Euroopa Liidu
Nõukogu

Brüssel, 5. november 2018
(OR. en)

Institutsioonidevaheline dokument: 2018/0339(NLE)

13711/18
ADD 1

TRANS 488

MÄRKUS

Saatja:	Nõukogu peasekretariaat
Saaja:	Delegatsioonid
Eelmise dok nr:	ST 13711/18 TRANS 448
Komisjoni dok nr:	ST 12727/18 TRANS 426 + ADD 1
Teema:	Nõukogu otsus seisukoha kohta, mis võetakse Euroopa Liidu nimel ÜRO Euroopa Majanduskomisjoni rahvusvahelisel autoveol töötava sõiduki meeskonna töö alase Euroopa kokkuleppe eksperdirühmas

Eespool nimetatud nõukogu otsuse lisa.

LISA

AETRi uus liide

4. liide

Sõnumiedastussüsteemi TACHOnet kirjeldus

1. Reguleerimisala ja eesmärk

1.1. Käesolevas liites määratakse kindlaks tingimused AETRi osaliste ühendamiseks sõnumiedastussüsteemiga TACHOnet platvormi eDelivery kaudu.

1.2. Platvormi eDelivery kaudu sõnumiedastussüsteemiga TACHOnet ühenduvad kokkuleppeosalised täidavad käesolevas liites kehtestatud sätteid.

2. Mõisted

a) „kokkuleppeosaline“ või „osaline“ – AETRi osaline;

b) „eDelivery“ – Euroopa Komisjoni väljatöötatud teenus, mis võimaldab edastada kolmandate isikute vahel andmeid elektrooniliselt, tõendab edastatud andmete käitlemist, sealhulgas andmete saatmist ja kättesaamist, ning kaitseb edastatud andmeid lubamatu muutmise eest;

c) „TACHOnet“ – määruse (EL) nr 165/2014 artikli 31 lõikes 2 osutatud süsteem juhikaarte käsitleva teabe elektrooniliseks vahetamiseks kokkuleppeosaliste vahel;

d) „kesksüsteem“ – teabesüsteem, mis võimaldab edastada sõnumiedastussüsteemi TACHOnet teateid päringud esitanud ja päringutele vastavate osaliste vahel;

e) „päringu esitanud osaline“ – kokkuleppeosaline, kes esitab sõnumiedastussüsteemi TACHOnet kaudu päringu või teate, mille kesksüsteem seejärel edastab sobivale, päringule vastavale osalisele;

f) „päringule vastav osaline“ – osaline, kellele sõnumiedastussüsteemi TACHOnet päring või teade on adresseeritud;

g) „kaarte väljaandev asutus“ – kokkuleppeosalise volitatud asutus, kes annab välja ja haldab sõidumeerikukaarte.

3. Üldised kohustused

3.1. Ükski kokkuleppeosaline ei või käesolevale liitele tuginedes sõlmida teise osalise nimel kokkuleppeid juurdepääsuks sõnumiedastussüsteemile TACHOnet ega esindada teist kokkuleppeosalist ühelgi teisel viisil. Ükski kokkuleppeosaline ei tegutse käesolevas liites osutatud toimingutes teise kokkuleppeosalise alltöövõtjana.

3.2. Kokkuleppeosalised tagavad sõnumiedastussüsteemi TACHOnet kaudu juurdepääsu oma riiklikele juhikaartide registritele alaliites 4.6 sätestatud viisil ja teenusetasemega.

3.3. Kokkuleppeosalised teatavad üksteisele viivitamatult, kui nad märkavad oma vastutusvaldkonnas häireid või vigu, mis võivad ohustada sõnumiedastussüsteemi TACHOnet normaalse toimimise tagamist.

3.4. Iga osaline teatab AETRi sekretariaadile sõnumiedastussüsteemi TACHOnet kontaktisikud. Kontaktisikute võimalikust muutmisest tuleb AETRi sekretariaati kirjalikult teavitada.

4. Sõnumiedastussüsteemiga TACHOnet ühendatuse katsetamine

4.1. Kokkuleppeosalise ühendus sõnumiedastussüsteemiga TACHOnet on loodud siis, kui ühendamise, integreerimise ja toimivuse katsed on juhiste järgi ja Euroopa Komisjoni järelevalve all edukalt lõpule viidud.

4.2. Kui eelkatsed ebaõnnestuvad, võib Euroopa Komisjon katseetapi ajutiselt peatada. Katsed jätkuvad siis, kui kokkuleppeosaline on teatanud Euroopa Komisjonile, et riiklikul tasandil on vastu võetud vajalikud tehnilised parandused, mis võimaldavad eelkatsed edukalt läbi viia.

4.3. Eelkatsete maksimaalne kestus on kuus kuud.

5. Usalduse arhitektuur

5.1. Sõnumiedastussüsteemi TACHOnet teadete konfidentsiaalsus, terviklus ja salgamise vääramine tagatakse selle usalduse arhitektuuriga.

5.2. Sõnumiedastussüsteemi TACHOnet usalduse arhitektuur põhineb Euroopa Komisjoni juurutatud avaliku võtme taristul (PKI), millele esitatavad nõuded on kehtestatud alaliidetes 4.8 ja 4.9.

