Kunsill
tal-Unjoni Ewropea

Brussell, 14 ta' Marzu 2019
(OR. en)

7510/19
ADD 3

TRANS 199
DELACT 68

NOTA TA' TRASMISSJONI

minn:	Segretarju Ġenerali tal-Kummissjoni Ewropea, iffirmat mis-Sur Jordi AYET PUIGARNAU, Direttur
lil:	Is-Sur Jeppe TRANHOLM-MIKKELSEN, Segretarju Ġenerali tal-Kunsill tal-Unjoni Ewropea
Nru dok. Cion:	C(2019) 1789 final - Annex 3
Suġġett:	ANNESS tar- Regolament Delegat tal-Kummissjoni li jissupplimenta d-Direttiva 2010/40/UE tal-Parlament Ewropew u tal-Kunsill fir-rigward tal-iskjerament u l-użu operattiv ta' sistemi ta' trasport intelliġenti kooperattivi

Id-delegazzjonijiet għandhom isibu mehmuż id-dokument C(2019) 1789 final - Annex 3.

Mehmuż: C(2019) 1789 final - Annex 3

IL-KUMMISSJONI
EWROPEA

Brussell, 13.3.2019
C(2019) 1789 final

ANNEX 3

ANNESS

tar-

Regolament Delegat tal-Kummissjoni

li jissupplimenta d-Direttiva 2010/40/UE tal-Parlament Ewropew u tal-Kunsill fir-rigward tal-iskjerament u l-użu operattiv ta' sistemi ta' trasport intelliġenti kooperattivi

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

WERREJ

ANNESS III

1. INTRODUZZJONI

1.1. Ħarsa ġenerali u l-ambitu ta' din il-politika

Din il-politika taċ-ċertifikati tiddefinixxi l-mudell ta' fiduċja Ewropew tas-C-ITS ibbażat fuq l-infrastruttura tal-kjavi pubblika (PKI) fl-ambitu tas-sistema ġenerali tal-UE għall-immaniġġjar tal-kredenzjali tas-sigurtà (CCMS tal-UE). Din tiddefinixxi r-rekwiżiti għall-immaniġġjar taċ-ċertifikati tal-kjavi pubblika għal applikazzjonijiet tas-C-ITS minn entitajiet emittenti u l-użu tagħhom minn entitajiet aħħarija fl-Ewropa. Fl-ogħla livell tagħha, il-PKI hi magħmula minn sett ta' root CAs "attivati" wara li l-maniġer tal-lista ta' fiduċja (TLM) idaħħal iċ-ċertifikati tagħhom f'lista ta' fiduċja Ewropea taċ-ċertifikati (ECTL), li hi maħruġa u ppubblikata mit-TLM tal-entità ċentrali (ara t-taqsimiet 1.2 u 1.3).

Din il-politika torbot lill-entitajiet kollha li jieħdu sehem fis-sistema fdata tas-C-ITS fl-Ewropa. Din tgħin fil-valutazzjoni tal-livell ta' fiduċja li jista' jkun stabbilit fl-informazzjoni riċevuta minn xi riċevitur ta' messaġġ awtentikat minn ċertifikat ta' entità aħħarija tal-PKI. Biex tkun tista' ssir il-valutazzjoni tal-fiduċja fiċ-ċertifikati pprovduti mis-CCMS tal-UE, din tistabbilixxi sett ta' rekwiżiti vinkolanti għat-tħaddim tat-TLM tal-entità ċentrali u l-kumpilazzjoni u l-immaniġġjar tal-ECTL. Minħabba f'hekk, dan id-dokument jirregola l-aspetti li ġejjin relatati mal-ECTL:

- l-identifikazzjoni u l-awtentikazzjoni ta' prinċipali li jiksbu rwoli tal-PKI għat-TLM, inkluż dikjarazzjonijiet tal-privileġġi allokati għal kull rwol;
- rekwiżiti minimi għal prattiki tas-sigurtà lokali għat-TLM, inkluż kontrolli fiżiċi, tal-persunal u proċedurali;
- rekwiżiti minimi għal prattiki tas-sigurtà teknika għat-TLM, inkluż is-sigurtà tal-kompjuter, is-sigurtà tan-network u l-kontrolli kriptografiċi tal-inġinerija tal-moduli;
- rekwiżiti minimi għal prattiki operazzjonali għat-TLM, inkluż ir-reġistrazzjoni ta' ċertifikati ġodda ta' root CA, it-tneħħija mir-reġistrazzjoni temporanja jew permanenti tar-root CAs eżistenti inklużi, u l-pubblikazzjoni u d-distribuzzjoni tal-aġġornamenti tal-ECTL;
- profil ECTL, inkluż l-entrati kollha obbligatorji u fakultattivi tad-*data* fl-ECTL, l-algoritmi kriptografiċi li għandhom jintużaw, il-format eżatt tal-ECTL u r-rakkomandazzjonijiet għall-ipproċessar tal-ECTL;
- l-immaniġġjar taċ-ċiklu tal-ħajja taċ-ċertifikat fl-ECTL, inkluż id-distribuzzjoni taċ-ċertifikati fl-ECTL, l-attivazzjoni, l-iskadenza u r-revoka; u
- l-immaniġġjar tar-revoka tal-fiduċja ta' root CAs fejn meħtieġ.

L-affidabbiltà tal-ECTL ma tiddependix biss fuq l-ECTL stess, iżda fil-biċċa l-kbira tkun tiddependi wkoll fuq ir-root CAs li jiffurmaw il-PKI u s-sub-CAs tagħhom, u għalhekk din il-politika tistabbilixxi wkoll rekwiżiti minimi li huma obbligatorji għas-CAs parteċipanti kollha (ir-root CAs u s-sub-CAs). L-oqsma tar-rekwiżiti huma dawn li ġejjin:

- l-identifikazzjoni u l-awtentikazzjoni ta' prinċipali li jiksbu rwoli tal-PKI (eż. uffiċjal tas-sigurtà, uffiċjal tal-privatezza, amministratur tas-sigurtà, amministratur tad-direttorju u utent finali), inkluż dikjarazzjoni tad-dmirijiet,

tar-responsabbiltajiet, tal-obbligazzjonijiet u tal-privileġġi assoċjati ma' kull rwol;

- l-immaniġġjar tal-kjavi, inkluż algoritmi aċċettabbli u obbligatorji għall-iffirmar taċ-ċertifikati u għall-iffirmar tad-*data*, u l-perjodi ta' validità taċ-ċertifikati;
- rekwiżiti minimi għal prattiki tas-sigurtà lokali, inkluż kontrolli fiżiċi, tal-persunal u proċedurali;
- rekwiżiti minimi għal prattiki tas-sigurtà teknika bħas-sigurtà tal-kompjuter, is-sigurtà tan-network u l-kontrolli kriptografiċi tal-inġinerija tal-moduli;
- rekwiżiti minimi għal prattiki operazzjonali tas-CA, EA, AA u entitajiet aħħarija, inkluż aspetti tar-reġistrazzjoni, tat-tneħħija mir-reġistrazzjoni (jiġifieri t-tneħħija mill-elenkar), tar-revoka, tal-kompromess tal-kjavi, tat-tkeċċija għal xi kawża, tal-aġġornament taċ-ċertifikat, tal-prattiki tal-awditjar u tan-nuqqas ta' żvelar ta' informazzjoni relatata mal-privatezza;
- profil taċ-ċertifikat u tas-CRL, inkluż il-formati, l-algoritmi aċċettabbli, l-oqsma tad-*data* obbligatorji u fakultattivi u l-entrati tal-valuri validi tagħhom, u kif il-verifikaturi huma mistennija jipproċessaw iċ-ċertifikati;
- id-dmirijiet ta' monitoraġġ, rapportar, twissija u restawr regolari tal-entitajiet ta' mudell ta' fiduċja tas-C-ITS biex tiġi stabbilita operazzjoni sigura, inkluż f'każijiet ta' mġiba ħażina.

Flimkien ma' dawn ir-rekwiżiti minimi, l-entitajiet li jmexxu r-root CAs u s-sub-CAs jistgħu jiddeċiedu rekwiżiti addizzjonali tagħhom stess u jistabbilixxuhom fid-dikjarazzjonijiet rilevanti dwar il-prattika taċ-ċertifikat (CPSs), diment li dawn ma jkunux jikkontradixxu r-rekwiżiti stabbiliti fil-politika taċ-ċertifikati. Ara t-taqsima 1.5 għal dettalji dwar kif is-CPSs jiġu awditjati u ppubblikati.

Is-CP tiddikjara wkoll l-għanijiet li għalihom jistgħu jintużaw ir-root CAs, is-sub-CAs u ċ-ċertifikati maħruġa tagħhom. Din tistabbilixxi r-responsabbiltajiet preżunti minn:

- it-TLM;
- kull root CA li ċ-ċertifikati tagħha huma elenkati fl-ECTL;
- is-sub-CAs tar-root CA (EA u AA); u
- kull membru jew organizzazzjoni responsabbli għal xi waħda mill-entitajiet tal-mudell ta' fiduċja tas-C-ITS, jew li joperawha.

Is-CP tiddefinixxi wkoll obbligi obbligatorji li japplikaw għal:

- it-TLM;
- kull root CA li ċ-ċertifikati tagħha huma elenkati fl-ECTL;
- kull sub-CA ċċertifikata b'root CA;
- l-entitajiet aħħarija kollha; u
- kull organizzazzjoni membru responsabbli għal xi waħda mill-entitajiet tal-mudell ta' fiduċja tas-C-ITS, jew li toperaha.

Finalment, is-CP tistabbilixxi r-rekwiżiti fir-rigward tad-dokumentazzjoni tal-limitazzjonijiet għar-responsabbiltajiet u l-obbligi fis-CPS ta' kull root CA li ċ-ċertifikati tagħha huma elenkati fl-ECTL.

Din is-CP hi konformi mal-politika taċ-ċertifikati u mal-qafas tal-prattiki taċ-ċertifikazzjoni adottat mill-Internet Engineering Task Force (IETF) [3].

1.2. Definizzjonijiet u akronimi

Japplikaw id-definizzjonijiet fil-punti [2], [3] u [4].

AA	awtorità tal-awtorizzazzjoni
AT	biljett ta' awtorizzazzjoni
CA	awtorità taċ-ċertifikazzjoni
CP	politika taċ-ċertifikati
CPA	awtorità tal-politika taċ-ċertifikati tas-C-ITS
CPOC	punt ta' kuntatt tas-C-ITS
CPS	dikjarazzjoni dwar il-prattika taċ-ċertifikati
CRL	lista tar-revoka taċ-ċertifikati
EA	awtorità tar-reġistrazzjoni
EC	kredenzjali għar-reġistrazzjoni
ECIES	skema integrata ta' kriptaġġ tal-kurva ellittika
EE	entità aħħarija (jiġifieri stazzjon tas-C-ITS)
ECTL	lista ta' fiduċja Ewropea taċ-ċertifikati
CCMS tal-UE	sistema tal-immaniġġjar tal-kredenzjali tas-sigurtà tas-C-ITS tal-UE
GDPR	Ir-Regolament Ġenerali dwar il-Protezzjoni tad-*Data*
HSM	Modulu tas-sigurtà tal-ħardwer
PKI	infrastruttura tal-kjavi pubblika
RA	awtorità tar-reġistrazzjoni
sub-CA	EA u AA
TLM	maniġer tal-lista ta' fiduċja

Glossarju

applikant	Il-persuna fiżika jew l-entità ġuridika li tapplika għal ċertifikat (jew li tipprova ġġeddu). Ladarba jinħoloq iċ-ċertifikat inizjali (l-inizjalizzazzjoni), l-applikant jibda jissejjaħ l-abbonat. Għal ċertifikati maħruġa lill-entitajiet aħħarija, l-abbonat (l-applikant għaċ-ċertifikat) hu l-entità li tikkontrolla jew topera/tmantni l-entità aħħarija li lilha jinħareġ iċ-ċertifikat, anke jekk l-entità aħħarija tkun hi li qed tibgħat it-talba proprja għaċ-ċertifikat.
awtorità tal-awtorizzazzjoni	F'dan id-dokument, it-terminu "awtorità tal-awtorizzazzjoni" (AA) jirreferi mhux biss għall-funzjoni speċifika tal-AA, iżda anki għall-entità ġuridika u/jew operazzjonali li timmaniġġjaha.
awtorità taċ-ċertifikazzjoni	L-awtorità taċ-ċertifikazzjoni root, l-awtorità tar-reġistrazzjoni u l-awtorità tal-awtorizzazzjoni huma kumulattivament imsejħa l-awtorità taċ-ċertifikazzjoni (CA).
mudell ta' fiduċja tas-C-ITS	Il-mudell ta' fiduċja tas-C-ITS hu responsabbli biex jistabbilixxi relazzjoni ta' fiduċja bejn l-istazzjonijiet tas-C-ITS. Dan jiġi implimentat bl-użu ta' PKI magħmula minn root CAs, is-CPOC, it-TLM, l-EAs, l-AAs u network sigur.
aġilità kriptografika	Il-kapaċità tal-entitajiet tal-mudell ta' fiduċja tas-C-ITS li jadattaw is-CP għal ambjenti li jinbidlu jew għal rekwiżiti futuri ġodda, eż. b'tibdil fl-algoritmi kriptografiċi u fit-tul tal-kjavi matul iż-żmien
modulu kriptografiku	Element sigur ibbażat fuq il-ħardwer li fih jiġu ġġenerati u/jew maħżuna kjavi, jiġu ġġenerati numri każwali u tiġi ffirmata jew kriptata id-*data*.
awtorità tar-reġistrazzjoni	F'dan id-dokument, it-terminu "awtorità tar-reġistrazzjoni" (EA) jirreferi mhux biss għall-funzjoni speċifika tal-EA, iżda anki għall-entità ġuridika u/jew operazzjonali li timmaniġġjaha.
Parteċipanti tal-PKI	Entitajiet tal-mudell ta' fiduċja tas-C-ITS, jiġifieri t-TLM, ir-root CAs, l-EAs, l-AAs u l-istazzjonijiet tas-C-ITS.
rikjavar	Dan is-sottokomponent jintuża biex jiddeskrivi ċerti elementi relatati ma' abbonat jew parteċipant ieħor li jiġġenera par kjavi ġdid u japplika għall-ħruġ ta' ċertifikat ġdid li jiċċertifika l-kjavi pubblika l-ġdida, kif deskritt fi [3].
repożitorju	Ir-repożitorju użat għall-ħażna taċ-ċertifikati u l-informazzjoni dwar iċ-ċertifikati pprovduti mill-entitajiet tal-mudell ta' fiduċja tas-C-ITS, kif definit fit-taqsima 2.3.
awtorità taċ-ċertifikazzjoni root	F'dan id-dokument, it-terminu "awtorità taċ-ċertifikazzjoni root" (CA) jirreferi mhux biss għall-funzjoni speċifika tas-CA, iżda anki għall-entità ġuridika u/jew operazzjonali li timmaniġġjaha.
suġġett	Il-persuna fiżika, l-apparat, is-sistema, l-unità jew l-entità ġuridika identifikati f'ċertifikat bħala s-suġġett, jiġifieri l-abbonat jew apparat fil-kontroll u t-tħaddim tal-abbonat.
abbonat	Persuna fiżika jew entità ġuridika li lilha jinħareġ ċertifikat u li hi marbuta legalment minn abbonat jew minn ftehim dwar it-termini tal-użu.
ftehim tal-abbonat	Ftehim bejn is-CA u l-applikant/l-abbonat li jispeċifika d-drittijiet u r-responsabbiltajiet tal-partijiet.

1.3. Parteċipanti tal-PKI

1.3.1. Introduzzjoni

Il-parteċipanti tal-PKI għandhom rwol fil-PKI kif definit minn din il-politika. Sakemm ma jkunx ipprojbit espliċitament, parteċipant jista' jassumi diversi rwoli fl-istess ħin. Jista' jkun ipprojbit milli jassumi rwoli speċifiċi fl-istess ħin biex jiġu evitati kunflitti ta' interess jew biex tkun żgurata s-segregazzjoni tad-dmirijiet.

Il-parteċipanti jistgħu wkoll jiddelegaw partijiet mir-rwol tagħhom lil entitajiet oħra bħala parti minn kuntratt ta' servizz. Pereżempju, meta tiġi pprovduta informazzjoni dwar l-istatus tar-revoka bl-użu ta' CRLs, is-CA hi wkoll l-emittent tas-CRL iżda tista' tiddelega r-responsabbiltà għall-ħruġ tas-CRLs lil entità differenti.

Ir-rwoli tal-PKI jikkonsistu minn:

- rwoli awtorevoli, jiġifieri kull rwol hu istanzjat b'mod uniku;
- rwoli operazzjonali, jiġifieri rwoli li jistgħu jiġu istanzjati f'entità waħda jew aktar.

Pereżempju, root CA jista' jiġi implimentat minn entità kummerċjali, grupp ta' interess komuni, organizzazzjoni nazzjonali u/jew organizzazzjoni Ewropea.

Il-Grafika 1 turi l-arkitettura tal-mudell ta' fiduċja tas-C-ITS ibbażata fuq [2]. L-arkitettura hi deskritta fil-qosor hawnhekk, iżda l-elementi prinċipali huma deskritti f'aktar dettall fit-taqsimiet 1.3.2 sa 1.3.6.

Is-CPA taħtar lit-TLM, li għalhekk hu entità fdata għall-parteċipanti kollha tal-PKI. Is-CPA tapprova l-operazzjoni tar-root CA u tikkonferma li t-TLM jista' jafda lir-root CA(s). It-TLM joħroġ l-ECTL li jipprovdi il-parteċipanti kollha tal-PKI b'fiduċja fir-root CAs approvati. Ir-root CA toħroġ ċertifikati lill-EA u lill-AA, u b'hekk tipprovdi fiduċja fl-operat tagħhom. L-EA toħroġ ċertifikati ta' reġistrazzjoni lill-istazzjonijiet tas-C-ITS mittenti u trażmittenti (bħall-entitajiet aħħarija), u b'hekk tipprovdi fiduċja fl-operazzjoni tagħhom. L-AA toħroġ ATs lill-istazzjonijiet tas-C-ITS abbażi tal-fiduċja fl-EA.

L-istazzjon tas-C-ITS li jirċievi u jittrażmetti (bħala l-parti tat-trażmissjoni) jista' jafda stazzjonijiet tas-C-ITS oħra, għax l-ATs jinħarġu minn AA li hi fdata minn root CA, li hi fdata mit-TLM u s-CPA.

Ta' min wieħed jinnota li l-Grafika 1 tiddeskrivi biss il-livell tar-root CA tal-mudell ta' fiduċja tas-C-ITS. Id-dettalji tas-saffi ta' taħt huma pprovduti fit-taqsimiet sussegwenti ta' din is-CP jew fis-CPS tar-root CAs speċifiċi.

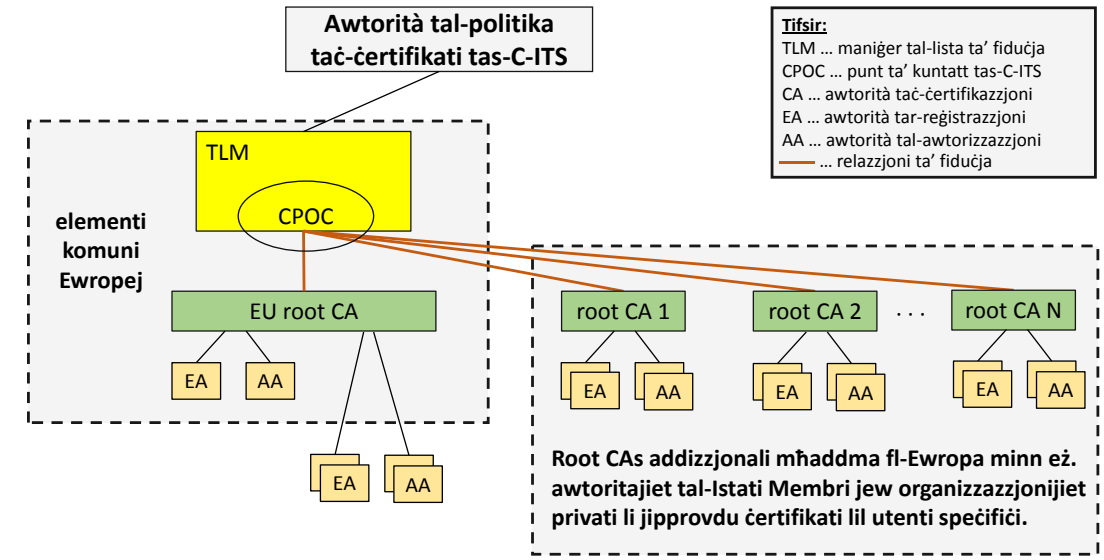
Il-Grafika 2 tipprovdi ħarsa ġenerali tal-flussi tal-informazzjoni bejn il-parteċipanti tal-PKI. It-tikek ħodor jindikaw flussi li jeħtieġu komunikazzjoni bejn magna u oħra. Il-flussi tal-informazzjoni bl-aħmar għandhom rekwiżiti tas-sigurtà definiti.

Il-mudell ta' fiduċja tas-C-ITS hu bbażat fuq arkitettura b'root CAs multipli, fejn iċ-ċertifikati tar-root CA huma trażmessi perjodikament (kif stabbilit hawn taħt) lill-punt ċentrali ta' kuntatt (is-CPOC) permezz ta' protokoll sigur (eż. ċertifikati tal-konnessjoni) iddefinit mis-CPOC.

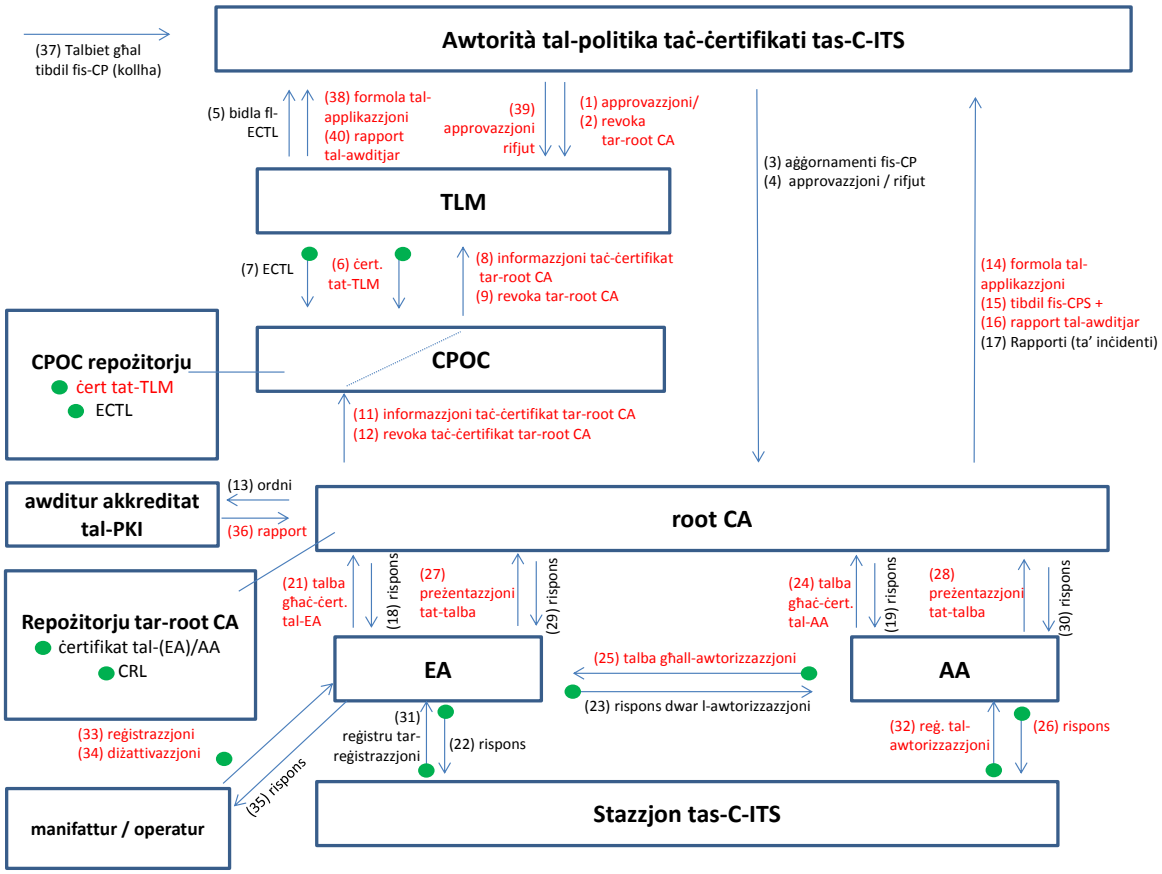
Ir-root CA tista' titħaddem minn organizzazzjoni governattiva jew privata. L-arkitettura tal-mudell ta' fiduċja tas-C-ITS fiha mill-anqas root CA waħda (ir-root CA tal-UE bl-istess livell bħar-root CAs l-oħra). Ir-root CA tal-UE hi ddelegata mill-entitajiet kollha li jipparteċipaw fil-mudell ta' fiduċja tas-C-ITS li ma jridux

jistabbilixxu r-root CA tagħhom stess. Is-CPOC jittrażmetti ċ-ċertifikati tar-root CA li jirċievi lit-TLM, li hu responsabbli mill-ġbir u mill-iffirmar tal-lista taċ-ċertifikati tar-root CA u biex jibgħathom lura lis-CPOC, li jagħmilhom pubblikament disponibbli għal kulħadd (ara hawn taħt).

Ir-relazzjonijiet ta' fiduċja bejn l-entitajiet fil-mudell ta' fiduċja tas-C-ITS huma deskritti fil-grafiki, fit-tabelli u fit-taqsimiet li ġejjin.



Grafika 1: arkitettura tal-mudell ta' fiduċja tas-C-ITS



Grafika 2: flussi tal-informazzjoni tal-mudell ta' fiduċja tas-C-ITS

ID tal-fluss	Minn	Sa	Kontenut	Referenza
(1).	CPA	TLM	approvazzjoni tal-applikazzjoni tar-root CA	8
(2).	CPA	TLM	informazzjoni dwar ir-revoka tar-root CA	8.5
(3).	CPA	root CA	aġġornamenti tas-CP	1.5
(4).	CPA	root CA	approvazzjoni/rifjut tal-formola tal-applikazzjoni tar-root CA jew it-tibdil fit-talba tas-CPS jew il-proċess tal-awditjar.	8.5, 8.6
(5).	TLM	CPA	notifika ta' tibdil fl-ECTL	4, 5.8.1
(6).	TLM	CPOC	ċertifikat tat-TLM	4.4.2
(7).	TLM	CPOC	ECTL	4.4.2
(8).	CPOC	TLM	informazzjoni dwar iċ-ċertifikat tar-root CA	4.3.1.1
(9).	CPOC	TLM	revoka taċ-ċertifikat tar-root CA	7.3
(10).	CPOC	l-entitajiet aħħarija kollha	ċertifikat tat-TLM	4.4.2
(11).	root CA	CPOC	informazzjoni dwar iċ-ċertifikat tar-root CA	4.3.1.1
(12).	root CA	CPOC	revoka taċ-ċertifikat tar-root CA	7.3
(13).	root CA	awditur	ordni tal-awditjar	8
(14).	root CA	CPA	formola tal-applikazzjoni tar-root CA — talba inizjali	4.1.2.1
(15).	root CA	CPA	formola tal-applikazzjoni tar-root CA — tibdil tas-CPS	1.5.1
(16).	root CA	CPA	formola tal-applikazzjoni tar-root CA — rapport tal-awditjar	8.6
(17).	root CA	CPA	rapporti tal-inċidenti tar-root CA, inkluż ir-revoka ta' sub-CA (EA, AA)	l-Anness III, 7.3.1
(18).	root CA	EA	rispons dwar iċ-ċertifikat tal-EA	4.2.2.3
(19).	root CA	AA	rispons dwar iċ-ċertifikat tal-AA	4.2.2.3
(20).	root CA	Kollha	ċertifikat tal-EA/AA, CRL	4.4.2
(21).	EA	root CA	talba għal ċertifikat tal-EA	4.2.2.3
(22).	EA	Stazzjon tas-C-ITS	rispons dwar il-kredenzjali għar-reġistrazzjoni	4.3.1.4
(23).	EA	AA	rispons dwar l-awtorizzazzjoni	4.2.2.5
(24).	AA	root CA	talba għal ċertifikat tal-AA	4.2.2.3
(25).	AA	EA	talba ta' awtorizzazzjoni	4.2.2.5
(26).	AA	Stazzjon tas-C-ITS	rispons dwar il-biljett tal-awtorizzazzjoni	4.3.1.5
(27).	EA	root CA	preżentazzjoni tat-talba	4.1.2.3

(28).	AA	root CA	preżentazzjoni tat-talba	4.1.2.3
(29).	root CA	EA	rispons	4.12 u 4.2.1
(30).	root CA	AA	rispons	4.12 u 4.2.1
(31).	Stazzjon tas-C-ITS	EA	talba għall-kredenzjali għar-reġistrazzjoni	4.2.2.4
(32).	Stazzjon tas-C-ITS	AA	talba għall-biljett tal-awtorizzazzjoni	4.2.2.5
(33).	manifattur / operatur	EA	reġistrazzjoni	4.2.1.4
(34).	manifattur / operatur	EA	diżattivazzjoni	7.3
(35).	EA	manifattur / operatur	rispons	4.2.1.4
(36).	awditur	root CA	rapport	8.1
(37).	kollha	CPA	talbiet għal tibdil fis-CP	1.5
(38).	TLM	CPA	formola tal-applikazzjoni	4.1.2.2
(39).	CPA	TLM	approvazzjoni/rifjut	4.1.2.2
(40).	TLM	CPA	rapport tal-awditjar	4.1.2.2

Tabella 1: Deskrizzjoni dettaljata tal-flussi tal-informazzjoni fil-mudell ta' fiduċja tas-C-ITS

1.3.2. Awtorità tal-politika taċ-ċertifikati tas-C-ITS

(1) L-awtorità tal-politika taċ-ċertifikati tas-C-ITS (CPA) hi magħmula mir-rappreżentanti tal-partijiet konċernati pubbliċi u privati (eż. Stati Membri, manifatturi tal-vetturi, eċċ.) li jipparteċipaw fil-mudell ta' fiduċja tas-C-ITS. Din responsabbli għal żewġ sub-irwoli:

(1) l-immaniġġjar tal-politika taċ-ċertifikati, inkluż:

- l-approvazzjoni ta' din is-CP u tat-talbiet futuri għal tibdil fis-CP;
- id-deċiżjoni dwar ir-reviżjoni tat-talbiet għal tibdil fis-CP u tar-rakkomandazzjonijiet ippreżentati minn parteċipanti jew entitajiet oħra tal-PKI;
- id-deċiżjoni dwar ir-rilaxx ta' verżjonijiet ġodda tas-CP;

(2) l-immaniġġjar tal-awtorizzazzjoni tal-PKI, inkluż:

- id-definizzjoni, id-deċiżjoni u l-pubblikazzjoni tal-approvazzjoni tas-CPS u l-proċeduri tal-awditjar tas-CA (kollettivament imsejħa "proċeduri tal-approvazzjoni tas-CA");
- l-awtorizzazzjoni tas-CPOC biex jopera u jirrapporta regolarment;
- l-awtorizzazzjoni tat-TLM biex jopera u jirrapporta regolarment;
- l-approvazzjoni tas-CPS tar-root CA, jekk tkun konformi mas-CP komuni u valida;

- l-iskrutinju tar-rapporti tal-awditjar mill-awditur akkreditat tal-PKI għar-root CAs kollha;
- in-notifika lit-TLM dwar il-lista tar-root CAs approvati jew mhux approvati u ċ-ċertifikati tagħhom abbażi tar-rapporti riċevuti tal-approvazzjoni tar-root CAs u rapporti regolari tal-operazzjonijiet.

