, pénzügyi vagy egyéb nyomásnak, amely kedvezőtlenül befolyásolná a hitelesítésszolgáltató által nyújtott szolgáltatásokba vetett bizalmat.

(221) A mobil C-ITS-állomásokat kiszolgáló EA-nak és AA-nak különálló operatív szervezetnek kell lennie, saját IT-infrastruktúrával és IT-menedzsment csapatokal. Az általános adatvédelmi rendeletnek megfelelően, az EA és AA nem cserélhet egymással személyes adatokat, kivéve az AT-kérelmek engedélyezését. Az AT-kérelmek jóváhagyásával kapcsolatos adatokat kizárólag az [1] szabványban meghatározott engedélyezésvalidálási protokoll segítségével, egy erre a célra szánt biztonságos felületen keresztül továbbíthatják. Más protokollok is alkalmazhatók, amennyiben az [1] követelményei teljesülnek.

(222) Az EA és AA által tárolt naplófájlok kizárólag az elfogott rosszindulatú CAM/DENM üzenetekben szereplő, rendellenesen viselkedő EC-k – AT-k alapján történő – visszavonására használhatók. Miután valamely CAM/DENM

üzenetet rosszindulatúként azonosítottak, az AA a kiállítási naplókban kikeresi az AT verifikációs kulcsát, és az EA-hoz visszavonási kérelmet nyújt be; a kérelemnek tartalmaznia kell az AT kibocsátása során használt EC titkos kulcs szerinti titkosított aláírást. Valamennyi naplófájlt megfelelően védeni kell az illetéktelen hozzáférőkkel szemben, és azok más szervezettel vagy hatósággal nem megoszthatók.

Megjegyzés: A hitelesítési házirend e változatának megszövegezésekor a rendellenesen viselkedő funkció kialakítását még nem definiálták. A tervek szerint a rendellenesen viselkedő funkció kialakításával a hitelesítési házirend jövőbeni felülvizsgálatai foglalkoznak majd.

5.3. Személyzeti ellenőrzések

5.3.1. Képesítések, tapasztalat és engedélyezési követelmények

(223) A C-ITS megbízhatósági modell elemei elegendő számú olyan munkatársat alkalmaznak, akik rendelkeznek a munkaköri funkciókhoz és szolgáltatásokhoz szükséges szakértői tudással, tapasztalattal és képzettséggel. A PKI-munkatársak a fenti követelményeknek az iskolarendszerű képzések és bizonyítványok, a tényleges tapasztalat, illetve a kettő együttese révén felelnek meg. A tanúsítványalkalmazási nyilatkozatban meghatározottak szerint a megbízható szerepeket és felelősségeket a munkaköri leírások dokumentálják és határozzák meg egyértelműen. A PKI-alvállalkozók is rendelkeznek munkaköri leírással, hogy így biztosítsák a feladatkörök és kiváltságok elkülönítését; a pozíció érzékenységét pedig a feladatkörök és hozzáférési szintek, a háttérszűrés, a munkavállalói képzések és tudatosság alapján határozzák meg.

5.3.2. Háttér-ellenőrzési eljárások

(224) A C-ITS megbízhatósági modell elemei azon munkatársaknál, akik megbízható személyekké kívánnak válni, háttérellenőrzést végeznek. A háttérellenőrzéseket a megbízható pozíciókban lévő munkatársak esetében legalább ötévente meg kell ismételni.

(225) A háttérellenőrzés során feltárt azon tényezők, amelyek alapot szolgáltathatnak arra, hogy a megbízható pozícióra pályázó jelöltet elutasítsák vagy egy megbízható személy ellen eljárást indítsanak, – a teljesség igénye nélkül – a következők:

- a jelölt vagy megbízható személy által adott megtévesztő információk;
- rendkívül előnytelen vagy nem megbízható szakmai referenciák;
- bizonyos büntetőítéletek;
- a pénzügyi felelősség hiányára utaló jelzések.

(226) A fentiekről beszámoló jelentéseket a HR munkatársak értékelik ki, akik a háttérellenőrzés során feltárt viselkedési minta típusa, súlyossága és gyakorisága alapján indokolt, reális intézkedéseket hoznak. Az ilyen intézkedések köre kiterjed egészen addig, hogy a megbízható pozícióra pályázó jelölteknek adott állásajánlatot visszavonják vagy, megbízható személy esetében, a munkaviszonyt megszüntetik. Az, hogy a háttérellenőrzés során feltárt információkat hogyan lehet az előbbi intézkedések alapjául felhasználni, a vonatkozó jogszabálytól függ.

(227) Azon személyek háttérvizsgálata, akik megbízható személyekké kívánnak válni, – a teljesség igénye nélkül – a következőkből áll:

- korábbi munkaviszony(ok) igazolása;
- szakmai referenciák ellenőrzése – a munkában eltöltött legalább öt évre visszamenőleg;
- a legmagasabb vagy leginkább releváns megszerzett iskolai végzettség igazolása;
- bűnügyi előélet vizsgálata.

5.3.3. Képzési követelmények

(228) A C-ITS megbízhatósági modell elemei a saját személyzet részére biztosítják azt a képzést, amelyek a CA műveletekkel összefüggő feladatok teljes körű és kielégítő végrehajtásához szükségesek.

(229) A képzési programok rendszeres időközönként áttekintésre kerülnek, a képzéseknek pedig a saját személyzet által ellátott funkciókhoz kapcsolódó témakörökre kell irányulniuk.

(230) A képzési programoknak a képzésben résztvevő saját környezetéhez kapcsolódó témaköröket kell magukban foglalniuk, ideértve:

- a C-ITS megbízhatósági modell elemeinek biztonsági elvei és mechanizmusai;
- a használatban lévő hardverek és szoftverek verziói
- a személy által ellátandó feladatkörök, valamint belső és külső jelentéstételi folyamatok és ciklusok;
- a PKI üzleti folyamatai és munkafolyamatai;
- incidensek és támadások jelentése és kezelése;
- katasztrófa utáni helyreállítási és üzletmenet-folytonossági eljárások;
- elégséges informatikai ismeretek.

5.3.4. Továbbképzések gyakorisága és követelményei

(231) A megbízható szerepet betöltő személyeknek a képzési környezeten keresztül folyamatosan fel kell frissíteniük a képzés során szerzett ismereteket. A képzést szükség szerint, de legalább két évente meg kell ismételni.

(232) A C-ITS megbízhatósági modell elemei ismétlő képzéseket biztosítanak a munkafeladatok teljes körű és kielégítő végrehajtásához elvárt tudásszint fenntartásához szükséges mértékben és gyakoriság szerint.

(233) A megbízható szerepet betöltő személyeknek tisztában kell lenniük a PKI-műveleteket érintő esetleges változásokkal. A műveletekkel kapcsolatos jelentős változtatásokhoz képzési (tudatosságnövelési) tervet kell társítani, és e terv végrehajtását dokumentálni kell.

5.3.5. A munkahelycsere gyakorisága és folyamata

(234) Nincs meghatározva mindaddig, amíg a műszaki készségek, tapasztalat és hozzáférési jogosultságok biztosítottak. A C-ITS megbízhatósági modell

elemei adminisztrátorainak gondoskodniuk kell arról, hogy a személyi állományt érintő változások ne gyakoroljanak hatást a rendszer biztonságára.

5.3.6. A nem engedélyezett műveletekre vonatkozó szankciók

(235) A C-ITS megbízhatósági modell minden egyes elemének olyan formális fegyelmi eljárást kell kidolgoznia, amellyel biztosítható a nem engedélyezett műveletek megfelelő szankcionálása. Súlyos esetekben a megbízásokat és a hozzá tartozó jogosultságokat vissza kell vonni.

5.3.7. Független alvállalkozóra vonatkozó követelmények

(236) A C-ITS megbízhatósági modell elemei lehetővé teszik független alvállalkozók vagy tanácsadók számára, hogy megbízható személyek legyenek olyan mértékben, amely egyértelműen meghatározott kiszervezési viszony létesítéséhez szükséges, valamint azzal a feltétellel, hogy a szervezet ugyanolyan mértékben megbízik az alvállalkozókban vagy tanácsadókban, mintha azok az alkalmazottjai lennének és teljesítenék az alkalmazottakra vonatkozó követelményeket.

(237) Ellenkező esetben a független alvállalkozók és tanácsadók csak akkor férhetnek hozzá a C-ITS PKI biztonságos létesítményeihez, ha megnízható személyek kísérik és közvetlenül felügyelik őket.

5.3.8. A személyzet részére benyújtott dokumentáció

(238) A C-ITS megbízhatósági modell elemei a személyzet részére a munkafeladataik teljes körű és kielégítő végrehajtásához szükséges képzést és dokumentációhoz való hozzáférést biztosítanak.

5.4. Auditnaplózási eljárások

(239) Ez a szakasz a rögzítendő eseménytípusokra és az auditnaplók kezelésére vonatkozó követelményeket ismerteti.

5.4.1. Az egyes CA-k által rögzítendő és lejelentendő eseménytípusok

(240) A CA-képviselő rendszeresen áttekinti a CA-naplókat, -eseményeket és -eljárásokat.