5.3. Sõnumiedastussüsteemi TACHOnet usalduse arhitektuuris osalevad järgmised üksused:

a) sertifitseerimisasutus, kelle vastutusalas on registripidaja poolt kokkuleppeosaliste riikide ametiasutustele (nende poolt nimetatud volitatud kullerite kaudu) edastatavate digisertifikaatide genereerimine ning digisertifikaatide väljaandmise, tühistamise ja uuendamise tehnilise taristu loomine;

b) domeeni omanik, kelle vastutusalas on alaliites 4.1 osutatud kesksüsteemi käitamine ning sõnumiedastussüsteemi TACHOnet usalduse arhitektuuri kinnitamine ja kooskõlastamine;

c) registripidaja, kelle vastutusalas on digisertifikaatide väljaandmise, tühistamise ja uuendamise taotluste registreerimine ja heakskiitmine ning volitatud kullerite isikusamasuse kontrollimine;

d) volitatud kuller on riigi ametiasutuse poolt määratud isik, kelle vastutusalas on avaliku võtme edastamine registripidajale ning sertifitseerimisasutuse genereeritava vastava sertifikaadi kättesaamine;

e) kokkuleppeosalise riigi ametiasutus, kes:

i) genereerib sertifitseerimisasutuse poolt genereeritavatesse sertifikaatidesse lisatavad privaatvõtmed ja neile vastavad avalikud võtmed;

ii) taotleb sertifitseerimisasutuselt digisertifikaate;

iii) nimetab volitatud kulleri.

5.4. Sertifitseerimisasutuse ja registripidaja nimetab Euroopa Komisjon.

5.5. Iga sõnumiedastussüsteemiga TACHOnet ühenduv kokkuleppeosaline peab alaliite 4.9 kohaselt taotlema digisertifikaadi väljaandmist, et sõnumiedastussüsteemi TACHOnet teade allkirjastada ja krüpteerida.

5.6. Sertifikaadi võib tühistada alaliite 4.9 kohaselt.

6. Andmekaitse ja konfidentsiaalsus

6.1. Osalised, täites rahvusvahelisi ja riiklikke andmekaitsealaseid õigusakte, eelkõige isikuandmete automatiseeritud töötlemisel isiku kaitse konventsiooni, võtavad kõik vajalikud tehnilised ja korralduslikud meetmed, et tagada sõnumiedastussüsteemi TACHOnet andmete turvalisus ning vältida selliste andmete muutmist, kadumist, volitamata töötlemist või nendele juurdepääsu (eelkõige autentsus, andmete konfidentsiaalsus, jälgitavus, terviklus, kättesaadavus ning teadete salgamise vääramine ja turvalisus).

6.2. Iga osaline kaitseb enda riiklikke süsteeme ebaseadusliku kasutamise, ründekoodide, viiruste, arvutitesse sissetungimise, andmete rikkumise ja ebaseadusliku manipuleerimise ning muu kolmandate isikute samaväärse tegevuse eest. Osalised lepivad kokku, et teevad majanduslikult mõistlikke jõupingutusi, et vältida viiruste, viitpommide, ussviiruste või sarnaste elementide edastamist ning programmeerimistavasid, mis võivad kahjustada teise osalise arvutisüsteeme.

7. Kulud

7.1. Kokkuleppeosalised kannavad ise arendus- ja käitamiskulud, mis seonduvad nende andmesüsteemide ja menetlustega, mis on vajalikud käesolevast liitest tulenevate kohustuste täitmiseks.

7.2. Kesksüsteemi osutatavad teenused, mida käsitletakse liites 4.1, on tasuta.

8. Alltöövõtt

8.1. Kokkuleppeosalised võivad kasutada alltöövõttu kõigi teenuste puhul, mille eest nad käesoleva liite alusel vastutavad.

8.2. Selline alltöövõtt ei vabasta osalist käesoleva liite kohasest vastutusest, sh vastutusest liitele 4.6 vastava nõutava teenusetaseme eest.

Alaliide 4.1

Sõnumiedastussüsteemi TACHOnet üldkirjeldus

1. Üldkirjeldus

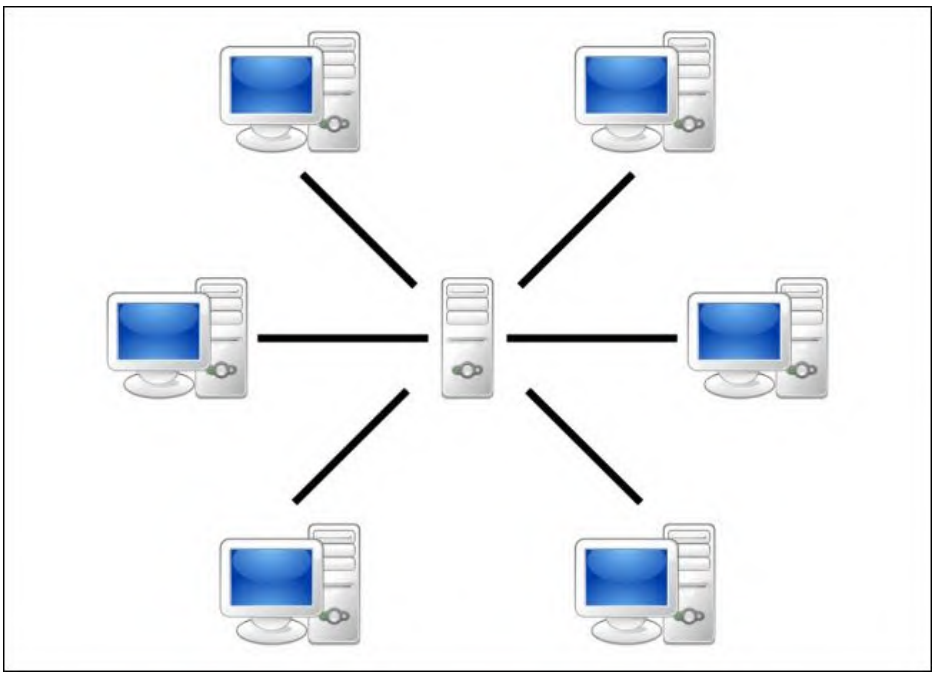
TACHOnet on elektrooniline süsteem juhikaarte käsitleva teabe vahetamiseks AETRi osaliste vahel. TACHOnet suunab päringu esitanud osaliste teabenõuded päringutele vastavatele osalistele ning viimati nimetatute vastused esimestena nimetatutele. Sõnumiedastussüsteemiga TACHOnet liitunud kokkuleppeosalised peavad süsteemiga ühendama oma riiklikud juhikaartide registrid.