(2) Ir-rappreżentant awtorizzat tas-CPA hu responsabbli mill-awtentikazzjoni tar-rappreżentant awtorizzat tat-TLM u mill-approvazzjoni tal-formola tal-applikazzjoni għall-proċess tar-reġistrazzjoni tat-TLM. Is-CPA hi responsabbli biex tawtorizza lit-TLM jopera kif imsemmi f'din it-taqsima.

1.3.3. Maniġer tal-lista ta' fiduċja

(3) It-TLM hu entità waħda maħtura mis-CPA.

(4) It-TLM hu responsabbli:

- biex iħaddem l-ECTL skont is-CP komuni valida u jirrapporta b'mod regolari dwar l-attività lis-CPA għall-operazzjoni sigura ġenerali tal-mudell ta' fiduċja tas-C-ITS;
- biex jirċievi ċ-ċertifikati tar-root CA mis-CPOC;
- biex jinkludi/jeskludi ċ-ċertifikati tar-root CA fl-ECTL man-notifika mis-CPA;
- biex jiffirma l-ECTL; u
- mit-trażmissjoni regolari u f'waqtha tal-ECTL lis-CPOC.

1.3.4. Awditur akkreditat tal-PKI

(5) L-awditur akkreditat tal-PKI hu responsabbli minn:

- it-twettiq jew l-organizzazzjoni tal-awditjar tar-root CAs, tat-TLM u tas-sub-CAs; u
- id-distribuzzjoni tar-rapport tal-awditjar (minn awditjar inizjali jew perjodiku) lis-CPA b'konformità mar-rekwiżiti fit-taqsima 8 hawn taħt. Ir-rapport tal-awditjar għandu jinkludi rakkomandazzjonijiet mill-awditur akkreditat tal-PKI;
- biex jinnotifika lill-entità li timmaniġġja r-root CA dwar it-twettiq b'suċċess jew bla suċċess ta' awditjar inizjali jew perjodiku tas-sub-CAs;
- jivvaluta l-konformità tas-CPSs ma' din is-CP.

1.3.5. Punt ta' kuntatt tas-C-ITS (CPOC)

(6) Is-CPOC hu entità waħda maħtura mis-CPA. Ir-rappreżentant awtorizzat tas-CPA hu responsabbli mill-awtentikazzjoni tar-rappreżentant awtorizzat tas-CPOC u mill-approvazzjoni tal-formola tal-applikazzjoni għall-proċess tar-reġistrazzjoni tas-CPOC. Is-CPA hi responsabbli biex tawtorizza lis-CPOC jopera kif stabbilit f'din it-taqsima.

(7) Is-CPOC hu responsabbli biex:

- jistabbilixxi u jikkontribwixxi għall-iskambju sigur tal-komunikazzjoni bejn l-entitajiet kollha tal-mudell ta' fiduċja tas-C-ITS b'mod effiċjenti u veloċi;

- jirrevedi talbiet għal tibdil proċedurali u rakkomandazzjonijiet ippreżentati minn parteċipanti oħra tal-mudell ta' fiduċja (eż. ir-root CAs);
- jittrażmetti ċ-ċertifikati tar-root CAs lit-TLM;
- jippubblika l-ankra komuni ta' fiduċja (il-kjavi pubblika attwali u ċ-ċertifikat tal-konnessjoni tat-TLM); u
- jippubblika l-ECTL.

Dettalji sħaħ tal-ECTL jinsabu fit-taqsima 7.

1.3.6. Rwoli operazzjonali

(8) L-entitajiet li ġejjin, iddefiniti fi [2], jaqdu rwol operazzjonali, kif definit fl-RFC 3647:

Element funzjonali	Rwol PKI ([3] u [4])	Rwol dettaljat ([2])
awtorità taċ-ċertifikazzjoni root	CA/RA (awtorità tar-reġistrazzjoni)	Tipprovdi prova lill-EA u lill-AA biex tkun tista' toħroġ ECs jew ATs
awtorità tar-reġistrazzjoni	abbonat għar-root CA / suġġett taċ-ċertifikat tal-EA CA/RA	tawtentika stazzjon tas-C-ITS u tagħtih aċċess għall-komunikazzjonijiet tal-ITS
awtorità tal-awtorizzazzjoni	abbonat għar-root CA / suġġett taċ-ċertifikat tal-AA CA/RA	tipprovdi stazzjon tas-C-ITS bi prova awtorevoli li jista' juża servizzi speċifiċi tal-ITS
stazzjon tas-C-ITS mittenti	suġġett taċ-ċertifikat (EC) tal-entità aħħarija (EE)	takkwista drittijiet mill-EA biex taċċessa l-komunikazzjonijiet tal-ITS tinnegozja d-drittijiet mill-AA biex tinvoka s-servizzi tal-ITS tibgħat messaġġi ta' komunikazzjoni single-hop u trażmessi
stazzjon tas-C-ITS tat-trażmissjoni (li jgħaddi l-messaġġ)	parti tat-trażmissjoni / suġġett taċ-ċertifikat tal-EE	tirċievi messaġġ ta' komunikazzjoni mill-istazzjon tas-C-ITS mittenti u tgħaddih lill-istazzjon tas-C-ITS riċeventi jekk ikun meħtieġ
stazzjon tas-C-ITS riċeventi	parti tat-trażmissjoni	tirċievi messaġġi ta' komunikazzjoni mill-istazzjon tas-C-ITS mittenti jew trażmittenti
manifattur	abbonat għall-EA	jinstalla l-informazzjoni meħtieġa għall-immaniġġjar tas-sigurtà fl-istazzjon tas-C-ITS waqt il-produzzjoni
operatur	abbonat għall-EA / AA	jinstalla u jaġġorna l-informazzjoni meħtieġa għall-imaniġġjar tas-sigurtà fl-istazzjon tas-C-ITS waqt it-tħaddim

Tabella 2: Rwoli operazzjonali

Nota: skont [4], jintużaw termini differenti f'din is-CP għall-"abbonat" li jikkuntratta mas-CA għall-ħruġ ta' ċertifikati u għas-"suġġett" li għalih japplika ċ-ċertifikat. L-abbonati huma l-entitajiet kollha li għandhom relazzjoni kuntrattwali ma' CA. Is-suġġetti huma l-entitajiet li għalihom japplika ċ-ċertifikat. L-EA/AAs huma abbonati u suġġetti tar-root CA u jistgħu jitolbu ċertifikati tal-EA/AA. L-istazzjonijiet tas-C-ITS huma suġġetti u jistgħu jitolbu ċertifikati tal-entità aħħarija.

(9) Awtoritajiet tar-reġistrazzjoni:

L-EA għandha twettaq ir-rwol tal-awtorità tar-reġistrazzjoni għall-entitajiet aħħarija. Abbonat awtentikat u awtorizzat biss jista' jirreġistra entitajiet aħħarija ġodda (stazzjonijiet tas-C-ITS) fl-EA. Ir-root CAs rilevanti għandhom iwettqu r-rwol tal-awtoritajiet tar-reġistrazzjoni għall-EAs u l-AAs.

1.4. Użu taċ-ċertifikat

1.4.1. Dominji applikabbli tal-użu

(10) Iċ-ċertifikati maħruġa b'din is-CP huma maħsuba biex jintużaw biex jivvalidaw il-firem diġitali fil-kuntest tal-komunikazzjoni kooperattiva tal-ITS skont l-arkitettura ta' referenza ta' [2].

(11) Il-profili taċ-ċertifikat f'[5] jiddeterminaw l-użi taċ-ċertifikat għat-TLM, ir-root CAs, l-EAs, l-AAs u l-entitajiet aħħarija.

1.4.2. Limiti tar-responsabbiltà

(12) Iċ-ċertifikati mhumiex maħsuba, u lanqas awtorizzati, għall-użu:

- f'ċirkostanzi li jmorru kontra jew jiksru kwalunkwe liġi, regolament (eż. il-GDPR), digriet jew ordni tal-gvern applikabbli;
- f'ċirkostanzi li jiksru jew ma josservawx d-drittijiet ta' ħaddieħor;
- bi ksur ta' din is-CP jew tal-ftehim tal-abbonat rilevanti;
- f'ċirkostanzi meta l-użu tagħhom jista' jwassal direttament għal mewt, korriment personali jew ħsara ambjentali gravi (eż. permezz ta' falliment fl-operazzjoni ta' faċilitajiet nukleari, navigazzjoni jew komunikazzjoni tal-inġenji tal-ajru, jew sistemi ta' kontroll tal-armi);
- f'ċirkostanzi li jmorru kontra l-għanijiet ġenerali ta' sikurezza aħjar fit-toroq u trasport bit-triq aktar effiċjenti fl-Ewropa.

1.5. Amministrazzjoni tal-politika taċ-ċertifikati

1.5.1. Aġġornament tas-CPSs tas-CAs elenkati fl-ECTL

(13) Kull root CA elenkata fl-ECTL għandha tippubblika s-CPS tagħha stess, li għandha tkun konformi ma' din il-politika. Ir-root CA tista' żżid rekwiżiti addizzjonali, iżda għandha tiżgura li r-rekwiżiti kollha ta' din is-CP jiġu ssodisfati f'kull ħin.

(14) Kull root CA elenkata fl-ECTL għandha timplimenta proċess ta' bidla xieraq għad-dokument tas-CPS tagħha. Il-karatteristiċi ewlenin tal-proċess tal-bidla għandhom jiġu ddokumentati fil-parti pubblika tas-CPS.

(15) Il-proċess tal-bidla għandu jiżgura li l-bidliet kollha f'din is-CP jiġu analizzati bir-reqqa u, jekk meħtieġ għall-konformità mas-CP kif emendata, is-CPS tiġi aġġornata fit-terminu ta' żmien stabbilit fl-istadju tal-implimentazzjoni tal-proċess tal-bidla għas-CP. B'mod partikolari, il-proċess tal-bidla għandu jinvolvi proċeduri ta' tibdil ta' emerġenza li jiżguraw l-implimentazzjoni f'waqtha ta' bidliet rilevanti għas-sigurtà fis-CP.

(16) Il-proċess tal-bidla għandu jinkludi miżuri xierqa li jivverifikaw il-konformità tas-CP għall-bidliet kollha fis-CPS. Kull bidla fis-CPS għandha tiġi ddokumentata b'mod ċar. Qabel ma tiġi implimentata verżjoni ġdida tas-CPS,

il-konformità tagħha mas-CP għandha tiġi kkonfermata minn awditur akkreditat tal-PKI.

(17) Ir-root CA għandha tinnotifika lis-CPA bi kwalunkwe bidla li ssir fis-CPS b'tal-anqas l-informazzjoni li ġejja:

- deskrizzjoni eżatta tal-bidla;
- ir-raġunament għall-bidla;
- rapport mingħand l-awditur akkreditat tal-PKI li jikkonferma l-konformità mas-CP;
- id-dettalji ta' kuntatt tal-persuna responsabbli mis-CPS;
- l-iskeda taż-żmien ippjanata għall-implimentazzjoni.

1.5.2. Proċeduri tal-approvazzjoni tas-CPS

(18) Qabel ma tibda l-operazzjonijiet tagħha, ir-root CA prospettiva għandha tippreżenta s-CPS tagħha lil awditur akkreditat tal-PKI bħala parti minn ordni għall-awditjar tal-konformità (il-fluss 13) u lis-CPA għall-approvazzjoni (il-fluss 15).

(19) Ir-root CA għandha tippreżenta t-tibdil fis-CPS tagħha lil awditur akkreditat tal-PKI bħala parti minn ordni għall-awditjar tal-konformità (il-fluss 13) u lis-CPA għall-approvazzjoni (il-fluss 15) qabel ma jsir dan it-tibdil.

(20) L-EA/l-AA għandha tippreżenta s-CPS tagħha jew it-tibdil fis-CPS tagħha lir-root CA. Ir-root CA tista' tordna ċertifikat ta' konformità mingħand il-korp nazzjonali jew entità privata responsabbli għall-approvazzjoni tal-EA/AA, kif iddefinit fit-taqsimiet 4.1.2 u 8.

(21) L-awditur akkreditat tal-PKI għandu jivvaluta s-CPS skont it-taqsima 8.

(22) L-awditur akkreditat tal-PKI għandu jikkomunika r-riżultati tal-valutazzjoni tas-CPS bħala parti mir-rapport tal-awditjar, kif stabbilit fit-taqsima 8.1. Is-CPS għandha tiġi aċċettata jew rifjutata bħala parti mill-aċċettazzjoni tar-rapport tal-awditjar imsemmi fit-taqsimiet 8.5 u 8.6.

2. RESPONSABBILTAJIET TA' PUBBLIKAZZJONI U REPOŻITORJU

2.1. Metodi għall-pubblikazzjoni tal-informazzjoni taċ-ċertifikati

(23) L-informazzjoni taċ-ċertifikat tista' tiġi ppubblikata skont it-taqsima 2.5:

- b'mod regolari jew perjodiku; jew
- bi tweġiba għal talba mingħand xi waħda mill-entitajiet parteċipanti.

F'kull każ, japplikaw gradi differenti ta' urġenza għall-pubblikazzjoni, jiġifieri japplikaw skedi tal-ħin, iżda l-entitajiet iridu jkunu lesti għaż-żewġ tipi ta' arranġamenti.

(24) Bil-pubblikazzjoni regolari tal-informazzjoni taċ-ċertifikat tkun tista' tiġi stabbilita skadenza massima sa meta l-informazzjoni taċ-ċertifikat tiġi aġġornata għan-nodi kollha tan-network tas-C-ITS. Il-frekwenza tal-pubblikazzjoni tal-informazzjoni kollha taċ-ċertifikat hi stabbilita fit-taqsima 2.2.

(25) Fuq it-talba tal-entitajiet li jipparteċipaw fin-network tas-C-ITS, kwalunkwe wieħed mill-parteċipanti jista' jibda jippubblika informazzjoni taċ-ċertifikat fi kwalunkwe ħin u, skont l-istatus tiegħu, jitlob sett attwali ta' informazzjoni taċ-ċertifikat biex isir nodu fdat għalkollox tan-network tas-C-ITS. L-iskop ta' din il-pubblikazzjoni hu prinċipalment li taġġorna lill-entitajiet dwar l-istatus attwali ġenerali tal-informazzjoni taċ-ċertifikat fin-network u tippermettilhom jikkomunikaw abbażi tal-fiduċja sal-pubblikazzjoni regolari tal-informazzjoni li jmiss.

(26) Root CA waħda tista' wkoll tibda l-pubblikazzjoni tal-informazzjoni taċ-ċertifikat fi kwalunkwe ħin billi tibgħat sett aġġornat taċ-ċertifikati lill-"membri kollha abbonati" tan-network tas-C-ITS li huma riċevituri regolari ta' din l-informazzjoni. Dan jappoġġa l-operat tas-CAs u jippermettilhom jindirizzaw lill-membri bejn id-dati għall-pubblikazzjoni regolari u skedata taċ-ċertifikati.

(27) It-taqsima 2.5 tistabbilixxi l-mekkaniżmu u l-proċeduri kollha għall-pubblikazzjoni taċ-ċertifikati tar-root CA u tal-ECTL.

(28) Is-CPOC għandu jippubblika ċ-ċertifikati tar-root CA (kif inkluż fl-ECTL u maħsuba għall-konsum pubbliku), iċ-ċertifikat tat-TLM, u l-ECTL li dan joħroġ.

(29) Ir-root CAs għandhom jippubblikaw iċ-ċertifikati tal-EA/AA u s-CRLs tagħhom, u jkunu jistgħu jappoġġaw it-tliet mekkaniżmi msemmija hawn biex jippubblikawhom lill-membri abbonati u lill-partijiet dipendenti tagħhom, billi jieħdu l-passi kollha meħtieġa biex jiżguraw trażmissjoni sigura, kif imsemmi fit-taqsima 4.

2.2. Żmien jew frekwenza tal-pubblikazzjoni

(30) Ir-rekwiżiti dwar l-iskeda tal-pubblikazzjoni għal ċertifikati u CRLs għandhom jiġu ddeterminati fid-dawl tal-fatturi varji li jillimitaw in-nodi uniċi tas-C-ITS, bil-għan ġenerali li joperaw "network fdat" u jippubblikaw aġġornamenti malajr kemm jista' jkun għall-istazzjonijiet tas-C-ITS kollha involuti.

- Għall-pubblikazzjoni regolari ta' informazzjoni aġġornata taċ-ċertifikati (eż. bidliet fil-kompożizzjoni tal-ECTL jew tas-CRL), hu meħtieġ perjodu massimu ta' tliet xhur għat-tħaddim sikur tan-network C-ITS.
- Ir-root CAs għandhom jippubblikaw iċ-ċertifikati tas-CA u s-CRLs tagħhom kemm jista' jkun malajr wara l-ħruġ.
- Għall-pubblikazzjoni tas-CRL għandu jintuża r-repożitorju tar-root CA.

Barra minn hekk, is-CPS għal kull CA għandha tispeċifika l-perjodu ta' żmien li matulu se jkun ippubblikat iċ-ċertifikat wara li s-CA toħroġ iċ-ċertifikat.

Din it-taqsima tispeċifika biss iż-żmien jew il-frekwenza tal-pubblikazzjoni regolari. Il-mezzi ta' konnettività biex jiġu aġġornati l-istazzjonijiet tas-C-ITS mal-ECTL u s-CRLs fi żmien ġimgħa mill-pubblikazzjoni tagħhom (f'kundizzjonijiet ta' tħaddim normali, eż. b'kopertura ċellulari, vettura f'kundizzjonijiet operattivi reali, eċċ.) għandhom jiġu implimentati skont ir-rekwiżiti f'dan id-dokument.

2.3. Repożitorji

(31) Ir-rekwiżiti dwar l-istruttura tar-repożitorju għall-ħażna taċ-ċertifikati u liema informazzjoni hi pprovduta mill-entitajiet tan-network C-ITS huma kif ġej għall-entitajiet uniċi:

- b'mod ġenerali, kull root CA għandha tuża repożitorju tal-informazzjoni taċ-ċertifikat tal-EA/AA li hu attiv bħalissa u tagħha stess u CRL biex tippubblika ċertifikati għall-parteċipanti l-oħra tal-PKI (eż. servizz tad-direttorju bbażat fuq LDAP). Ir-repożitorju ta' kull root CA għandu jappoġġa l-kontrolli tal-aċċess kollha meħtieġa (it-taqsima 2.4) u l-ħinijiet tat-trażmissjoni (it-taqsima 2.2) għal kull metodu tad-distribuzzjoni tal-informazzjoni relatata mas-C-ITS;
- ir-repożitorju tat-TLM (li jaħżen iċ-ċertifikati tal-ECTL u tat-TLM ippubblikati mis-CPOC, pereżempju) għandu jkun ibbażat fuq mekkaniżmu tal-pubblikazzjoni li jkun kapaċi jiżgura l-ħinijiet tat-trażmissjoni stabbiliti fit-taqsima 2.2 għal kull metodu tad-distribuzzjoni.

Ir-rekwiżiti tal-AAs mhumiex definiti, iżda għandhom jappoġġaw l-istess livelli ta' sigurtà bħall-entitajiet l-oħra u dawn għandhom jiġu ddikjarati fis-CPS tagħhom.

2.4. Kontrolli tal-aċċess fuq ir-repożitorji

(32) Ir-rekwiżiti dwar il-kontroll tal-aċċess għar-repożitorji tal-informazzjoni taċ-ċertifikat għandhom minn tal-anqas jikkonformaw mal-istandards ġenerali tal-immaniġġjar sigur tal-informazzjoni deskritti f'ISO/IEC 27001 u mar-rekwiżiti fit-taqsima 4. Barra minn hekk, għandhom jirriflettu l-ħtiġijiet tas-sigurtà tal-proċess li għandhom jiġu stabbiliti għall-istadji tal-proċess uniku fil-pubblikazzjoni tal-informazzjoni taċ-ċertifikat.

- Dan jinkludi l-implimentazzjoni tar-repożitorju għaċ-ċertifikati tat-TLM u għall-ECTL fit-TLM/CPOC. Kull CA jew operatur tar-repożitorju għandhom jimplimentaw il-kontrolli tal-aċċess fir-rigward tal-entitajiet kollha tas-C-ITS u tal-partijiet esterni għal mill-anqas tliet livelli differenti (eż. pubbliku, ristrett għall-entitajiet tas-C-ITS, fil-livell tar-root CA) biex jiġi evitat li entitajiet mhux awtorizzati jżidu mal-entrati fir-repożitorju, jemendawhom jew iħassruhom.
- Il-mekkaniżmi eżatti tal-kontroll tal-aċċess tal-entità unika għandhom ikunu parti mis-CPS rispettiva.
- Għal kull root CA, ir-repożitorji tal-EA u tal-AA għandhom jikkonformaw mal-istess rekwiżiti għall-proċeduri ta' kontroll tal-aċċess irrispettivament mill-post jew mill-konnessjoni kuntrattwali mal-fornitur tas-servizz li jopera r-repożitorju.

Bħala punt ta' tluq għal-livelli ta' kontroll tal-aċċess, kull root CA jew operatur tar-repożitorju għandhom jipprovdu mill-anqas tliet livelli differenti (eż. pubbliku, ristrett għall-entitajiet tas-C-ITS, fil-livell tar-root CA).

2.5. Pubblikazzjoni tal-informazzjoni taċ-ċertifikat

2.5.1. Pubblikazzjoni tal-informazzjoni taċ-ċertifikat mit-TLM

(33) It-TLM fid-dominju ta' fiduċja komuni Ewropew tas-C-ITS għandu jippubblika l-informazzjoni li ġejja permezz tas-CPOC:

- iċ-ċertifikati kollha attwalment validi tat-TLM għall-perjodu ta' operazzjoni li jmiss (ċertifikat attwali u tal-konnessjoni jekk disponibbli);
- informazzjoni dwar il-punt ta' aċċess biex ir-repożitorju tas-CPOC jagħti l-lista ffirmata tar-root CAs (ECTL);
- il-punt ta' informazzjoni ġenerali għall-użu tal-ECTL u tas-C-ITS.

2.5.2. Pubblikazzjoni tal-informazzjoni taċ-ċertifikat mis-CAs

(34) Ir-root CAs fid-dominju ta' fiduċja komuni Ewropew tas-C-ITS għandhom jippubblikaw l-informazzjoni li ġejja:

- iċ-ċertifikati tar-root CA (attwalment validi) maħruġa (ċertifikati attwali u dawk li għaddew mill-fażi ta' rikjavar b'mod korrett, inkluż ċertifikat tal-konnessjoni) fir-repożitorju msemmi fit-taqsima 2.3;
- l-entitajiet EA, AA kollha validi, bl-ID tal-operatur u l-perjodu ppjanat tal-operazzjoni tagħhom;
- iċ-ċertifikati tas-CA maħruġa fir-repożitorji msemmija fit-taqsima 2.3;
- is-CRLs għaċ-ċertifikati revokati kollha tas-CA li jkopru l-EAs u l-AAs subordinati tagħhom;
- informazzjoni dwar il-punt tal-aċċess tar-root CA għall-informazzjoni tas-CRL u tas-CA.

L-informazzjoni kollha taċ-ċertifikat għandha tiġi kkategorizzata skont tliet livelli ta' kunfidenzjalità u d-dokumenti għall-pubbliku ġenerali għandhom ikunu disponibbli għall-pubbliku mingħajr restrizzjonijiet.

3. IDENTIFIKAZZJONI U AWTENTIKAZZJONI

3.1. Għoti tal-isem

3.1.1. Tipi ta' isem

3.1.1.1. Ismijiet għal TLM, root CAs, EAs, AAs

(35) L-isem fiċ-ċertifikat tat-TLM għandu jkun magħmul minn attribut subject_name wieħed bil-valur riżervat "EU_TLM".

(36) L-isem għar-root CAs għandu jkun magħmul minn attribut subject_name wieħed b'valur allokat mis-CPA. L-uniċità tal-ismijiet hi r-responsabbiltà unika tas-CPA u t-TLM għandu jżomm ir-reġistru tal-ismijiet tar-root CAs wara notifika mis-CPA (approvazzjoni, revoka/tneħħija ta' root CA). L-ismijiet tas-suġġetti fiċ-ċertifikati huma limitati għal 32 byte. Kull root CA tipproponi isimha lis-CPA fil-formola tal-applikazzjoni (il-fluss 14). Is-CPA hi responsabbli biex tivverifika l-uniċità tal-isem. Jekk l-isem ma jkunx uniku, il-formola tal-applikazzjoni tiġi rifjutata (il-fluss 4).

(37) L-isem f'kull ċertifikat tal-EA/AA jista' jkun magħmul minn attribut subject_name wieħed b'valur iġġenerat mill-emittent taċ-ċertifikat. L-uniċità tal-ismijiet hi r-responsabbiltà unika tar-root CA emittenti.

(38) Iċ-ċertifikati tal-EA u tal-AA ma għandhomx jużaw isem akbar minn 32 byte, għax l-attribut subject_name fiċ-ċertifikati hu limitat għal 32 byte.

(39) L-ATs ma għandux ikollhom isem.

3.1.1.2. Ismijiet għall-entitajiet aħħarija

(40) Kull stazzjon tas-C-ITS għandu jiġi assenjat żewġ tipi ta' identifikatur uniku:

- l-ID kanonika li tkun maħżuna mar-reġistrazzjoni inizjali tal-istazzjon tas-C-ITS fir-responsabbiltà tal-manifattur. Din għandu jkun fiha substring li tidentifika l-manifattur jew l-operatur biex dan l-identifikatur ikun uniku;
- subject_name, li jista' jkun parti mill-EC tal-istazzjon tas-C-ITS, fir-responsabbiltà tal-EA.

3.1.1.3. Identifikazzjoni taċ-ċertifikati

(41) Iċ-ċertifikati li jsegwu l-format ta' [5] għandhom jiġu identifikati billi jiġi kkalkulat valur HashedId8 kif definit f'[5] .

3.1.2. Ħtieġa li l-ismijiet ikunu sinifikattivi

L-ebda stipulazzjoni.