(241) A C-ITS megbízhatósági modell elemei az auditesemény alábbi típusait rögzítik (adott esetben):

- fizikai létesítményhez való hozzáférés – a fizikai személyeknek a létesítményekhez való hozzáférése a hozzáférési kérelmek okoskártyákon keresztüli tárolásával kerül rögzítésre. Esemény jön létre minden olyan alkalommal, amikor bejegyzés jön létre;
- megbízható szerepek kezelése – a különböző beosztásokhoz tartozó hozzáférés meghatározásában és szintjében való változás is rögzítésre kerül – az egyes beosztások jellemzőinek módosítását is ideértve. Esemény jön létre minden olyan alkalommal, amikor bejegyzés jön létre;
- logikai hozzáférés – esemény jön létre, amikor egy szervezet (pl. egy program) érzékeny területekhez (vagyis hálózatokhoz és kiszolgálókhoz) rendelkezik hozzáféréssel;
- biztonsági mentések kezelése – esemény jön létre valahányszor biztonsági mentés történik, akár sikeresen, akár sikertelenül;

- naplókezelés – a naplókat eltárolják. Esemény jön létre valahányszor a napló mérete túllép egy bizonyos méretet;
- az előfizetőkhöz és a C-ITS megbízhatósági modell elemeihez kapcsolódó hitelesítési folyamatból érkező adatok – események jönnek létre minden, az előfizetők és a C-ITS megbízhatósági modell elemei által eljuttatott hitelesítési kérelem esetén;
- a tanúsítványkérelmek (ideértve a tanúsítványok létrehozását és megújítását) elfogadása és elutasítása – meghatározott időközönként esemény jön létre az előző hét napban elfogadott és elutasított tanúsítványkérelmek listájával;
- gyártó regisztrálása – esemény jön létre, amikor egy gyártót regisztrálnak;
- C-ITS-állomás regisztrálása – esemény jön létre a C-ITS állomás regisztrálásakor;
- Humánerőforrás-menedzsment – esemény jön létre a humánerőforrás-menedzsmenttel kapcsolatos biztonsági esemény rögzítésekor;
- Informatika és hálózat kezelése a PKI-rendszerek vonatkozásában – esemény jön létre, amikor a PKI-kiszolgáló leáll és újraindul;
- biztonságirányítás (sikeres és sikertelen hozzáférési kísérletek a PKI-rendszerhez, valamint a biztonsági rendszerben végrehajtott műveletek, a biztonsági profil megváltoztatása, a rendszer összeomlása, hardverhibák és más rendellenességek, illetve tűzfallal és routerrel összefüggő tevékenységek; továbbá a PKI-létesítményekbe való belépések és onnan való kilépések);
- az eseményekkel kapcsolatos adatokat legalább öt évig meg kell őrizni – hacsak eltérő nemzeti előírások nem vonatkoznak.

(242) Az általános adatvédelmi rendelettel összhangban az auditnaplók nem tehetik lehetővé a C-ITS állomás magáncélú járműveivel kapcsolatos személyes adatokhoz való hozzáférést.

(243) Ahol lehetséges, biztonsági auditnaplókat kell automatikusan gyűjteni. Ahol ez nem lehetséges, naplókönyvet, papíralapú űrlapot vagy más fizikai mechanizmust kell alkalmazni. Minden biztonsági auditnaplót (elektronikus és nem elektronikus) meg kell őrizni és elérhetővé kell tenni a megfelelőségi auditok folyamán.

(244) A tanúsítvány életciklusával kapcsolatos minden esemény naplózása úgy történik, hogy azt a műveletet végrehajtó személyhez lehessen társítani. A személyazonossággal kapcsolatos adatokat titkosítják és illetéktelen hozzáféréssel szemben védik.

(245) Minden auditbejegyzésnek legalább az alábbiakat kell tartalmaznia (automatikusan vagy minden ellenőrzés alá vont esemény során manuálisan):

- eseménytípus (a fenti listából);
- az esemény bekövetkezésének megbízható dátuma és időpontja;
- az esemény eredménye – adott esetben sikeres vagy sikertelen;

- az eseményt kiváltó szervezet és/vagy kezelő személyazonossága;
- annak a szervezetnek a személyazonossága, amelyre az esemény irányul.

5.4.2. A naplófeldolgozás gyakorisága

(246) Az auditnaplókat a CA-rendszerekben jelentkező rendellenességek és incidensek alapján keletkező riasztásokra reagálva, illetve évente egyszer át kell tekinteni.

(247) Az auditnaplók feldolgozásának az auditnaplók áttekintését, valamint az auditnapló összefoglalásában szereplő jelentősebb események indoklásának dokumentálását kell magában foglalnia. Az auditnaplók áttekintése magában foglalja annak ellenőrzését, hogy a naplót nem manipulálták, valamint az összes naplóbejegyzés és a naplóban lévő riasztások vagy rendellenességek kivizsgálását is. Az auditnaplók áttekintése alapján tett intézkedéseket dokumentálni kell.

(248) Az auditnaplókat legalább hetente archiválni kell. A rendszergazdának manuálisan kell archiválnia az auditnaplót, ha az ahhoz tartozó szabad lemezterület kisebb, mint amit az adott héten várhatóan az auditnaplóba kerülő adatok igényelnek.

5.4.3. Az auditnaplókra vonatkozó megőrzési időszak

(249) A tanúsítvány életciklusához kapcsolódó naplóbejegyzéseket a vonatkozó tanúsítvány lejártát követően legalább öt évig meg kell őrizni.

5.4.4. Az auditnapló védelme

(250) Az auditnapló épségét és titkosságát feladatkörökhöz kapcsolt hozzáférés-ellenőrzési mechanizmus garantálja. A belső auditnaplókhoz csak rendszergazdák férhetnek hozzá; az auditnaplókhoz kapcsolódó tanúsítvány életciklusához is csak megfelelő jogosultságokkal rendelkező felhasználók férhetnek hozzá egy weboldalon keresztül, felhasználói bejelentkezést követően. A hozzáférés csak többfelhasználós (legalább kétfelhasználós) és legalább kétszintű hitelesítéssel adható meg. Műszakilag biztosítani kell azt, hogy a felhasználók ne férhessenek hozzá a saját naplófájljaikhoz.

(251) Minden naplóbejegyzést a HSM által biztosított kulccsal kell aláírni.

(252) Olyan információkat tartalmazó eseménynaplók, amelyek egy személy azonosítását teszik lehetővé (például magáncélú gépjármű) titkosításra kerülnek, hogy azokat csak arra illetékes személyek olvashassák.

(253) Az események naplózása olyan módon történik, hogy azok a megőrzési időszak alatt ne törlődhessenek vagy semmisülhessenek meg könnyedén (hosszan tároló adattárba történő áthelyezés kivételével).

(254) Az eseménynaplók olyan védelmet kapnak, amely lehetővé teszi, hogy a megőrzési időszak alatt olvashatók maradjanak.

5.4.5. Auditnaplók biztonsági mentésének eljárásai

(255) Az auditnaplók és összefoglalók biztonsági mentése vállalati biztonsági mentési mechanizmusokon keresztül, engedélyezett megbízható szerepek ellenőrzése mellett, az összetevők forrásgenerálásától elkülönítetten történik. Az auditnaplók biztonsági mentéseit az eredeti naplókra vonatkozó megbízhatósággal azonos szintű védelemmel kell ellátni.

5.4.6. Auditgyűjtési rendszer (belső vagy külső)

(256) A C-ITS megbízhatósági modell elemeihez tartozó eszközöknek a rendszer indításakor aktiválniuk kell az auditfolyamatokat, és azokat csak a rendszer leállításakor deaktiválhatják. Ha az auditfolyamatok nem elérhetők, akkor a C-ITS megbízhatósági modell elemeinek fel kell függeszteniük a működésüket.

(257) Az egyes működési időszakok végén és a tanúsítványok kulcsainak megújításakor az eszközök összegzett állapotát a műveleti vezető és a vonatkozó PKI-elemhez tartozó műveleteket szabályozó szerv felé kell jelenteni.

5.4.7. Eseményt kiváló alany részére adott értesítés

(258) Ha egy eseményt az auditgyűjtő rendszer naplóz, akkor az garantálja, hogy az esemény megbízható szerephez társítását.

5.4.8. Sebezhetőségi értékelés

(259) Az audit lefolytatásával megbízott szerep és a PKI-rendszernek a C-ITS megbízhatósági modell elemein belüli működtetéséért felelős szerepek egy auditnapló-összefoglalásban írják le az összes jelentős eseményt. E felülvizsgálatok során ellenőrzik, hogy a naplót nem manipulálták-e és nem merült-e fel a folytonosság hiánya vagy az auditadatok más jellegű elvesztése, majd röviden átvizsgálják az összes naplóbejegyzést, amely során a naplókban lévő riasztásokat és rendellenességeket alaposabb ellenőrzés alá vonják. E felülvizsgálatok eredményeként tett intézkedéseket dokumentálni kell.

(260) A C-ITS megbízhatósági modell elemeinek:

- szervezeti és/vagy műszaki észlelési és megelőzési ellenőrzéseket kell végrehajtaniuk a C-ITS megbízhatósági modell elemeinek felügyelete alatt a PKI-rendszerek vírusok és kártékony szoftverek elleni védelme érdekében;
- dokumentálniuk és követniük kell a sebezhetőségek azonosítására, felülvizsgálatára, elhárítására és javítására irányuló sebezhetőségkorrekciós folyamatot;
- sebezhetőségi átvilágítás alá kell vetniük magukat vagy ilyet kell végrehajtaniuk:
  - minden olyan a rendszert vagy hálózatot érintő változtatás után, amelyet a C-ITS megbízhatósági modell elemei a PKI-összetevők vonatkozásában jelentősnek ítél meg; valamint
  - legalább havonta egyszer a CA és CPOC által, a PKI alá tartozó rendszerekként azonosított nyilvános és privát IP-címeken,
- illegális behatolási vizsgálat alá kell vetniük magukat a PKI-hez tartozó rendszerek esetén legalább évente egyszer, illetve az infrastruktúra vagy alkalmazás olyan frissítései vagy módosításai után, amelyeket a C-ITS megbízhatósági modell elemei a CA PKI-összetevői vonatkozásában jelentősnek ítél meg;
- az online rendszerek vonatkozásában rögzítik minden, olyan személy vagy szervezet (vagy ezek csoportja) által végrehajtott sebezhetőségi átvilágítás és illegális behatolási vizsgálat bizonyítékát, aki rendelkezik a megbízható sebezhetőségi és illegális behatolási vizsgálat lefolytatásához szükséges készségekkel, eszközökkel, hozzáértéssel, etikai kódexszel és függetlenséggel;
- a sebezhetőségek nyomon követése és kijavítása a vállalati kiberbiztonsági szabályokkal és kockázatcsökkentési módszertannal összhangban.