2. Arhitektuur

Sõnumiedastussüsteem TACHOnet koosneb järgmistest osadest.

2.1. Kesksüsteem, mis suudab päringu selle esitanud osaliselt vastu võtta, heaks kiita ja seda töödelda, edastades selle päringule vastavale osalisele. Kesksüsteem peab ootama, kuni saab vastuse igalt päringule vastavalt osaliselt, koguma vastused ja saatma koondvastuse päringu esitanud osalisele.

2.2. Osaliste riiklikud süsteemid, millel peavad olema liidesed, mis suudavad päringuid saata kesksüsteemile ja võtta vastu saabunud vastuseid. Riiklikud süsteemid võivad kesksüsteemile teadete saatmiseks ja nende vastuvõtmiseks kasutada omand- või kommertstarkvara.



3. Haldamine

3.1. Kesksüsteemi haldab Euroopa Komisjon, kes vastutab selle tehnilise käitamise ja hooldamise eest.

3.2. Kesksüsteem ei säilita andmeid kauem kui kuus kuud, välja arvatud alaliites 4.7 sätestatud logi- ja statistikaandmed.

3.3. Kesksüsteem ei tohi anda juurdepääsu isikuandmetele, välja arvatud selleks volitatud Euroopa Komisjoni töötajatele, kui see on vajalik järelevalve ja hoolduse tegemiseks ning rikete kõrvaldamiseks.

3.4. Kõik kokkuleppeosalised vastutavad järgmise eest:

3.4.1. riiklike süsteemide, sealhulgas kesksüsteemiga suhtlevate liideste loomine ja haldamine;

3.4.2. riiklike süsteemide, sealhulgas nii omand- kui ka kommertsriist- ja tarkvara installeerimine ja hooldamine;

3.4.3. riikliku süsteemi ja kesksüsteemi nõuetekohase koostalitluse tagamine, sealhulgas kesksüsteemist tulnud veateadete haldamine;

3.4.4. teabe konfidentsiaalsuse, tervikluse ja kättesaadavuse tagamine kõikide vajalike meetmete abil;

3.4.5. riiklike süsteemide käitamine vastavalt alaliites 4.6 sätestatud teenusetasemetele.

Alaliide 4.2

Sõnumiedastussüsteemi TACHOnet funktsioonid

1. Sõnumiedastussüsteemil TACHOnet on järgmised funktsioonid.

1.1. võimaldab päringu esitanud osalisel saata kaartide kontrollimise taotluse ühele või mitmele, päringule vastavale osalisele, et teha kindlaks, kas kaardi taotlejal on juba mõne teise päringule vastava osalise kaarti. Päringule vastavad osalised vastavad päringule CIC-tüüpi vastuse saatmisega.

1.2. võimaldab päringu esitanud osalisel CCS-tüüpi päringu saatmisega küsida päringule vastavalt osaliselt viimati nimetatu poolt väljaantud kaardi andmeid. Päringule vastav osaline vastab päringule CCS-tüüpi vastuse saatmisega.

1.3. võimaldab päringu esitanud osalisel teatada päringule vastavale osalisele MCS-tüüpi teate saatmisega, et päringule vastava osalise väljaantud kaardi staatus on muutunud. Päringule vastav osaline vastab päringule MCS-tüüpi kinnituse saatmisega.

1.4. võimaldab päringu esitanud osalisel teatada päringule vastavale osalisele ICDL-tüüpi teate saatmisega, et päringu esitanud osaline on päringule vastava osalise juhiloa alusel välja andnud juhikaardi. Päringule vastav osaline vastab päringule ICDL-tüüpi vastuse saatmisega.

2. Edaspidi lisatakse sõnumiedastussüsteemi TACHOnet muid tõhusaks toimimiseks sobivaks peetavaid teatetüüpe, näiteks veateated.

3. Riiklikud süsteemid peavad suutma välja selgitada tabelis 1 loetletud kaardistaatusi, et kasutada punktis 1 kirjeldatud funktsioone. Osalised ei ole kohustatud rakendama haldusmenetlust, mis kasutab kõiki loetletud staatusi.

4. Kui osaline saab vastuse või teate, millega antakse staatus, mida ei kasutata liikmesriigi haldusmenetlustes, peab riiklik süsteem teisendama teates nimetatud staatuse kõnealuse menetlusega sobivaks. Päringule vastav osaline ei tohi teadet tagasi lükata, kui selle staatus on loetletud tabelis 1.

5. Tabelis 1 loetletud kaardistaatust ei tohi kasutada selleks, et teha kindlaks, kas juhikaart on juhtimiseks kehtiv. Kui osaline teeb kaardi väljaandnud riigi ametiasutuse registrilt CCS-tüüpi funktsiooni kaudu päringu, peab vastus sisaldama asjakohast välja „kehtiv juhtimiseks“. Riigi haldusmenetlused peavad olema sellised, et CCS-tüüpi vastus sisaldaks alati teadet „kehtiv juhtimiseks“.