3.1.3. Anonimità u psewdonimità tal-entitajiet aħħarija

(42) L-AA għandha tiżgura li l-psewdonimità ta' stazzjon tas-C-ITS tkun stabbilita billi tipprovdi lill-istazzjon tas-C-ITS b'ATs li ma fihom l-ebda isem jew informazzjoni li jistgħu jagħmlu konnessjoni bejn is-suġġett u l-identità vera tiegħu.

3.1.4. Regoli għall-interpretazzjoni ta' diversi forom ta' ismijiet

L-ebda stipulazzjoni.

3.1.5. Uniċità tal-ismijiet

(43) L-ismijiet għat-TLM, ir-root CAs, l-EAs, l-AAs u l-IDs kanoniċi għall-istazzjonijiet tas-C-ITS għandhom ikunu uniċi.

(44) It-TLM għandu jiżgura fil-proċess tar-reġistrazzjoni ta' root CA partikolari fl-ECTL li l-identifikatur taċ-ċertifikat tagħha (HashedId8) ikun uniku. Ir-root CA għandha tiżgura fil-proċess tal-ħruġ li l-identifikatur taċ-ċertifikat (HashedId8) ta' kull CA subordinata jkun uniku.

(45) Il-HashedId8 ta' EC għandu jkun uniku fi ħdan is-CA emittenti. Il-HashedId8 ta' AT ma għandux għalfejn ikun uniku.

3.2. Validazzjoni tal-identità inizjali

3.2.1. Metodu biex tingħata prova tal-pussess tal-kjavi privata

(46) Ir-root CA għandha tagħti prova li għandha ġustament il-kjavi privata fil-pussess tagħha li tikkorrispondi għall-kjavi pubblika fiċ-ċertifikat iffirmat minnha stess. Is-CPOC għandu jivverifika din il-prova.

(47) L-EA/AA għandhom jagħtu prova li għandhom ġustament il-kjavi privata fil-pussess tagħhom li tikkorrispondi għall-kjavi pubblika li se tiġi elenkata fiċ-ċertifikat. Ir-root CA għandha tivverifika din il-prova.

(48) Għall-pussess ta' kjavi privata ġdida (għal rikjavar) għandha tingħata prova bl-iffirmar tat-talba bil-kjavi privata l-ġdida (firma interna), segwita mill-ġenerazzjoni ta' firma esterna fuq it-talba ffirmata bil-kjavi privata valida attwali (biex tiġi ggarantita l-awtentiċità tat-talba). L-applikant għandu jippreżenta t-talba ffirmata taċ-ċertifikat lis-CA emittenti permezz ta'

komunikazzjoni sigura. Is-CA emittenti għandha tivverifika li l-firma diġitali tal-applikant fuq il-messaġġ tat-talba nħolqot bl-użu tal-kjavi privata li tikkorrispondi għall-kjavi pubblika mehmuża mat-talba taċ-ċertifikat. Ir-root CA għandha tispeċifika liema talba taċ-ċertifikat u liema risposti tappoġġa fis-CPS tagħha.

3.2.2. Awtentikazzjoni tal-identità tal-organizzazzjoni

3.2.2.1. Awtentikazzjoni tal-identità tal-organizzazzjoni tar-root CAs

(49) F'formola tal-applikazzjoni lis-CPA (jiġifieri l-fluss 14), ir-root CA għandha tipprovdi l-identità tal-organizzazzjoni u l-informazzjoni tar-reġistrazzjoni, magħmula minn:

- isem l-organizzazzjoni;
- l-indirizz postali;
- l-email;
- isem persuna fiżika ta' kuntatt fl-organizzazzjoni;
- in-numru tat-telefown;
- il-marki tas-swaba' diġitali (jiġifieri hashvalue SHA 256) taċ-ċertifikat tar-root CA b'format stampat;
- informazzjoni kriptografika (jiġifieri algoritmi kriptografiċi, tulijiet tal-kjavi) fiċ-ċertifikat tar-root CA;
- il-permessi kollha li r-root CA hi permessa li tuża u tgħaddi lis-sub-CAs.

(50) Is-CPA għandha tivverifika l-identità tal-organizzazzjoni u l-informazzjoni l-oħra tar-reġistrazzjoni pprovduta mill-applikant għaċ-ċertifikat għall-inklużjoni ta' ċertifikat tar-root CA fl-ECTL.

(51) Is-CPA għandha tiġbor provi diretti, jew attestazzjoni mingħand sors xieraq u awtorizzat, tal-identità (eż. l-isem) u, jekk applikabbli, kwalunkwe attributi speċifiċi ta' suġġetti li lilhom jinħareġ iċ-ċertifikat. Il-prova ppreżentata tista' tkun fil-forma ta' dokumentazzjoni stampata jew elettronika.

(52) L-identità tas-suġġett għandha tkun ivverifikata fil-ħin tar-reġistrazzjoni b'mezzi xierqa u skont il-politika ta' dan iċ-ċertifikat.

(53) F'kull applikazzjoni għal ċertifikat, għandha tingħata prova ta':

- l-isem sħiħ tal-entità organizzattiva (organizzazzjoni privata, entità tal-gvern jew entità mhux kummerċjali);
- reġistrazzjoni rikonoxxuta nazzjonalment jew attributi oħra li jistgħu jintużaw, kemm jista' jkun, biex jiddistingwu l-entità organizzattiva minn oħrajn bl-istess isem.

Ir-regoli ta' hawn fuq huma bbażati fuq it-TS 102 042 [4]: *Is-CA għandha tiżgura li l-prova tal-identifikazzjoni tal-abbonat u tas-suġġett, u l-eżattezza tal-ismijiet tagħhom u tad-data assoċjata jkunu eżaminati kif xieraq bħala parti mis-servizz definit jew inkella, meta applikabbli, jiġu konklużi permezz ta' eżami tal-attestazzjonijiet mingħand sorsi xierqa u awtorizzati, u li t-talbiet għaċ-ċertifikat huma preċiżi, awtorizzati u kompluti skont il-provi jew l-attestazzjoni miġbura.*

3.2.2.2. Awtentikazzjoni tal-identità tal-organizzazzjoni tat-TLM

(54) L-organizzazzjoni li topera t-TLM għandha tagħti prova tal-identifikazzjoni u tal-eżattezza tal-isem u tad-*data* assoċjata biex tkun tista' ssir verifika xierqa waqt il-ħolqien inizjali u waqt ir-rikjavar taċ-ċertifikat tat-TLM.

(55) L-identità tas-suġġett għandha tkun ivverifikata waqt il-ħolqien taċ-ċertifikat jew waqt ir-rikjavar b'mezzi xierqa u skont din is-CP.

(56) Il-prova tal-organizzazzjoni għandha tiġi pprovduta kif speċifikat fit-taqsima 3.2.2.1.

3.2.2.3. Awtentikazzjoni tal-identità tal-organizzazzjoni tas-sub-CAs

(57) Ir-root CA għandha tivverifika l-identità tal-organizzazzjoni u informazzjoni oħra tar-reġistrazzjoni pprovduta minn applikanti għaċ-ċertifikat għal ċertifikati tas-sub-CA (EA/AA).

(58) Bħala minimu, ir-root CA għandha:

- tiddetermina li l-organizzazzjoni teżisti bl-użu ta' mill-anqas servizz ta' prova tal-identità jew bażi tad-*data* ta' parti terza waħda, jew inkella dokumentazzjoni organizzattiva maħruġa minn jew ippreżentata lill-aġenzija governattiva rilevanti jew lill-awtorità rikonoxxuta li tikkonferma l-eżistenza tal-organizzazzjoni;
- tuża l-posta jew proċedura komparabbli li titlob lill-applikant għaċ-ċertifikat jikkonferma ċerta informazzjoni dwar l-organizzazzjoni, li hu awtorizza l-applikazzjoni għaċ-ċertifikat u li l-persuna li tippreżenta l-applikazzjoni f'isem l-applikant hi awtorizzata li tagħmel hekk. Jekk iċ-ċertifikat ikun jinkludi l-isem ta' individwu bħala rappreżentant awtorizzat tal-organizzazzjoni, l-applikant għandu jikkonferma wkoll li dan jimpjega lil dak l-individwu u li awtorizzah jaġixxi f'ismu.

(59) Il-proċeduri ta' validazzjoni għall-ħruġ ta' ċertifikati tas-CA għandhom jiġu ddokumentati f'CPS tar-root CA.

3.2.2.4. Awtentikazzjoni tal-organizzazzjoni tal-abbonat tal-entitajiet aħħarija

(60) Qabel ma l-abbonat ta' entitajiet aħħarija (manifattur/operatur) ikun jista' jirreġistra ma' EA fdata biex jippermetti lill-entitajiet aħħarija tiegħu jibagħtu talbiet għal ċertifikat tal-EC, l-EA għandha:

- tivverifika l-identità tal-organizzazzjoni tal-abbonat u informazzjoni oħra tar-reġistrazzjoni pprovduta mill-applikant għaċ-ċertifikat;
- tivverifika li t-tip ta' stazzjon tas-C-ITS (jiġifieri l-prodott konkret ibbażat fuq id-ditta, il-mudell u l-verżjoni tal-istazzjon tas-C-ITS) jissodisfa l-kriterji kollha tal-valutazzjoni tal-konformità.

(61) Bħala minimu, l-EA għandha:

- tiddetermina li l-organizzazzjoni teżisti bl-użu ta' mill-anqas servizz ta' prova tal-identità jew bażi tad-*data* ta' parti terza waħda, jew inkella dokumentazzjoni organizzattiva maħruġa minn jew ippreżentata lill-aġenzija governattiva rilevanti jew lill-awtorità rikonoxxuta li tikkonferma l-eżistenza tal-organizzazzjoni;

- tuża l-posta jew proċedura komparabbli biex titlob lill-applikant għaċ-ċertifikat jikkonferma ċerta informazzjoni dwar l-organizzazzjoni, li hu awtorizza l-applikazzjoni għaċ-ċertifikat u li l-persuna li tippreżenta l-applikazzjoni f'ismu hi awtorizzata li tagħmel hekk. Jekk iċ-ċertifikat ikun jinkludi l-isem ta' individwu bħala rappreżentant awtorizzat tal-organizzazzjoni, l-applikant għandu jikkonferma wkoll li dan jimpjega lil dak l-individwu u li awtorizzah jaġixxi f'ismu.

(62) Il-proċeduri ta' validazzjoni għar-reġistrazzjoni ta' stazzjon tas-C-ITS mill-abbonat tiegħu għandhom jiġu ddokumentati f'CPS tal-EA.

3.2.3. Awtentikazzjoni tal-entità individwali

3.2.3.1. Awtentikazzjoni tal-entità individwali tat-TLM/CA

(63) Għall-awtentikazzjoni ta' entità individwali (persuna fiżika) identifikata f'assoċjazzjoni ma' persuna ġuridika jew entità organizzattiva (eż. l-abbonat), għandha tingħata prova ta':

- l-isem sħiħ tas-suġġett (inkluż il-kunjom u l-ismijiet mogħtija, b'konformità mal-liġi applikabbli u l-prattiki ta' identifikazzjoni nazzjonali);
- id-data u l-post tat-twelid, referenza għal dokument ta' identità rikonoxxut nazzjonalment jew attributi oħra tal-abbonat li jistgħu jintużaw, kemm jista' jkun, biex jiddistingwu l-persuna minn oħrajn bl-istess isem;
- l-isem sħiħ u l-istatus legali tal-persuna ġuridika assoċjata jew ta' entità organizzattiva oħra (eż. l-abbonat);
- kwalunkwe informazzjoni tar-reġistrazzjoni rilevanti (eż. reġistrazzjoni tal-kumpanija) tal-persuna ġuridika assoċjata jew entità organizzattiva oħra;
- prova li s-suġġett hu assoċjat mal-persuna ġuridika jew ma' entità organizzattiva oħra.

Il-prova ppreżentata tista' tkun fil-forma ta' dokumentazzjoni stampata jew elettronika.

(64) Biex jivverifika l-identità tiegħu, ir-rappreżentant awtorizzat ta' root CA, EA, AA jew ta' abbonat għandu jipprovdi dokumentazzjoni li turi li jaħdem għall-organizzazzjoni (ċertifikat ta' awtorizzazzjoni). Dan għandu juri wkoll ID uffiċjali.

(65) Għall-proċess ta' reġistrazzjoni inizjali (il-fluss 31/32), ir-rappreżentant tal-EA/AA għandu jipprovdi l-informazzjoni kollha meħtieġa lir-root CA korrispondenti (ara t-taqsima 4.1.2).

(66) Il-persunal fir-root CA għandu jivverifika l-identità tar-rappreżentant tal-applikant għaċ-ċertifikat u d-dokumenti assoċjati kollha, billi japplika r-rekwiżiti ta' "persunal fdat" kif stabbilit fit-taqsima 5.2.1. (Il-proċess tal-validazzjoni tal-informazzjoni tal-applikazzjoni u tal-ġenerazzjoni taċ-ċertifikat mir-root CA għandhom iwettquh "persuni fdati" fir-root CA, tal-anqas b'superviżjoni doppja, għax dawn huma operazzjonijiet sensittivi fis-sens tat-taqsima 5.2.2).

3.2.3.2. Awtentikazzjoni tal-identità tal-abbonat tal-istazzjonijiet tas-C-ITS

(67) L-abbonati huma rappreżentati minn utenti aħħarija awtorizzati fl-organizzazzjoni li huma rreġistrati fl-EA u l-AA emittenti. Dawn l-utenti aħħarija nominati minn organizzazzjonijiet (manifatturi jew operaturi) għandhom juru l-identità u l-awtenticità tagħhom qabel ma:

- jirreġistraw l-EE fl-EA korrispondenti tagħha, inkluż il-kjavi pubblika kanonika tagħha, l-ID kanonika (identifikatur uniku) u l-permessi skont l-EE;
- jirreġistraw fl-AA u jiżguraw il-prova ta' ftehim tal-abbonat li jista' jintbagħat lill-EA.

3.2.3.3. Awtentikazzjoni tal-identità tal-istazzjonijiet tas-C-ITS

(68) Is-suġġetti tal-EE tal-ECs għandhom jawtentikaw ruħhom meta jitolbu ECs (il-fluss 31) billi jużaw il-kjavi privata kanonika tagħhom għall-awtentikazzjoni inizjali. L-EA għandha tivverifika l-awtentikazzjoni billi tuża l-kjavi pubblika kanonika li tikkorrispondi għall-EE. Il-kjavi pubbliċi kanoniċi tal-EEs jingiebu lill-EA qabel ma ssir it-talba inizjali, permezz ta' kanal sigur bejn il-manifattur jew l-operatur tal-istazzjon tas-C-ITS u l-EA (fluss 33).

(69) Is-suġġetti tal-EE tal-ATs għandhom jawtentikaw ruħhom meta jitolbu l-ATs (il-fluss 32) billi jużaw il-kjavi privata unika tar-reġistrazzjoni tagħhom. L-AA għandha tibgħat il-firma lill-EA (il-fluss 25) għall-validazzjoni; l-EA għandha tivvalidaha u tikkonferma r-riżultat lill-AA (il-fluss 23).

3.2.4. Informazzjoni mhux verifikata dwar l-abbonat

L-ebda stipulazzjoni.

3.2.5. Validazzjoni tal-awtorità

3.2.5.1. Validazzjoni ta' TLM, root CA, EA, AA

(70) Kull organizzazzjoni għandha tidentifika fis-CPS mill-anqas rappreżentant wieħed (eż. uffiċjal tas-sigurtà) responsabbli biex jitlob ċertifikati ġodda u tiġdid. Għandhom japplikaw ir-regoli dwar l-ismijiet fit-taqsima 3.2.3.

3.2.5.2. Validazzjoni tal-abbonati ta' stazzjon tas-C-ITS

(71) Mill-anqas persuna fiżika waħda responsabbli biex tirreġistra l-istazzjonijiet tas-C-ITS f'EA (eż. uffiċjal tas-sigurtà) għandha tkun magħrufa u approvata mill-EA (ara t-taqsima 3.2.3).

3.2.5.3. Validazzjoni tal-istazzjonijiet tas-C-ITS

(72) Abbonat ta' stazzjon tas-C-ITS jista' jirreġistra stazzjonijiet tas-C-ITS f'EA speċifika (il-fluss 33) diment li dan ikun awtentikat f'dik l-EA.

Meta l-istazzjon tas-C-ITS ikun irreġistrat f'EA b'ID kanonika unika u bi kjavi pubblika kanonika, dan jista' jitlob EC billi juża talba ffirmata bil-kjavi privata kanonika relatata mal-kjavi pubblika kanonika li tkun ġiet irreġistrata qabel.

3.2.6. Kriterji għall-interoperazzjoni

(73) Għall-komunikazzjoni bejn l-istazzjonijiet tas-C-ITS u l-EAs (jew l-AAs), l-istazzjon tas-C-ITS għandu jkun kapaċi jistabbilixxi komunikazzjoni sigura mal-EAs (jew mal-AAs), jiġifieri biex jimplimenta funzjonijiet ta' awtentikazzjoni, kunfidenzjalità u integrità, kif speċifikat f'[1]. Jistgħu

jintużaw protokolli oħra, diment li [1] jiġi implimentat. L-EA u l-AA għandhom jappoġġaw din il-komunikazzjoni sigura.

(74) L-EA u l-AA għandhom jappoġġaw talbiet għal ċertifikati u risposti li jikkonformaw ma' [1], li jipprevedi protokoll sigur ta' talba/rispons għal AT li jappoġġa l-anonimità ta' min jagħmel it-talba fil-konfront tal-AA u s-separazzjoni tad-dmirijiet bejn l-AA u l-EA. Jistgħu jintużaw protokolli oħra, diment li [1] jiġi implimentat. Biex jiġi evitat l-iżvelar tal-identità fit-tul tal-istazzjonijiet tas-C-ITS, il-komunikazzjoni bejn stazzjon mobbli tas-C-ITS u l-EA għandha tkun kunfidenzjali (eż. id-*data* tal-komunikazzjoni għandha tkun kriptata minn tarf sa tarf).

(75) L-AA għandha tippreżenta talba għall-validazzjoni tal-awtorizzazzjoni (il-fluss 25) għal kull talba ta' awtorizzazzjoni li tirċievi mingħand suġġett taċ-ċertifikat tal-EE. L-EA għandha tivvalida din it-talba fir-rigward ta':

- l-istatus tal-EE fl-EA;
- il-validità tal-firma;
- l-IDs mitluba tal-Applikazzjoni tal-ITS (ITS-AID) u l-permessi;
- l-istatus tal-forniment tas-servizz tal-AA lill-abbonat.

3.3. Identifikazzjoni u awtentikazzjoni għal talbiet tar-rikjavar

3.3.1. Identifikazzjoni u awtentikazzjoni għal talbiet ta' rikjavar ta' rutina

3.3.1.1. Ċertifikati tat-TLM

(76) It-TLM jiġġenera par kjavi u żewġ ċertifikati: wieħed iffirmat minnu stess u l-ieħor ċertifikat tal-konnessjoni kif imsemmi fit-taqsima 7.

3.3.1.2. Ċertifikati tar-root CA

Mhux applikabbli.

3.3.1.3. Tiġdid jew rikjavar taċ-ċertifikati tal-EA/AA

(77) Qabel l-iskadenza ta' ċertifikat tal-EA/AA, l-EA/AA għandha titlob ċertifikat ġdid (il-fluss 21/il-fluss 24) biex iżżomm il-kontinwità tal-użu taċ-ċertifikat. L-EA/AA għandha tiġġenera par kjavi ġdid biex tissostitwixxi l-par kjavi li jkun se jiskadi u tiffirma t-talba għar-rikjavar li jkun fiha l-kjavi pubblika l-ġdida bil-kjavi privata valida attwali ("ir-rikjavar"). L-EA jew l-AA jiġġeneraw par kjavi ġdid u jiffirmaw it-talba bil-kjavi privata l-ġdida (firma interna) biex jagħtu prova tal-pussess tal-kjavi privata l-ġdida. It-talba kollha hi ffirmata (sovraffirmata) bil-kjavi privata valida attwali (firma esterna) biex tiżgura l-integrità u l-awtenticità tat-talba. Jekk jintuża par kjavi tal-kriptaġġ u tad-dekriptaġġ, għandha tingħata prova tal-pussess ta' kjavi privati tad-dekriptaġġ (għal deskrizzjoni dettaljata tar-rikjavar, ara t-taqsima 4.7.3.3).

(78) Il-metodu tal-identifikazzjoni u tal-awtentikazzjoni għar-rikjavar ta' rutina hu l-istess bħal dak għall-ħruġ inizjali ta' validazzjoni taċ-ċertifikat inizjali tar-root CA, kif stabbilit fit-taqsima 3.2.2.

3.3.1.4. Kredenzjali għar-reġistrazzjoni tal-entitajiet aħħarija

(79) Qabel l-iskadenza ta' EC eżistenti, l-EE għandha titlob ċertifikat ġdid (il-fluss 31) biex iżżomm il-kontinwità tal-użu taċ-ċertifikat. L-EE għandha tiġġenera par kjavi ġdid biex jissostitwixxi l-par kjavi li jkun se jiskadi u titlob

ċertifikat ġdid li jkun fih il-kjavi pubblika l-ġdida; it-talba għandha tiġi ffirmata bil-kjavi privata valida attwali tal-EC.

(80) L-EE tista' tiffirma t-talba bil-kjavi privata li tkun għadha kif ġiet maħluqa (firma interna) biex tagħti prova tal-pussess tal-kjavi privata l-ġdida. Imbagħad it-talba kollha tiġi ffirmata (sovraffirmata) bil-kjavi privata valida attwali (firma esterna) u kriptata lill-EA riċeventi kif speċifikat f'[1], biex tiġi żgurata l-kunfidenzjalità, l-integrità u l-awtenticità tat-talba. Jistgħu jintużaw protokolli oħra, diment li [1] jiġi implimentat.

3.3.1.5. Biljetti għall-awtorizzazzjoni tal-entitajiet aħħarija

(81) Ir-rikjavar taċ-ċertifikat għall-ATs hu bbażat fuq l-istess proċess bħall-awtorizzazzjoni inizjali, kif definit f'[1]. Jistgħu jintużaw protokolli oħra, diment li [1] jiġi implimentat.

3.3.2. Identifikazzjoni u awtentikazzjoni għal talbiet ta' rikjavar wara r-revoka

3.3.2.1. Ċertifikati tas-CA

(82) L-awtentikazzjoni ta' organizzazzjoni tas-CA għal rikjavar taċ-ċertifikat tar-root CA, tal-EA u tal-AA wara r-revoka hi trattata bl-istess mod bħall-ħruġ inizjali ta' ċertifikat tas-CA, kif stabbilit fit-taqsima 3.2.2.

3.3.2.2. Kredenzjali għar-reġistrazzjoni tal-entitajiet aħħarija

(83) L-awtentikazzjoni ta' EE għal rikjavar taċ-ċertifikat tal-EC wara r-revoka hi trattata bl-istess mod bħall-ħruġ inizjali ta' ċertifikat tal-EE, kif stabbilit fit-taqsima 3.2.2.

3.3.2.3. Talbiet għall-awtorizzazzjoni tal-entitajiet aħħarija

Mhux applikabbli għax l-ATs ma jiġux revokati.

3.4. Identifikazzjoni u awtentikazzjoni tat-talba għal revoka

3.4.1. Ċertifikati tar-root CA/tal-EA/tal-AA

(84) It-talbiet biex jitħassar ċertifikat tar-root CA mill-ECTL għandhom ikunu awtentikati mir-root CA lit-TLM (il-flussi 12 u 9). It-talbiet għar-revoka ta' ċertifikat tal-EA/tal-AA għandhom jiġu awtentikati mir-root CA rilevanti u mis-sub-CA nnifisha.

(85) Il-proċeduri aċċettabbli għall-awtentikazzjoni tat-talbiet għal revoka ta' abbonat jinkludu:

- messaġġ bil-miktub u ffirmat fuq il-karta korporattiva mill-abbonat li jitlob ir-revoka, b'referenza għaċ-ċertifikat li għandu jiġi revokat;
- komunikazzjoni mal-abbonat li tipprovdi assigurazzjonijiet raġonevoli li l-persuna jew l-organizzazzjoni li titlob ir-revoka hi fil-fatt l-abbonat. Skont iċ-ċirkostanzi, din il-komunikazzjoni tista' tinkludi waħda jew aktar minn dawn li ġejjin: email, posta jew servizz ta' kurrier.

3.4.2. Kredenzjali għar-reġistrazzjoni ta' stazzjon tas-C-ITS

(86) L-abbonat tal-istazzjon tas-C-ITS jista' jirrevoka l-EC ta' stazzjon tas-C-ITS irreġistrat qabel fl-EA (il-fluss 34). L-abbonat rikjedenti għandu joħloq talba għar-revoka ta' stazzjon tas-C-ITS partikolari jew ta' lista ta' stazzjonijiet tas-C-ITS. L-EA għandha tawtentika t-talba għal revoka qabel ma tipproċessaha u tikkonferma r-revoka tal-istazzjonijiet tas-C-ITS u l-ECs tagħhom.

(87) L-EA tista' tirrevoka l-EC ta' stazzjon tas-C-ITS skont it-taqsima 7.3.

3.4.3. Biljetti tal-awtorizzazzjoni ta' stazzjon tas-C-ITS

(88) L-ATs ma jiġux revokati u għalhekk l-validità tagħhom għandha tkun limitata għal perjodu speċifiku. Il-firxa ta' perjodi ta' validità aċċettabbli f'din il-politika taċ-ċertifikati hi speċifikata fit-taqsima 7.

4. REKWIŻITI OPERAZZJONALI TAĊ-ĊIKLU TAL-ĦAJJA TAĊ-ĊERTIFIKATI

4.1. Applikazzjoni għal ċertifikat

(89) Din it-taqsima tistabbilixxi r-rekwiżiti għal applikazzjoni inizjali għall-ħruġ ta' ċertifikat.

(90) It-terminu "applikazzjoni għal ċertifikat" jirreferi għall-proċessi li ġejjin:

- ir-reġistrazzjoni u l-istabbiliment ta' relazzjoni ta' fiduċja bejn it-TLM u s-CPA;
- ir-reġistrazzjoni u l-istabbiliment ta' relazzjoni ta' fiduċja bejn ir-root CA u s-CPA u t-TLM, inkluż l-inklużjoni tal-ewwel ċertifikat tar-root CA fl-ECTL;
- ir-reġistrazzjoni u l-istabbiliment ta' relazzjoni ta' fiduċja bejn l-EA/AA u r-root CA, inkluż il-ħruġ ta' ċertifikat tal-EA/tal-AA ġdid;
- ir-reġistrazzjoni tal-istazzjon tas-C-ITS fl-EA mill-manifattur/operatur;
- it-talba tal-istazzjon tas-C-ITS għal EC/AT.

4.1.1. Min jista' jippreżenta applikazzjoni għal ċertifikat

4.1.1.1. Root CAs

(91) Ir-root CAs jiġġeneraw il-pari tal-kjavi tagħhom stess u joħorġu ċ-ċertifikat root tagħhom huma stess. Ir-root CA tista' tippreżenta applikazzjoni għal ċertifikat permezz tar-rappreżentant nominat tagħha (il-fluss 14).

4.1.1.2. *TLM*

(92) It-TLM jiġġenera l-pari tal-kjavi tiegħu stess u joħroġ iċ-ċertifikat tiegħu stess. Il-ħolqien inizjali taċ-ċertifikat tat-TLM għandu jkun ipproċessat minn rappreżentant tal-organizzazzjoni tat-TLM bil-kontroll tas-CPA.

4.1.1.3. *EA u AA*

(93) Ir-rappreżentant awtorizzat tal-EA jew tal-AA jista' jippreżenta l-applikazzjoni għat-talba għal ċertifikat tas-sub-CA (EA u/jew AA) lir-rappreżentant awtorizzat tar-root CA rilevanti (il-fluss 27/28).

4.1.1.4. Stazzjon tas-C-ITS

(94) L-abbonati għandhom jirreġistraw kull stazzjon tas-C-ITS fl-EA skont it-taqsima 3.2.5.3.

(95) Kull stazzjon tas-C-ITS irreġistrat fl-EA jista' jibgħat talbiet għal EC (il-fluss 31).

(96) Kull stazzjon tas-C-ITS jista' jibgħat talbiet għal AT (il-fluss 32) mingħajr ma jitlob xi interazzjoni tal-abbonat. Qabel ma jitlob AT, stazzjon tas-C-ITS għandu jkollu EC.

4.1.2. Proċess ta' reġistrazzjoni u responsabbiltajiet

(97) Il-permessi għar-root CAs u s-sub-CAs li joħorġu ċ-ċertifikati għal skopijiet (governattivi) speċjali (jiġifieri stazzjonijiet speċjali mobbli u fissi tas-C-ITS) jistgħu jingħataw biss mill-Istati Membri fejn jinsabu l-organizzazzjonijiet.

4.1.2.1. Root CAs

(98) Wara li jiġu awditjati (il-fluss 13 u 36, it-taqsima 8), ir-root CAs jistgħu japplikaw għall-inklużjoni taċ-ċertifikat(i) tagħhom fl-ECTL fis-CPA (il-fluss 14). Il-proċess ta' reġistrazzjoni hu bbażat fuq formola tal-applikazzjoni manwali ffirmata li għandha titwassal fiżikament lis-CPA mir-rappreżentant awtorizzat tar-root CA u li jkun fiha mill-anqas l-informazzjoni msemmija fit-taqsimiet 3.2.2.1, 3.2.3 u 3.2.5.1.