5.5. Feljegyzések archiválása

5.5.1. Az archivált feljegyzések típusai

(261) A C-ITS megbízhatósági modell elemeinek olyan részletességű feljegyzéseket kell archiválniuk, amely lehetővé teszi az aláírás érvényességének és a PKI megfelelő működésének ellenőrzését. Legalább az alábbi PKI-eseményfeljegyzéseket kell archiválni (adott esetben):

- a C-ITS megbízhatósági modell elemeinek fizikai létesítményhez tartozó hozzáférési naplója (legalább egy év);
- a megbízható szerepek kezelési naplója a C-ITS megbízhatósági modell elemei vonatkozásában (legalább 10 év);
- informatikai hozzáférési napló a C-ITS megbízhatósági modell elemei vonatkozásában (legalább öt év);
- CA kulcs létrehozásáról, használatáról és megsemmisítéséről szóló napló (legalább öt év) (a TLM és CPOC esetén nem);

- tanúsítvány létrehozásáról, használatáról és megsemmisítéséről szóló napló (legalább két év);
- CPA-kérelmek naplója (legalább két év);
- aktiváló adatok kezelési naplója a C-ITS megbízhatósági modell elemei vonatkozásában (legalább öt év);
- informatikai és hálózati napló a C-ITS megbízhatósági modell elemei vonatkozásában (legalább öt év);
- PKI-dokumentáció a C-ITS megbízhatósági modell elemei vonatkozásában (legalább öt év);
- biztonsági incidensek jelentései és auditjelentések a C-ITS megbízhatósági modell elemei vonatkozásában (legalább 10 év);
- rendszereszközök, szoftverek és konfiguráció (legalább öt év).

(262) A C-ITS megbízhatósági modell elemeinek az alábbi, a tanúsítványkérelmekhez és azok hitelesítéséhez kapcsolódó dokumentumokat, valamint minden ezekhez tartozó TLM-et, gyökérszintű CA- és CA-tanúsítványt meg kell őrizniük legalább hét évig azt követően, hogy az adott dokumentumon alapuló tanúsítvány érvényét veszíti:

- a C-ITS megbízhatósági modell elemei által őrzött PKI-auditdokumentáció;
- a C-ITS megbízhatósági modell elemei által őrzött CPS-dokumentumok;
- a CPA és más szervezetek között létrejött, a C-ITS megbízhatósági modell elemei által őrzött szerződések;
- a gyökérszintű CA és TLM által őrzött tanúsítványok (vagy más, visszavonásra vonatkozó információ);
- a gyökérszintű CA rendszerben lévő tanúsítványkérelmekre vonatkozó feljegyzések (a TLM-re nem vonatkozik);
- az archivált tartalom hitelesítéséhez elégséges más adatok vagy alkalmazások;
- minden, a C-ITS megbízhatósági modell elemeinek és a megfelelőségi ellenőrök vonatkozásában elvégzett munka.

(263) A CA szervezetnek legalább az adott dokumentum alapján kiállított tanúsítvány érvénytelenné válását követő hét évig meg kell őriznie a tanúsítványkérelmekkel és azok hitelesítésével kapcsolatos valamennyi dokumentumot, valamint minden tanúsítványt és azok visszavonását.

5.5.2. Az archívum megőrzési ideje

(264) A hosszabb archiválási időt előíró rendeletek sérelme nélkül a C-ITS megbízhatósági modell elemeinek legalább a vonatkozó tanúsítvány lejárata után öt évig meg kell őrizniük minden dokumentumot.

5.5.3. Az archívum védelme

(265) A C-ITS megbízhatósági modell elemeinek biztonságos és védett tárolólétesítményben kell tárolniuk a dokumentumok archívumát a PKI-nél

alkalmazottakkal egyenértékű vagy azoknál jobb fizikai és eljárásbeli biztonsági ellenőrzésekkel.

(266) Az archívumot illetéktelen megtekintés, módosítás, törlés vagy manipuláció ellen megbízható rendszerben történő tárolással kell védeni.

(267) Az archív adatokat tároló adattárolókat és a feldolgozásukhoz szükséges alkalmazásokat úgy kell tárolni, hogy azok a jelen hitelesítési házirendben meghatározott időszak alatt hozzáférhetők legyenek.

5.5.4. Rendszerarchívum és -tároló

(268) A C-ITS megbízhatósági modell elemeinek bővülő jelleggel, napi rendszerességgel kell biztonsági mentést készíteniük az ilyen információk rendszerarchívumairól, hetente pedig teljes körű biztonsági mentést kell végrehajtaniuk. A papíralapú dokumentumok példányait a telephelyen kívüli, biztonságos létesítményben kell őrizni.

5.5.5. A bejegyzések időbélyegzőjével kapcsolatos követelmények

(269) A C-ITS megbízhatósági modell visszavonási adatbázist kezelő eleminek gondoskodniuk kell arról, hogy a dokumentumok információt tartalmazzanak a visszavonási dokumentumok létrehozásának dátumáról és időpontjáról. Ezen információk épségét kriptográfiai megoldásokkal biztosítják.

5.5.6. Archívumgyűjtő rendszer (belső vagy külső)

(270) Az archívumgyűjtő rendszer egy belső rendszer.

5.5.7. Az archív információk beszerzésére és hitelesítésére irányuló eljárások

(271) A C-ITS megbízhatósági modell valamennyi eleme csak engedélyezett megbízható személyek részére teheti lehetővé az archívumhoz való hozzáférést. A gyökérszintű CA-k és CA-k ismertetik az archív információk CPS-ben történő létrehozásával, hitelesítésével, becsomagolásával, továbbításával és tárolásával kapcsolatos eljárásokat.

(272) A gyökérszintű CA-k és CA-k berendezései ellenőrzik az információ épségét, mielőtt azt helyreállítanák.

5.6. A kulcs cseréje a C-ITS megbízhatósági modell elemei esetén

(273) A C-ITS megbízhatósági modell alábbi elemeihez a kulcsok cseréje tekintetében egyéni követelmények tartoznak: TLM-, gyökérszintű CA, valamint EA/AA-tanúsítványok.

*5.6.1. **TLM***

(274) A TLM-nek a vonatkozó tanúsítvány lejártakor törölnie kell a titkos kulcsát. Új kulcspárt és megfelelő TLM-tanúsítványt kell generálnia az aktuálisan érvényes titkos kulcs deaktiválása előtt. Ennek biztosítania kell, hogy egy új (hivatkozási) tanúsítvány kerüljön az ECTL-be még kellő időben ahhoz, hogy az érvényessé válása előtt valamennyi C-ITS-állomásra kioszthatóó legyen. A hivatkozási tanúsítvány és az új, önaláírt tanúsítvány átkerül a CPOC-ba.

5.6.2. Gyökérszintű CA

(275) A gyökérszintű Ca-nak deaktiválnia és törölnie kell az aktuális titkos kulcsot (ideértve a kulcsok biztonsági másolatait), hogy az ne állítson ki olyan EA/AA-

tanúsítványokat, amelyek érvényessége meghaladja a gyökérszintű CA-tanúsítvány érvényességét.

(276) A gyökérszintű CA-nak új kulcspárt és megfelelő gyökérszintű CA- és hivatkozási tanúsítványt kell generálnia az aktuális titkos kulcs (ideértve a kulcsok biztonsági másolatait) deaktiválása előtt, és ezt az ECTL-be történő beillesztés céljából a TLM-be kell küldenie. Az új gyökérszintű CA-tanúsítvány érvényessége az aktuális titkos kulcs tervezett deaktiválásával kezdődik. A gyökérszintű CA-nak gondoskodnia kell arról, hogy a új tanúsítvány ECTL-be történő beillesztése kellő időben megtörténjen ahhoz, hogy az érvényesség kezdete előtt az összes C-ITS-állomáshoz kiosztásra kerülhessen.

(277) A gyökérszintű CA akkor aktiválja az új titkos kulcsot, amikor a vonatkozó gyökérszintű CA-tanúsítvány érvényessé válik.

5.6.3. EA/AA-tanúsítvány

(278) Az EA/AA-nak deaktiválnia kell az összes aktuális titkos kulcsot, hogy az ne állítson ki olyan érvényességű EC-ket/AT-kat, amely meghaladja az EA/AA-tanúsítvány érvényességét.

(279) Az EA/AA-nak új kulcspárt kell generálnia, és kérelmeznie kell egy EA/AA-tanúsítványt még az aktuális titkos kulcs deaktiválása előtt. Az új EA/AA-tanúsítvány érvényességi ideje az aktuális titkos kulcs tervezett deaktiválásának időpontjában kezdődik. Az EA/AA-nak gondoskodnia kell arról, hogy az új tanúsítvány kellő időben kiadásra kerüljön ahhoz, hogy az érvényesség kezdete előtt az összes C-ITS-állomáshoz kiosztásra kerülhessen.

(280) Az EA/AA-nak akkor kell az új titkos kulcsot aktiválnia, amikor a vonatkozó EA/AA-tanúsítvány érvényessé válik.

5.6.4. Ellenőr

Nincs rendelkezés.

5.7. Támadás és katasztrófa utáni helyreállítás

5.7.1. Indicensek és támadások kezelése

(281) A C-ITS megbízhatósági modell elemeinek folyamatosan felügyelniük kell eszközeiket, hogy észlelni tudják az esetleges behatolási kísérleteket vagy a támadás más formáit. Ilyen esetben vizsgálatot kell tartaniuk a kár jellegének és mértékének megállapítása érdekében.