Tabel 1

Kaardi staatused

Kaardi staatus	**Määratlus**
Taotlus	Kaarte väljaandev asutus on saanud taotluse anda välja juhikaart. See teave on registreeritud ja salvestatud andmebaasi koos genereeritud otsingutunnustega.
Heakskiidetud	Kaarte väljaandev asutus on kiitnud heaks sõidumeerikukaardi taotluse.
Tagasilükatud	Kaarte väljaandev asutus ei kiitnud taotlust heaks.
Individualiseeritud	Sõidumeerikukaart on individualiseeritud.
Saadetud	Liikmesriigi asutus on saatnud juhikaardi asjaomasele juhile või vahendusasutusele.
Kätteantud	Liikmesriigi asutus on juhikaardi asjaomasele juhile kätte andnud.
Konfiskeeritud	Pädev asutus on juhikaardi juhilt ära võtnud.
Peatatud kehtivusega	Juhikaart on juhilt ajutiselt ära võetud.
Tagasivõetud	Kaarte väljaandev asutus on otsustanud juhikaardi tagasi võtta. Kaart on lõplikult kehtetuks tunnistatud.
Loovutatud	Sõidumeerikukaart on kaarte väljaandvale asutusele tagastatud ega ole enam vajalik.
Kadunud	Kaarte väljaandvale asutusele on teatatud, et sõidumeerikukaart on kadunud.
Varastatud	Kaarte väljaandvale asutusele on teatatud, et sõidumeerikukaart on varastatud. Varastatud kaart loetakse kadunud kaardiks.
Mittetoimiv	Kaarte väljaandvale asutusele on teatatud, et sõidumeerikukaart ei toimi korralikult.
Aegunud	Sõidumeerikukaardi kehtivusaeg on lõppenud.
Asendatud	Sõidumeerikukaart, mille kohta on teatatud, et see on kadunud, varastatud või ei toimi korralikult, on asendatud uue kaardiga. Uuel kaardil on samad andmed, välja arvatud kaardi numbri asendusindeks, mida on suurendatud ühe võrra.

Uuendatud	Sõidumeerikukaart on kas uuendatud haldusandmete muutumise tõttu või seda on pikendatud kehtivusaja lõppemise tõttu. Uuel kaardil on number sama, välja arvatud kaardi numbri uuendusindeks, mida on suurendatud ühe võrra.
Vahetamisel	Juhikaardi väljaandnud asutus on saanud teate, et teise osalise kaarte väljaandev asutus on alustanud nimetatud kaardi asendamist juhikaardiga.
Vahetatud	Kaarte väljaandev asutus on saanud teate, et teise osalise kaarte väljaandev asutus on lõpule viinud nimetatud kaardi kokkuleppeosalise juhikaardiga asendamise.

Alaliide 4.3

Sõnumiedastussüsteemi TACHOnet teadete seaded

1. Üldised tehnilised nõuded

1.1. Kesksüsteemil peavad olema teadetevahetuseks nii sünkroonsed kui ka asünkroonsed liidesed. Osalised võivad valida oma rakendustes liidese jaoks kõige sobivama tehnilise lahenduse.

1.2. Kõik kesksüsteemi ja kokkuleppeosaliste süsteemide vahel edastatavad teated peavad olema kodeeritud teisendusvorminguga UTF-8.

1.3. Kokkuleppeosaliste süsteemid peavad olema võimelised vastu võtma ja töötlema kreeka või kirillitsa tähemärke sisaldavaid teateid.

2. Märgistuskeeles XML koostatud teadete ülesehitus ja andmetüübi määratlus (XSD)

2.1. XML-tüüpi teadete struktuur järgib XSD-andmetüüpe, mis on installeeritud kesksüsteemi.

2.2. Kesksüsteem ja riiklikud süsteemid peavad suutma edastada ja vastu võtta teateid, mis ühilduvad XSD-andmetüüpidega.

2.3. Riiklikud süsteemid peavad võimaldama saata, vastu võtta ja töödelda kõiki alaliites 4.2 sätestatud funktsioonidele vastavaid teateid.

2.4. XML-tüüpi teated peavad vastama vähemalt tabelis 2 sätestatud miinimumnõuetele.

Tabel 2

XML-tüüpi teadete miinimumnõuded

Ühine päis		**Kohustuslik**
Versioon	Märgistuskeele XML ametlik versioon on määratud kindlaks teate XSDs määratletud nimeruumiga ning iga XML-tüüpi teate päise elemendi versiooni atribuudiga. Versiooni number („n.m“) määratakse kindlaks fikseeritud väärtusega iga XML-i andmetüübi määratlusfaili (XSD) väljastamisel.	Jah
Katse tunnuskood	Valikuline tunnuskood katsetamiseks. Katse korraldaja sisestab tunnuskoodi ja kõik töövoos osalejad edastavad ja tagastavad sama tunnuskoodi.	Ei
Tehniline tunnus	UUID – ainulaadne tunnus, millega on iga teade kordumatult määratletud. Saatja tekitab tunnuse UUID ja sisestab selle tunnuse. Neid andmeid ei kasutata äriotstarbel.	Jah
Töövoo tunnus	Töövoo tunnus on UUID ja selle peab moodustama päringu esitanud osaline. Seejärel kasutatakse seda tunnust kõikides teadetes töövoo vastavuse näitamiseks.	Jah
Millal saadetud	Teate saatmise kuupäev ja kellaaeg (UTC).	Jah
Aegumisaeg	See atribuut on valikuline kuupäeva ja kellaaja (UTC vormingus) atribuut. Selle väärtuse annab kesksüsteem edastatud päringutele. See annab päringule vastavale osalisele teada, millal päring aegub. Seda väärtust ei nõua MS2TCN_<x>_Req ega ükski vastusteade. Selle kasutamine on vabatahtlik, seega saab sama päise määratlust kasutada kõikide teatetüüpide puhul, sõltumata sellest, kas aegumisaja väärtuse atribuuti nõutakse või mitte.	Ei
Kellelt	Teate saatnud kokkuleppeosalise ISO 3166-1 Alpha 2 kood või „EL“.	Jah
Kellele	Teate saanud kokkuleppeosalise ISO 3166-1 Alpha 2 kood või „EL“.	Jah