(99) Il-formola tal-applikazzjoni tar-root CA għandha tkun iffirmata mir-rappreżentant awtorizzat tagħha.

(100) Minbarra l-formola tal-applikazzjoni, ir-rappreżentant awtorizzat tar-root CA għandu jipprovdi kopja tas-CPS tar-root CA (il-fluss 15) u tar-rapport tal-awditjar tagħha lis-CPA għall-approvazzjoni (il-fluss 16). F'każijiet ta' approvazzjoni pożittiva, is-CPA tiġġenera u tibgħat ċertifikat ta' konformità lis-CPOC/lit-TLM u lir-root CA korrispondenti.

(101) Imbagħad ir-rappreżentant awtorizzat tar-root CA għandu jġib il-formola tal-applikazzjoni tiegħu (li jkun fiha l-marki tas-swaba' taċ-ċertifikat iffirmat minnu stess), l-ID uffiċjali u prova tal-awtorizzazzjoni lis-CPOC/lit-TLM. Iċ-ċertifikat iffirmat minnu stess għandu jiġi kkonsenjat b'mod elettroniku lis-CPOC/lit-TLM. Is-CPOC/it-TLM għandu jivverifika d-dokumenti kollha u ċ-ċertifikat iffirmat minnu stess.

(102) F'każijiet ta' verifiki pożittivi, it-TLM għandu jżid iċ-ċertifikat tar-root CA mal-ECTL abbażi tan-notifika mis-CPA (il-flussi 1 u 2). Il-proċess dettaljat hu deskritt fis-CPS tat-TLM.

(103) Għandha tkun tista' ssir proċedura addizzjonali biex tinkiseb l-approvazzjoni tas-CPS u r-rapport tal-awditjar tar-root CA mingħand korp nazzjonali ta' pajjiżi speċifiċi.

4.1.2.2. *TLM*

(104) Wara li jkun awditjat, it-TLM jista' jirreġistra mas-CPA. Il-proċess ta' reġistrazzjoni hu bbażat fuq formola tal-applikazzjoni manwali ffirmata li għandha titwassal fiżikament lis-CPA (il-fluss 38) mir-rappreżentant awtorizzat tat-TLM u li jkun fiha mill-anqas l-informazzjoni msemmija fit-taqsimiet 3.2.2.2 u 3.2.3.

(105) Il-formola tal-applikazzjoni tat-TLM għandha tkun iffirmata mir-rappreżentant awtorizzat tiegħu.

(106) L-ewwel nett, it-TLM jiġġenera ċ-ċertifikat tiegħu ffirmat minnu stess u jittrażmettih b'mod sigur lis-CPA. Imbagħad it-TLM iġib il-formola tal-applikazzjoni tiegħu (li jkun fiha l-marki tas-swaba' taċ-ċertifikat iffirmat minnu stess), kopja tas-CPS tiegħu, l-ID uffiċjali, prova tal-awtorizzazzjoni u r-rapport tal-awditjar tiegħu lis-CPA (il-fluss 40). Is-CPA għandha tivverifika d-dokumenti kollha u ċ-ċertifikat iffirmat minnu stess. F'każijiet ta' verifika pożittiva tad-dokumenti kollha, taċ-ċertifikat iffirmat minnu stess u tal-marki

tas-swaba', is-CPA għandha tikkonferma l-proċess tar-reġistrazzjoni billi tibgħat l-approvazzjoni tagħha lit-TLM u lis-CPOC (il-fluss 39). Is-CPA għandha taħżen l-informazzjoni tal-applikazzjoni mibgħuta mit-TLM. Iċ-ċertifikat tat-TLM imbagħad jinħareġ permezz tas-CPOC.

4.1.2.3. *EA u AA*

(107) Matul il-proċess tar-reġistrazzjoni, l-EA/AA għandhom jgħaddu d-dokumenti rilevanti (eż. is-CPS u r-rapport tal-awditjar) lir-root CA korrispondenti għall-approvazzjoni (il-fluss 27/28). F'każijiet ta' verifiki pożittivi tad-dokumenti, ir-root CA tibgħat approvazzjoni lir-root sub-CAs korrispondenti (il-fluss 29/30). Is-sub-CA (EA jew AA) għandha mbagħad tittrażmetti t-talba ffirmata tagħha b'mod elettroniku, u fiżikament twassal il-formola tal-applikazzjoni tagħha (skont it-taqsima 3.2.2.1), il-prova tal-awtorizzazzjoni u d-dokument tal-ID lir-root CA korrispondenti. Ir-root CA tivverifika t-talba u d-dokumenti li tirċievi (il-formola tal-applikazzjoni li jkun fiha l-marki tas-swaba', li hi l-hashvalue SHA 256 tat-talba tas-sub-CA, il-prova tal-awtorizzazzjoni u d-Dokument tal-ID). Jekk il-verifiki kollha jwasslu għal riżultat pożittiv, ir-root CA toħroġ iċ-ċertifikat tas-sub-CA korrispondenti. L-informazzjoni dettaljata dwar kif issir it-talba inizjali hi deskritta fis-CPS speċifika tagħha.

(108) Minbarra l-formola tal-applikazzjoni tas-sub-CA, ir-rappreżentant awtorizzat tas-sub-CA għandu jehmeż kopja tas-CPS lir-root CA.

(109) L-informazzjoni għandha tingħata lil awditur akkreditat tal-PKI għal awditjar skont it-taqsima 8.

(110) Jekk is-sub-CA hi proprjetà ta' entità differenti mill-entità li tippossjedi r-root CA, qabel ma toħroġ talba għal ċertifikat tas-sub-CA, l-entità tas-sub-CA għandha tiffirma kuntratt rigward is-servizz tar-root CA.

4.1.2.4. Stazzjon tas-C-ITS

(111) Ir-reġistrazzjoni inizjali tas-suġġetti tal-entitajiet aħħarija (stazzjonijiet tas-C-ITS) għandu jagħmilha l-abbonat responsabbli (manifattur/operatur) mal-EA (il-flussi 33 u 35) wara awtentikazzjoni b'suċċess tal-organizzazzjoni tal-abbonat u ta' wieħed mir-rappreżentanti tagħha b'konformità mat-taqsimiet 3.2.2.4 u 3.2.5.2.

(112) L-istazzjon tas-C-ITS jista' jiġġenera par kjavi tal-EC (ara t-taqsima 6.1) u joħloq talba ffirmata għal EC skont [1]. Jistgħu jintużaw protokolli oħra, diment li [1] jiġi implimentat.

(113) Waqt ir-reġistrazzjoni ta' stazzjon normali tas-C-ITS (għall-kuntrarju ta' stazzjon speċjali mobbli jew fiss tas-C-ITS), l-EA għandha tivverifika li l-permessi fit-talba inizjali mhumiex għal użu governattiv. Il-permessi għal użu governattiv huma ddefiniti mill-Istati Membri korrispondenti. Il-proċedura dettaljata għar-reġistrazzjoni u r-rispons tal-EA lill-manifattur/operatur (il-flussi 33 u 35) għandha tkun stabbilita fis-CPS korrispondenti tal-EA.

(114) L-istazzjon tas-C-ITS għandu jkun irreġistrat f'EA (it-taqsima 3.2.5.3) billi jibgħat it-talba inizjali tal-EC tiegħu skont [1].

(115) Malli ssir ir-reġistrazzjoni inizjali minn rappreżentant awtentikat tal-abbonat, l-EA tapprova liema ATs jista' jikseb is-suġġett tal-entità aħħarija (jiġifieri l-istazzjon tas-C-ITS). Barra minn hekk, kull entità aħħarija hi assenjata livell ta'

assigurazzjoni ta' fiduċja, li jkun relatat maċ-ċertifikazzjoni tal-entità aħħarija skont wieħed mill-profili tal-protezzjoni elenkati fit-taqsima 6.1.5.2.

(116) Il-vetturi regolari għandu jkollhom stazzjon tas-C-ITS wieħed biss li jkun irreġistrat f'EA waħda. Vetturi bi skop speċjali (bħall-karozzi tal-pulizija u vetturi oħra bi skop speċjali bi drittijiet speċifiċi) jistgħu jiġu rreġistrati f'EA addizzjonali jew ikollhom stazzjon ieħor addizzjonali tas-C-ITS għall-awtorizzazzjonijiet fi ħdan l-ambitu tal-iskop speċjali. Il-vetturi li għalihom tapplika dan l-eżenzjoni għandhom jiġu ddefiniti mill-Istati Membri responsabbli. Il-permessi għal stazzjonijiet speċjali mobbli u fissi tas-C-ITS għandhom jingħataw biss mill-Istati Membri responsabbli. Is-CPS tar-root CAs jew sub-CAs li joħorġu ċertifikati għal dawk il-vetturi f'dawk l-Istati Membri għandhom jiddeterminaw kif il-proċess taċ-ċertifikat japplika għal dawk il-vetturi.

(117) Jekk l-abbonat ikun fil-proċess li jemigra stazzjon tas-C-ITS minn EA waħda għal EA oħra, l-istazzjon tas-C-ITS jista' jkun irreġistrat f'żewġ EAs (simili).

(118) L-istazzjon tas-C-ITS jiġġenera par kjavi tal-AT (ara t-taqsima 6.1) u joħloq talba għal AT skont [1]. Jistgħu jintużaw protokolli oħra, diment li [1] jiġi implimentat.

(119) L-istazzjonijiet tas-C-ITS jibagħtu talba għall-awtorizzazzjoni lill-URL tal-AA (il-flussi 32 u 26) billi jibagħtu mill-anqas l-informazzjoni meħtieġa msemmija fit-taqsima 3.2.3.3). L-AA u l-EA jivvalidaw l-awtorizzazzjoni għal kull talba skont it-taqsimiet 3.2.6 u 4.2.2.5.

4.2. Ipproċessar ta' applikazzjoni għal ċertifikat

4.2.1. Twettiq ta' funzjonijiet ta' identifikazzjoni u awtentikazzjoni

4.2.1.1. Identifikazzjoni u awtentikazzjoni ta' root CAs

(120) Ir-rappreżentant awtorizzat tas-CPA hu responsabbli għall-awtentikazzjoni tar-rappreżentant awtorizzat tar-root CA u għall-approvazzjoni tal-proċess tar-reġistrazzjoni tagħha skont it-taqsima 3.

4.2.1.2. Identifikazzjoni u awtentikazzjoni tat-TLM

(121) Ir-rappreżentant awtorizzat tas-CPA hu responsabbli mill-awtentikazzjoni tar-rappreżentant awtorizzat tat-TLM u milll-approvazzjoni tal-formola tal-applikazzjoni għall-proċess tar-reġistrazzjoni tiegħu skont it-taqsima 3.

4.2.1.3. Identifikazzjoni u awtentikazzjoni tal-EA u l-AA

(122) Ir-root CA korrispondenti hi responsabbli mill-awtentikazzjoni tar-rappreżentant awtorizzat tal-EA/AA u mill-approvazzjoni tal-formola tal-applikazzjoni għall-proċess tar-reġistrazzjoni tagħha skont it-taqsima 3.

(123) Ir-root CA għandha tikkonferma l-validazzjoni pożittiva tagħha tal-formola tal-applikazzjoni lill-EA/AA. Imbagħad l-EA/AA tista' tibgħat talba għal ċertifikat lir-root CA (il-fluss 21/24), li għandha toħroġ ċertifikati lill-EA/AA korrispondenti (il-fluss 18/19).

4.2.1.4. Identifikazzjoni u awtentikazzjoni tal-abbonat tal-EE

(124) Qabel ma stazzjon tas-C-ITS ikun jista' jitlob ċertifikat tal-EC, l-abbonat tal-EE għandu jittrażmetti b'mod sigur l-informazzjoni tal-identifikatur tal-istazzjon tas-C-ITS lill-EA (il-fluss 33). L-EA għandha tivverifika t-talba u

f'każijiet ta' verifika pożittiva tirreġistra l-informazzjoni dwar l-istazzjon tas-C-ITS fil-bażi tad-*data* tagħha u tikkonferma dan lill-abbonat tal-EE (il-fluss 35). Din l-operazzjoni ssir darba biss mill-manifattur jew mill-operatur għal kull stazzjon tas-C-ITS. Ladarba l-istazzjon tas-C-ITS ikun irreġistrat minn EA, dan jista' jitlob sa ċertifikat wieħed tal-EC li jeħtieġ (il-fluss 31) f'xi mument. L-EA tawtentika u tivverifika li l-informazzjoni fit-talba għaċ-ċertifikat tal-EC hi valida għall-istazzjon tas-C-ITS.

4.2.1.5. Biljetti tal-awtorizzazzjoni

(125) Matul talbiet għall-awtorizzazzjoni (il-fluss 32), skont [1], l-AA għandha tawtentika l-EA li mingħandha l-istazzjon tas-C-ITS ikun irċieva l-EC tiegħu. Jistgħu jintużaw protokolli oħra, diment li [1] jiġi implimentat. Jekk l-AA ma tkunx tista' tawtentika l-EA, it-talba tiġi rifjutata (il-fluss 26). Bħala rekwiżit, l-AA għandu jkollha ċ-ċertifikat tal-EA biex tawtentika l-EA u tivverifika r-rispons tagħha (il-flussi 25 u 23, it-taqsima 3.2.5.3).

(126) L-EA tawtentika l-istazzjon tas-C-ITS li jitlob l-AT billi tivverifika l-EC tiegħu (il-flussi 25 u 23).

4.2.2. Approvazzjoni jew rifjut ta' applikazzjonijiet għal ċertifikat

4.2.2.1. Approvazzjoni jew rifjut ta' ċertifikati ta' root CA

(127) It-TLM idaħħal/iħassar iċ-ċertifikati tar-root CA fl-ECTL skont l-approvazzjoni tas-CPA (fluss 1/2).

(128) It-TLM għandu jivverifika l-firma, l-informazzjoni u l-kodifikazzjoni taċ-ċertifikati tar-root CA wara li jirċievi l-approvazzjoni tas-CPA (il-fluss 1). Wara validazzjoni pożittiva u l-approvazzjoni tas-CPA, it-TLM għandu jpoġġi ċ-ċertifikat root korrispondenti fl-ECTL u jinnotifika lis-CPA (il-fluss 5).

4.2.2.2. *Approvazzjoni jew rifjut ta' ċertifikat tat-TLM*

(129) Is-CPA hi responsabbli mill-approvazzjoni jew ir-rifjut taċ-ċertifikati tat-TLM.

4.2.2.3. *Approvazzjoni jew rifjut ta' ċertifikati tal-EA u tal-AA*

(130) Ir-root CA tivverifika t-talbiet għaċ-ċertifikati tas-sub-CA (il-fluss 21/24) u r-rapporti rilevanti (maħruġa mill-awditur akkreditat tal-PKI) meta tirċevihom (il-fluss 36, it-taqsima 8) mingħand is-sub-CA korrispondenti tar-root CA. Jekk il-verifika tat-talba twassal għal riżultat pożittiv, ir-root CA korrispondenti toħroġ ċertifikat lill-EA/AA rikjedenti (il-fluss 18/19); inkella, it-talba tiġi rifjutata u ma għandu jinħareġ l-ebda ċertifikat lill-EA/AA.

4.2.2.4. Approvazzjoni jew rifjut ta' EC

(131) L-EA għandha tivverifika u tivvalida t-talbiet għall-EC skont it-taqsimiet 3.2.3.2 u 3.2.5.3.

(132) Jekk it-talba għal ċertifikat skont [1] hi korretta u valida, l-EA għandha tiġġenera ċ-ċertifikat mitlub.

(133) Jekk it-talba għal ċertifikat mhix valida, l-EA tirrifjutaha u tibgħat rispons li jistabbilixxi r-raġuni għar-rifjut skont [1]. Jekk l-istazzjon tas-C-ITS xorta jkun irid l-EC, dan għandu jagħmel talba ġdida għal ċertifikat. Jistgħu jintużaw protokolli oħra, diment li [1] jiġi implimentat.

4.2.2.5. Approvazzjoni jew rifjut ta' AT

(134) It-talba għal ċertifikat hi vverifikata mill-EA. L-AA għandha tistabbilixxi komunikazzjoni mal-EA biex tivvalida t-talba (il-fluss 25). L-EA għandha tawtentika l-istazzjon tas-C-ITS rikjedenti u tivvalida jekk hux intitolat li jirċievi l-AT mitlub b'konformità mas-CP (eż. billi tivverifika l-istatus tar-revoka u tivvalida l-validità tal-ħin/tar-reġjun taċ-ċertifikat, il-permessi, il-livell ta' assigurazzjoni, eċċ.). L-EA għandha tirritorna rispons ta' validazzjoni (il-fluss 23) u, jekk ir-rispons ikun pożittiv, l-AA għandha tiġġenera ċ-ċertifikat mitlub u tittrażmettih lill-istazzjon tas-C-ITS. Jekk it-talba għal AT ma tkunx korretta jew ir-rispons tal-validazzjoni tal-EA ikun negattiv, l-AA tirrifjuta t-talba. Jekk l-istazzjon tas-C-ITS xorta jkun jeħtieġ l-AT, dan għandu jagħmel talba ġdida għall-awtorizzazzjoni.

4.2.3. Żmien biex tiġi pproċessata l-applikazzjoni għal ċertifikat

4.2.3.1. Applikazzjoni għal ċertifikat ta' root CA

(135) Il-proċess tal-identifikazzjoni u tal-awtentikazzjoni ta' applikazzjoni għal ċertifikat isir matul il-ġranet tax-xogħol u għandu jkun soġġett għal limitu ta' żmien massimu stabbilit fis-CPS tar-root CA.

4.2.3.2. *Applikazzjoni għal ċertifikat tat-TLM*

(136) L-ipproċessar tal-applikazzjoni taċ-ċertifikat tat-TLM għandu jkun soġġett għal limitu ta' żmien massimu stabbilit fis-CPS tat-TLM.

4.2.3.3. *Applikazzjoni għal ċertifikat tal-EA u tal-AA*

(137) Il-mument meta jsir l-ipproċessar tal-proċess tal-identifikazzjoni u tal-awtentikazzjoni ta' applikazzjoni għal ċertifikat hu matul ġurnata tax-xogħol skont il-ftehim u l-kuntratt bejn l-Istat Membru/l-organizzazzjoni privata tar-root CA u s-sub-CA. Il-ħin għall-ipproċessar tal-applikazzjoni taċ-ċertifikat tas-sub-CA għandu jkun soġġett għal-limitu ta' żmien massimu stabbilit fis-CPS tas-Sub-CA.

4.2.3.4. *Applikazzjoni għal EC*

(138) L-ipproċessar tal-applikazzjonijiet għal EC għandu jkun soġġett għal limitu ta' żmien massimu stabbilit fis-CPS tal-EA.

4.2.3.5. *Applikazzjoni għal AT*

(139) L-ipproċessar tal-applikazzjonijiet għal AT għandu jkun soġġett għal limitu ta' żmien massimu stabbilit fis-CPS tal-AA.

4.3. Ħruġ ta' ċertifikat

4.3.1. Azzjonijiet tas-CA matul il-ħruġ ta' ċertifikat

4.3.1.1. Ħruġ ta' ċertifikat tar-root CA

(140) Ir-root CAs joħorġu ċ-ċertifikati tar-root CA tagħhom stess iffirmati minnhom stess, iċ-ċertifikati tal-konnessjoni, iċ-ċertifikati tas-sub-CA u s-CRLs.

(141) Wara l-approvazzjoni tas-CPA (il-fluss 4), ir-root CA tibgħat iċ-ċertifikat tagħha lit-TLM permezz tas-CPOC li għandu jiżdied mal-ECTL (il-flussi 11 u 8) (ara t-taqsima 4.1.2.1). It-TLM jivverifika jekk is-CPA approvatx iċ-ċertifikat (il-fluss 1).

4.3.1.2. *Ħruġ ta' ċertifikat tat-TLM*

(142) It-TLM joħroġ iċ-ċertifikat tat-TLM u tal-konnessjoni tiegħu stess iffirmat minnu stess u jibagħtu lis-CPOC (il-fluss 6).

4.3.1.3. Ħruġ ta' ċertifikat tal-EA u tal-AA

(143) Is-sub-CAs jiġġeneraw talba ffirmata għal ċertifikat u jittrażmettuha lir-root CA korrispondenti (il-flussi 21 u 24). Ir-root CA tivverifika t-talba u toħroġ ċertifikat lis-sub-CA rikjedenti skont [5] kemm jista' jkun malajr, kif stabbilit fis-CPS għal prattiki operattivi tas-soltu, iżda sa mhux aktar tard minn ħamest ijiem tax-xogħol wara li tkun irċeviet it-talba.

(144) Ir-root CA għandha taġġorna r-repożitorju li fih iċ-ċertifikati tas-sub-CAs.

4.3.1.4. Ħruġ ta' EC

(145) L-istazzjon tas-C-ITS għandu jibgħat talba għal EC lill-EA skont [1]. L-EA għandha tawtentika u tivverifika li l-informazzjoni fit-talba għaċ-ċertifikat hi valida għall-istazzjon tas-C-ITS. Jistgħu jintużaw protokolli oħra, diment li [1] jiġi implimentat.

(146) F'każijiet ta' validazzjoni pożittiva, l-EA għandha toħroġ ċertifikat skont ir-reġistrazzjoni tal-istazzjon tas-C-ITS (ara 4.2.1.4) u tibagħtu lill-istazzjon tas-C-ITS billi tuża messaġġ ta' rispons tal-EC skont [1]. Jistgħu jintużaw protokolli oħra, diment li [1] jiġi implimentat.

(147) Jekk ma jkun hemm l-ebda reġistrazzjoni, l-EA għandha tiġġenera kodiċi ta' errur u tibagħtu lill-istazzjon tas-C-ITS billi tuża messaġġ ta' rispons tal-EC skont [1]. Jistgħu jintużaw protokolli oħra, diment li [1] jiġi implimentat.

(148) It-talbiet għal EC u r-rispons tal-EC għandhom ikunu kriptati biex tiġi żgurata l-kunfidenzjalità u jkunu ffirmati biex jiġu żgurati l-awtentikazzjoni u l-integrità.

4.3.1.5. Ħruġ ta' AT

(149) L-istazzjon tas-C-ITS għandu jibgħat messaġġ ta' talba għal AT lill-AA, skont [1]. L-AA għandha tibgħat talba għall-validazzjoni tal-AT skont [1] lill-EA. L-EA għandha tibgħat rispons għall-validazzjoni tal-AT lill-AA. F'każijiet ta' rispons pożittiv, l-AA għandha tiġġenera AT u tibagħtu lill-istazzjon tas-C-ITS billi tuża messaġġ ta' rispons tal-AT skont [1]. F'każijiet ta' rispons negattiv, l-AA għandha tiġġenera kodiċi ta' errur u tibagħtu lill-istazzjon tas-C-ITS billi tuża messaġġ ta' rispons tal-AT skont [1]. Jistgħu jintużaw protokolli oħra, diment li [1] jiġi implimentat.

(150) It-talbiet għal AT u r-rispons tal-AT għandhom jiġu kriptati (dan hu meħtieġ biss għall-istazzjonijiet mobbli tas-C-ITS) biex tiġi żgurata l-kunfidenzjalità u jiġu ffirmati biex ikunu żgurati l-awtentikazzjoni u l-integrità.

4.3.2. Notifika tas-CA lill-abbonat dwar il-ħruġ ta' ċertifikati.

Mhux applikabbli.

4.4. Aċċettazzjoni taċ-ċertifikat

4.4.1. Twettiq ta' aċċettazzjoni taċ-ċertifikat

4.4.1.1. *Root CA*

Mhux applikabbli.

4.4.1.2. *TLM*

Mhux applikabbli.

4.4.1.3. *EA u AA*

(151) L-EA/AA għandhom jivverifikaw it-tip taċ-ċertifikat, il-firma u l-informazzjoni fiċ-ċertifikat riċevut. L-EA/AA għandhom iwarrbu ċ-ċertifikati kollha tal-EA/AA li mhumiex ivverifikati sew u joħorġu talba ġdida.

4.4.1.4. Stazzjon tas-C-ITS

(152) L-istazzjon tas-C-ITS għandu jivverifika r-rispons tal-EC/AT riċevut mill-EA/AA kontra t-talba oriġinali tiegħu, inkluż il-firma u l-katina taċ-ċertifikat. Għandu jwarrab ir-rispons kollu tal-EC/AT li mhux ivverifikat sew. F'dawn il-każijiet, dan għandu jibgħat talba ġdida tal-EC/AT.

4.4.2. Pubblikazzjoni taċ-ċertifikat

(153) Iċ-ċertifikati tat-TLM u ċ-ċertifikati tal-konnessjoni tagħhom għandhom ikunu disponibbli għall-parteċipanti kollha permezz tas-CPOC.

(154) Iċ-ċertifikati tar-root CA jiġu ppubblikati mis-CPOC permezz tal-ECTL, li tiġi ffirmata mit-TLM.

(155) Iċ-ċertifikati tas-sub-CAs (tal-EAs u tal-AAs) jiġu ppubblikati mir-root CA.

(156) L-ECs u l-ATs ma jiġux ippubblikati.

4.4.3. Notifika tal-ħruġ taċ-ċertifikat

Mhemmx notifiki tal-ħruġ.

4.5. Par kjavi u użu taċ-ċertifikat

4.5.1. ***Kjavi privata u użu taċ-ċertifikat***

4.5.1.1. Kjavi privata u użu taċ-ċertifikat għat-TLM

(157) It-TLM għandu juża l-kjavi privati tiegħu biex jiffirma ċ-ċertifikati tiegħu stess (tat-TLM u tal-konnessjoni) u l-ECTL.

(158) Iċ-ċertifikat tat-TLM għandu jintuża mill-parteċipanti tal-PKI biex jivverifikaw l-ECTL u jawtentikaw it-TLM.

4.5.1.2. Kjavi privata u użu taċ-ċertifikati għar-root CAs

(159) Ir-root CAs għandhom jużaw il-kjavi privati tagħhom biex jiffirmaw iċ-ċertifikati tagħhom stess, is-CRL, iċ-ċertifikati tal-konnessjoni u ċ-ċertifikati tal-EA/AA.

(160) Iċ-ċertifikati tar-root CA għandhom jintużaw mill-parteċipanti tal-PKI biex jivverifikaw iċ-ċertifikati assoċjati tal-AA u tal-EA, iċ-ċertifikati tal-konnessjoni u s-CRLs.

4.5.1.3. Kjavi privata u użu taċ-ċertifikat għal EAs u AAs

(161) L-EAs għandhom jużaw il-kjavi privati tagħhom biex jiffirmaw l-ECs u għad-dekriptaġġ tat-talba għar-reġistrazzjoni.

(162) Iċ-ċertifikati tal-EA għandhom jintużaw biex jivverifikaw il-firma tal-ECs assoċjati u għall-kriptaġġ tat-talba għal EC u AT mill-EEs kif definit f'[1].

(163) L-AAs għandhom jużaw il-kjavi privati tagħhom biex jiffirmaw l-ATs u għad-dekriptaġġ tat-talba għal AT.

(164) Iċ-ċertifikati tal-AA għandhom jintużaw mill-EEs biex jivverifikaw l-ATs assoċjati u għall-kriptaġġ tat-talba għal AT kif definit f'[1].

4.5.1.4. Kjavi privata u użu taċ-ċertifikat għall-entità aħħarija

(165) L-EEs għandhom jużaw il-kjavi privata li tikkorrispondi għal EC valida biex jiffirmaw talba ġdida għar-reġistrazzjoni kif definit f'[1]. Il-kjavi privata l-ġdida għandha tintuża biex tinbena l-firma interna fit-talba biex tingħata prova tal-pussess tal-kjavi privata li tikkorrispondi għall-kjavi pubblika l-ġdida tal-EC.

(166) L-EEs għandhom jużaw il-kjavi privata li tikkorrispondi għal EC valida biex jiffirmaw talba għall-awtorizzazzjoni kif definit f'[1]. Il-kjavi privata li tikkorrispondi għall-AT l-ġdid għandha tintuża biex tinbena l-firma interna fit-talba biex tingħata prova tal-pussess tal-kjavi privata li tikkorrispondi għall-kjavi pubblika l-ġdida tal-AT.

(167) L-EE għandha tuża l-kjavi privata li tikkorrispondi għal AT xieraq biex tiffirma messaġġi tas-C-ITS kif definit f'[5].

4.5.2. ***Kjavi pubblika tal-parti dipendenti u użu taċ-ċertifikat***

(168) Il-partijiet dipendenti jużaw il-passaġġ taċ-ċertifikazzjoni fdat u l-kjavi pubbliċi assoċjati għall-għanijiet imsemmija fiċ-ċertifikati u biex jawtentikaw l-identità komuni fdata tal-ECs u tal-ATs.