(282) Ha a gyökérszintű CA vagy TLM irányításáért felelős személyzet esetleges behatolási kísérletet vagy a támadás más formáit észleli, akkor vizsgálatot kell tartania a károsodás jellegének és mértékének megállapítása érdekében. Amennyiben a titkos kulcs sérült, akkor a gyökérszintű CA-tanúsítványt vissza kell vonni. A CPA információbiztonsági szakembereinek ki kell vizsgálniuk az esetleges kár kiterjedését, hogy meg lehessen állapítani, hogy a PKI-t újra kell-e építeni, csak néhány tanúsítványt kell-e visszavonni és/vagy a PKI sérült-e. Ezenkívül a CPA megállapítja, hogy mely szolgáltatásokat és hogyan kell fenntartani (visszavonás és tanúsítvány állapotinformációi) a CPA üzletmenet-folytonossági tervével összhangban.

(283) A CPS kiterjed az incidensekre, támadásokra és üzletmenet-folytonosságra, amely megvalósítása érdekében más vállalati erőforrásokra és tervekre is támaszkodhat.

(284) Ha az EA/AA/CPOC kezeléséért felelős személyzet esetleges behatolási kísérletet vagy a támadás más formáját észleli, akkor vizsgálatot kell tartania a kár jellegének és mértékének megállapítása érdekében. A CA vagy a CPOC-szervezet irányításáért felelős személyzetnek ki kell vizsgálnia az esetleges kár kiterjedését, hogy meg lehessen állapítani, hogy a PKI-összetevőt újra kell-e építeni, csak néhány tanúsítványt kell-e visszavonni és/vagy a PKI-összetevő sérült-e. Emellett az alacsonyabb szintű CA határozza meg, hogy mely szolgáltatásokat és hogyan kell fenntartani – az alacsonyabb szintű tanúsítványkiadó üzletmenet-folytonossági tervével összhangban. Amennyiben egy PKI-összetevő titkossága sérült, a CA szervezetnek a CPOC-n keresztül riasztania kell a saját gyökérszintű CA-ját és TLM-jét.

(285) A gyökérszintű CA vagy TLM CPS-e vagy – CPOC esetén – más, vonatkozó dokumentum kiterjed az incidensekre, támadásokra és üzletmenet-folytonosságra, és más vállalati erőforrásokra és tervekre is támaszkodhat ennek érdekében.

(286) A gyökérszintű CA és CA riasztást és az incidens következményeiről pontos tájékoztatást ad minden olyan tagállami képviselő és gyökérszintű CA részére, amellyel a C-ITS-szel összefüggésben megállapodással rendelkezik, hogy ezáltal lehetővé tegye számukra a saját incidenskezelési tervük aktiválását.

5.7.2. A számítógépes erőforrások, szoftverek és/vagy adatok sérülése

(287) Ha olyan katasztrófát fedeznek fel, amely megakadályozza a C-ITS megbízhatósági modell elem megfelelő működését, akkor az elemnek fel kell függesztenie a működését és ki kell vizsgálnia, hogy a titkos kulcs sérült-e (kivéve a CPOC esetén). A meghibásodott hardvereket a lehető legrövidebb időn belül ki kell cserélni, és az 5.7.3. és 5.7.4. szakaszokban ismertetett eljárásokat kell alkalmazni.

(288) A számítógépes erőforrások, szoftverek és/vagy adatok sérülését a gyökérszintű CA felé 24 órán belül jelenteni kell a legmagasabb kockázati szintek esetén. Minden egyéb eseményt fel kell tüntetni a gyökérszintű CA, EA-k és AA-k időszakos jelentésében.

5.7.3. Szervezet titkos kulcsának sérülésére vonatkozó eljárások

(289) Ha valamely gyökérszintű CA titkos kulcsa titkossága sérült, elveszett, megsemmisült vagy felmerül a gyanúja annak, hogy titkossága sérült, akkor a gyökér-CA:

- felfüggeszti a működését;
- katasztrófa utáni helyreállítási és migrációs tervet hajt végre;
- visszavonja a gyökérszintű CA-tanúsítványát;
- kivizsgálja a titkosság sérülését kiváltó „fő problémát”, és értesíti a CPA-t, amely a TLM-en keresztül visszavonja a gyökérszintű CA-tanúsítványt (lásd: 7. szakasz);
- riasztást küld az összes olyan előfizető részére, akivel megállapodást kötött.

(290) Ha az EA/AA-kulcs titkossága sérült, elveszett, megsemmisült vagy felmerül a gyanúja annak, hogy titkossága sérült, akkor az EA/AA:

- felfüggeszti a működését;
- visszavonja a saját tanúsítványát;
- kivizsgálja a „fő problémát”, és értesíti a gyökérszintű CA-t;
- riasztást küld az összes olyan előfizető részére, akivel megállapodást kötött.

(291) Ha egy C-ITS-állomáshoz tartozó EC- vagy AT-kulcs titkossága sérült, elveszett, megsemmisült vagy felmerül a gyanúja annak, hogy titkossága sérült, akkor az az EA/AA, amelyre a C-ITS állomás előfizetett:

- visszavonja az érintett ITS EC-jét;
- kivizsgálja a „fő problémát”, és értesíti a gyökérszintű CA-t;
- riasztást küld az összes olyan előfizető részére, akivel megállapodást kötött.

(292) Ahol a gyökérszintű CA és/vagy CA vagy C-ITS-állomások által alkalmazott algoritmusok vagy társított paraméterek a fennmaradó szándékolt felhasználásra elégtelenné válnak, akkor a CPA (kriptográfiai szakértők ajánlásával) tájékoztatja azt a gyökérszintű CA szervezetet, amellyel megállapodást kötött, és módosítja a használt algoritmusokat. (A részletekért lásd a 6. szakaszt, valamint a gyökérszintű CA és az al-CA CPS-eit).

5.7.4. Katasztrófa utáni üzletmenet-folytonossági képességek

(293) A C-ITS megbízhatósági modellnek a CA műveletei részére biztonságos létesítményeket működtető elemeinek katasztrófa utáni helyreállítási tervet kell kidolgozniuk, tesztelniük, fenntartaniuk és végrehajtaniuk azzal a céllal, hogy csökkentsék a természeti vagy az ember okozta katasztrófák hatásait. Ezeknek a terveknek ki kell térniük az információs rendszerek szolgáltatásainak és a fő üzleti funkciók helyreállítására.

(294) Egy adott kockázati szintű incidens esetén a megtámadott CA-t újból auditálnia kell egy akkreditált PKI-ellenőrnek (lásd: 8. szakasz).

(295) Ahol a megtámadott CA nem képes tovább működni (pl. súlyos incidens után), egy migrációs tervet kell kidolgozni funkcióinak egy másik gyökérszintű CA-hoz történő áthelyezésére. Legalább az uniós gyökérszintű CA-nak alkalmasnak kell lennie a migrációs terv támogatására. A megtámadott CA felfüggeszti a funkcióit.

(296) A gyökérszintű CA-knak a katasztrófa utáni helyreállítási tervet és egy migrációs tervet kell a CPS-be beépíteniük.

5.8. Megszűnés és áthelyezés

*5.8.1. **TLM***

(297) A TLM nem szünteti be a működését, azonban a TLM-et működtető szervezet átvehet egy másik szervezetet.

(298) A működtető szervezet megváltozása esetén:

- a CPA jóváhagyását kell kérni ahhoz, hogy a TLM működtetését a régi szervezettől az új szervezet vegye át;
- a CPA-nak jóvá kell hagynia a TLM működtetését érintő változtatást;
- minden auditnaplót és archivált dokumentumot át kell helyezni a régi működtető szervezettől az új szervezethez.

5.8.2. Gyökérszintű CA

(299) A gyökérszintű CA nem szüntetheti meg/kezdheti meg működését olyan migrációs terv kidolgozása (a vonatkozó CPS-ben) nélkül, amely valamennyi előfizető számára garantálja a folytonos működést.

(300) A gyökérszintű CA szolgáltatásának megszűnése esetén a gyökérszintű CA:

- értesíti a CPA-t;
- értesíti a TLM-et, hogy az törölni tudja a gyökérszintű CA-tanúsítványt a ECTL-ből;
- visszavonja a vonatkozó gyökérszintű CA-t egy, önmagát tartalmazó CRL kiállításával;
- riasztást küld az EA/AA-tanúsítványok megújításáról azon gyökérszintű CA-knak, amelyekkel megállapodást kötött;
- megsemmisít a gyökérszintű CA titkos kulcsát;
- közli a legutóbbi visszavonási állapotinformációkat (a gyökérszintű CA által aláírt CRL) az érintettféllel, egyértelműen feltüntetve azt, hogy ez a legutóbbi visszavonásra vonatkozó információ;
- archiválja az összes auditnaplót és minden, a PKI megszűnését megelőző más dokumentumot;
- továbbítja az archivált dokumentumokat a megfelelő hatóság felé.

(301) A TLM törli a vonatkozó gyökérszintű CA-tanúsítványt az ECTL-ből.