Alaliide 4.4

Translitereerimine ja NYSIIS (New York State Identification and Intelligence System – New Yorgi osariigi identifitseerimis- ja jälitussüsteem)

1. Kesksüsteem kasutab NYSIISi algoritmi kõikide riiklikus registris leiduvate juhtide nimede kodeerimiseks.

2. Otsides CIC-funktsiooni abil kaarti, tuleb esimese otsingumehhanismina kasutada NYSIISi võtmeid.

3. Lisaks sellele võivad osalised täiendavate tulemuste saamiseks kasutada oma algoritmi.

4. Otsingutulemustes tuleb näidata, millise algoritmiga tulemus leiti – kas kasutati NYSIISi või oma algoritmi.

5. Kui osaline otsustab registreerida ICDLi teateid, tuleb ICDLi andmete juurde salvestada NYSIISi võtmed, mis on teates. ICDLi andmete otsingul peab osaline kasutama taotleja nime jaoks NYSIISi võtmeid.

Alaliide 4.5

Turvanõuded

1. Teadete vahetamiseks riiklike süsteemide ja kesksüsteemi vahel kasutatakse edastusprotokolli HTTPS.

2. Turvalisuse tagamiseks teadete edastamisel riiklike süsteemide ja kesksüsteemi vahel peavad riiklikud süsteemid kasutama alaliidetes 4.8 ja 4.9 osutatud digisertifikaate.

3. Riiklikud süsteemid peavad rakendama sertifikaate, milles kasutatakse vähemalt räsialgoritmi SHA-2 (SHA-256) ja 2048-bitist avalikku võtit.

Alaliide 4.6

Teenusetasemed

1. Riiklikud süsteemid peavad vastama vähemalt järgmisele teenusetasemele.

1.1. Nad peavad olema kättesaadavad 24 tundi ööpäevas ja seitse päeva nädalas.

1.2. Nende kättesaadavust jälgitakse tukseteadetega, mida saadab kesksüsteem.

1.3. Nende kättesaadavusmäär peab olema 98 % vastavalt järgmisele tabelile (arvud on ümardatud sobiva ühikuni):

Kättesaadavusele	vastab mittekättesaadavus järgmise aja vältel		
	Iga päev	Iga kuu	Iga aasta
98%	0.5 hours	15 tundi	7.5 days

Osalisi kutsutakse üles täitma igapäevase kättesaadavuse nõuet, kuid on selge, et teatavad vajalikud toimingud, nagu süsteemi hooldus, nõuavad rohkem aega kui 30 minutit. Igakuise ja -aastase kättesaadavuse nõue on kohustuslik.

1.4. Nad peavad igas kalendrikuus vastama vähemalt 98 % neile edastatud päringutele.

1.5. Nad peavad vastama päringule 10 sekundi jooksul.

1.6. Üldine päringuviivitus (aeg, mille jooksul taotleja võib oodata vastust) ei tohi ületada 20 sekundit.

1.7. Nad peavad suutma teenindada kuus teadet sekundis.

1.8. Riiklikud süsteemid ei tohi saata sõnumiedastussüsteemi TACHOnet kesksüsteemi üle kahe päringu sekundis.

1.9. Iga riiklik süsteem peab suutma toime tulla kesksüsteemi või teiste kokkuleppeosaliste riiklike süsteemide tehniliste probleemidega. Sellised probleemid hõlmavad muu hulgas järgmist:

a) kaob ühendus kesksüsteemiga;

b) päringule ei tule vastust;

c) vastused päringule saabuvad pärast päringuviivituse möödumist;

d) soovimatute teadete vastuvõtmine;

e) kehtetute teadete vastuvõtmine.

2. Kesksüsteem peab:

2.1. tagama 98 % kättesaadavuse;

2.2. teatama riiklikele süsteemidele vigade ilmnemisest kas vastusteatega või selleks otstarbeks loodud veateatega. Riiklikud süsteemid peavad veateated vastu võtma ja käivitama töövoo, mis suudaks võtta vajalikke meetmeid teatatud vea parandamiseks.

3. Hooldus

Osalised teavitavad veebirakenduse kaudu korrapäraselt teisi osalisi ja Euroopa Komisjoni igast hooldusest vähemalt üks nädal enne hooldust, kui see on tehniliselt võimalik.

Alaliide 4.7

Kesksüsteemi kogutud andmete logi ja statistika

1. Eraelu puutumatuse kaitse tagamiseks on statistilised andmed anonüümsed. Kaardi, juhi ja juhiloa tuvastamise andmed peavad olema kättesaadavad statistika tegemiseks.

2. Logiandmete abil peab saama jälgida kõiki kontrollimis- ja korrigeerimistoiminguid ning koostada statistikat kõnealuste toimingute kohta.

3. Isikuandmeid ei tohi logides säilitada kauem kui kuus kuud. Statistilist teavet tuleb säilitada tähtajatult.

4. Aruandluse jaoks kasutatavad statistilised andmed hõlmavad järgmist:

   a) päringu esitanud osaline;

   b) päringule vastav osaline;

   c) teate tüüp;

   d) vastuse staatuse kood;

   e) teate kuupäev ja kellaaeg;

   f) vastuse aeg.