(169) Iċ-ċertifikati, l-ECs u l-ATs tar-root CA, tal-EA u tal-AA ma għandhomx jintużaw mingħajr verifika preliminari minn parti dipendenti.

4.6. Tiġdid taċ-ċertifikat

Mhux permess.

4.7. Rikjavar taċ-ċertifikat

4.7.1. Ċirkostanzi għar-rikjavar taċ-ċertifikat

(170) Ir-rikjavar taċ-ċertifikat għandu jiġi pproċessat meta ċertifikat jasal fi tmiem il-ħajja tiegħu jew meta l-kjavi privata tasal fi tmiem l-użu operazzjonali, iżda r-relazzjoni ta' fiduċja mas-CA tkun għadha teżisti. Par kjavi ġdid u ċ-ċertifikat korrispondenti għandhom jiġu ġġenerati u maħruġa fil-każijiet kollha.

4.7.2. Min jista' jitlob rikjavar

4.7.2.1. *Root CA*

(171) Ir-root CA ma titlobx rikjavar. Il-proċess ta' rikjavar hu proċess intern għar-root CA, għax iċ-ċertifikat tagħha hu ffirmat minnha stess. Ir-root CA għandha twettaq ir-rikjavar biċ-ċertifikati tal-konnessjoni jew bi ħruġ ġdid (ara t-taqsima 4.3.1.1).

4.7.2.2. *TLM*

(172) It-TLM ma jitlobx rikjavar. Il-proċess ta' rikjavar hu intern għat-TLM, għax iċ-ċertifikat tat-TLM hu ffirmat minnu stess.

4.7.2.3. *EA u AA*

(173) It-talba għaċ-ċertifikat tas-sub-CA trid tiġi ppreżentata fi żmien xieraq biex ikun żgur li jkun hemm ċertifikat ġdid tas-sub-CA u par kjavi tas-sub-CA operazzjonali qabel ma tiskadi l-kjavi privata attwali tas-sub-CA. Id-data tal-preżentazzjoni għandha tqis ukoll iż-żmien meħtieġ għall-approvazzjoni.

4.7.2.4. Stazzjon tas-C-ITS

Mhux applikabbli.

4.7.3. Proċess ta' rikjavar

4.7.3.1. Ċertifikat tat-TLM

(174) It-TLM jiddeċiedi li jagħmel rikjavar abbażi tar-rekwiżiti fit-taqsimiet 6.1 u 7.2. Il-proċess dettaljat hu stabbilit fis-CPS tiegħu.

(175) It-TLM għandu jwettaq il-proċess ta' rikjavar fi żmien xieraq biex tkun tista' ssir id-distribuzzjoni taċ-ċertifikat il-ġdid tat-TLM u ċ-ċertifikat tal-konnessjoni lill-parteċipanti kollha qabel ma jiskadi ċ-ċertifikat attwali tat-TLM.

(176) It-TLM għandu juża ċ-ċertifikati tal-konnessjoni għar-rikjavar u biex jiggarantixxi r-relazzjoni ta' fiduċja taċ-ċertifikat il-ġdid iffirmat minnu stess. It-TLM u ċ-ċertifikat tal-konnessjoni ġġenerati ġodda jiġu ttrasferiti lis-CPOC.

4.7.3.2. Ċertifikat ta' root CA

(177) Ir-root CA tiddeċiedi li tagħmel ir-rikjavar abbażi tar-rekwiżiti tat-taqsimiet 6.1.5 u 7.2. Il-proċess dettaljat għandu jiġi ddefinit fis-CPS tagħha.

(178) Ir-root CA għandha twettaq il-proċess ta' rikjavar fi żmien xieraq (qabel ma jiskadi ċ-ċertifikat tar-root CA) biex tkun tista' ssir inklużjoni taċ-ċertifikat il-ġdid fl-ECTL qabel ma ċ-ċertifikat tar-root CA isir validu (ara t-taqsima 5.6.2). Il-proċess ta' rikjavar għandu jitwettaq permezz taċ-ċertifikati tal-konnessjoni jew bħala talba inizjali.

4.7.3.3. Ċertifikati tal-EA u l-AA

(179) L-EA jew l-AA għandhom jitolbu ċertifikat ġdid kif ġej:

Stadju	**Indikazzjoni**	**Talba għal rikjavar**
1	**Ġenerazzjoni tal-par kjavi**	Is-sub-CAs (EAs u AAs) għandhom jiġġeneraw pari kjavi ġodda skont it-taqsima 6.1.
2	**Ġenerazzjoni tat-talba għal ċertifikat u tal-firma ta' interna**	Is-sub-CA tiġġenera talba għal ċertifikat mill-kjavi pubblika li tkun għada kif ġiet iġġenerata billi tikkunsidra l-iskema tal-ismijiet (subject_info) tat-taqsima 3, l-algoritmu tal-firma, il-Permessi Speċifiċi għas-Servizz (l-SSPs) u parametru addizzjonali fakultattiv, u tiġġenera l-firma interna bil-kjavi privata l-ġdida korrispondenti. Jekk tkun meħtieġa kjavi tal-kriptaġġ, is-sub-CA għandha wkoll tagħti prova tal-pussess tal-kjavi privata tad-dekriptaġġ korrispondenti.
3	**Ġenerazzjoni tal-firma esterna**	It-talba kollha għandha tiġi ffirmata bil-kjavi privata valida attwali biex tiġi ggarantita l-awtenticità tat-talba ffirmata.
4	**Talba mibgħuta lir-root CA**	It-talba ffirmata għandha tiġi ppreżentata lir-root CA korrispondenti.
5	**Verifika tat-talba**	Ir-root CA korrispondenti għandha tivverifika l-integrità u l-awtenticità

		tat-talba. L-ewwel nett, għandha tivverifika l-firma esterna. Jekk il-verifika hi pożittiva, għandha tivverifika l-firma interna. Meta jkun hemm prova tal-pussess tal-kjavi privata tad-dekriptaġġ, għandha tivverifika wkoll din il-prova.
6	**Aċċettazzjoni jew rifjut tat-talba**	Jekk il-verifiki kollha jwasslu għal riżultat pożittiv, ir-root CA taċċetta t-talba; inkella, tiċħad it-talba.
7	**Ġenerazzjoni u ħruġ taċ-ċertifikat**	Ir-root CA tiġġenera ċertifikat ġdid u tqassmu lis-sub-CA rikjedenti.
8	**Rispons mibgħut**	Is-sub-CA għandha tibgħat messaġġ dwar l-istatus (dwar jekk irċevietx iċ-ċertifikat jew le) lir-root CA.

Tabella 3: Proċess ta' rikjavar għall-EAs u l-AAs

(180) Waqt rikjavar awtomatiku għas-sub-CAs, ir-root CA għandha tiżgura li min jagħmel it-talba jkun tabilħaqq fil-pussess tal-kjavi privata tagħha. Għandhom jiġu applikati protokolli xierqa għall-prova tal-pussess tal-kjavi privati tad-dekriptaġġ, pereżempju kif definit fl-RFC 4210 u 4211. Għal kjavi ta' firma privata, għandha tintuża l-firma interna.

4.7.3.4. Ċertifikati ta' stazzjon tas-C-ITS

Mhux applikabbli għall-AT.

4.8. Modifika taċ-ċertifikat

Mhux permess.

4.9. Revoka u sospensjoni taċ-ċertifikat

Ara t-taqsima 7

4.10. Servizzi tal-istatus taċ-ċertifikat

4.10.1. Karatteristiċi operazzjonali

Ma japplikax

4.10.2. Disponibbiltà tas-servizz

Ma japplikax

4.10.3. Karatteristiċi mhux obbligatorji

Ma japplikax

4.11. Tmiem l-abbonament

Ma japplikax

4.12. Kjavi miżmuma minn terzi u rkupru tal-kjavi

4.12.1. Abbonat

4.12.1.1. Liema par kjavi jista' jinżamm minn terzi

Mhux applikabbli.

4.12.1.2. Min jista' jippreżenta applikazzjoni għall-irkupru

Mhux applikabbli.

4.12.1.3. Proċess ta' rkupru u responsabbiltajiet

Mhux applikabbli.

4.12.1.4. Identifikazzjoni u awtentikazzjoni

Mhux applikabbli.

4.12.1.5. Approvazzjoni jew rifjut ta' applikazzjonijiet għall-irkupru

Mhux applikabbli.

4.12.1.6. Azzjonijiet KEA u KRA matul l-irkupru tal-par kjavi

Mhux applikabbli.

4.12.1.7. Disponibbiltà ta' KEA u KRA

Mhux applikabbli.

4.12.2. Inkapsulament tal-kjavi tas-sessjoni u politika u prattiki tal-irkupru

Mhux applikabbli.

5. KONTROLLI TAL-FAĊILITÀ, TAL-IMANIĠĠJAR U OPERAZZJONALI

(181) Il-PKI hi magħmula mir-root CA, l-EA/AA, is-CPOC u t-TLM, inkluż il-komponenti tal-ICT tagħhom (eż. networks u servers).

(182) F'din it-taqsima, l-entità responsabbli minn element tal-PKI hi identifikata mill-element innifsu. Fi kliem ieħor, is-sentenza "is-CA hi responsabbli mit-twettiq tal-awditjar" hi ekwivalenti għal "l-entità jew il-persunal li jimmaniġġjaw is-CA huma responsabbli mit-twettiq…".

(183) It-terminu "elementi tal-mudell ta' fiduċja tas-C-ITS" jinkludi r-root CA, it-TLM, l-EA/AA, is-CPOC u n-network sigur.

5.1. Kontrolli fiżiċi

(184) L-operazzjonijiet kollha tal-mudell ta' fiduċja tas-C-ITS għandhom jitwettqu f'ambjent fiżikament protett li jiskoraġġixxi, jipprevjeni u jidentifika l-użu mhux awtorizzat ta', l-aċċess għal jew l-iżvelar ta' informazzjoni u sistemi sensittivi. L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom jużaw kontrolli tas-sigurtà fiżika b'konformità ma' ISO 27001 u ISO 27005.

(185) L-entitajiet li jimmaniġġjaw l-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom jiddeskrivu l-kontrolli tas-sigurtà fiżiċi, proċedurali u tal-persunal fis-CPS tagħhom. B'mod partikolari, is-CPS għandha tkopri informazzjoni dwar il-post tas-sit u l-kostruzzjoni tal-bini u l-kontrolli tas-sigurtà fiżika tagħhom li jiggarantixxu aċċess ikkontrollat għall-kmamar kollha użati fil-faċilità tal-entitajiet tal-mudell ta' fiduċja tas-C-ITS.

5.1.1. Post tas-sit u kostruzzjoni

5.1.1.1. Root CA, CPOC, TLM

(186) Il-post u l-kostruzzjoni tal-faċilità li takkomoda t-tagħmir u d-*data* tar-root CA, tas-CPOC u tat-TLM (HSM, *data* tal-attivazzjoni, backup tal-par kjavi, kompjuter, reġistru, skript taċ-ċerimonja tal-kjavi, talba għaċ-ċertifikat, eċċ.) għandhom ikunu konsistenti mal-faċilitajiet użati biex jakkomodaw informazzjoni ta' valur għoli u sensittiva. Ir-root CA għandha titħaddem f'żona fiżika ddedikata separata minn żoni fiżiċi oħra ta' komponenti tal-PKI.

(187) Ir-root CA, is-CPOC u t-TLM għandhom jimplimentaw politiki u proċeduri biex jiżguraw li jinżamm livell għoli ta' sigurtà fl-ambjent fiżiku li fih jiġi installat it-tagħmir tar-root CA, biex jiggarantixxu li:

- jkun iżolat minn networks barra l-mudell ta' fiduċja;
- jkun separat f'serje ta' (mill-anqas tnejn) perimetri fiżiċi progressivament aktar siguri;
- *data* sensittiva (HSM, backup tal-par kjavi, *data* tal-attivazzjoni, eċċ.) tkun maħżuna f'sejf apposta li jkun jinsab f'żona fiżika apposta b'kontroll ta' aċċess multiplu.

(188) It-tekniki tas-sigurtà użati għandhom ikunu ddisinjati biex jirreżistu numru kbir u kombinazzjoni ta' forom differenti ta' attakki. Il-mekkaniżmi użati għandhom jinkludu mill-anqas:

- allarmi tal-perimetru, televiżjoni b'ċirkwit magħluq, ħitan rinfurzati u diteters tal-moviment;
- awtentikazzjoni b'żewġ fatturi (eż. smartcard u PIN) għal kull persuna u badge biex tidħol u toħroġ mill-faċilitajiet tar-root CA u miż-żona protetta fiżika sikura.

(189) Ir-root CA, is-CPOC u t-TLM jużaw persunal awtorizzat biex kontinwament jimmonitorjaw il-faċilità li takkomoda t-tagħmir abbażi ta' 7x24x365. L-ambjent operattiv (eż. il-faċilità fiżika) qatt ma għandu jitħalla waħdu. Il-persunal tal-ambjent operattiv qatt ma għandu jkollu aċċess għaż-żoni siguri tar-root CAs jew tas-sub-CAs sakemm ma jkunx awtorizzat.

5.1.1.2. *EA/AA*

(190) Japplikaw l-istess dispożizzjonijiet tat-taqsima 5.1.1.1.

5.1.2. Aċċess fiżiku

5.1.2.1. Root CA, CPOC, TLM

(191) It-tagħmir u d-*data* (HSM, *data* tal-attivazzjoni, backup tal-par kjavi, kompjuter, reġistru, skript taċ-ċerimonja tal-kjavi, talba għal ċertifikat, eċċ.) għandhom dejjem ikunu protetti minn aċċess mhux awtorizzat. Il-mekkaniżmi tas-sigurtà fiżika għat-tagħmir għandhom mill-anqas:

- jimmonitorjaw, manwalment jew b'mod elettroniku, għal dħul mhux awtorizzat f'kull ħin;
- jiżguraw li ma jkun permess l-ebda aċċess mhux awtorizzat għall-ħardwer u għad-*data* tal-attivazzjoni;
- jiżguraw li l-midja trasferibbli u l-karti kollha li jkun fihom informazzjoni sensittiva b'test sempliċi jinħażnu f'kontenitur sigur;
- jiżguraw li kwalunkwe individwu li jidħol fiż-żoni siguri li mhux awtorizzat fuq bażi permanenti ma għandux jitħalla mingħajr superviżjoni minn impjegat awtorizzat tal-faċilitajiet tar-root CA, tas-CPOC u tat-TLM;
- jiżguraw li r-reġistru tal-aċċess jinżamm u jiġi spezzjonat perjodikament;

- jipprovdu mill-anqas żewġ saffi ta' sigurtà li tiżdied progressivament, eż. fil-livell tal-perimetru, tal-bini u tal-kamra operattiva;
- jeħtieġu żewġ kontrolli ta' aċċess fiżiku ta' rwol ta' fiduċja għall-HSM kriptografiċi u d-*data* tal-attivazzjoni.

(192) Għandha titwettaq verifika tas-sigurtà tal-faċilità li takkomoda t-tagħmir jekk tkun se titħalla waħedha. Bħala minimu, il-verifika għandha tivverifika li:

- it-tagħmir hu fi stat li jixraq għall-mod ta' tħaddim attwali;
- għall-komponenti offline, it-tagħmir kollu jkun mitfi;
- kwalunkwe kontenitur tas-sigurtà (envelopp li ma jippermettix tbagħbis, sejf, eċċ.) hu protett sew;
- is-sistemi ta' sigurtà fiżika (eż. serraturi tal-bibien, għata tal-ventilazzjoni, elettriku) qed jaħdmu sew;
- iż-żona hi protetta kontra aċċess mhux awtorizzat.

(193) Il-moduli kriptografiċi li jistgħu jitneħħew għandhom jiġu diżattivati qabel il-ħażna. Meta ma jkunux qed jintużaw, dawn il-moduli u d-*data* tal-attivazzjoni użata biex jiġu aċċessati jew biex jiġu attivati għandhom jitqiegħdu f'sejf. Id-*data* tal-attivazzjoni għandha jew tkun memorizzata jew irreġistrata u maħżuna b'mod proporzjonat mas-sigurtà mogħtija lill-modulu kriptografiku. Ma għandhomx jinħażnu bil-modulu kriptografiku, biex jiġi evitat li persuna waħda biss ikollha aċċess għall-kjavi privata.

(194) Persuna jew grupp ta' rwoli fdati għandhom ikunu responsabbli b'mod espliċitu biex jagħmlu dawn il-verifiki. Meta grupp ta' nies ikunu responsabbli, għandu jinżamm reġistru li jidentifika l-persuna li twettaq kull verifika. Jekk ma jkunx hemm xi ħadd kontinwament fil-faċilità, l-aħħar persuna li titlaq għandha tniżżel l-inizjali tagħha fuq il-folja tal-ħruġ li tindika d-data u l-ħin, u tikkonferma li l-mekkaniżmi kollha meħtieġa ta' protezzjoni fiżika huma stabbiliti u attivati.

5.1.2.2. *EA/AA*

(195) Japplikaw l-istess dispożizzjonijiet tat-taqsima 5.1.2.1.

5.1.3. Enerġija u arja kundizzjonata

(196) Il-faċilitajiet siguri tal-elementi tal-mudell ta' fiduċja tas-C-ITS (root CA, CPOC, TLM, EA u AA) għandhom ikunu mgħammra b'aċċess affidabbli għall-enerġija elettrika biex jiżguraw tħaddim mingħajr ħsarat jew bi ħsarat żgħar. L-installazzjonijiet primarji u tal-backup huma meħtieġa fil-każ ta' qtugħ estern fl-enerġija u waqfien bla xkiel tat-tagħmir tal-mudell ta' fiduċja tas-C-ITS fil-każ ta' nuqqas ta' enerġija. Il-faċilitajiet tal-mudell ta' fiduċja tas-C-ITS għandhom ikunu mgħammra b'sistemi ta' tisħin/ventilazzjoni/arja kundizzjonata biex iżommu t-temperatura u l-umdità relattiva tat-tagħmir tal-mudell ta' fiduċja tas-C-ITS fil-firxa operattiva. Is-CPS tal-element tal-mudell ta' fiduċja tas-C-ITS se tiddeskrivi fid-dettall il-pjan u l-proċessi għall-implimentazzjoni ta' dawn ir-rekwiżiti.

5.1.4. Esponimenti għall-ilma

(197) Il-faċilitajiet siguri tal-elementi tal-mudell ta' fiduċja tas-C-ITS (root CA, CPOC, TLM, EA u AA) għandhom jiġu protetti b'mod li jimminimizza l-

impatt mill-esponiment għall-ilma. Għal din ir-raġuni, il-pajpijiet tal-ilma u tal-ħamrija għandhom jiġu evitati. Is-CPS tal-element tal-mudell ta' fiduċja tas-C-ITS se tiddeskrivi fid-dettall il-pjan u l-proċessi għall-implimentazzjoni ta' dawn ir-rekwiżiti.

5.1.5. Prevenzjoni u protezzjoni min-nar

(198) Biex tiġi evitata l-espożizzjoni dannuża għall-fjammi jew għad-duħħan, il-faċilitajiet siguri tal-elementi tal-mudell ta' fiduċja tas-C-ITS (root CA, CPOC, TLM, EA u AA) għandhom jinbnew u jkunu mgħammra kif xieraq u għandhom jiġu implimentati proċeduri biex jindirizzaw it-theddid relatat man-nar. Il-ħażna tal-midja għandha tkun protetta kontra n-nar f'kontenituri xierqa.

(199) L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom jipproteġu l-midja fiżika li jkollha l-backups tad-*data* kritika tas-sistema jew kwalunkwe informazzjoni sensittiva oħra minn perikli ambjentali u użu mhux awtorizzat ta', aċċess għal jew żvelar ta' din il-midja. Is-CPS tal-element tal-mudell ta' fiduċja tas-C-ITS se tiddeskrivi fid-dettall il-pjan u l-proċessi għall-implimentazzjoni ta' dawn ir-rekwiżiti.

5.1.6. L-immaniġġjar tal-midja

(200) Il-midja użata fl-elementi tal-mudell ta' fiduċja tas-C-ITS (root CA, CPOC, TLM, EA u AA) hi mmaniġġjata b'mod sigur biex tkun protetta minn ħsara, serq u aċċess mhux awtorizzat. Il-proċeduri ta' mmaniġġjar tal-midja huma implimentati biex jipproteġu kontra l-obsolexxenza u d-deterjorazzjoni tal-midja fil-perjodu li għalih iridu jinżammu r-rekords.

(201) Id-*data* sensittiva għandha tkun protetta milli tiġi aċċessata meta l-oġġetti tal-ħażna jintużaw mill-ġdid (eż. fajls imħassra), li jistgħu jagħmlu d-*data* sensittiva aċċessibbli għal utenti mhux awtorizzati.

(202) Għandu jinżamm inventarju tal-assi kollha tal-informazzjoni u r-rekwiżiti stabbiliti għall-protezzjoni ta' dawn l-assi li huma konsistenti mal-analiżi tar-riskju. Is-CPS tal-element tal-mudell ta' fiduċja tas-C-ITS se tiddeskrivi fid-dettall il-pjan u l-proċessi għall-implimentazzjoni ta' dawn ir-rekwiżiti.

5.1.7. Rimi tal-iskart

(203) L-elementi tal-mudell ta' fiduċja tas-C-ITS (root CA, CPOC, TLM, EA u AA) għandhom jimplimentaw proċeduri għar-rimi sigur u irriversibbli tal-iskart (karti, midja jew kwalunkwe skart ieħor) biex jipprevjenu l-użu mhux awtorizzat ta', l-aċċess għal jew l-iżvelar ta' skart li jkun fih informazzjoni kunfidenzjali/privata. Il-mezzi kollha użati għall-ħażna ta' informazzjoni sensittiva, bħalma huma l-kjavi, id-*data* tal-attivazzjoni jew il-fajls, għandhom jinqerdu qabel ma jiġu rilaxxati għar-rimi. Is-CPS tal-element tal-mudell ta' fiduċja tas-C-ITS se tiddeskrivi fid-dettall il-pjan u l-proċessi għall-implimentazzjoni ta' dawn ir-rekwiżiti.

5.1.8. Backup mhux fuq il-post

5.1.8.1. Root CA, CPOC u TLM

(204) Il-backups sħaħ tal-komponenti tar-root CA, tas-CPOC u tat-TLM, li huma biżżejjed biex jirkupraw minn ħsara fis-sistema, isiru offline wara t-tnedija tar-root CA, tas-CPOC u tat-TLM u wara kull ġenerazzjoni ġdida tal-par kjavi. Il-

kopji tal-backup tal-informazzjoni essenzjali tan-negozju (par kjavi u CRL) u tas-softwer isiru b'mod regolari. Il-faċilitajiet tal-backup adegwati huma pprovduti biex jiżguraw li l-informazzjoni u s-softwer essenzjali tan-negozju kollha jkunu jistgħu jiġu rkuprati wara diżastru jew falliment tal-midja. L-arranġamenti tal-backup għal sistemi individwali jiġu ttestjati regolarment biex jiġi żgurat li jissodisfaw ir-rekwiżiti tal-pjan tal-kontinwità tan-negozju. Mill-anqas kopja waħda sħiħa tal-backup hi maħżuna f'post barra mis-sit (irkupru minn diżastru). Il-kopja tal-backup tinħażen f'sit b'kontrolli fiżiċi u proċedurali proporzjonati għal dawk tas-sistema operattiva tal-PKI.

(205) Id-*data* tal-backup hi soġġetta għall-istess rekwiżiti tal-aċċess bħad-*data* operattiva. Id-*data* tal-backup għandha tkun kriptata u maħżuna mhux fuq il-post. Fil-każ ta' telf sħiħ tad-*data*, l-informazzjoni meħtieġa għat-tħaddim mill-ġdid tar-root CA, tas-CPOC u tat-TLM għandha tiġi rkuprata kollha mid-*data* tal-backup.

(206) Il-materjal ewlieni privat tar-root CA, tas-CPOC u tat-TLM ma għandhiex issir backup tiegħu bl-użu ta' mekkaniżmi tal-backup standard, iżda bl-użu tal-funzjoni tal-backup tal-modulu kriptografiku.

5.1.8.2. *EA/AA*

(207) Il-proċessi deskritti fit-taqsima 5.1.8.1 japplikaw għal din it-taqsima.

5.2. Kontrolli proċedurali

Din it-taqsima tiddeskrivi r-rekwiżiti għal rwoli, dmirijiet u identifikazzjoni tal-persunal.

5.2.1. Rwoli fdati

(208) L-impjegati, il-kuntratturi u l-konsulenti li huma assenjati għal rwoli fdati għandhom jiġu kkunsidrati bħala "persuni fdati". Il-persuni li jkunu qed ifittxu li jsiru persuni fdati biex jiksbu pożizzjoni ta' fiduċja għandhom jissodisfaw ir-rekwiżiti tat-tgħarbil ta' din il-politika taċ-ċertifikati.

(209) Il-persuni fdati għandhom aċċess għal jew jikkontrollaw l-awtentikazzjoni jew l-operazzjonijiet kriptografiċi li jistgħu jaffettwaw b'mod materjali:

- il-validazzjoni tal-informazzjoni fl-applikazzjonijiet taċ-ċertifikat;
- l-aċċettazzjoni, ir-rifjut jew ipproċessar ieħor tal-applikazzjonijiet għal ċertifikati, talbiet għal revoka jew talbiet għal tiġdid;
- il-ħruġ jew ir-revoka ta' ċertifikati, inkluż persunal li jkollu aċċess għal porzjonijiet ristretti tar-repożitorju tiegħu jew l-immaniġġjar ta' informazzjoni jew talbiet tal-abbonati.

(210) Ir-rwoli fdati jinkludu, imma mhumiex limitati għal:

- servizz tal-klijenti;
- amministrazzjoni tas-sistema;
- inġinerija magħżula;
- eżekuttivi inkarigati mill-immaniġġjar tal-affidabbiltà infrastrutturali.

(211) Is-CA għandha tipprovdi deskrizzjonijiet ċari tar-rwoli fdati kollha fis-CPS tagħha.

5.2.2. Numru ta' persuni meħtieġa għal kull kompitu

(212) L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom jistabbilixxu, iżommu u jinfurzaw il-proċeduri ta' kontroll rigoruż biex tiġi żgurata is-separazzjoni tad-dmirijiet ibbażati fuq rwoli fdati u biex jiġi żgurat li persuni fdati multipli jkunu meħtieġa jwettqu kompiti sensittivi. L-elementi tal-mudell ta' fiduċja tas-C-ITS (TLM, CPOC, root CA, EA u AA) għandhom jikkonformaw ma' [4] u mar-rekwiżiti fil-paragrafi li ġejjin.

(213) Il-proċeduri tal-politika u ta' kontroll huma fis-seħħ biex jiżguraw is-separazzjoni tad-dmirijiet ibbażati fuq ir-responsabbiltajiet tax-xogħol. Il-kompiti l-aktar sensittivi, bħall-aċċess għal u l-immaniġġjar tal-ħardwer kriptografiku tas-CA (HSM) u l-materjal ewlieni assoċjat tiegħu, għandhom jeħtieġu l-awtorizzazzjoni ta' persuni fdati multipli.

(214) Dawn il-proċeduri ta' kontroll intern għandhom ikunu ddisinjati biex jiżguraw li mill-anqas żewġ persuni fdati huma meħtieġa li jkollhom aċċess fiżiku jew loġiku għall-apparat. Ir-restrizzjonijiet fuq l-aċċess għal ħardwer kriptografiku tas-CA għandhom jiġu infurzati strettament minn persuni fdati multipli matul iċ-ċiklu tal-ħajja tiegħu, minn meta jasal u jiġi spezzjonat sal-qerda loġika u/jew fiżika finali. Ladarba l-modulu jiġi attivat bil-kjavi operattivi, jiġu invokati aktar kontrolli tal-aċċess biex jinżamm kontroll maqsum fuq l-aċċess kemm fiżiku kif ukoll loġiku għall-apparat.

5.2.3. Identifikazzjoni u awtentikazzjoni ta' kull rwol

(215) Il-persuni kollha assenjati rwol, kif deskritt f'din is-CP, huma identifikati u awtentikati biex jiggarantixxu li r-rwol jippermettilhom iwettqu d-dmirijiet tal-PKI tagħhom.

(216) L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom jivverifikaw u jikkonfermaw l-identità u l-awtorizzazzjoni tal-persunal kollu li qed ifittex li jsir parti mill-persuni fdati qabel ma:

- jinħarġilhom l-apparat tal-aċċess tagħhom u jingħataw l-aċċess għall-faċilitajiet meħtieġa;
- jingħataw kredenzjali elettroniċi biex jaċċessaw u jwettqu funzjonijiet speċifiċi fuq is-sistemi tas-CA.

(217) Is-CPS tiddeskrivi l-mekkaniżmi użati biex jiġu identifikati u awtentikati l-individwi.

5.2.4. Rwoli li jeħtieġu separazzjoni tad-dmirijiet

(218) Ir-rwoli li jeħtieġu separazzjoni tad-dmirijiet jinkludu (imma mhumiex limitati għal):

- l-aċċettazzjoni, ir-rifjut u r-revoka ta' talbiet, u pproċessar ieħor ta' applikazzjonijiet għal ċertifikati tas-CA;
- il-ġenerazzjoni, il-ħruġ u l-qerda ta' ċertifikat tas-CA.