*5.8.3. **EA/AA***

(302) Az EA/AA-szolgáltatás megszűnése esetén az EA/AA-szervezet a megszűnés előtt értesítést küld. EA vagy AA nem szüntetheti meg/kezdheti meg működését olyan migrációs terv kidolgozása (a vonatkozó CPS-ben) nélkül, amely valamennyi előfizető számára garantálja a folytonos működést. Az EA/AA:

- ajánlott levélben tájékoztatja a gyökérszintű CA-t;
- megsemmisít a CA titkos kulcsát;
- továbbítja az adatbázisát a gyökérszintű CA által megjelölt szervezet felé;
- nem állít ki több tanúsítványt;
- adatbázisa továbbítása során, és amíg az adatbázis az új szervezetnél teljesen működésbe nem lép, fenntartja azon képességét, hogy a felelős adatvédelmi hatóságtól érkező kérelmeket jóváhagyja;

- amennyiben egy alacsonyabb szintű CA-t ért támadás, a gyökérszintű CA-nak vissza kell vonnia az alacsonyabb szintű CA-t, és új CRL-t kell kibocsátania, melyben megtalálható a visszavont alacsonyabb szintű CA-k listája;
- archiválja az összes auditnaplót és minden, a PKI megszűnését megelőző más dokumentumot;
- továbbítja az archivált dokumentumait a gyökérszintű CA által megjelölt szervezet felé;

(303) A CA szolgáltatásainak megszűnése esetén a CA felelőssége megőrizni a CA és a PKI-összetevők szükségleteivel összefüggő összes dokumentumot.

6. MŰSZAKI BIZTONSÁGI ELLENŐRZÉSEK

6.1. Kulcspárok létrehozása és telepítése

6.1.1. A TLM, a gyökér-CA, az EA és AA

(304) A kulcspár létrehozási folyamatának az alábbi követelményeket kell teljesítenie:

- minden résztvevőnek létre kell tudnia hozni a saját kulcspárjait a 6.1.4. és 6.1.5. szakaszok szerint;
- a tanúsítványkérelmekhez szükséges szimmetrikus titkosító kulcsok és MAC-kulcs kinyerését (ECIES) az [1] és [5] szerint kell végrehajtani;
- a kulcs létrehozásának folyamata során a 6.1.4.1. és 6.1.4.2 szakaszokban ismertetett algoritmusokat és kulcshosszokat kell alkalmazni;
- a kulcspár létrehozási folyamatára a „titkos kulcsok biztonságos tárolása” követelmények (lásd: 6.1.5. szakasz) vonatkoznak;
- a gyökérszintű CA-knak és előfizetőiknek (alacsonyabb szintű CA-k) gondoskodniuk kell arról, hogy a nyilvános kulcsaik és a társított paraméterek megőrizzék épségüket és hitelességüket a regisztrált alacsonyabb szintű CA-hoz történő kiosztás alatt.

6.1.2. EE – mobil C-ITS-állomás

(305) Minden mobil C-ITS-állomásnak létre kell hoznia a saját kulcspárjait a 6.1.4. és 6.1.5. szakaszok szerint;

(306) A tanúsítványkérelmekhez szükséges szimmetrikus titkosító kulcsok és MAC-kulcs kinyerését (ECIES) az [1] és [5] szerint kell végrehajtani;

(307) A kulcs létrehozásának folyamata során a 6.1.4.1. és 6.1.4.2. szakaszokban ismertetett algoritmusokat és kulcshosszokat kell alkalmazni;

(308) A kulcspár létrehozási folyamatain alkalmazni kell a „titkos kulcsok biztonságos tárolása” követelményeket (lásd: 6.1.5 szakasz);

6.1.3. EE – fix C-ITS-állomás

(309) Minden fix C-ITS-állomásnak létre kell hoznia a saját kulcspárját a 6.1.4 és 6.1.5 szakaszok szerint;

(310) A kulcs létrehozásának folyamata során a 6.1.4.1. és 6.1.4.2. szakaszokban ismertetett algoritmusokat és kulcshosszokat kell alkalmazni;

(311) A kulcspár létrehozási folyamatain alkalmazni kell a „titkos kulcsok biztonságos tárolása” követelményeket (lásd: 6.1.5 szakasz);

6.1.4. Kriptográfiai követelmények

(312) A PKI-résztvevőknek teljesíteniük kell az alábbi bekezdésekben ismertetett, aláírási algoritmusra, kulcshosszra, véletlenszerű számgenerátorra és hivatkozási tanúsítványokra vonatkozó kriptográfiai követelményeket.

6.1.4.1. *Algoritmus és kulcshosszúság – aláírási algoritmusok*

(313) Valamennyi PKI-résztvevőnek (TLM, gyökérszintű CA, EA, AA és C-ITS állomások) képesnek kell lennie kulcspárokat létrehozni és titkos kulcsot használni a műveletek kiválasztott algoritmusokkal történő aláírásához legkésőbb e rendelet hatálybalépését követő két éven belül, a 4. táblázatnak megfelelően.

(314) Valamennyi az ECTL, tanúsítványok és/vagy aláírt üzenetek épségének az 1.3.6. szakaszban meghatározott szerepe szerinti ellenőrzésére kötelezett PKI-résztvevőnek támogatnia kell az 5. táblázatban hitelesítésre felsorolt, vonatkozó algoritmusokat. A C-ITS-állomásoknak különösen képesnek kell lenniük az ECTL épségének ellenőrzésére.

	TLM	gyökérszintű CA	EA	AA	C-ITS-állomás
ECDSA_nistP256_with_SHA 256	-	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA 256	-	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA 384	X	X	X	-	-
Az „X” kötelező támogatást jelent					

4. táblázat: Kulcspárok létrehozása és titkos kulcs használata aláírási műveletekre

	TLM	gyökérszintű CA	EA	AA	C-ITS-állomás
ECDSA_nistP256_with_SHA 256	X	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA 256	X	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA 384	X	X	X	X	X
Az „X” kötelező támogatást jelent					

5. táblázat: Hitelesítés áttekintése

(315) Ha a CPA újonnan feltárt kriptográfiai gyenge pontok alapján úgy dönt, az összes C-ITS-állomásnak mielőbb át kell állnia két algoritmus közül az egyikre (ECDSA_nistP256_with_SHA 256 vagy ECDSA_brainpoolP256_with_SHA 256). A ténylegesen használandó algoritmust (vagy algoritmusokat) a vonatkozó nyilvános kulcshoz a tanúsítványt kiállító CA CPS-ében határozzák meg a jelen hitelesítési házirenddel összhangban.

6.1.4.2. *Algoritmus és kulcshosszúság – titkosítási algoritmusok a nyilvántartásba vételhez és hitelesítéshez*

(316) Valamennyi PKI-résztvevőnek (EA, AA és C-ITS-állomások) képesnek kell lennie nyilvános kulcsokat használni a nyilvántartásba vételi és hitelesítési kérelmek/válaszok kiválasztott algoritmusokkal történő titkosítására legkésőbb e rendelet hatálybalépését követő két éven belül, a 6. táblázatnak megfelelően. A ténylegesen használandó algoritmust (vagy algoritmusokat) a vonatkozó nyilvános kulcshoz a tanúsítványt kiállító CA CPS-ében határozzák meg a jelen hitelesítési házirenddel összhangban.

(317) A 6. táblázatban megnevezett algoritmusok a kulcshosszt és a hash algoritmus hosszát jelölik, és ezeket az [5] szerint kell alkalmazni.

	TLM	gyökérszintű CA	EA	AA	C-ITS-állomás
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES 128_CCM	-	-	X	X	X
Az „X” kötelező támogatást jelent					

6. táblázat: Nyilvános kulcsok használata a nyilvántartásba vételi és hitelesítési kérelmek/válaszok titkosítására

(318) Valamennyi PKI-résztvevőnek (EA, AA és C-ITS-állomások) képesnek kell lennie kulcspárok létrehozására és titkos kulcsokat használni a nyilvántartásba vételi és hitelesítési kérelmek/válaszok a kiválasztott algoritmusokkal történő titkosítására legkésőbb e rendelet hatálybalépését követő két éven belül, a 7. táblázatnak megfelelően.

	TLM	gyökérszintű CA	EA	AA	C-ITS-állomás
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES 128_CCM	-	-	X	X	X
Az „X” kötelező támogatást jelent					

7. táblázat: Kulcspárok létrehozása és titkos kulcs használata a nyilvántartásba vételi és hitelesítési kérelmek/válaszok titkosítására

6.1.4.3. *Kriptoagilitás*

(319) A kulcshosszra és algoritmusokra vonatkozó követelményeket idővel változtatni kell a megfelelő szintű biztonság fenntartása érdekében. A CPA-nak nyomon kell követnie ezeknek a változtatásoknak a szükségességét a tényleges sebezhetőségek és a kriptográfia aktuális állásának megfelelően. A CPA frissítést készít, hagy jóvá és bocsát ki ehhez a hitelesítési házirendhez, ha úgy dönt, hogy a kriptográfiai algoritmusokat frissíteni kell. Amennyiben a jelen hitelesítési házirend új kiadása az algoritmussal és/vagy kulcshosszal kapcsolatos változást jelez, a CPA migrációs stratégiát fogad el, mely magában foglalja azokat az átmeneti időszakokat, amelyek során a régi algoritmusok és az új algoritmusok is támogatottak.

(320) Az új algoritmusokra és/vagy kulcshosszokra való átállás lehetővé tétele és elősegítése érdekében javasolt minden PKI-résztvevő számára, hogy olyan hardvereket és/vagy szoftvereket alkalmazzon, amelyek alkalmasak a kulcshosszokkal és algoritmusokkal kapcsolatos változtatások kezelésére.

(321) A gyökérszintű és TLM-tanúsítványok megváltoztatását hivatkozási tanúsítványokkal kell támogatni és végrehajtani (lásd: 4.6. szakasz), melyeket a régi és új gyökérszintű tanúsítványok közötti átmeneti időszak során használnak („a megbízhatósági modell migrálása”).

6.1.5. Titkos kulcsok biztonságos tárolása

Ez a szakasz a kulcspároknak és véletlenszerű számoknak a CA-k és végfelhasználók részére történő biztonságos tárolása és létrehozása követelményeit ismerteti. Ezeket a követelményeket a kriptográfiai modulokhoz definiálják, és az alábbi albekezdések ismertetik.