Alaliide 4.8

Sõnumiedastussüsteemi TACHOnet digivõtmeid ja -sertifikaate käsitlevad üldsätted

1. Euroopa Komisjoni informaatika peadirektoraat (DIGIT) teeb platvormi eDelivery kaudu sõnumiedastussüsteemiga TACHOnet ühenduvatele AETRi osalistele (edaspidi „riigi ametiasutused“) kättesaadavaks Euroopa ühendamise rahastu avaliku võtme taristu (PKI) teenuse[1].

2. Digisertifikaatide taotlemise ja tühistamise menetlus ning nende kasutamise üksikasjalikud tingimused on kindlaks määratud liites.

3. Sertifikaatide kasutamine

3.1. Riigi ametiasutus[2] kasutab väljaantud sertifikaati üksnes sõnumiedastussüsteemi TACHOnet raames. Sertifikaati võib kasutada järgmistel eesmärkidel:

a) andmete päritolu autentimine;

b) andmete krüpteerimine;

c) andmete tervikluse rikkumiste avastamise tagamine.

3.2. Kõik kasutusviisid, mis ei ole lubatud kasutusviisidena sõnaselgelt lubatud, on keelatud.

4. Kokkuleppeosalised:

a) kaitsevad oma privaatvõtmeid loata kasutamise eest;

b) hoiduvad privaatvõtmete kolmandatele isikutele edastamisest või avaldamisest, ka esindajatena;

---

[1] PKI on kogum rolle, poliitikaid, menetlusi ja süsteeme, mis on vajalikud digisertifikaatide loomiseks, haldamiseks, levitamiseks ja tühistamiseks.

[2] Identifitseeritakse atribuudi väärtusega „O=“ väljaantud sertifikaadi teema eraldusnimes.

c) tagavad sõnumiedastussüsteemis TACHOnet genereeritud, salvestatud ja seal kasutatavate privaatvõtmete konfidentsiaalsuse, tervikluse ja kättesaadavuse;

d) hoiduvad pärast sertifikaadi kehtivuse lõppu või selle tühistamist privaatvõtme kasutamise jätkamisest, v.a krüpteeritud andmete vaatamiseks (nt e-kirjade dekrüpteerimiseks). Aegunud võtmed kas hävitatakse või neid hoitakse viisil, millega välditakse nende kasutamist;

e) annavad registripidajale nende volitatud esindajate nimed, kes on volitatud taotlema organisatsioonile väljastatud sertifikaatide tühistamist (tühistamistaotlusele lisatakse tühistamissalasõna ja üksikasjad sündmuste kohta, mille tõttu tühistamine on vajalik);

f) väldivad privaatvõtme kuritarvitamist, taotledes privaatvõtme salajasuse kahjustumisel sellega seotud avaliku võtme sertifikaadi tühistamist või privaatvõtme aktiveerimisandmete kustutamist;

g) on vastutustundlikud ja täidavad kohustust taotleda sertifikaadi tühistamist tingimustel, mis on kindlaks määratud sertifitseerimisasutuse sertifitseerimispoliitikas ja -tavades;

h) teatavad registripidajale viivitamata kõigi sõnumiedastussüsteemi TACHOnet raames kasutatavate AETRi võtmete kaotamisest, vargusest või võimalikust salajasuse kahjustamisest.

5. Kohustused

Ilma et see piiraks Euroopa Komisjoni vastutust viisil, mis on vastuolus kohaldatavas siseriiklikus õiguses sätestatud mis tahes nõuetega, või nendel juhtudel, kui asjaomase õiguse alusel vastutust välistada ei saa, ei vastuta Euroopa Komisjon järgmise eest:

a) sertifikaadi sisu, mille eest vastutab ainult sertifikaadi omanik. Sertifikaadi sisu õigsuse kontrollimise eest vastutab sertifikaadi omanik;

b) sertifikaadi kasutamine selle omaniku poolt.

Alaliide 4.9

Sõnumiedastussüsteemi TACHOnet PKI teenuse kirjeldus

1. Sissejuhatus

PKI on kogum rolle, poliitikaid, menetlusi ja süsteeme, mis on vajalikud digisertifikaatide loomiseks, haldamiseks, levitamiseks ja tühistamiseks[3]. Euroopa ühendamise rahastu PKI teenus eDelivery võimaldab välja anda ja hallata digisertifikaate, mida kasutatakse juurdepääsupunktide vahel vahetatava teabe konfidentsiaalsuse, tervikluse ja salgamise vääramise tagamiseks.

PKI teenus eDelivery põhineb lahenduse TeleSec Shared Business CA usalduskeskuse teenustel, mille suhtes kohaldatakse ettevõtja T-Systems International GmbH lahenduse TeleSec-Shared-Business-CA sertifitseerimispoliitikat ja -tavasid[4].

PKI teenuse raames antakse välja sertifikaate, mis sobivad erinevate äriprotsesside turvamiseks äriühingutes, organisatsioonides, riigi ametiasutustes ja institutsioonides ning mille puhul on lõppkasutaja autentsuse, tervikluse ja usaldusväärsuse tõendamiseks nõutav keskmine turvatase.