(219) Is-segregazzjoni tad-dmirijiet tista' tiġi infurzata bl-użu tat-tagħmir jew tal-proċeduri tal-PKI, jew tat-tnejn li huma. L-ebda individwu ma għandu jiġi assenjat aktar minn identità waħda sakemm ma jkunx approvat mir-root CA.

(220) Il-parti mir-root CA u mis-CA kkonċernata mill-immaniġġjar tal-ġenerazzjoni u tar-revoka taċ-ċertifikati għandha tkun indipendenti minn organizzazzjonijiet

oħra għad-deċiżjonijiet tagħha relatati mal-istabbiliment, il-forniment, iż-żamma u s-sospensjoni ta' servizzi b'konformità mal-politiki taċ-ċertifikati applikabbli. B'mod partikolari, l-uffiċjali għolja, il-persunal għoli u l-persunal tagħha fi rwoli fdati għandhom ikunu ħielsa minn kwalunkwe pressjoni kummerċjali, finanzjarja u oħra li tista' tinfluwenza b'mod negattiv il-fiduċja fis-servizzi li tipprovdi.

(221) L-EA u l-AA li jaqdu lill-istazzjonijiet mobbli tas-C-ITS għandhom ikunu entitajiet operattivi separati, b'infrastruttura tal-IT separata u b'timijiet tal-maniġment tal-IT separati. Skont il-GDPR, l-EA u l-AA ma għandhom jiskambjaw l-ebda *data* personali, ħlief għall-awtorizzazzjoni tat-talbiet għall-AT. Huma għandhom jittrasferixxu d-*data* relatata mal-approvazzjoni ta' talbiet għall-AT biss bl-użu tal-protokoll ta' validazzjoni tal-awtorizzazzjoni ta' [1] fuq interfaċċja sigura ddedikata. Jistgħu jintużaw protokolli oħra, diment li [1] jiġi implimentat.

(222) Il-fajls tar-reġistru maħżuna mill-EA u l-AA jistgħu jintużaw biss għall-finijiet tar-revoka tal-ECs li jaġixxu ħażin abbażi tal-ATs f'messaġġi malizzjuži CAM/DENM interċettati. Wara li messaġġ CAM/DENM ikun ġie identifikat bħala malizzjuż, l-AA għandha tfittex il-kjavi tal-verifika tal-AT fir-reġistri tal-ħruġ tagħha u tippreżenta talba għal revoka lill-EA li jkun fiha l-firma kriptata taħt il-kjavi privata tal-EC li tkun intużat matul il-ħruġ tal-AT. Il-fajls tar-reġistru kollha għandhom ikunu protetti b'mod adegwat kontra l-aċċess minn partijiet mhux awtorizzati u ma jistgħux jiġu kondiviżi ma' entitajiet jew awtoritajiet oħra.

Nota: Fiż-żmien tal-abbozzar ta' din il-verżjoni tas-CP, id-disinn tal-funzjoni li taġixxi ħażin mhuwiex definit. Hu ppjanat li potenzjalment tiġi ddisinjata l-funzjoni li taġixxi ħażin f'reviżjonijiet futuri tal-politika.

5.3. Kontrolli tal-persunal

5.3.1. Kwalifiki, esperjenza u rekwiżiti ta' approvazzjoni

(223) L-elementi tal-mudell ta' fiduċja tas-C-ITS jimpjegaw numru biżżejjed ta' persunal bl-għarfien espert, l-esperjenza u l-kwalifiki meħtieġa għall-funzjonijiet tax-xogħol u għas-servizzi offruti. Il-persunal tal-PKI jissodisfa dawn ir-rekwiżiti permezz ta' taħriġ u kredenzjali formali, esperjenza effettiva jew taħlita tat-tnejn. Ir-rwoli u r-responsabbiltajiet fdati, kif speċifikati fis-CPS, huma ddokumentati fid-deskrizzjonijiet tal-impjiegi u identifikati b'mod ċar. Is-sottokuntratturi tal-persunal tal-PKI għandhom deskrizzjonijiet tal-impjiegi ddefiniti biex jiżguraw is-separazzjoni tad-dmirijiet u tal-privileġġi, u s-sensittività tal-pożizzjoni hi ddeterminata abbażi tad-dmirijiet u tal-livelli tal-aċċess, it-tgħarbil tal-kondotta, u t-taħriġ u l-għarfien tal-impjegati.

5.3.2. Proċeduri ta' verifika tal-kondotta

(224) L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom iwettqu verifiki tal-kondotta fuq il-persunal li qed ifittex li jsir parti mill-persuni fdati. Il-verifiki tal-kondotta għandhom jiġu ripetuti għall-persunal li jkollu pożizzjonijiet fdati mill-anqas kull ħames snin.

(225) Il-fatturi żvelati waqt verifika tal-kondotta li jistgħu jiġi kkunsidrati bħala raġuni biex jiġu rifjutati kandidati għal pożizzjonijiet ta' fiduċja jew biex tittieħed azzjoni kontra persuna fdata eżistenti jinkludu (imma mhumiex limitati għal) dawn li ġejjin:

- rappreżentazzjonijiet foloz magħmula mill-kandidat jew mill-persuna fdata;
- referenzi professjonali sfavorevoli ħafna jew mhux affidabbli;
- ċerti kundanni kriminali;
- indikazzjonijiet ta' nuqqas ta' responsabbiltà finanzjarja.

(226) Ir-rapporti li jkun fihom din l-informazzjoni għandhom jiġu evalwati mill-persunal tar-riżorsi umani, li għandhom jieħdu azzjoni raġonevoli fid-dawl tat-tip, il-kobor u l-frekwenza tal-imġiba li toħroġ fid-dieher waqt il-verifika tal-kondotta. Din l-azzjoni tista' tinkludi miżuri sa u inkluż il-kanċellazzjoni ta' offerti ta' impjieg magħmula lil kandidati għal pożizzjonijiet ta' fiduċja jew it-terminazzjoni tal-impjieg ta' persuni fdati eżistenti. L-użu tal-informazzjoni li toħroġ fid-dieher waqt verifika tal-kondotta bħala bażi għal din l-azzjoni għandu jkun soġġett għal-liġi applikabbli.

(227) L-investigazzjoni tal-kondotta ta' persuni li qed ifittxu li jsiru persuna fdata tinkludi iżda mhix limitata għal:

- konferma tal-impjieg preċedenti;
- verifika tar-referenzi professjonali li jkopru l-impjieg tagħhom fuq perjodu ta' mill-anqas ħames snin;
- konferma tal-ogħla grad ta' edukazzjoni jew dak l-aktar rilevanti miksub;
- tfittxija ta' rekords kriminali.

5.3.3. Rekwiżiti ta' taħriġ

(228) L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom jipprovdu lill-persunal tagħhom bit-taħriġ meħtieġ biex iwettqu r-responsabbiltajiet tagħhom relatati mal-operazzjonijiet tas-CA b'mod kompetenti u sodisfaċenti.

(229) Il-programmi ta' taħriġ għandhom jiġu riveduti perjodikament u t-taħriġ tagħhom għandu jindirizza kwistjonijiet li huma rilevanti għall-funzjonijiet imwettqa mill-persunal tagħhom.

(230) Il-programmi ta' taħriġ għandhom jindirizzaw kwistjonijiet li huma rilevanti għall-ambjent partikolari tat-trainee, inkluż:

- il-prinċipji u l-mekkaniżmi tas-sigurtà tal-elementi tal-mudell ta' fiduċja tas-C-ITS;
- il-verżjonijiet tal-ħardwer u tas-softwer użati;
- id-dmirijiet kollha li l-persuna hi mistennija twettaq, u l-proċessi u s-sekwenzi ta' rapportar intern u estern;
- il-proċessi u l-flussi tax-xogħol tan-negozju tal-PKI;
- ir-rapportar u l-immaniġġjar tal-inċidenti u tal-kompromessi;
- il-proċeduri għall-irkupru minn diżastri u għall-kontinwità tan-negozju;
- għarfien biżżejjed tal-IT.

5.3.4. Frekwenza u rekwiżiti tat-taħriġ mill-ġdid

(231) Il-persuni assenjati għal rwoli fdati huma meħtieġa li jġeddu l-għarfien li jkunu kisbu mit-taħriġ fuq bażi kontinwa billi jużaw ambjent ta' taħriġ. It-taħriġ għandu jiġi ripetut kull meta jkun meħtieġ u mill-anqas kull sentejn.

(232) L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom jipprovdu lill-persunal tagħhom b'taħriġ u aġġornamenti mill-ġdid sal-punt u bil-frekwenza meħtieġa biex jiżguraw li jżommu l-livell meħtieġ ta' profiċjenza biex iwettqu r-responsabbiltajiet tax-xogħol tagħhom b'mod kompetenti u sodisfaċenti.

(233) L-individwi f'rwoli fdati għandhom ikunu konxji tal-bidliet fl-operazzjonijiet tal-PKI, kif applikabbli. Kwalunkwe bidla sinifikanti fl-operazzjonijiet għandha tkun akkumpanjata minn pjan ta' taħriġ (għarfien) u t-twettiq ta' dan il-pjan għandu jkun iddokumentat.

5.3.5. Frekwenza u sekwenza tar-rotazzjoni tax-xogħol

(234) L-ebda stipulazzjoni sakemm il-ħiliet tekniċi, l-esperjenza u d-drittijiet tal-aċċess huma żgurati. L-amministraturi tal-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom jiżguraw li t-tibdil fil-persunal ma jaffettwawx is-sigurtà tas-sistema.

5.3.6. Sanzjonijiet għal azzjonijiet mhux awtorizzati

(235) Kull element tal-mudell ta' fiduċja tas-C-ITS għandu jiżviluppa proċess dixxiplinarju formali biex jiġi żgurat li azzjonijiet mhux awtorizzati jiġu sanzjonati b'mod xieraq. F'każijiet gravi, l-assenjazzjonijiet tar-rwol u l-privileġġi korrispondenti għandhom jiġu rtirati.

5.3.7. Rekwiżiti tal-kuntrattur indipendenti

(236) L-elementi tal-mudell ta' fiduċja tas-C-ITS jistgħu jippermettu kuntratturi jew konsulenti indipendenti li jsiru parti mill-persuni fdati biss sal-punt meħtieġ biex jakkomodaw relazzjonijiet ta' esternalizzazzjoni definiti b'mod ċar u bil-kundizzjoni li l-entità tafda lill-kuntratturi jew lill-konsulenti bl-istess mod bħallikieku kienu impjegati u li huma jissodisfaw ir-rekwiżiti applikabbli għall-impjegati.

(237) Inkella, il-kuntratturi u l-konsulenti indipendenti għandu jkollhom aċċess għal faċilitajiet siguri tal-PKI tas-C-ITS biss jekk jiġu skortati u sorveljati direttament minn persuni fdati.

5.3.8. Dokumentazzjoni fornuta lill-persunal

(238) L-elementi tal-mudelli ta' fiduċja tas-C-ITS għandhom jipprovdu lill-persunal tagħhom taħriġ meħtieġ u aċċess għad-dokumentazzjoni li jeħtieġu biex iwettqu r-responsabbiltajiet tax-xogħol tagħhom b'mod kompetenti u sodisfaċenti.

5.4. Proċeduri ta' reġistrazzjoni tal-awditjar

(239) Din it-taqsima tistipula r-rekwiżiti fir-rigward tat-tipi ta' avvenimenti li għandhom jiġu rreġistrati u l-immaniġġjar tar-reġistri tal-awditjar.

5.4.1. Tipi ta' avvenimenti li għandhom jiġu rreġistrati u rrapportati minn kull CA

(240) Ir-rappreżentant tas-CA għandu jirrevedi regolarment ir-reġistri, l-avvenimenti u l-proċeduri tas-CA.

(241) L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom jirreġistraw it-tipi ta' avvenimenti tal-awditjar li ġejjin (jekk applikabbli):

- l-aċċess fiżiku għall-faċilità – l-aċċess minn persuni fiżiċi għall-faċilitajiet se jiġi rreġistrat billi jinħażnu t-talbiet għall-aċċess permezz ta' smartcards. Se jinħoloq avveniment kull darba li tinħoloq rekord;
- l-immaniġġjar tar-rwoli fdati – kwalunkwe tibdil fid-definizzjoni u fil-livell tal-aċċess tar-rwoli differenti se jiġi rreġistrat, inkluż il-modifika tal-attributi tar-rwoli. L-avveniment se jinħoloq kull darba li tinħoloq rekord;
- l-aċċess loġiku – l-avveniment se jiġi ġġenerat meta l-entità (eż. programm) ikollha aċċess għal żoni sensittivi (jiġifieri networks u servers);
- l-immaniġġjar tal-backup – l-avveniment jinħoloq kull darba li titlesta l-backup, b'suċċess jew mingħajr suċċess;
- l-immaniġġjar tar-reġistru – ir-reġistri jiġu maħżuna. Jinħoloq avveniment meta d-daqs tar-reġistru jaqbeż daqs speċifiku;
- id-*data* mill-proċess tal-awtentikazzjoni għall-abbonati u l-elementi tal-mudell ta' fiduċja tas-C-ITS – se jiġu ġġenerati avvenimenti għal kull talba ta' awtentikazzjoni minn abbonati u minn elementi tal-mudell ta' fiduċja tas-C-ITS;
- l-aċċettazzjoni u r-rifjut ta' talbiet għal ċertifikati, inkluż il-ħolqien u t-tiġdid taċ-ċertifikati – se jiġi ġġenerat avveniment perjodikament b'lista ta' talbiet għal ċertifikati aċċettati u rifjutati fis-sebat ijiem ta' qabel;
- ir-reġistrazzjoni tal-manifattur – se jinħoloq avveniment meta jiġi rreġistrat il-manifattur;
- ir-reġistrazzjoni tal-istazzjon tas-C-ITS – se jinħoloq avveniment meta jiġi rreġistrat l-istazzjon tas-C-ITS;
- l-immaniġġjar tal-HSM – se jinħoloq avveniment meta jiġi rreġistrat ksur tas-sigurtà tal-HSM;
- l-immaniġġjar tal-IT u tan-network, kif jirrelataw mas-sistemi tal-PKI – se jinħoloq avveniment meta s-server tal-PKI jintefa jew jerġa' jinxtegħel;
- l-immaniġġjar tas-sigurtà (tentattivi ta' aċċess għas-sistema tal-PKI ta' suċċess u li ma rnexxewx, azzjonijiet imwettqa fuq il-PKI u fuq is-sistema tas-sigurtà, tibdil fil-profil tas-sigurtà, ħsarat fis-sistema, ħsarat fil-ħardwer u anomaliji oħra, attivitajiet tal-firewall u tar-router; u dħul fil-faċilitajiet tal-PKI u ħruġ minnhom);
- id-*data* relatata mal-avvenimenti se tinħażen għal mill-anqas ħames snin sakemm ma japplikawx regoli nazzjonali addizzjonali.

(242) Skont il-GDPR, ir-reġistri tal-awditjar ma għandhomx jippermettu aċċess għal *data* relatata mal-privatezza li tikkonċerna vetturi privati tal-istazzjon tas-C-ITS.

(243) Fejn possibbli, ir-reġistri tal-awditjar tas-sigurtà għandhom jinġabru b'mod awtomatiku. Fejn dan ma jkunx possibbli, għandu jintuża ġurnal, f'forma stampata jew mekkaniżmu fiżiku ieħor. Ir-reġistri kollha tal-awditjar tas-sigurtà, kemm elettroniċi kif ukoll mhux elettroniċi, għandhom jinżammu u jkunu disponibbli matul l-awditjar tal-konformità.

(244) Kull avveniment relatat maċ-ċiklu tal-ħajja taċ-ċertifikat hu rreġistrat b'tali mod li jista' jiġi attribwit lill-persuna li wettqitu. Id-*data* kollha relatata ma' identità personali hi kriptata u protetta kontra aċċess mhux awtorizzat.

(245) Bħala minimu, kull rekord tal-awditjar jinkludi dan li ġej (irreġistrat b'mod awtomatiku jew manwalment għal kull avveniment li jista' jiġi awditjat):

- it-tip ta' avveniment (mil-lista ta' hawn fuq);
- id-data u l-ħin fdati li fihom seħħ l-avveniment;
- ir-riżultat tal-avveniment – suċċess jew falliment fejn xieraq;
- l-identità tal-entità u/jew tal-operatur li kkawża l-avveniment jekk applikabbli;
- l-identità tal-entità li għaliha hu indirizzat l-avveniment.

5.4.2. Frekwenza tal-ipproċessar tar-reġistru

(246) Ir-reġistri tal-awditjar għandhom jiġu riveduti bi tweġiba għal twissijiet ibbażati fuq irregolaritajiet u inċidenti fis-sistemi tas-CA u barra minn hekk perjodikament kull sena.

(247) L-ipproċessar tar-reġistru tal-awditjar għandu jkun magħmul minn reviżjoni tar-reġistri tal-awditjar u d-dokumentazzjoni tar-raġuni għall-avvenimenti sinifikanti kollha f'sommarju tar-reġistru tal-awditjar. Ir-reviżjonijiet tar-reġistru tal-awditjar għandhom jinkludu verifika li r-reġistru ma jkunx ġie mbagħbas, spezzjoni tal-entrati kollha fir-reġistru u investigazzjoni ta' kwalunkwe allert jew irregolarità fir-reġistri. L-azzjoni meħuda abbażi tar-reviżjonijiet tar-reġistru tal-awditjar għandha tiġi ddokumentata.

(248) Ir-reġistru tal-awditjar jiġi arkivjat mill-anqas kull ġimgħa. L-amministratur għandu jarkivjah manwalment jekk l-ispazju liberu tad-diska għar-reġistru tal-awditjar ikun taħt l-ammont mistenni ta' *data* tar-reġistru tal-awditjar prodott dik il-ġimgħa.

5.4.3. Perjodu ta' żamma għar-reġistru tal-awditjar

(249) Ir-rekords tar-reġistru relatati maċ-ċikli tal-ħajja taċ-ċertifikat jinżammu għal mill-anqas ħames snin wara li jiskadi ċ-ċertifikat korrispondenti.

5.4.4. Protezzjoni tar-reġistru tal-awditjar

(250) L-integrità u l-kunfidenzjalità tar-reġistru tal-awditjar huma ggarantiti minn mekkaniżmu ta' kontroll tal-aċċess ibbażat fuq ir-rwol. Ir-reġistri tal-awditjar intern jistgħu jiġu aċċessati biss mill-amministraturi; ir-reġistri tal-awditjar relatati maċ-ċiklu tal-ħajja taċ-ċertifikat jistgħu jiġu aċċessati wkoll minn utenti bl-awtorizzazzjoni xierqa permezz ta' paġna web bil-login tal-utent. L-aċċess għandu jingħata b'utenti multipli (mill-anqas żewġ utenti) u tal-anqas b'awtentikazzjoni fuq żewġ livelli. Għandu jiġi żgurat teknikament li l-utenti ma jkunux jistgħu jaċċessaw il-fajls tar-reġistru tagħhom stess.

(251) Kull entrata fir-reġistru għandha tiġi ffirmata bl-użu ta' materjal ewlieni mill-HSM.

(252) Ir-reġistri tal-avvenimenti li jkun fihom informazzjoni li tista' twassal għal identifikazzjoni personali, bħal vettura privata, huma kriptati b'tali mod li persuni awtorizzati biss ikunu jistgħu jaqrawhom.

(253) L-avvenimenti huma rreġistrati b'tali mod li ma jistgħux jitħassru jew jinqerdu faċilment (ħlief għat-trasferiment fuq midja għal perjodu twil) fil-perjodu li għalih iridu jinżammu r-reġistri.

(254) Ir-reġistri tal-avvenimenti huma protetti b'tali mod li jibqgħu jinqraw għat-tul tal-perjodu tal-ħażna tagħhom.

5.4.5. Proċeduri ta' backup għar-reġistru tal-awditjar

(255) Il-backup tar-reġistri u tas-sommarji tal-awditjar isir permezz ta' mekkaniżmi tal-backup tal-intrapriża, taħt il-kontroll ta' rwoli fdati awtorizzati, separati mill-ġenerazzjoni tas-sors tal-komponent tagħhom. Il-backups tar-reġistru tal-awditjar huma protetti bl-istess livell ta' fiduċja li japplika għar-reġistri oriġinali.

5.4.6. Sistema ta' ġbir tal-awditjar (interna jew esterna)

(256) It-tagħmir tal-elementi tal-mudell ta' fiduċja tas-C-ITS għandu jattiva l-proċessi tal-awditjar waqt l-istartjar tas-sistema u jiddiżattivahom biss meta tintefa s-sistema. Jekk il-proċessi tal-awditjar ma jkunux disponibbli, l-element tal-mudell ta' fiduċja tas-C-ITS għandu jissospendi l-operat tiegħu.

(257) Fl-aħħar ta' kull perjodu ta' ħaddim u meta jsir ir-rikjavar taċ-ċertifikati, l-istatus kollettiv tat-tagħmir għandu jkun irrapportat lill-maniġer tal-operazzjonijiet u lill-korp li jirregola l-operazzjoni tal-element rispettiv tal-PKI.

5.4.7. Notifika lis-suġġett li jikkawża l-avveniment

(258) Meta l-avveniment jiġi rreġistrat mis-sistema tal-ġbir tal-awditjar, din tiggarantixxi li l-avveniment jiġi marbut ma' rwol fdat.

5.4.8. Valutazzjoni tal-vulnerabbiltà

(259) Ir-rwol responsabbli mit-twettiq tal-awditjar u r-rwoli responsabbli mit-twettiq tal-operazzjoni tas-sistema tal-PKI fl-elementi tal-mudell ta' fiduċja tas-C-ITS jispjegaw l-avvenimenti sinifikanti kollha f'sommarju tar-reġistru tal-awditjar. Dawn ir-reviżjonijiet jinvolvu l-verifika li r-reġistru ma ġiex imbagħbas u li m'hemm l-ebda diskontinwità jew telf ieħor ta' *data* tal-awditjar, u mbagħad jiġu spezzjonati fil-qosor l-entrati kollha tar-reġistru, b'investigazzjoni aktar bir-reqqa ta' kwalunkwe allerti jew irregolaritajiet fir-reġistri. L-azzjoni meħuda bħala riżultat ta' dawn ir-reviżjonijiet hi ddokumentata.

(260) L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom:

- jimplimentaw kontrolli organizzattivi u/jew tekniċi ta' detezzjoni u prevenzjoni taħt il-kontroll tal-elementi tal-mudell ta' fiduċja tas-C-ITS biex jipproteġu s-sistemi tal-PKI minn vajrusis u softwer malizzjuż;
- jiddokumentaw u jsegwu proċess ta' korrezzjoni tal-vulnerabbiltà li jindirizza l-identifikazzjoni, ir-reviżjoni, ir-rispons u r-rimedjazzjoni tal-vulnerabbiltajiet;
- jagħmlu jew iwettqu skennjar tal-vulnerabbiltà:
  - wara kwalunkwe tibdil fis-sistema jew fin-network iddeterminat mill-elementi tal-mudell ta' fiduċja tas-C-ITS bħala sinifikanti għall-komponenti tal-PKI; kif ukoll
  - minn tal-anqas darba fix-xahar, fuq indirizzi tal-IP pubbliċi u privati identifikati mis-CA, mis-CPOC bħala s-sistemi tal-PKI,
- jgħaddu minn test tal-penetrazzjoni fuq is-sistemi tal-PKI mill-anqas fuq bażi annwali u wara aġġornamenti jew modifiki tal-infrastruttura jew tal-applikazzjoni ddeterminati mill-elementi tal-mudell ta' fiduċja tas-C-ITS bħala sinifikanti għall-komponent tal-PKI tas-CA;
- għal sistemi online, jirreġistraw l-prova li kull skennjar tal-vulnerabbiltà u test tal-penetrazzjoni twettaq minn persuna jew entità (jew grupp kollettiv tagħhom) bil-ħiliet, bl-għodod, bil-profiċjenza, bil-kodiċi ta' etika u bl-indipendenza meħtieġa biex jipprovdu test affidabbli tal-vulnerabbiltà jew tal-penetrazzjoni;
- jintraċċaw u jirrimedjaw il-vulnerabbiltajiet b'konformità mal-politiki taċ-ċibersigurtà tal-intrapriża u l-metodoloġija tal-mitigazzjoni tar-riskju.

5.5. Arkivjar tar-rekords

5.5.1. Tipi ta' rekords arkivjati

(261) L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom jarkivjaw ir-rekords dettaljati biżżejjed biex jistabbilixxu l-validità ta' firma u tal-operazzjoni xierqa tal-PKI. Bħala minimu, ir-rekords tal-avvenimenti tal-PKI li ġejjin għandhom jiġu arkivjati (jekk applikabbli):

- ir-reġistru tal-aċċess fiżiku għall-faċilità tal-elementi tal-mudell ta' fiduċja tas-C-ITS (minimu ta' sena);
- ir-reġistru tal-immaniġġjar tar-rwoli fdati għall-elementi tal-mudell ta' fiduċja tas-C-ITS (minimu ta' 10 snin);
- ir-reġistru tal-aċċess għall-IT għall-elementi tal-mudell ta' fiduċja tas-C-ITS (minimu ta' ħames snin);
- ir-reġistru tal-ħolqien, l-użu u l-qerda tal-kjavi tas-CA (minimu ta' ħames snin) (mhux għat-TLM u s-CPOC);
- ir-reġistru tal-ħolqien, l-użu u l-qerda taċ-ċertifikat (minimu ta' sentejn);
- ir-reġistru tat-talbiet tas-CPA (minimu ta' sentejn);
- ir-reġistru tal-immaniġġjar tad-*data* tal-attivazzjoni għall-elementi tal-mudell ta' fiduċja tas-C-ITS (minimu ta' ħames snin);

- ir-reġistru tal-IT u tan-network għall-elementi tal-mudell ta' fiduċja tas-C-ITS (minimu ta' ħames snin);
- id-dokumentazzjoni tal-PKI għall-elementi tal-mudell ta' fiduċja tas-C-ITS (minimu ta' ħames snin);
- ir-rapport tal-inċidenti tas-sigurtà u tal-awditjar għall-elementi tal-mudell ta' fiduċja tas-C-ITS (minimu ta' 10 snin);
- it-tagħmir, is-softwer u l-konfigurazzjoni tas-sistema (minimu ta' ħames snin).

(262) L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom iżommu d-dokumentazzjoni li ġejja li għandha x'taqsam mat-talbiet għaċ-ċertifikati u l-verifika tagħhom, u ċ-ċertifikati kollha tat-TLM, tar-root CAs u tas-CA u s-CRL tagħhom, għal mill-anqas seba' snin wara li kwalunkwe ċertifikat ibbażat fuq dik id-dokumentazzjoni ma jibqax validu:

- dokumentazzjoni tal-awditjar tal-PKI miżmuma mill-elementi tal-mudell ta' fiduċja tas-C-ITS;
- dokumenti tas-CPS miżmuma mill-elementi tal-mudell ta' fiduċja tas-C-ITS;
- kuntratt bejn is-CPA u entitajiet oħra miżmum mill-elementi tal-mudell ta' fiduċja tas-C-ITS;
- ċertifikati (jew informazzjoni oħra ta' revoka) miżmuma mis-CA u mit-TLM;
- rekords tat-talba għal ċertifikati fis-sistema tar-root CA (mhux applikabbli għat-TLM);
- *data* jew applikazzjonijiet oħra biżżejjed biex jivverifikaw il-kontenut tal-arkivju;
- ix-xogħol kollu relatat ma' jew mill-elementi tal-mudell ta' fiduċja tas-C-ITS u mill-awdituri tal-konformità.

(263) L-entità tas-CA għandha żżomm id-dokumentazzjoni kollha relatata mat-talbiet għaċ-ċertifikati u l-verifika tagħhom, u ċ-ċertifikati kollha u r-revoka tagħhom, għal mill-anqas seba' snin wara li kwalunkwe ċertifikat ibbażat fuq dik id-dokumentazzjoni ma jibqax validu.

5.5.2. Perjodu ta' żamma għall-arkivju

(264) Mingħajr preġudizzju għar-regolamenti li jeħtieġu perjodu itwal għall-arkivjar, l-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom iżommu r-rekords kollha għal mill-anqas ħames snin wara li ċ-ċertifikat korrispondenti jkun skada.

5.5.3. Protezzjoni tal-arkivju

(265) L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom jaħżnu l-arkivju tar-rekords f'faċilità tal-ħażna sikura, sigura u separata mit-tagħmir tas-CA, b'kontrolli tas-sigurtà fiżiċi u proċedurali ekwivalenti għal jew aħjar minn dawk tal-PKI.

(266) L-arkivju għandu jkun protett kontra wiri, modifika, tħassir jew tbagħbis ieħor mhux awtorizzat permezz tal-ħażna f'sistema affidabbli.