6.1.5.1. *Gyökérszintű CA, al-CA és TLM szint*

(322) Kriptográfiai modult kell használni:

- a titkos kulcsok létrehozása, használata, kezelése és tárolása;
- véletlenszerű számok létrehozása és használata (a véletlenszerű számok létrehozása funkció értékelésének szerepelnie kell a biztonsági értékelésben és tanúsításban);

- titkos kulcsokról a 6.1.6. szakasz szerinti biztonsági másolat készítése;
- titkos kulcsok törlése.

A kriptográfiai modult az alábbi védelmi profilok (PP-k) valamelyike szerint kell tanúsítani EAL-4 vagy magasabb biztonsági szinten:

- PP-k HSM-ek részére:
  - CEN EN 419 221-2: Védelmi profilok TSP kriptográfiai modulokhoz – 2. rész: Kriptográfiai modul biztonsági mentéssel rendelkező CSP aláírási műveletekhez;
  - CEN EN 419 221-4: Védelmi profilok TSP kriptográfiai modulokhoz – 4. rész: Kriptográfiai modul biztonsági mentés nélküli CSP aláírási műveletekhez;
  - CEN EN 419 221-5: Védelmi profilok TSP kriptográfiai modulokhoz – 5. rész: Kriptográfiai modul megbízható szolgáltatások részére;
- PP-k okoskártyákhoz:
  - CEN EN 419 211-2: Biztonságos aláírás-létrehozó eszköz védelmi profilja – 2. rész: Kulcsgeneráló eszközök;
  - CEN EN 419 211-3: Biztonságosaláírás-létrehozó eszköz védelmi profilja – 3. rész: Kulcsimportáló eszközök.

A kriptográfiai modulhoz való manuális hozzáféréshez kéttényezős hitelesítés szükséges a rendszergazda részéről. Ezenkívül ehhez két illetékességgel bíró személy részvétele szükséges.

A kriptográfiai modul alkalmazásához gondoskodni kell arról, hogy a kulcsok ne legyenek hozzáférhetők a kriptográfiai modulon kívül. A kriptográfiai modulnak tartalmaznia kell egy hozzáférést szabályozó mechanizmust a titkos kulcsok illetéktelen használatának megelőzése érdekében.

6.1.5.2. *Végfelhasználó*

(323) A végfelhasználók számára biztosított kriptográfiai modul az alábbiakra használható:

- a titkos kulcsok létrehozása, használata, kezelése és tárolása;
- véletlenszerű számok létrehozása és használata (a véletlenszerű számok létrehozása funkció értékelésének szerepelnie kell a biztonsági értékelésben és tanúsításban);
- titkos kulcs biztonságos törlése.

(324) A kriptográfiai modult védeni kell az illetéktelen eltávolítás, kiváltás és módosítás ellen. Valamennyi védelmi profilt és a kriptográfiai modul biztonsági tanúsítására érvényes kapcsolódó dokumentumot az ISO 15408-as szabvánnyal összhangban kell értékelni, validálni és tanúsítani a vezető tisztviselők információs rendszerek biztonságával foglalkozó csoportjának (Senior Officials Group on Information Systems Security, SOG-IS) az informatikai biztonságértékelési tanúsítványok kölcsönös elismeréséről szóló megállapodása (Mutual Recognition Agreement of Information Technology

Security Evaluation Certificates) vagy egy, a vonatkozó európai kiberbiztonsági keretrendszerhez tartozó, egyenértékű európai kiberbiztonsági tanúsítási rendszer használatával.

(325) Tekintettel arra, hogy mennyire fontos a lehető legmagasabb biztonsági szint fenntartása, a kriptográfiai modulra vonatkozó biztonsági tanúsítványokat vagy a SOG-IS-megállapodás keretében az irányítóbizottság által elismert megfelelőségértékelő szervezetnek kell kiállítania a közös kritériumokon alapuló tanúsítási rendszer (ISO 15408) szerint, vagy egy tagállam nemzeti kiberbiztonsági tanúsító hatósága által akkreditált megfelelőségértékelő szervezetnek. Az említett megfelelőségértékelő szervezeteknek az SOG-IS kölcsönös elismerési egyezményében meghatározottakkal legalább egyenértékű követelményeknek megfelelően kell végezniük a biztonsági értékelést.

Megjegyzés: a kriptográfiai modul és a C-ITS-állomás közötti kapcsolatot védelemmel kell ellátni.

6.1.6. Titkos kulcsok biztonsági másolatai

(326) A titkos kulcsok biztonsági másolatai létrehozásának, tárolásának és használatának legalább az eredeti kulcsokhoz előírt biztonsági szint követelményeit kell teljesítenie.

(327) A titkos kulcsok biztonsági másolatait a gyökérszintű CA-k, EA-k és AA-k készítik el.

(328) Titkos kulcsokról nem készíthetők biztonsági másolatok az EC-k és AT-k esetén.

6.1.7. Titkos kulcsok megsemmisülése

(329) A gyökérszintű CA-k, EA-k, AA-k, valamint a mobil és fix C-ITS-állomások kötelesek megsemmisíteni titkos kulcsukat és a hozzá tartozó biztonsági másolatokat, ha egy új kulcspár és megfelelő tanúsítvány jön létre és települ sikeresen, és az átfedési idő (ha van ilyen – csak CA) letelt. A titkos kulcsot a kulcs tárolására használt kriptográfiai modul által felajánlott mechanizmus segítségével vagy a 6.1.5.2. szakaszban említett megfelelő PP-ben leírtak szerint kell megsemmisíteni.

6.2. Az aktiválásravonatkozó adatok

(330) A tevékenységre vonatkozó adatok a kriptográfiai moduloknak az illetéktelen hozzáférés megelőzése érdekében való működtetéséhez szükséges hitelesítési tényezőket foglalják magukban. Valamely CA kriptográfiai eszközének tevékenységére vonatkozó adatainak használatához két illetékes személy beavatkozása szükséges.

6.3. Számítógép-biztonsági ellenőrzések

(331) A CA számítógép-biztonsági ellenőrzéseit az ISO/IEC 27002 szabványban foglalt követelmények szerint a legmagasabb biztonsági szinthez kell kialakítani.

6.4. Az életciklus alatti műszaki ellenőrzések

(332) A CA műszaki ellenőrzései a CA teljes életciklusát lefedik. Ez különösen a 6.1.4.3. szakaszban („Kriptoagilitás”) foglalt követelményeket jelenti.

6.5. Hálózatbiztonsági ellenőrzések

(333) A CA-k hálózatait (gyökérszintű CA, EA és AA) az ISO/IEC 27001 és ISO/IEC 27002 szabványok követelményei és alkalmazásra vonatkozó iránymutatásai szerint kell felkészíteni a támadásokra.

(334) A CA hálózatainak elérhetőségét a várható forgalom függvényében kell megtervezni.

7. TANÚSÍTVÁNYPROFILOK, CRL ÉS CTL

7.1. Tanúsítványprofil

(335) Az [5] szerinti tanúsítványprofilokat a TLM-hez, gyökértanúsítványokhoz, EA-tanúsítványokhoz, AA-tanúsítványokhoz, AT-khez és EC-khez kell használni. A nemzeti kormány EA-i más tanúsítványprofilokat használhatnak az EC-khez.

(336) A gyökérszintű CA, EA- és AA-tanúsítványoknak fel kell tüntetniük az arra vonatkozó engedélyeket, hogy mely CA-k (gyökérszintű CA, EA és AA) állíthatnak ki tanúsítványokat.

(337) Az [5] alapján:

- minden egyes gyökérszintű CA-nak a saját aláíró titkos kulcsát kell használnia a CRL-ek kibocsátására;
- a TLM-nek a saját aláíró titkos kulcsát kell használnia a ECTL-ek kibocsátására;

7.2. A tanúsítvány érvényessége

(338) Minden C-ITS-tanúsítványprofilnak tartalmaznia kell egy kibocsátási és lejárati dátumot, ami egyben a tanúsítvány érvényességi idejét is meghatározza. Az egyes PKI-szinteken a tanúsítványokat a lejárat előtt kellő időben kell létrehozni.

(339) A CA- és EC-tanúsítványok érvényességi ideje magában foglalja az átfedési időszakot. A TLM- és gyökérszintű CA-tanúsítványokat a tanúsítványon szereplő kezdési idő alapján az érvényesség kezdete előtt legfeljebb három, legalább egy hónappal kell kibocsátani és az ECTL-en elhelyezni. Ez az előzetes feltöltési szakasznak biztosítosítania kell a tanúsítványok biztonságos kiosztását az összes érintett fél számára a 2.2 szakasznak megfelelően. Ezzel biztosítható, hogy az átfedési időszak elejétől minden érintett fél hitelesíteni tudja az új tanúsítvánnyal kiállított üzeneteit.

(340) Az átfedési időszak elején az egymást követő CA-, EC- és AT-tanúsítványokat ki kell állítani (adott esetben), ki kell osztani és telepíteni kell a megfelelő érintett felek részére. Az átfedési időszak alatt csak az aktuális tanúsítvány használható hitelesítésre.

(341) A 8. táblázatban felsorolt érvényességi idők nem haladhatják meg a felsőbbrendű tanúsítvány érvényességi idejét, ezért az alábbi korlátozások vannak érvényben:

- maximumvalidity(gyökérszintű CA) = privatekeyusage(gyökérszintű CA) + maximumvalidity(EA,AA);
- maximumvalidity(EA) = privatekeyusage(EA) + maximumvalidity(EC);

- maximumvalidity(AA) = privatekeyusage(AA) + preloadingperiod(AT).