2. Sertifikaadi taotlemise protsess

2.1. Rollid ja kohustused

2.1.1. Sertifikaati taotlev „organisatsioon“ või „riigi ametiasutus“

2.1.1.1. Riigi ametiasutus taotleb sertifikaate seoses sõnumiedastussüsteemi TACHOnet projektiga.

2.1.1.2 Riigi ametiasutus teeb järgmist:

a) taotleb Euroopa ühendamise rahastu PKI teenuse sertifikaate;

[3] https://en.wikipedia.org/wiki/Public_key_infrastructure

[4] Sertifitseerimispoliitika ja -tavade ajakohaseim versioon on kättesaadav aadressil https://www.telesec.de/en/sbca-en/support/download-area/

b) genereerib sertifitseerimisasutuse poolt väljaantud sertifikaatidesse lisatavad privaatvõtmed ja neile vastavad avalikud võtmed;

c) sertifikaadi heakskiitmisel laadib selle alla;

d) allkirjastab ja saadab registripidajale:

i) kontaktisikuid ja volitatud kullereid käsitleva teabevormi,

ii) allkirjastatud ühekordse volikirja[5].

2.1.2. Volitatud kuller

2.1.2.1. Volitatud kulleri nimetab riigi ametiasutus.

2.1.2.2. Volitatud kuller:

a) annab avaliku võtme registripidajale üle näost näkku toimuval tuvastamis- ja registreerimisprotsessil;

b) võtab registripidajalt vastu vastava sertifikaadi.

2.1.3. Domeeni omanik

2.1.3.1. Domeeni omanik on liikuvuse ja transpordi peadirektoraat.

2.1.3.2. Domeeni omanik:

a) kinnitab ja kooskõlastab sõnumiedastussüsteemi TACHOnet võrgustiku ja usalduse arhitektuuri, sh sertifikaatide väljaandmise menetlused;

b) käitab sõnumiedastussüsteemi TACHOnet kesksüsteemi ja kooskõlastab osaliste tegevust sõnumiedastussüsteemi TACHOnet toimimise vallas;

c) katsetab koos riikide ametiasutustega ühendust sõnumiedastussüsteemiga TACHOnet.

---

[5] Volikiri on juriidiline dokument, millega organisatsioon volitab Euroopa Komisjoni (keda esindab kindlaksmääratud ametnik, kes vastutab Euroopa ühendamise rahastu PKI teenuse eest) tema nimel taotlema sertifikaadi genereerimist ettevõtja T-Systems International GmbH lahenduses TeleSec Shared Business CA. Vt ka punkt 6.

2.1.4. Registripidaja

2.1.4.1. Registripidaja on Teadusuuringute Ühiskeskus.

2.1.4.2. Registripidaja vastutusalas on volitatud kullerite isikusamasuse kontrollimine ning digisertifikaatide väljaandmise, tühistamise ja uuendamise taotluste registreerimine ja heakskiitmine.

2.1.4.3. Registripidaja:

a) määrab riigi ametiasutusele kordumatu tunnuse;

b) kontrollib riigi ametiasutuse, selle kontaktpunktide ja volitatud kullerite isikusamasust;

c) suhtleb Euroopa ühendamise rahastu tugimeeskonnaga riigi ametiasutuse, selle kontaktpunktide ja volitatud kullerite isikusamasuse teemal;

d) teatab riigi ametiasutusele sertifikaadi heakskiitmisest või tagasilükkamisest.

2.1.5. Sertifitseerimisasutus

2.1.5.1. Sertifitseerimisasutuse vastutusalasse kuulub digisertifikaatide taotlemise, väljastamise ja tühistamise tehnilise taristu pakkumine.

2.1.5.2. Sertifitseerimisasutus:

a) tagab riikide ametiasutuste sertifikaaditaotluste menetlemise tehnilise taristu;

b) kinnitab või lükkab sertifikaaditaotluse tagasi;

c) suhtleb vajaduse korral registripidajaga taotleva organisatsiooni identiteedi kontrollimiseks.

2.2. Sertifikaadi väljaandmine

2.2.1. Sertifikaadi väljaandmisel läbitakse joonisel 1 kujutatud üksteisele järgnevad etapid:

a) **1. etapp:** volitatud kulleri identifitseerimine;