(267) Il-midja li żżomm id-*data* tal-arkivju u l-applikazzjonijiet meħtieġa biex jipproċessawha għandhom jinżammu biex jiġi żgurat li jkunu jistgħu jiġu aċċessati għall-perjodu stabbilit f'din is-CP.

5.5.4. Arkivju u ħażna tas-sistema

(268) L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom b'mod inkrementali jagħmlu backup kuljum tal-arkivji tas-sistema ta' din l-informazzjoni u jwettqu backups sħaħ kull ġimgħa. Il-kopji ta' rekords tal-karti għandhom jinżammu f'faċilità sigura mhux fuq il-post.

5.5.5. Rekwiżiti għall-ittimbrar tal-ħin tar-rekords

(269) L-elementi tal-mudell ta' fiduċja tas-C-ITS li jimmaniġġjaw bażi tad-*data* ta' revoka għandhom jiżguraw li r-rekords ikun fihom informazzjoni dwar il-ħin u d-data meta jinħolqu r-rekords ta' revoka. L-integrità ta' din l-informazzjoni se tiġi implimentata b'soluzzjonijiet fuq bażi kriptografika.

5.5.6. Sistema ta' ġbir tal-arkivju (interna jew esterna)

(270) Is-sistema ta' ġbir tal-arkivju hi interna.

5.5.7. Proċeduri għall-ksib u l-verifika tal-informazzjoni tal-arkivju

(271) L-elementi kollha tal-mudell ta' fiduċja tas-C-ITS għandhom jippermettu biss persuni fdati awtorizzati biex jaċċessaw l-arkivju. Ir-root CAs u s-CAs għandhom jiddeskrivu l-proċeduri għall-ħolqien, il-verifika, l-ippakkjar, it-trażmissjoni u l-ħażna ta' informazzjoni tal-arkivju fis-CPS.

(272) It-tagħmir tar-root CA u tas-CA għandu jivverifika l-integrità tal-informazzjoni qabel ma tiġi restawrata.

5.6. Bidla tal-kjavi għall-elementi tal-mudell ta' fiduċja tas-C-ITS

(273) L-elementi li ġejjin tal-mudell ta' fiduċja tas-C-ITS għandhom rekwiżiti speċifiċi għall-bidla tal-kjavi tagħhom: TLM, root CA u ċertifikati tal-EA/AA.

*5.6.1. **TLM***

(274) It-TLM għandu jħassar il-kjavi privata tiegħu meta jiskadi ċ-ċertifikat korrispondenti. Għandu jiġġenera par kjavi ġdid u ċertifikat tat-TLM korrispondenti qabel ma tiġi diżattivata l-kjavi privata valida attwali. Għandu jieħu ħsieb li ċ-ċertifikat il-ġdid (tal-konnessjoni) jiddaħħal fl-ECTL fil-ħin biex jitqassam lill-istazzjonijiet kollha tas-C-ITS qabel ma jsir validu. Iċ-ċertifikat tal-konnessjoni u ċ-ċertifikat il-ġdid iffirmat minnu stess jiġu ttrasferiti lis-CPOC.

5.6.2. Root CA

(275) Ir-root CA għandha tiddiżattiva u tħassar il-kjavi privata attwali (inkluż il-kjavi tal-backup), biex ma toħroġx ċertifikati tal-EA/AA b'validità li testendi lil hinn mill-validità taċ-ċertifikat tar-root CA.

(276) Ir-root CA għandha tiġġenera par kjavi ġdid u ċertifikat korrispondenti tar-root CA u tal-konnessjoni qabel ma tiġi diżattivata l-kjavi privata attwali (inkluż il-kjavi tal-backup) u tibagħtu lit-TLM għall-inklużjoni fl-ECTL. Il-perjodu ta' validità taċ-ċertifikat il-ġdid tar-root CA għandu jibda mad-diżattivazzjoni ppjanata tal-kjavi privata attwali. Ir-root CA għandha tieħu ħsieb li ċ-ċertifikat il-ġdid jiddaħħal fl-ECTL fil-ħin biex jitqassam lill-istazzjonijiet kollha tas-C-ITS qabel ma jsir validu.

(277) Ir-root CA għandha tattiva l-kjavi privata l-ġdida meta ċ-ċertifikat korrispondenti tar-root CA jsir validu.

5.6.3. Ċertifikat tal-EA/AA

(278) L-EA/AA għandha tiddiżattiva l-kjavi privata attwali biex ma toħroġx ECs/ATs b'validità li testendi lil hinn mill-validità taċ-ċertifikat tal-EA/AA.

(279) L-EA/AA għandha tiġġenera par kjavi ġdid u titlob ċertifikat korrispondenti tal-EA/AA qabel ma tiġi diżattivata l-kjavi privata attwali. Il-perjodu ta' validità taċ-ċertifikat il-ġdid tal-EA/AA għandu jibda mad-diżattivazzjoni ppjanata tal-kjavi privata attwali. L-EA/AA għandha tieħu ħsieb li ċ-ċertifikat il-ġdid ikun jista' jiġi ppubblikat fil-ħin biex jitqassam lill-istazzjonijiet kollha tas-C-ITS qabel ma jsir validu.

(280) L-EA/AA għandha tattiva l-kjavi privata l-ġdida meta ċ-ċertifikat korrispondenti tal-EA/AA jsir validu.

5.6.4. Awditur

Ebda dispożizzjoni.

5.7. Kompromess u rkupru minn diżastru

5.7.1. Immaniġġjar ta' inċidenti u kompromessi

(281) L-elementi tal-mudell ta' fiduċja tas-C-ITS għandhom jimmonitorjaw it-tagħmir tagħhom fuq bażi kontinwa, biex jidentifikaw attentati potenzjali ta' hacking jew forom oħra ta' kompromess. F'dan il-każ, dawn għandhom jinvestigaw biex jiddeterminaw in-natura u l-grad tal-ħsara.

(282) Jekk il-persunal responsabbli mill-immaniġġjar tar-root CA jew tat-TLM jidentifika attentat potenzjali ta' hacking jew forma oħra ta' kompromess, għandu jinvestiga biex jiddetermina n-natura u l-grad tal-ħsara. Fil-każ li l-kjavi privata tiġi kompromessa, iċ-ċertifikat tar-root CA għandu jiġi revokat. L-esperti tas-sigurtà tal-IT tas-CPA għandhom jivvalutaw l-ambitu tal-ħsara potenzjali biex jiddeterminaw jekk il-PKI għandhiex bżonn terġa' tinbena, jekk humiex biss xi ċertifikati li għandhom jiġu revokati u/jew jekk il-PKI ġietx kompromessa. Barra minn hekk, is-CPA tiddetermina liema servizzi għandhom jinżammu (informazzjoni dwar l-istatus tar-revoka u taċ-ċertifikat) u kif, skont il-pjan tal-kontinwità tan-negozju tas-CPA.

(283) L-inċidenti, il-kompromess u l-kontinwità tan-negozju huma koperti fis-CPS, li tista' tiddependi wkoll fuq riżorsi oħra tal-intrapriża u pjanijiet għall-implimentazzjoni tagħha.

(284) Jekk il-persunal responsabbli mill-immaniġġjar tal-EA/AA/CPOC jidentifika attentat potenzjali ta' hacking jew forma oħra ta' kompromess, għandu jinvestiga biex jiddetermina n-natura u l-grad tal-ħsara. Il-persunal responsabbli mill-immaniġġjar tal-entità tas-CA jew tas-CPOC għandu jivvaluta l-ambitu tal-ħsara potenzjali biex jiddetermina jekk il-komponent tal-PKI għandux bżonn jerġa' jinbena, jekk humiex biss xi ċertifikati li għandhom jiġu revokati u/jew jekk il-komponent tal-PKI ġiex kompromess. Barra minn hekk, l-entità tas-sub-CA tiddetermina liema servizzi għandhom jinżammu u kif, skont il-pjan tal-kontinwità tan-negozju tal-entità tas-sub-CA. Fil-każ li komponent tal-PKI jiġi kompromess, l-entità tas-CA għandha tavża lir-root CA u lit-TLM tagħha stess permezz tas-CPOC.

(285) L-inċidenti, il-kompromess u l-kontinwità tan-negozju huma koperti fis-CPS tar-root CA jew tat-TLM jew dokumenti rilevanti oħra fil-każ tas-CPOC, li jistgħu jiddependu wkoll fuq riżorsi oħra tal-intrapriża u pjanijiet għall-implimentazzjoni tagħhom.

(286) Ir-root CA u s-CA għandhom javżaw, b'informazzjoni preċiża dwar il-konsegwenzi tal-inċident, lil kull rappreżentant tal-Istati Membri u lir-root CA li magħhom għandhom ftehim fil-kuntest tas-C-ITS, biex ikunu jistgħu jattivaw il-pjan tagħhom għall-immaniġġjar tal-inċidenti.

5.7.2. Korruzzjoni ta' riżorsi tal-kompjuter, softwer u/jew data

(287) Jekk jinstab diżastru li jipprevjeni t-tħaddim xieraq ta' element tal-mudell ta' fiduċja tas-C-ITS, dak l-element għandu jissospendi l-operat tiegħu u jinvestiga jekk il-kjavi privata ġietx kompromessa (għajr għas-CPOC). Il-ħardwer difettuż għandu jinbidel malajr kemm jista' jkun u għandhom japplikaw il-proċeduri deskritti fit-taqsimiet 5.7.3 u 5.7.4.

(288) Il-korruzzjoni ta' riżorsi tal-kompjuter, softwer u/jew *data* għandha tiġi rrapportata lir-root CA fi żmien 24 siegħa għall-ogħla livelli ta' riskju. L-avvenimenti l-oħra kollha għandhom jiġu inklużi fir-rapport perjodiku tar-root CA, tal-EAs u tal-AAs.

5.7.3. Proċeduri ta' kompromess tal-kjavi privata tal-entità

(289) Jekk il-kjavi privata tar-root CA tkun kompromessa, mitlufa, meqruda jew suspettata li ġiet kompromessa, ir-root CA għandha:

- tissospendi l-operat tagħha;
- tibda l-pjan ta' rkupru minn diżastri u migrazzjoni;
- tirrevoka ċ-ċertifikat tar-root CA tagħha;
- tinvestiga l-"kwistjoni ewlenija" li ġġenerat il-kompromess u tinnotifika lis-CPA, li mbagħad tirrevoka ċ-ċertifikat tar-root-CA permezz tat-TLM (ara t-taqsima 7);
- tavża lill-abbonati kollha li magħhom għandha ftehim.

(290) Jekk il-kjavi tal-EA/AA tkun kompromessa, mitlufa, meqruda jew suspettata li ġiet kompromessa, l-EA/AA għandha:

- tissospendi l-operat tagħha;
- tirrevoka ċ-ċertifikat tagħha stess;
- tinvestiga l-"kwistjoni ewlenija" u tinnotifika lir-root CA;
- tavża lill-abbonati li magħhom jeżisti ftehim.

(291) Jekk il-kjavi tal-EC jew tal-AT tal-istazzjon tas-C-ITS tkun kompromessa, mitlufa, meqruda jew suspettata li ġiet kompromessa, l-EA/AA li għaliha hu sottoskritt l-istazzjon tas-C-ITS għandha:

- tirrevoka l-EC tal-ITS afettwata;
- tinvestiga l-"kwistjoni ewlenija" u tinnotifika lir-root CA;
- tavża lill-abbonati li magħhom għandha ftehim.

(292) Fejn xi wieħed mill-algoritmi jew il-parametri assoċjati użati mir-root CA u/jew mis-CA jew mill-istazzjonijiet tas-C-ITS isir insuffiċjenti għall-użu maħsub li jifdal, is-CPA (b'rakkomandazzjoni minn esperti kriptografiċi) għandha tinforma lill-entità tar-root CA li magħha għandha ftehim u tibdel l-algoritmi użati. (Għad-dettalji, ara t-taqsima 6 u s-CPSs tar-root CA u tas-sub-CA).

5.7.4. Kapaċitajiet tal-kontinwità tan-negozju wara diżastru

(293) L-elementi tal-mudell ta' fiduċja tas-C-ITS li joperaw faċilitajiet siguri għall-operazzjonijiet tas-CA għandhom jiżviluppaw, jittestjaw, iżommu u jimplimentaw pjan ta' rkupru minn diżastri mfassal biex itaffi l-effetti ta' kwalunkwe diżastru naturali jew ikkawżat mill-bniedem. Dawn il-pjanijiet jindirizzaw ir-restawr tas-servizzi tas-sistemi tal-informazzjoni u l-funzjonijiet tan-negozju ewlenin.

(294) Wara inċident ta' ċertu livell ta' riskju, is-CA kompromessa għandha tkun awditjata mill-ġdid minn awditur akkreditat tal-PKI (ara t-taqsima 8).

(295) Fejn is-CA kompromessa ma tkunx tista' topera aktar (eż. wara inċident serju), għandu jitfassal pjan ta' migrazzjoni għat-trasferiment tal-funzjonijiet tagħha għal root CA oħra. Mill-anqas ir-root CA tal-UE għandha tkun disponibbli biex tappoġġja l-pjan ta' migrazzjoni. Is-CA kompromessa għandha twaqqaf il-funzjonijiet tagħha.

(296) Ir-root CAs għandhom jinkludu l-pjan ta' rkupru minn diżastri u l-pjan ta' migrazzjoni fis-CPS.

5.8. Tmiem u trasferiment

*5.8.1. **TLM***

(297) It-TLM ma għandux itemm l-operat tiegħu, imma entità li timmaniġġja t-TLM tista' tieħu f'idejha entità oħra.

(298) Fil-każ li l-entità tal-immaniġġjar tinbidel:

- din għandha titlob l-approvazzjoni tas-CPA għal bidla fil-immaniġġjar tat-TLM mill-entità l-qadima għall-entità l-ġdida;
- is-CPA għandha tagħti prova tal-bidla fl-immaniġġjar tat-TLM;
- ir-reġistri kollha tal-awditjar u r-rekords arkivjati għandhom jiġu ttrasferiti mill-entità l-qadima tal-immaniġġjar għall-entità l-ġdida.

5.8.2. Root CA

(299) Ir-root CA ma għandhiex ittemm/tibda l-operat tagħha mingħajr ma tistabbilixxi pjan ta' migrazzjoni (stabbilit fis-CPS rilevanti) li jiggarantixxi l-operat kontinwu għall-abbonati kollha.

(300) Fil-każ tat-tmiem tas-servizz tar-root CA, ir-root CA għandha:

- tinnotifika lis-CPA;
- tinnotifika lit-TLM biex ikun jista' jħassar iċ-ċertifikat tar-root CA mill-ECTL;
- tirrevoka r-root CA korrispondenti billi toħroġ CRL li tinkludi lilha nnifisha;

- tavża lir-root CAs li magħhom għandha ftehim għat-tiġdid taċ-ċertifikati tal-EA/AA;
- teqred il-kjavi privata tar-root CA;
- tikkomunika l-aħħar informazzjoni dwar l-istatus tar-revoka (is-CRL iffirmata mir-root CA) lill-parti dipendenti, u tindika b'mod ċar li hi l-aħħar informazzjoni dwar ir-revoka;
- tarkivja r-reġistri kollha tal-awditjar u rekords oħra qabel it-tmiem tal-PKI;
- tittrasferixxi rekords arkivjati lil awtorità xierqa.

(301) It-TLM għandu jħassar iċ-ċertifikat korrispondenti tar-root CA mill-ECTL.

5.8.3. ***EA/AA***

(302) Fil-każ tat-tmiem tas-servizz tal-EA/AA, l-entità tal-EA/AA tipprovdi avviż qabel it-tmiem. EA jew AA ma għandhiex ittemm/tibda l-operat tagħha mingħajr ma tistabbilixxi pjan ta' migrazzjoni (stabbilit fis-CPS rilevanti) li jiggarantixxi l-operat kontinwu għall-abbonati kollha. L-EA/AA għandha:

- tinforma lir-root CA b'ittra rreġistrata;
- teqred il-kjavi privata tas-CA;
- tittrasferixxi l-bażi tad-*data* tagħha lill-entità maħtura mir-root CA;
- tieqaf toħroġ iċ-ċertifikati;
- matul it-trasferiment tal-bażi tad-*data* tagħha u sakemm il-bażi tad-*data* tkun kompletament operattiva f'entità ġdida, iżżomm il-kapaċità li tawtorizza talbiet mill-awtorità tal-privatezza responsabbli;
- fejn is-sub-CA tkun ġiet kompromessa, ir-root CA għandha tirrevoka s-sub-CA u toħroġ CRL ġdida b'lista ta' sub-CAs revokati;
- tarkivja r-reġistri kollha tal-awditjar u rekords oħra qabel ittemm il-PKI;
- tittrasferixxi rekords arkivjati lil entità magħżula mir-root CA.

(303) Fil-każ tat-tmiem tas-servizzi tas-CAs, is-CA għandha tkun responsabbli biex iżżomm ir-rekords rilevanti kollha rigward il-ħtiġijiet tal-komponenti tas-CA u tal-PKI.

6. KONTROLLI TAS-SIGURTÀ TEKNIKA

6.1. Ġenerazzjoni u installazzjoni tal-par kjavi

6.1.1. TLM, root CA, EA, AA

(304) Il-proċess tal-ġenerazzjoni tal-par kjavi għandu jissodisfa r-rekwiżiti li ġejjin:

- kull parteċipant għandu jkun jista' jiġġenera l-pari tal-kjavi tiegħu stess skont it-taqsimiet 6.1.4 u 6.1.5;
- il-proċess tad-derivazzjoni tal-kjavi simetriċi tal-kriptaġġ u tal-kjavi MAC għat-talbiet għal ċertifikati (ECIES) għandu jitwettaq f'konformità ma' [1] u [5];

- il-proċess tal-ġenerazzjoni tal-kjavi għandu juża l-algoritmi u t-tulijiet tal-kjavi deskritti fit-taqsimiet 6.1.4.1 u 6.1.4.2;
- il-proċess tal-ġenerazzjoni tal-par kjavi għandu jkun soġġett għar-rekwiżiti ta' "ħażna sigura ta' kjavi privati" (ara t-taqsima 6.1.5);
- ir-root CAs u l-abbonati tagħhom (sub-CAs) għandhom jiżguraw li l-integrità u l-awtenticità tal-kjavi pubbliċi tagħhom u kwalunkwe parametru assoċjat jinżammu matul id-distribuzzjoni lil entitajiet irreġistrati fis-sub-CA.

6.1.2. EE — stazzjon mobbli tas-C-ITS

(305) Kull stazzjon mobbli tas-C-ITS għandu jiġġenera l-pari tal-kjavi tiegħu stess skont it-taqsimiet 6.1.4 u 6.1.5.

(306) Il-proċess tad-derivazzjoni tal-kjavi simetriċi tal-kriptaġġ u tal-kjavi MAC għat-talbiet għal ċertifikati (ECIES) għandu jitwettaq skont [1] u [5].

(307) il-proċessi tal-ġenerazzjoni tal-kjavi għandhom jużaw l-algoritmi u t-tulijiet tal-kjavi deskritti fit-taqsimiet 6.1.4.1 u 6.1.4.2;

(308) il-proċessi tal-ġenerazzjoni tal-par kjavi għandhom ikunu soġġetti għar-rekwiżiti ta' "ħażna sigura ta' kjavi privati" (ara t-taqsima 6.1.5);

6.1.3. EE — stazzjon fiss tas-C-ITS

(309) Kull stazzjon fiss tas-C-ITS għandu jiġġenera l-par kjavi tiegħu stess skont it-taqsimiet 6.1.4 u 6.1.5.

(310) il-proċessi tal-ġenerazzjoni tal-kjavi għandhom jużaw l-algoritmi u t-tulijiet tal-kjavi deskritti fit-taqsimiet 6.1.4.1 u 6.1.4.2;

(311) il-proċessi tal-ġenerazzjoni tal-par kjavi għandhom ikunu soġġetti għar-rekwiżiti ta' "ħażna sigura ta' kjavi privati" (ara t-taqsima 6.1.5);

6.1.4. Rekwiżiti kriptografiċi

(312) Il-parteċipanti kollha tal-PKI għandhom jissodisfaw ir-rekwiżiti kriptografiċi stabbiliti fil-paragrafi li ġejjin fir-rigward tal-algoritmu tal-firma, it-tul tal-kjavi, il-ġeneratur tan-numru każwali u ċ-ċertifikati tal-konnessjoni.

6.1.4.1. *Algoritmu u tul tal-kjavi – algoritmi tal-firma*

(313) Il-parteċipanti kollha tal-PKI (TLM, root CA, EA, AA u stazzjonijiet tas-C-ITS) għandhom ikunu jistgħu jiġġeneraw pari tal-kjavi u jużaw il-kjavi privata għall-iffirmar tal-operazzjonijiet b'algoritmi magħżula mhux aktar tard minn sentejn wara d-dħul fis-seħħ ta' dan ir-Regolament skont it-Tabella 4.

(314) Il-parteċipanti kollha tal-PKI li għandhom jivverifikaw l-integrità tal-ECTL, iċ-ċertifikati u/jew il-messaġġi ffirmati skont ir-rwol tagħhom, kif iddefinit fit-taqsima 1.3.6, għandhom jappoġġjaw l-algoritmi korrispondenti mniżżla fit-Tabella 5 għall-verifika. B'mod partikolari, l-istazzjonijiet tas-C-ITS għandhom ikunu jistgħu jivverifikaw l-integrità tal-ECTL.

	TLM	root CA	EA	AA	Stazzjon tas-C-ITS

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	-	-
X tindika appoġġ obbligatorju					

Tabella 4: Il-ġenerazzjoni tal-pari tal-kjavi u l-użu tal-kjavi privata għall-iffirmar tal-operazzjonijiet

	TLM	root CA	EA	AA	Stazzjon tas-C-ITS
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
X tindika appoġġ obbligatorju					

Tabella 5: Ħarsa ġenerali lejn il-verifika

(315) Jekk is-CPA tiddeċiedi hekk abbażi ta' dgħufijiet kriptografiċi li nstabu ġodda, l-istazzjonijiet kollha tas-C-ITS għandhom ikunu jistgħu jaqilbu għal wieħed miż-żewġ algoritmi (ECDSA_nistP256_with_SHA 256 jew ECDSA_brainpoolP256_with_SHA 256) kemm jista' jkun malajr. L-algoritmu(i) attwali li huwa/huma użati għandhom jiġu ddeterminati fis-CPS tas-CA li toħroġ iċ-ċertifikat għall-kjavi pubblika korrispondenti, skont din is-CP.

6.1.4.2. *Algoritmu u tul tal-kjavi – algoritmi ta' kriptaġġ għar-reġistrazzjoni u l-awtorizzazzjoni*

(316) Il-parteċipanti kollha tal-PKI (EA, AA u stazzjonijiet tas-C-ITS) għandhom ikunu jistgħu jużaw kjavi pubbliċi għall-kriptaġġ ta' talbiet/risposti għar-reġistrazzjoni u l-awtorizzazzjoni b'algoritmi magħżula mhux aktar tard minn sentejn wara d-dħul fis-seħħ ta' dan ir-Regolament skont it-Tabella 6. L-algoritmu(i) attwali li huwa/huma użati għandhom jiġu ddeterminati fis-CPS tas-CA li toħroġ iċ-ċertifikat għall-kjavi pubblika korrispondenti, skont din is-CP.

(317) L-algoritmi msemmija fit-Tabella 6 jindikaw it-tul tal-kjavi u t-tul tal-algoritmu tal-hash u għandhom jiġu implimentati skont [5].

	TLM	root CA	EA	AA	Stazzjon tas-C-ITS
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES 128_CCM	-	-	X	X	X
X tindika appoġġ obbligatorju					

Tabella 6: L-użu tal-kjavi pubbliċi għall-kriptaġġ ta' talbiet/risposti għar-reġistrazzjoni u l-awtorizzazzjoni

(318) Il-parteċipanti kollha tal-PKI (EA, AA u stazzjonijiet tas-C-ITS) għandhom ikunu jistgħu jiġġeneraw pari tal-kjavi u jużaw il-kjavi privata għall-kriptaġġ ta' talbiet/risposti għar-reġistrazzjoni u l-awtorizzazzjoni b'algoritmi magħżula mhux aktar tard minn sentejn wara d-dħul fis-seħħ ta' dan ir-Regolament skont it-Tabella 7:

	TLM	root CA	EA	AA	Stazzjon tas-C-ITS
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES 128_CCM	-	-	X	X	X
X tindika appoġġ obbligatorju					

Tabella 7: Il-ġenerazzjoni tal-pari kjavi u l-użu tal-kjavi privata għad-dekriptaġġ ta' talbiet/risposti għar-reġistrazzjoni u l-awtorizzazzjoni

6.1.4.3. *Aġilità kriptografika*

(319) Ir-rekwiżiti dwar it-tulijiet tal-kjavi u l-algoritmi għandhom jinbidlu maż-żmien biex jinżamm livell xieraq ta' sigurtà. Is-CPA għandha timmonitorja l-ħtieġa għal dawn il-bidliet fid-dawl tal-vulnerabbiltajiet effettivi u l-aktar kriptografija avvanzata. Din se tabbozza, tapprova u tippubblika aġġornament ta' din il-politika taċ-ċertifikati jekk tiddeċiedi li l-algoritmi kriptografiċi għandhom jiġu aġġornati. Fejn kwistjoni ġdida ta' din is-CP tindika bidla fl-algoritmu u/jew fit-tul tal-kjavi, is-CPA għandha tadotta strateġija ta' migrazzjoni, li tinkludi perjodi ta' tranżizzjoni li matulhom l-algoritmi u t-tulijiet tal-kjavi l-qodma għandhom jiġu appoġġjati.

(320) Biex ikun jista' jsir u jiġi ffaċilitat it-trasferiment għal algoritmi u/jew tulijiet tal-kjavi ġodda, hu rakkomandat li l-parteċipanti kollha tal-PKI jimplimentaw ħardwer u/jew softwer li hu kapaċi għal bidla fit-tulijiet tal-kjavi u fl-algoritmi.

(321) It-tibdil fiċ-ċertifikati root u fiċ-ċertifikati tat-TLM għandu jiġi appoġġjat u mwettaq bl-għajnuna ta' ċertifikati tal-konnessjoni (ara t-taqsima 4.6) li jintużaw biex ikopru l-perjodu ta' tranżizzjoni bejn iċ-ċertifikati root il-qodma u l-ġodda ("il-migrazzjoni tal-mudell ta' fiduċja").

6.1.5. Ħażna sigura ta' kjavi privati

Din it-taqsima tiddeskrivi r-rekwiżiti għall-ħażna sigura u l-ġenerazzjoni ta' pari tal-kjavi u numri każwali għas-CAs u għall-entitajiet aħħarija. Dawn ir-rekwiżiti huma ddefiniti għall-moduli kriptografiċi u deskritti fis-subtaqsimiet li ġejjin.

6.1.5.1. *Livell ta' root CA, sub-CA u TLM*

(322) Il-modulu kriptografiku għandu jintuża:

- għall-ġenerazzjoni, l-użu, l-amministrazzjoni u l-ħażna ta' kjavi privati;
- għall-ġenerazzjoni u l-użu ta' numri każwali (il-valutazzjoni tal-funzjoni tal-ġenerazzjoni tan-numri każwali għandha tkun parti mill-evalwazzjoni u ċ-ċertifikazzjoni tas-sigurtà);
- għall-ħolqien ta' backups tal-kjavi privati skont it-taqsima 6.1.6;

- għat-tħassir tal-kjavi privati.

Il-modulu kriptografiku għandu jiġi ċċertifikat b'wieħed mill-profili ta' protezzjoni (PPs) li ġejjin, b'livell ta' assigurazzjoni EAL-4 jew ogħla:

- PPs għall-HSMs:
  - CEN EN 419 221-2: Profili ta' protezzjoni għal moduli kriptografiċi TSP – Parti 2: Modulu kriptografiku għall-operazzjonijiet tal-iffirmar tas-CSP bil-backup;
  - CEN EN 419 221-4: Profili ta' protezzjoni għal moduli kriptografiċi TSP – Parti 4: Modulu kriptografiku għall-operazzjonijiet tal-iffirmar tas-CSP mingħajr il-backup;
  - CEN EN 419 221-5: Profili ta' protezzjoni għal moduli kriptografiċi TSP – Parti 5: Modulu kriptografiku għas-servizzi ta' fiduċja;
- PPs għal smartcards:
  - CEN EN 419 211-2: Profili tal-protezzjoni għal apparat sigur għall-ħolqien ta' firem – Parti 2: Apparat b'ġeneratur tal-kodiċijiet;
  - CEN EN 419 211-3: Profili tal-protezzjoni għal apparat sigur għall-ħolqien ta' firem – Parti 3: Apparat b'importatur tal-kodiċijiet

L-aċċess manwali għall-modulu kriptografiku għandu jeħtieġ awtentikazzjoni b'żewġ fatturi mill-amministratur. Barra minn hekk, dan għandu jeħtieġ l-involviment ta' żewġ persuni awtorizzati.