(342) A hivatkozási tanúsítványok (gyökérszintű és TLM) érvényessége a megfelelő titkos kulcs használatakor veszi kezdetét és a gyökérszintű CA vagy TLM maximális érvényességi idejének lejártakor ér véget.

(343) A 8. táblázat a C-ITS CA-tanúsítványok maximális érvényességi idejét mutatja (az AT érvényességi idejével kapcsolatban lásd a 7.2.1. szakaszt).

Szervezet	Titkos kulcs max. használati időszaka	Max. érvényességi idő
Gyökérszintű CA	3 év	8 év
EA	2 év	5 év
AA	4 év	5 év
EC	3 év	3 év
TLM	3 év	4 év

8. táblázat: A C-ITS megbízhatósági modellen belüli tanúsítványok érvényességi idői

7.2.1. Álneves tanúsítványok

(344) Ebben a vonatkozásban az álneveket az AT-k alkalmazzák. Ennek megfelelően ez a szakasz az álnevek helyett inkább az AT-kr hivatkozik.

(345) Az ebben a szakaszban megállapított követelmények csak a CAM- és DENM-üzeneteket küldő, helyszíni adatvédelem kockázatát hordozó mobil C-ITS-állomások AT-jaira vonatkozik. A speciális funkciókra használt olyan fix és mobil C-ITS-állomások AT-jaira nem vonatkoznak speciális követelmények, ahol helyszíni adatvédelem kockázata nem merül fel (pl. megjelölt vészhelyzeti és bűnüldöző gépjárművek esetén).

(346) Az alábbi fogalommeghatározások érvényesek:

- „AT-k érvényességi ideje” – az az időszak, amelyben az AT érvényes, vagyis az AT kezdő időpontja és a lejárata közötti időszak;
- „az AT-k előzetes feltöltési időszaka” – az előzetes feltöltés a C-ITS-állomások számára lehetőséget nyújt arra, hogy az érvényességi idő kezdete előtt AT-ket szerezzenek be. Az előzetes feltöltési időszak az a maximálisan megengedett időszak, amely az AT-k igénylésétől a kérelmezett AT érvényességi idejének végéig tart;
- „az AT-k használati ideje” – olyan időszak, amelyben az AT-t ténylegesen CAM-/DENM-üzenetek aláírására használják;
- „a párhuzamos AT-k maximális száma” – az AT-k azon száma, amelyekről valamely C-ITS-állomás egy adott időpontban választhat a CAM-/DENM-üzenetek aláíráskor, vagyis egy C-ITS-állomás részére kibocsátott, egy adott időben érvényes különböző AT-k száma.

(347) Az alábbi követelményeket kell alkalmazni:

- az AT-k előzetes feltöltési időszaka nem lépheti túl a három hónapot;
- az AT-k érvényességi ideje nem haladhatja meg az egy hetet;

- a párhuzamos AT-k maximális száma nem haladhatja meg C-ITS állomásonként a 100-at;
- egy adott AT használati ideje az AT-váltási stratégiától és az adott gépjármű üzemben eltöltött idejétől függ, melyet azonban a párhuzamos AT-k maximális száma és az érvényességi idő korlátoz. Pontosabban egy C-ITS-állomás esetén az átlagos használati idő legalább a gépjármű üzemelési ideje egy érvényességi időn belül osztva a párhuzamos AT-k maximális számával.

7.2.2. Engedélyezési jegyek fix C-ITS-állomásokhoz

(348) A 7.2.1. szakaszban található fogalommeghatározásokat és az alábbi követelményeket kell alkalmazni:

- az AT-k előzetes feltöltési időszaka nem lépheti túl a három hónapot;
- a párhuzamos AT-k maximális száma nem haladhatja meg C-ITS-állomásonként a kettőt;

7.3. A tanúsítványok visszavonása

7.3.1. EA- és AA-tanúsítványok visszavonása

A gyökérszintű CA-, EA- és AA-tanúsítványoknak visszavonhatóknak kell lenniük. A CA-k, EA-k és AA-k visszavont tanúsítványait mielőbb, indokolatlan késedelem nélkül közzé kell tenni egy CRL-en. Ezt a CRL-t a megfelelő gyökérszintű CA-val alá kell írni, és a 7.4. szakaszban leírt profilt kell használni. A gyökérszintű CA-tanúsítványok visszavonásához a megfelelő gyökérszintű CA egy önmagát tartalmazó CRL-t bocsát ki. Ezenkívül biztonsági fenyegetés esetén az 5.7.3. szakaszt kell alkalmazni. A TLM-nek továbbá törölnie kell a visszavont gyökérszintű CA-kat a megbízhatósági listáról, majd új megbízhatósági listát kell kiadnia. A lejárt tanúsítványokat törölni kell a megfelelő CRL-ből és megbízhatósági listáról.

(349) A tanúsítványok visszavonásra kerülnek, ha:

- a gyökérszintű CA-k okkal feltételezik vagy erősen gyanítják, hogy a megfelelő titkos kulcs titkossága sérült;
- a gyökérszintű CA-k értesítést kapnak arról, hogy az előfizetővel kötött szerződés megszűnt;
- a tanúsítványon szereplő információk (pl. név és a CA és az alany kapcsolata) helytelenek vagy megváltoztak;
- olyan biztonsági incidens következik be, amely hatással van a tanúsítvány birtokosára;
- egy ellenőrzés (lásd: 8. szakasz) negatív eredménnyel zárul.

(350) Az előfizetőnek azonnal értesítenie kell a CA-t, ha tudomása van arról, hogy titkos kulcsának titkossága sérült, vagy ezt feltételezi. Gondoskodni kell arról, hogy csak a hitelesített kérelmek eredményezzenek visszavont tanúsítványokat.

7.3.2. A nyilvántartásba vételi hitelesítő adatok visszavonása

(351) Az EC-k visszavonását a C-ITS állomás előfizetője kezdeményezheti (34. lépés), és a visszavonási adatbázisban lévő, időbélyegzővel ellátott belső feketelista hajtja végre, melyet az egyes EA-k hoznak létre és tartanak fenn. A feketelista soha sem kerül közzétételre, azt bizalmasan kell kezelni, és csak a

megfelelő EA használhatja arra, hogy hitelesítse a megfelelő EC-k érvényességét AT-kre és új EC-kre irányuló kérelmeivel összefüggésben.

7.3.3. Az engedélyezési jegyek visszavonása

(352) Tekintettel arra, hogy az AT-kat nem a megfelelő CA-k vonják vissza, rövid élettartammal kell rendelkezniük és nem állíthatók ki az érvényessé válás előtt hosszabb idővel. A tanúsítvány életciklusának megengedett paraméterértékeit a 7.2. szakasz ismerteti.

7.4. Tanúsítvány-visszavonási lista

(353) A gyökérszintű CA-k által kibocsátott CRL formátumát és tartalmát az [1] határozza meg.

7.5. Európai tanúsítványok megbízhatósági listája

(354) A TLM-ek által kibocsátott ECTL formátumát és tartalmát az [1] határozza meg.

8. MEGFELELŐSÉGI AUDIT ÉS MÁS ÉRTÉKELÉSEK

8.1. Az audit tárgyát képező témakörök és az audit alapja

(355) A megfelelőségi audit célja ellenőrizni, hogy a TLM, gyökérszintű CA-k, EA-k és AA-k a jelen hitelesítési házirenddel összhangban működnek-e. A TLM-nek, gyökérszintű CA-knak, EA-knak és AA-knak a CPS-ük ellenőrzésére függetlenül eljáró és akkreditált PKI-ellenőrt kell választaniuk. Az auditot ISO/IEC 27001 és ISO/IEC 27002 szabvány szerinti értékeléssel kell egybekötni.

(356) A megfelelőségi auditot a gyökérszintű CA rendeli meg (13. lépés) magára a gyökérszintű CA-ra, alacsonyabb szintű CA esetén pedig a hozzá tartozó alárendelt EA/AA.

(357) A TLM megfelelőségi auditját a CPA rendeli meg (38. lépés).

(358) Kérésre egy akkreditált PKI-ellenőr megfelelőségi auditot hajt végre az alábbi szintek valamelyikén:

(1) a TLM-ek, gyökérszintű CA-k, EA-k vagy AA-k CPS-ének a jelen hitelesítési házirendnek való megfelelése;

(2) a TLM-ek, gyökérszintű CA-k, EA-k vagy AA-k gyakorlatainak a hozzá tartozó CPS-nek való megfelelése a működést megelőzően;

(3) a TLM-ek, gyökérszintű CA-k, EA-k vagy AA-k gyakorlatainak és operatív tevékenységeinek saját CPS-ének való megfelelése működés közben;

(359) Az audit kiterjed a jelen hitelesítési házirend valamennyi olyan követelményére, amelyet az ellenőrizendő TLM-nek, gyökérszintű CA-knak, EA-knak és AA-knak teljesítenie kell. Az auditnak továbbá ki kell terjednie a CA-nak a C-ITS PKI-ben való működésére – ideértve a CPS-ében említett valamennyi folyamatot, illetve a létesítményeket és felelős személyeket is.

(360) Az akkreditált PKI-ellenőrnek részletes jelentést kell küldenie a gyökérszintű CA (36. lépés), EA, AA vagy CPA (16. és 40. lépés) ellenőrzéséről.