L-implimentazzjoni tal-modulu kriptografiku għandha tiżgura li l-kjavi ma jkunux aċċessibbli barra mill-modulu kriptografiku. Il-modulu kriptografiku għandu jinkludi mekkaniżmu ta' kontroll tal-aċċess biex jipprevjeni l-użu mhux awtorizzat ta' kjavi privati.

6.1.5.2. *Entità aħħarija*

(323) Il-modulu kriptografiku għall-EEs għandu jintuża:

- għall-ġenerazzjoni, l-użu, l-amministrazzjoni u l-ħażna ta' kjavi privati;
- għall-ġenerazzjoni u l-użu ta' numri każwali (il-valutazzjoni tal-funzjoni tal-ġenerazzjoni tan-numri każwali għandha tkun parti mill-evalwazzjoni u ċ-ċertifikazzjoni tas-sigurtà);
- għat-tħassir sigur ta' kjavi privata.

(324) Il-modulu kriptografiku għandu jkun protett minn tneħħija, sostituzzjoni u modifika mhux awtorizzati. Il-PPs u d-dokumenti relatati kollha applikabbli għaċ-ċertifikazzjoni tas-sigurtà tal-modulu kriptografiku għandhom jiġu evalwati, ivvalidati u ċċertifikati skont l-ISO 15408, billi jiġi applikat il-Ftehim dwar ir-Rikonoxximent Reċiproku ta' Ċertifikati ta' Evalwazzjoni tas-Sigurtà tat-Teknoloġija tal-Informatika tal-Grupp ta' Uffiċjali Għoljin dwar is-Sigurtà tas-Sistemi tal-Informazzjoni (SOG-IS), jew skema Ewropea taċ-ċertifikazzjoni taċ-ċibersigurtà skont il-qafas Ewropew taċ-ċibersigurtà rilevanti.

(325) Minħabba l-importanza li jinżamm l-ogħla livell ta' sigurtà possibbli, iċ-ċertifikati tas-sigurtà għall-modulu kriptografiku għandhom jinħarġu skont l-iskema taċ-ċertifikazzjoni ta' kriterji komuni (ISO 15408) minn korp ta' valutazzjoni tal-konformità rikonoxxut mill-kumitat ta' tmexxija fil-qafas tal-Ftehim tas-SOG-IS, jew jinħarġu minn korp ta' valutazzjoni tal-konformità akkreditat minn awtorità nazzjonali taċ-ċertifikazzjoni taċ-ċibersigurtà ta' Stat Membru. Dan il-korp ta' valutazzjoni tal-konformità għandu jipprovdi mill-inqas kundizzjonijiet ekwivalenti ta' evalwazzjoni ta' sigurtà kif previsti mill-Ftehim ta' Rikonoxximent Reċiproku tas-SOG-IS.

Nota: ir-rabta bejn il-modulu kriptografiku u l-istazzjon tas-C-ITS0, għandha tkun protetta.

6.1.6. Backup tal-kjavi privati

(326) Il-ġenerazzjoni, il-ħażna u l-użu ta' backups tal-kjavi privati għandhom jissodisfaw ir-rekwiżiti ta' mill-anqas il-livell ta' sigurtà meħtieġ għall-kjavi oriġinali.

(327) Il-backups tal-kjavi privati għandhom isiru mir-root CAs, l-EAs u l-AAs.

(328) Il-backups tal-kjavi privati ma għandhomx isiru għall-ECs u l-ATs.

6.1.7. Qerda tal-kjavi privati

(329) Ir-root CAs, l-EAs, l-AAs, u l-istazzjonijiet mobbli u fissi tas-C-ITS għandhom jeqirdu l-kjavi privata tagħhom u kwalunkwe backups korrispondenti, jekk par kjavi ġdid u ċertifikat korrispondenti jkunu ġew iġġenerati u installati b'suċċess, u l-ħin tas-sovrapożizzjoni (jekk ikun hemm — għas-CA biss) ikun għadda. Il-kjavi privata għandha tinqered bl-użu tal-mekkaniżmu offrut mill-modulu kriptografiku użat għall-ħażna tal-kjavi jew kif deskritt fil-PP korrispondenti kif imsemmi fit-taqsima 6.1.5.2.

6.2. *Data* tal-attivazzjoni

(330) Id-*data* tal-attivazzjoni tirreferi għal fatturi ta' awtentikazzjoni meħtieġa biex jitħaddmu l-moduli kriptografiċi biex jipprevjenu l-aċċess mhux awtorizzat. L-użu tad-*data* tal-attivazzjoni tal-apparat kriptografiku tas-CA għandu jeħtieġ azzjoni minn żewġ persuni awtorizzati.

6.3. Kontrolli tas-sigurtà tal-kompjuter

(331) Il-kontrolli tas-sigurtà tal-kompjuter tas-CAs għandhom ikunu ddisinjati skont il-livell għoli ta' sigurtà billi josservaw bir-reqqa r-rekwiżiti ta' ISO/IEC 27002.

6.4. Kontrolli tekniċi taċ-ċiklu tal-ħajja

(332) Il-kontrolli tekniċi tas-CA għandhom ikopru ċ-ċiklu kollu tal-ħajja tas-CA. B'mod partikolari, dan jinkludi r-rekwiżiti tat-taqsima 6.1.4.3 ("Aġilità kriptografika").

6.5. Kontrolli tas-sigurtà tan-network

(333) In-networks tas-CAs (root CA, EA u AA) għandhom jiġu msaħħa kontra l-attakki b'konformità mar-rekwiżiti u l-gwida tal-implimentazzjoni ta' ISO/IEC 27001 u ISO/IEC 27002.

(334) Id-disponibbiltà tan-networks tas-CA għandha tkun iddisinjata fid-dawl tat-traffiku stmat.

7. PROFILI TAĊ-ĊERTIFIKAT, CRL U CTL

7.1. Profil taċ-ċertifikat

(335) Il-profili taċ-ċertifikati ddefiniti f'[5] għandhom jintużaw għat-TLM, għaċ-ċertifikati root, għaċ-ċertifikati tal-EA, għaċ-ċertifikati tal-AA, għall-ATs u għall-ECs. L-EAs tal-gvern nazzjonali jistgħu jużaw profili oħra taċ-ċertifikati għall-ECs.

(336) Iċ-ċertifikati tar-root CA, tal-EA u tal-AA għandhom jindikaw il-permessi li għalihom dawn is-CAs (root CAs, EA u AA) jitħallew joħorġu ċertifikati.

(337) Abbażi ta' [5]:

- kull root CA għandha tuża l-kjavi privata tal-iffirmar tagħha stess biex toħroġ is-CRLs;
- it-TLM għandu juża l-kjavi privata tal-iffirmar tiegħu stess biex joħroġ l-ECTL.

7.2. Validità taċ-ċertifikat

(338) Il-profili kollha taċ-ċertifikat tas-C-ITS għandhom jinkludu d-data tal-ħruġ u ta' skadenza, li jirrappreżentaw iż-żmien tal-validità taċ-ċertifikat. F'kull livell tal-PKI, iċ-ċertifikati għandhom jiġu ġġenerati fi żmien xieraq qabel l-iskadenza.

(339) Iż-żmien tal-validità taċ-ċertifikati tas-CA u tal-EC għandu jinkludi żmien ta' sovrapożizzjoni. Iċ-ċertifikati tat-TLM u tar-root CA għandhom jinħarġu u jitpoġġew fuq l-ECTL sa massimu ta' tliet xhur u mill-anqas xahar qabel ma tibda l-validità tagħhom skont il-ħin tal-bidu fiċ-ċertifikat. Din il-fażi ta' prellowdjar hi meħtieġa biex iċ-ċertifikati jitqassmu b'mod sikur lill-partijiet dipendenti korrispondenti kollha skont it-taqsima 2.2. Dan jiżgura li, mill-bidu taż-żmien ta' sovrapożizzjoni, il-partijiet dipendenti kollha diġà jkunu jistgħu jivverifikaw il-messaġġi maħruġa b'ċertifikat ġdid.

(340) Fil-bidu taż-żmien ta' sovrapożizzjoni, iċ-ċertifikati tas-CA, EC u AT suċċessivi għandhom jinħarġu (jekk applikabbli), jitqassmu lil u jiġu installati mill-partijiet dipendenti korrispondenti. Matul iż-żmien ta' sovrapożizzjoni, iċ-ċertifikat attwali għandu jintuża biss għall-verifika.

(341) Billi l-perjodi ta' validità elenkati fit-Tabella 8 ma għandhomx jaqbżu l-perjodu ta' validità taċ-ċertifikat superjuri, japplikaw ir-restrizzjonijiet li ġejjin:

- maximumvalidity(Root CA) = privatekeyusage(Root CA) + maximumvalidity(EA,AA);
- maximumvalidity(EA) = privatekeyusage(EA) + maximumvalidity(EC);
- maximumvalidity(AA) = privatekeyusage(AA) + preloadingperiod(AT).

(342) Il-validità taċ-ċertifikati tal-konnessjoni (Root u TLM) tibda bl-użu tal-kjavi privata korrispondenti u tispiċċa fil-ħin massimu tal-validità tar-root CA jew tat-TLM.

(343) It-Tabella 8 turi ż-żmien massimu tal-validità għaċ-ċertifikati tas-C-ITS tas-CA (għall-perjodi ta' validità tal-AT, ara t-taqsima 7.2.1).

Entità	Il-perjodu massimu tal-użu tal-kjavi privata	Iż-żmien massimu tal-validità
Root CA	3 snin	8 snin
EA	sentejn (2)	5 snin
AA	4 snin	5 snin
EC	3 snin	3 snin
TLM	3 snin	4 snin

Tabella 8: Perjodi ta' validità taċ-ċertifikati fil-mudell ta' fiduċja tas-C-ITS

7.2.1. Ċertifikati psewdonimi

(344) F'dan il-kuntest, il-psewdonimi huma implimentati mill-ATs. Bħala konsegwenza, din it-taqsima tirreferi għal ATs aktar milli għal psewdonimi.

(345) Ir-rekwiżiti stabbiliti f'din it-taqsima japplikaw biss għal ATs ta' stazzjonijiet mobbli tas-C-ITS li jibagħtu messaġġi CAM u DENM, fejn ir-riskju tal-privatezza tal-post hu applikabbli. L-ebda rekwiżiti speċifiċi fuq iċ-ċertifikati tal-AT ma japplikaw għal ATs għal stazzjonijiet fissi tas-C-ITS u għal stazzjonijiet mobbli tas-C-ITS użati għal funzjonijiet speċjali fejn il-privatezza tal-post mhijiex applikabbli (eż. vetturi mmarkati tal-emerġenza u tal-infurzar tal-liġi).

(346) Għandhom japplikaw id-definizzjonijiet li ġejjin:

- "perjodu ta' validità għall-ATs" – il-perjodu li fih l-AT ikun validu, jiġifieri l-perjodu bejn id-data tal-bidu tal-AT u d-data ta' skadenza tiegħu;
- "perjodu ta' prellowdjar għall-ATs" – il-prellowdjar hi l-possibbiltà għall-istazzjonijiet tas-C-ITS li jiksbu ATs qabel ma jibda l-perjodu ta' validità. Il-perjodu ta' prellowdjar hu l-perjodu ta' żmien massimu permess mit-talba għall-ATs sal-aħħar tmiem tad-data tal-validità ta' kwalunkwe AT mitlub;
- "perjodu ta' użu għall-ATs" – il-perjodu li matulu l-AT jintuża b'mod effettiv biex jiġu ffirmati l-messaġġi CAM/DENM;
- "numru massimu ta' ATs paralleli" – in-numru ta' ATs li minnhom stazzjon tas-C-ITS jista' jagħżel fi kwalunkwe ħin meta jiffirma messaġġ CAM/DENM, jiġifieri n-numru ta' ATs differenti maħruġa lil stazzjon tas-C-ITS wieħed li huma validi fl-istess ħin.

(347) Għandhom japplikaw ir-rekiwiżiti li ġejjin:

- il-perjodu ta' prellowdjar għall-ATs ma għandux jaqbeż it-tliet xhur;
- il-perjodu ta' validità għall-ATs ma għandux jaqbeż il-ġimgħa;
- in-numru massimu ta' ATs paralleli ma għandux jaqbeż il-100 għal kull stazzjon tas-C-ITS;
- il-perjodu tal-użu ta' AT jiddependi fuq l-istrateġija tal-bidla tal-AT u l-ammont ta' ħin li vettura tkun qed taħdem, iżda hu limitat min-numru

massimu ta' ATs paralleli u l-perjodu ta' validità. B'mod aktar speċifiku, il-perjodu medju tal-użu għal stazzjon tas-C-ITS wieħed hu mill-anqas il-ħin operattiv tal-vettura matul perjodu ta' validità wieħed diviż bl-għadd massimu ta' ATs paralleli.

7.2.2. Biljetti ta' awtorizzazzjoni għal stazzjonijiet fissi tas-C-ITS

(348) Japplikaw id-definizzjonijiet fit-taqsima 7.2.1 u r-rekwiżiti li ġejjin:

- il-perjodu ta' prellowdjar għall-ATs ma għandux jaqbeż it-tliet xhur;
- in-numru massimu ta' ATs paralleli ma għandux jaqbeż it-tnejn għal kull stazzjon tas-C-ITS.

7.3. Revoka taċ-ċertifikati

7.3.1. Revoka taċ-ċertifikati tas-CA, l-EA u l-AA

Iċ-ċertifikati tar-root CA, tal-EA u tal-AA għandhom ikunu revokabbli. Iċ-ċertifikati revokati tar-root CAs, tal-EAs u tal-AAs għandhom jiġu ppubblikati fuq CRL malajr kemm jista' jkun u mingħajr dewmien żejjed. Din is-CRL għandha tkun iffirmata mir-root CA korrispondenti tagħha u tuża l-profil deskritt fit-taqsima 7.4. Għar-revoka taċ-ċertifikati tar-root CA, ir-root CA korrispondenti toħroġ CRL li tinkludi lilha stess. Barra minn hekk, f'każijiet ta' kompromess tas-sigurtà, tapplika t-taqsima 5.7.3. Barra minn hekk, it-TLM għandu jneħħi r-root CAs revokati mil-lista ta' fiduċja u joħroġ lista ġdida ta' fiduċja. Iċ-ċertifikati skaduti għandhom jitneħħew mis-CRL korrispondenti u mil-lista ta' fiduċja.

(349) Iċ-ċertifikati jiġu revokati meta:

- ir-root CAs għandhom raġuni biex jemmnu jew jissuspettaw bil-qawwa li l-kjavi privata korrispondenti ġiet kompromessa;
- ir-root CAs ikunu ġew innotifikati li l-kuntratt mal-abbonat ġie tterminat;
- l-informazzjoni (bħall-isem u l-assoċjazzjonijiet bejn is-CA u s-suġġett) fiċ-ċertifikat mhijiex korretta jew inbidlet;
- iseħħ inċident tas-sigurtà li jaffettwa lis-sid taċ-ċertifikat;
- l-awditjar (ara t-taqsima 8) iwassal għal riżultat negattiv.

(350) L-abbonat għandu minnufih jinnotifika lis-CA dwar kompromess magħruf jew suspettat tal-kjavi privata tagħhom. Għandu jkun assigurat li talbiet awtentikati biss jirriżultaw f'ċertifikati revokati.

7.3.2. Revoka tal-kredenzjali tar-reġistrazzjoni

(351) Ir-revoka tal-ECs tista' tinbeda mill-abbonat tal-istazzjon tas-C-ITS (fluss 34) u għandha tkun implimentata minn lista sewda interna f'bażi tad-*data* ta' revoka bi kronogramma, li hi ġġenerata u miżmuma minn kull EA. Il-lista sewda qatt ma tiġi ppubblikata u għandha tinżamm kunfidenzjali u tintuża biss mill-EA korrispondenti biex tivverifika l-validità tal-ECs korrispondenti fil-kuntest tat-talbiet għal ATs u ECs ġodda.

7.3.3. Revoka tal-biljetti ta' awtorizzazzjoni

(352) Peress li l-ATs mhumiex revokati mis-CAs korrispondenti, dawn għandu jkollhom ħajja qasira u ma jistgħux jinħarġu wisq qabel ma jsiru validi.

Il-valuri tal-parametri taċ-ċiklu tal-ħajja permissibbli taċ-ċertifikat huma stabbiliti fit-taqsima 7.2.

7.4. Lista tar-revoka taċ-ċertifikati

(353) Il-format u l-kontenut tas-CRL maħruġa mir-root CAs għandhom ikunu kif stabbilit f'[1].

7.5. Lista ta' fiduċja Ewropea taċ-ċertifikati

(354) Il-format u l-kontenut tal-ECTL maħruġa mit-TLM għandhom ikunu kif stabbilit f'[1].

8. AWDITJAR TAL-KONFORMITÀ U VALUTAZZJONIJIET OĦRA

8.1. Suġġetti koperti mill-awditjar u l-bażi tal-awditjar

(355) L-awditjar tal-konformità għandu l-iskop li jivverifika li t-TLM, ir-root CAs, l-EAs u l-AAs joperaw skont din is-CP. It-TLM, ir-root CAs, l-EAs u l-AAs għandhom jagħżlu awditur akkreditat tal-PKI li jaġixxi b'mod indipendenti biex jawditja s-CPS tagħhom. L-awditjar għandu jkun ikkombinat ma' valutazzjoni ta' ISO/IEC 27001 u ISO/IEC 27002.

(356) L-awditjar tal-konformità jiġi ordnat minn root CA (fluss 13) għar-root CA nnifisha, u għal sub-CA mill-EA/AA subordinata tagħha.

(357) L-awditjar tal-konformità għat-TLM jiġi ordnat mis-CPA (fluss 38).

(358) Meta mitlub, l-awditur akkreditat tal-PKI għandu jwettaq l-awditjar tal-konformità f'wieħed mil-livelli li ġejjin:

(1) konformità tas-CPS tat-TLM, tar-root CA, tal-EA jew tal-AA ma' din is-CP;

(2) konformità tal-prattiki maħsuba tat-TLM, tar-root CA, tal-EA jew tal-AA mas-CPS tagħhom qabel l-operat;

(3) konformità tal-prattiki u tal-attivitajiet operattivi tat-TLM, tar-root CA, tal-EA jew tal-AA mas-CPS tagħhom matul l-operat.

(359) L-awditjar għandu jkopri r-rekwiżiti kollha ta' din is-CP li għandhom jiġu sodisfatti mit-TLM, mir-root CAs, mill-EAs u mill-AAs li se jiġu awditjati. Għandu jkopri wkoll l-operat tas-CA fil-PKI tas-C-ITS, inkluż il-proċessi kollha msemmija fis-CPS tagħha, il-bini u l-persuni responsabbli.

(360) L-awditur akkreditat tal-PKI għandu jipprovdi rapport dettaljat tal-awditjar lir-root CA (fluss 36), lill-EA, lill-AA jew lis-CPA (fluss 16 u 40), kif applikabbli.

8.2. Frekwenza tal-awditjar

(361) Ir-root CA, it-TLM, l-EA jew l-AA għandhom jordnaw l-awditjar tal-konformità tagħhom stess minn awditur akkreditat u indipendenti tal-PKI fil-każijiet li ġejjin:

- fl-ewwel twaqqif tagħha/tiegħu (konformità tal-livelli 1 u 2);
- ma' kull bidla tas-CP. Is-CPA għandha tiddefinixxi l-kontenut tal-bidla tas-CP u l-iskeda tat-tnedija u tiddetermina l-ħtiġijiet għall-awditjar (inkluż il-livell ta' konformità meħtieġ) kif xieraq;

- ma’ kull bidla tas-CPS tagħha/tiegħu (konformità tal-livelli 1, 2 u 3). Peress li l-entitajiet tal-immaniġġjar tar-root CAs, tat-TLM u tal-EAs/AAs jiddeċiedu liema bidliet fl-implimentazzjoni jsegwu l-aġġornament tas-CPS tagħhom, huma għandhom jordnaw l-awditjar tal-konformità qabel jimplimentaw dawk il-bidliet. F’każijiet ta’ bidliet żgħar biss fis-CPS (eż. ta’ natura editorjali), l-entità tal-immaniġġjar tista’ tibgħat talba debitament iġġustifikata lis-CPA għall-approvazzjoni tagħha biex taqbeż l-awditjar tal-konformità tal-livell 1, 2 jew 3;
- regolarment, u mill-anqas kull tliet snin matul l-operat tagħha/tiegħu (konformità tal-livell 3).

8.3. Identità/kwalifiki tal-awditur

(362) Is-CA li se tiġi awditjata għandha tagħżel kumpanija/organizzazzjoni akkreditata li taġixxi b’mod indipendenti (“korp tal-awditjar”) jew awdituri akkreditati tal-PKI biex jawditjawha skont din is-CP. Il-korp tal-awditjar għandu jkun akkreditat u ċċertifikat minn membru tal-Akkreditazzjoni Ewropea[1].

8.4. Relazzjoni tal-awditur mal-entità awditjata

(363) L-awditur akkreditat tal-PKI għandu jkun indipendenti mill-entità awditjata.

8.5. Azzjoni meħuda bħala riżultat ta’ defiċjenza

(364) Meta r-rapport tal-awditjar isib li t-TLM mhux konformi, is-CPA għandha tordna lit-TLM biex jieħu azzjoni preventiva/korrettiva immedjata.

(365) Meta r-root CA b’rapport tal-awditjar mhux konformi tagħmel applikazzjoni ġdida, is-CPA għandha tirrifjuta l-applikazzjoni u tibgħat rifjut korrispondenti lir-root CA (fluss 4). F’dawn il-każijiet, ir-root CA għandha tiġi sospiża. Għandha tieħu azzjoni korrettiva, tordna mill-ġdid l-awditjar u tagħmel talba ġdida għall-approvazzjoni tas-CPA. Ir-root CA ma għandhiex titħalla toħroġ ċertifikati matul is-sospensjoni.

(366) F’każijiet ta’ awditjar regolari tar-root CA jew ta’ tibdil fis-CPS tar-root CA, u skont in-natura tan-nuqqas ta’ konformità deskritt fir-rapport tal-awditjar, is-CPA tista’ tiddeċiedi li tirrevoka r-root CA u tikkomunika din id-deċiżjoni lit-TLM (il-fluss 2), biex twassal għat-tħassir taċ-ċertifikat tar-root CA mill-ECTL u l-inklużjoni tar-root CA fis-CRL. Is-CPA għandha tibgħat rifjut korrispondenti lir-root CA (fluss 4). Ir-root CA għandha tieħu azzjoni korrettiva, tordna mill-ġdid l-awditjar sħiħ (livell 1 sa 3) u tagħmel talba ġdida għall-approvazzjoni tas-CPA. Alternattivament, is-CPA tista’ tiddeċiedi li ma tirrevokax ir-root CA, iżda li tagħtiha perjodu ta’ grazzja li fih ir-root CA għandha tieħu azzjoni korrettiva, tordna mill-ġdid l-awditjar u terġa’ tippreżenta r-rapport tal-awditjar lis-CPA. F’dan il-każ, l-operazzjoni tar-root CA għandha tiġi sospiża u ma titħalliex toħroġ ċertifikati u CRLs.

(367) Fil-każ tal-awditjar tal-EA/AA, ir-root CA għandha tiddeċiedi jekk taċċettax ir-rapport jew le. Skont ir-riżultat tal-awditjar, ir-root CA għandha tiddeċiedi jekk tirrevokax iċ-ċertifikat tal-EA/AA skont ir-regoli fis-CPS tar-root CA. Ir-root CA għandha dejjem tiżgura l-konformità tal-EA/AA ma’ din is-CP.

---

[1] Il-membri tal-Korp Ewropew tal-Akkreditazzjoni huma elenkati fuq: http://www.european-accreditation.org/ea-members

8.6. Komunikazzjoni tar-riżultati

(368) Ir-root CA u t-TLM għandhom jibagħtu r-rapport tal-awditjar lis-CPA (fluss 16). Ir-root CA u t-TLM għandhom jaħżnu r-rapporti tal-awditjar kollha li jkunu ordnaw. Is-CPA għandha tibgħat approvazzjoni jew rifjut korrispondenti (fluss 4) lir-root CA u lit-TLM.

(369) Ir-root CA għandha tibgħat ċertifikat tal-konformità lill-EA/AA korrispondenti.

9. DISPOŻIZZJONIJIET OĦRA

9.1. Tariffi

(370) Prinċipju wieħed tal-mudell ta' fiduċja tas-C-ITS tal-UE implimentat hu li r-root CAs flimkien jiffinanzjaw b'mod sħiħ l-ispejjeż rikorrenti regolari tal-operat tas-CPA u l-elementi ċentrali (it-TLM u s-CPOC) relatati mal-attivitajiet stabbiliti f'din is-CP.

(371) Ir-root CAs (inkluż ir-root CA tal-UE) huma intitolati li jieħdu l-miżati mis-sub-CAs tagħhom.

(372) Matul il-perjodu kollu tal-operat tagħhom, kull parteċipant tal-mudell ta' fiduċja tas-C-ITS għandu jkollu aċċess għal mill-anqas root CA, EA u AA waħda fuq bażi mhux diskriminatorja.

(373) Kull root CA hi intitolata li tgħaddi l-miżati li tħallas għas-CPA u għall-elementi ċentrali (it-TLM u s-CPOC) lill-parteċipanti rreġistrati tal-mudell ta' fiduċja tas-C-ITS, inkluż l-istazzjonijiet tas-C-ITS irreġistrati u awtorizzati.

9.2. Responsabbiltà finanzjarja

(374) L-istabbiliment inizjali tar-root CA għandu jkopri perjodu ta' mill-anqas tliet snin ta' operazzjoni, biex din issir membru tal-mudell ta' fiduċja tas-C-ITS tal-UE. Is-CPS ta' operatur tar-root CA għandu jkun fiha wkoll dispożizzjonijiet dettaljati dwar ir-revoka jew l-għeluq tar-root CA.

(375) Kull root CA għandha turi l-vijabbiltà finanzjarja tal-entità legali li timplimentaha għal mill-anqas tliet snin. Dan il-pjan ta' vijabbiltà finanzjarja hu parti mis-sett inizjali ta' dokumenti għar-reġistrazzjoni u għandu jiġi aġġornat kull tliet snin u rrapportat lis-CPA.

(376) Kull sena, kull root CA għandha tirrapporta l-istruttura tal-imposti applikati għall-EAs/AAs u għall-istazzjonijiet irreġistrati u awtorizzati tas-C-ITS lill-maniġer tal-operazzjonijiet u lis-CPA biex turi s-sostenibbiltà finanzjarja tagħha.

(377) L-entitajiet finanzjarji u legali kollha responsabbli tar-root CA, tal-EA, tal-AA u tal-elementi ċentrali (is-CPOC u t-TLM) tal-mudell ta' fiduċja tas-C-ITS għandhom ikopru d-dmirijiet operattivi tagħhom b'livelli ta' assigurazzjoni adegwati biex jikkumpensaw għal erruri operattivi u rkupru finanzjarju tad-dmirijiet tagħhom jekk wieħed mill-elementi tekniċi jfalli.

9.3. Kunfidenzjalità tal-informazzjoni kummerċjali

(378) Dawn li ġejjin għandhom jinżammu kunfidenzjali u privati:

- ir-rekords tal-applikazzjonijiet tar-root CA, tal-EA u tal-AA, kemm jekk approvati jew irrifjutati;

- ir-rapporti tal-awditjar tar-root CA, tal-EA, tal-AA u tat-TLM;
- il-pjanijiet ta' rkupru minn diżastri tar-root CAs, tal-EAs, tal-AAs, tas-CPOCs u tat-TLM;
- il-kjavi privati tal-elementi tal-mudell ta' fiduċja tas-C-ITS (l-istazzjonijiet tas-C-ITS, it-TLM, l-EA, l-AA, ir-root CAs);
- kwalunkwe informazzjoni oħra identifikata bħala kunfidenzjali mis-CPA, mir-root CAs, mill-EA, mill-AA, mit-TLM u mis-CPOC.

9.4. Pjan tal-privatezza

(379) Is-CPSs tar-root CAs u l-EAs/AAs għandhom jistabbilixxu l-pjan u r-rekwiżiti għat-trattament tal-informazzjoni personali u l-privatezza skont il-GDPR u oqfsa leġiżlattivi applikabbli oħra (eż. nazzjonali).

10. REFERENZI

F'dan l-Anness qed jintużaw ir-referenzi li ġejjin:

[1] ETSI TS 102 941 V1.2.1, Intelligent transport systems (ITS) – security, trust and privacy management.

[2] ETSI TS 102 940 V1.3.1, Intelligent transport systems (ITS) – security, ITS communications security architecture and security management.

[3] Certificate policy and certification practices framework (RFC 3647, 1999).

[4] ETSI TS 102 042 V2.4.1 Policy requirements for certification authorities issuing public key certificates.

[5] ETSI TS 103 097 V1.3.1, Intelligent transport systems (ITS) – security, security header and certificate formats.

[6] Calder, A. (2006). *Information security based on ISO 27001/ISO 1779: a management guide.* Van Haren Publishing.

[7] ISO, I., & Std, I. E. C. (2011). ISO 27005 (2011) – information technology, security techniques, information security risk management. ISO.