8.2. Az auditok gyakorisága

(361) A gyökérszintű CA-nak, TLM-nek, EA-nak vagy AA-nak az alábbi esetekben kell megfelelőségi auditot rendelnie magára nézve egy független és akkreditált PKI-ellenőrtől:

- az első felállításkor (1. és 2. szintű megfelelőség);
- a hitelesítési házirend bármilyen módosításakor. A CPA-nak meg kell határoznia a tanúsítási házirend változásának tartalmát és a bevezetés időtervét, valamint ennek megfelelően meg kell határoznia a szükséges auditokat (ideértve a szükséges megfelelőségi szintet);
- a CPS-e bármilyen módosításakor (1., 2. és 3. szintű megfelelőség). Mivel a gyökérszintű CA-k működtető szervezetei, a TLM és az EA-k/AA-k döntenek arról, hogy milyen végrehajtási változtatásokat hajtanak végre a CPS-ük frissítését követően, nekik kell megrendelni a megfelelőségi auditot még a változtatások végrehajtása előtt. A CPS kisebb (pl. szerkesztési jellegű) változtatásai esetén a működtető szervezetnek egy megfelelő indoklással ellátott kérelmet kell küldenie a CPA részére jóváhagyásra az 1., 2. vagy 3. szintű megfelelőségi auditok kihagyásához.
- rendszeresen, de legalább három évente a működése alatt (3. szintű megfelelőség).

8.3. Az ellenőr személye/képesítése

(362) Az ellenőrizendő CA-nak egy függetlenül eljáró és akkreditált céget/szervezetet (ellenőrző szerv) vagy akkreditált PKI-ellenőrt kell választania a jelen hitelesítési házirend szerinti auditálására. Az ellenőrző szervet valamely európai akkreditációs tagnak[1] kell akkreditálnia és tanúsítania.

8.4. Az ellenőr és az ellenőrzött szervezet kapcsolata

(363) Az akkreditált PKI-ellenőrnek az ellenőrzött szervezettől függetlennek kell lennie.

8.5. Hiányosság esetén teendő intézkedés

(364) Amennyiben egy auditjelentés azt állapítja meg, hogy a TLM nem megfelelő, akkor a CPA-nak utasítania kell a TLM-et, hogy tegyen azonnali megelőző/korrekciós intézkedéseket.

(365) Ha egy nem megfelelő auditjelentéssel rendelkező gyökérszintű CA új kérelmet nyújt be, akkor a CPA-nak el kell utasítania a kérelmet, és ezt az elutasítást meg kell küldenie a gyökérszintű CA részére (4. lépés). Ebben az esetben a gyökérszintű CA felfüggesztésre kerül. A gyökérszintű CA-nak korrekciós intézkedést kell tennie, újra kell rendelnie az auditot, és új kérelmet kell benyújtania a CPA jóváhagyására. A gyökérszintű CA nem bocsáthat ki tanúsítványokat a felfüggesztés ideje alatt.

(366) Megfelelő gyökérszintű CA audit vagy a gyökérszintű CA CPS-ének módosítása esetén, illetve az auditjelentésben leírt nem megfelelőség jellegétől

[1] Az Európai Akkreditációs Szerv tagjainak listája: http://www.european-accreditation.org/ea-members

függően a CPA dönthet úgy, hogy visszavonja a gyökérszintű CA-t, és e döntését közli a TLM-mel (2. lépés), amely eredményeképp a gyökérszintű CA-tanúsítványát törlik az ECTL-ből, a gyökérszintű CA-t pedig beillesztik a CRL-be. A CPA-nak meg kell küldenie a megfelelő elutasítást a gyökérszintű CA részére (4. lépés). A gyökérszintű CA-nak korrekciós intézkedést kell tennie, teljes auditot kell ismét meg kell rendelnie (1. és 3. szint között), valamint új kérelmet kell benyújtania a CPA jóváhagyására. A CPA ugyanakkor dönthet úgy is, hogy nem vonja vissza a gyökér-CA-t, hanem türelmi időt biztosít, mely alatt a gyökérszintű CA korrekciós intézkedést tehet, ismét megrendelheti az auditot és újból benyújthatja az auditjelentést a CPA-nak. Ebben az esetben a gyökérszintű CA-t fel kell függeszteni, és nem bocsáthat ki tanúsítványokat és CRL-eket.

(367) EA-/AA-audit esetén a gyökérszintű CA-nak el kell döntenie, hogy elfogadja-e a jelentést. Az audit eredményétől függően a gyökérszintű CA-nak el kell döntenie, hogy visszavonja-e az EA-/AA-tanúsítványt a gyökérszintű CA CPS-ében leírt szabályok szerint. A gyökérszintű CA-nak mindenkor biztosítania kell az EA/AA-knak a jelen hitelesítési házirendnek való megfelelőségét.

8.6. Az eredmények közlése

(368) A gyökérszintű CA-nak és a TLM-nek meg kell küldenie az auditjelentést a CPA részére (16. lépés). A gyökérszintű CA és a TLM köteles megőrizni az általa megrendelt auditjelentéseket. Az CPA-nak meg kell küldenie a megfelelő jóváhagyást vagy elutasítást (4. lépés) a gyökér-CA és a TLM részére.

(369) A gyökérszintű CA-nak el kell juttatnia a megfelelőségi tanúsítványt a megfelelő EA/AA részére.

9. EGYÉB RENDELKEZÉSEK

9.1. Díjak

(370) A végrehajtott EU C-ITS megbízhatósági modell egyik elve, hogy a gyökérszintű CA-k együttesen teljes mértékben felelősek a CPA rendszeresen felmerülő működtetési költségeinek és a jelen hitelesítési házirendben meghatározott tevékenységekhez kapcsolódó központi elemeinek (TLM és CPOC) finanszírozásáért.

(371) A gyökérszintű CA-k (ideértve az uniós gyökérszintű CA-t) díjakat szedhetnek a hozzájuk tartozó alacsonyabb szintű CA-któl.

(372) A működési ideje alatt a C-ITS megbízhatósági modell minden résztvevőjének legalább egy gyökérszintű CA-hoz, EA-hoz és AA-hoz kell megkülönböztetésmentesen hozzáféréssel rendelkeznie;

(373) Mindegyik gyökérszintű CA áthárithatja a CPA-ért és a központi elemekért (TLM és CPOC) fizetett díjakat a C-ITS megbízhatósági modell regisztrált résztvevőire – ideértve a nyilvántartásba vett és engedélyezett C-ITS állomásokat is.

9.2. Pénzügyi felelősség

(374) A gyökérszintű CA első létrehozásának legalább három év működést kell magában foglalnia ahhoz, hogy az EU C-ITS megbízhatósági modell tagjává váljon. A gyökérszintű CA működtetője CPS-ének ugyancsak tartalmaznia kell

a gyökérszintű CA visszavonására vagy lezárására vonatkozó részletes rendelkezéseket.

(375) Mindegyik gyökérszintű CA-nak be kell mutatnia a végrehajtó jogi személy pénzügyi fenntarthatóságát legalább három év vonatkozásában. Ennek a pénzügyi fenntarthatósági tervnek a nyilvántartásba vételhez kapcsolódó első dokumentumokban kell szerepelnie, illetve három évente frissíteni kell és a CPA felé jelenteni kell.

(376) Mindegyik gyökérszintű CA-nak évente jelentenie kell az EA-kra/AA-kra és a nyilvántartásba vett és engedélyezett C-ITS állomásokra vonatkozó változtatások szerkezetét a műveleti vezető és a CPA felé a pénzügyi fenntarthatóságának igazolása érdekében.

(377) A gyökérszintű CA-ért, EA-ért, AA-ért és a C-ITS megbízhatósági modell központi elemeiért pénzügyileg és jogilag felelős szervezetnek működési feladatait megfelelő szintű biztosítási fedezettel kell biztosítania, hogy a működési hibákért kártérítést nyújtson és gondoskodjon feladatainak pénzügyi helyreállításért abban az esetben, ha valamely műszaki elem meghibásodna.

9.3. Üzleti információk bizalmas kezelése

(378) Az alábbiakat bizalmasan és titkosan kell kezelni:

- a gyökérszintű CA, EA és AA kérelmeihez tartozó dokumentumok – akár jóváhagyott, akár elutasított;
- a gyökérszintű CA, EA, AA és TLM auditjelentései;
- a gyökérszintű CA, EA, AA, CPOC és TLM katasztrófa utáni helyreállítási tervei;
- a C-ITS megbízhatósági modell elemeihez tartozó titkos kulcsok (C-ITS állomások, TLM, EA, AA és gyökérszintű CA-k);
- minden egyéb, a CPA, gyökérszintű CA-k, EA, AA, TLM és CPOC által bizalmassá minősített információ.

9.4. Titoktartási terv

(379) A gyökérszintű CA-k és az EA-k/AA-k CPS-einek tartalmazniuk kell a személyes adatok kezelésére és az általános adatvédelmi rendelet és más vonatkozó (pl. nemzeti) jogszabályi keretek szerinti adatvédelemre vonatkozó követelményeket.

10. HIVATKOZÁS

Ebben a mellékletben az alábbi hivatkozások szerepelnek.

[1] ETSI TS 102 941 V1.2.1, Intelligens közlekedési rendszerek (ITS) – biztonság, megbízhatóság és adatvédelem kezelése.

[2] ETSI TS 102 940 V1.3.1, Intelligens közlekedési rendszerek (ITS) – biztonság, ITS-kommunikáció biztonsági architektúrája és biztonságirányítása.

[3] Hitelesítési házirend és a hitelesítési gyakorlatok keretrendszere (RFC 3647, 1999).

[4] ETSI TS 102 042 V2.4.1 A nyilvános kulcsokat hiteleső tanúsítványokat kiállító hitelesítő hatóságokra vonatkozó szakpolitikai követelmények.

[5] ETSI TS 103 097 V1.3.1, Intelligens közlekedési rendszerek (ITS) – biztonság, biztonsági fejléc és tanúsítási formátumok.

[6] Calder, A. (2006). Az ISO 27001/ISO 1779 szabványon alapuló információbiztonság: kezelési útmutató. Van Haren Publishing.

[7] ISO, I., & Std, I. E. C. (2011). ISO 27005 (2011) – információs technológia, biztonsági technikák, információbiztonsági kockázatkezelés. ISO.