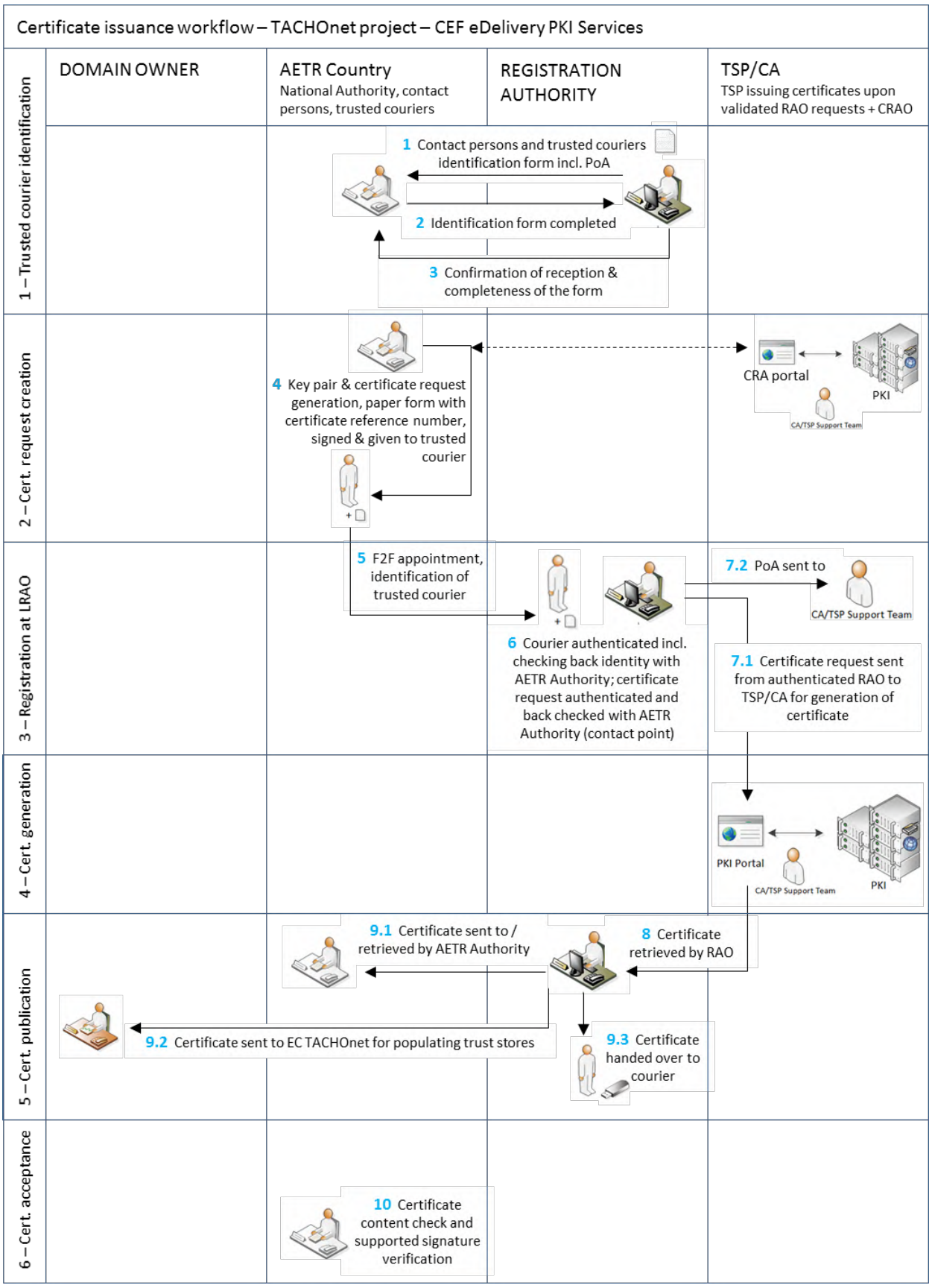
b) **2. etapp:** sertifikaaditaotluse loomine;

c) **3. etapp:** registreerimine registripidaja juures;

d) **4. etapp:** sertifikaadi genereerimine;

e) **5. etapp:** sertifikaadi avaldamine;

f) **6. etapp:** sertifikaadi heakskiitmine.



Joonis 1 – Sertifikaadi väljaandmise töövoog

2.2.2. 1. etapp: volitatud kulleri identifitseerimine

Volitatud kulleri identifitseerimiseks läbitakse järgmine protsess.

a) Registripidaja saadab riigi ametiasutusele kontaktisikuid ja volitatud kullereid käsitleva teabevormi[6]. Kõnealune vorm hõlmab ka organisatsiooni (AETRi sekretariaat) allkirjastatavat volikirja.

b) Riigi ametiasutus saadab täidetud teabevormi ja allkirjastatud volikirja registripidajale.

c) Registripidaja kinnitab teabevormi kättesaamist ja täielikkust.

d) Registripidaja edastab kontaktisikute ja volitatud kullerite ajakohastatud loetelu domeeni omanikule.

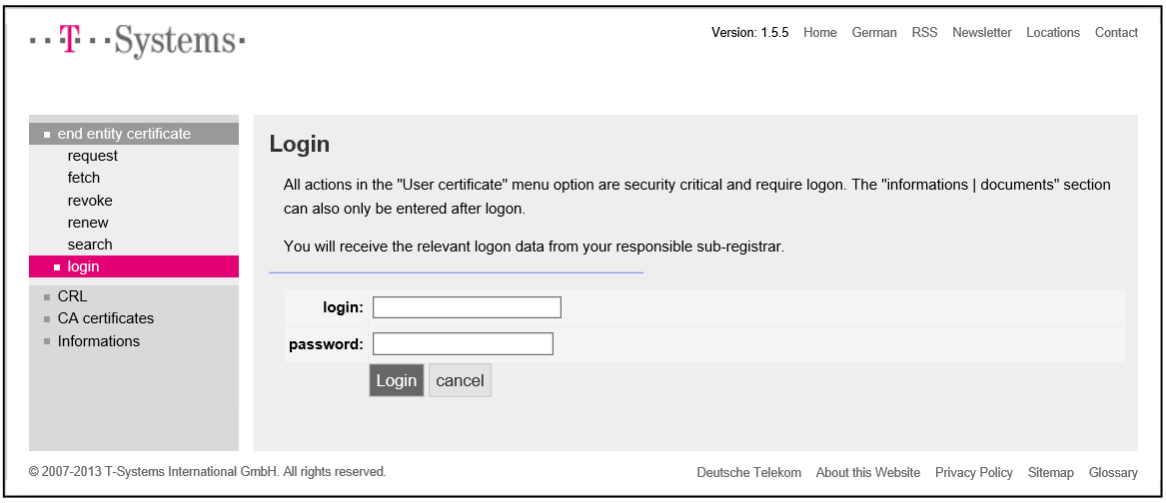
2.2.3. 2. etapp: sertifikaaditaotluse loomine

2.2.3.1. Sertifikaati taotletakse ja see saadakse kätte samast arvutist ja sama veebibrauseriga.

2.2.3.2. Sertifikaaditaotluse loomiseks läbitakse järgmine protsess.

a) Organisatsiooni esindaja avab sertifikaadi taotlemiseks kasutaja veebiliidese aadressil https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: , ja sisestab kasutajanime „**sbca/CEF_eDelivery.europa.eu**“ ja salasõna „**digit.333**“

6 Vt punkt 5.

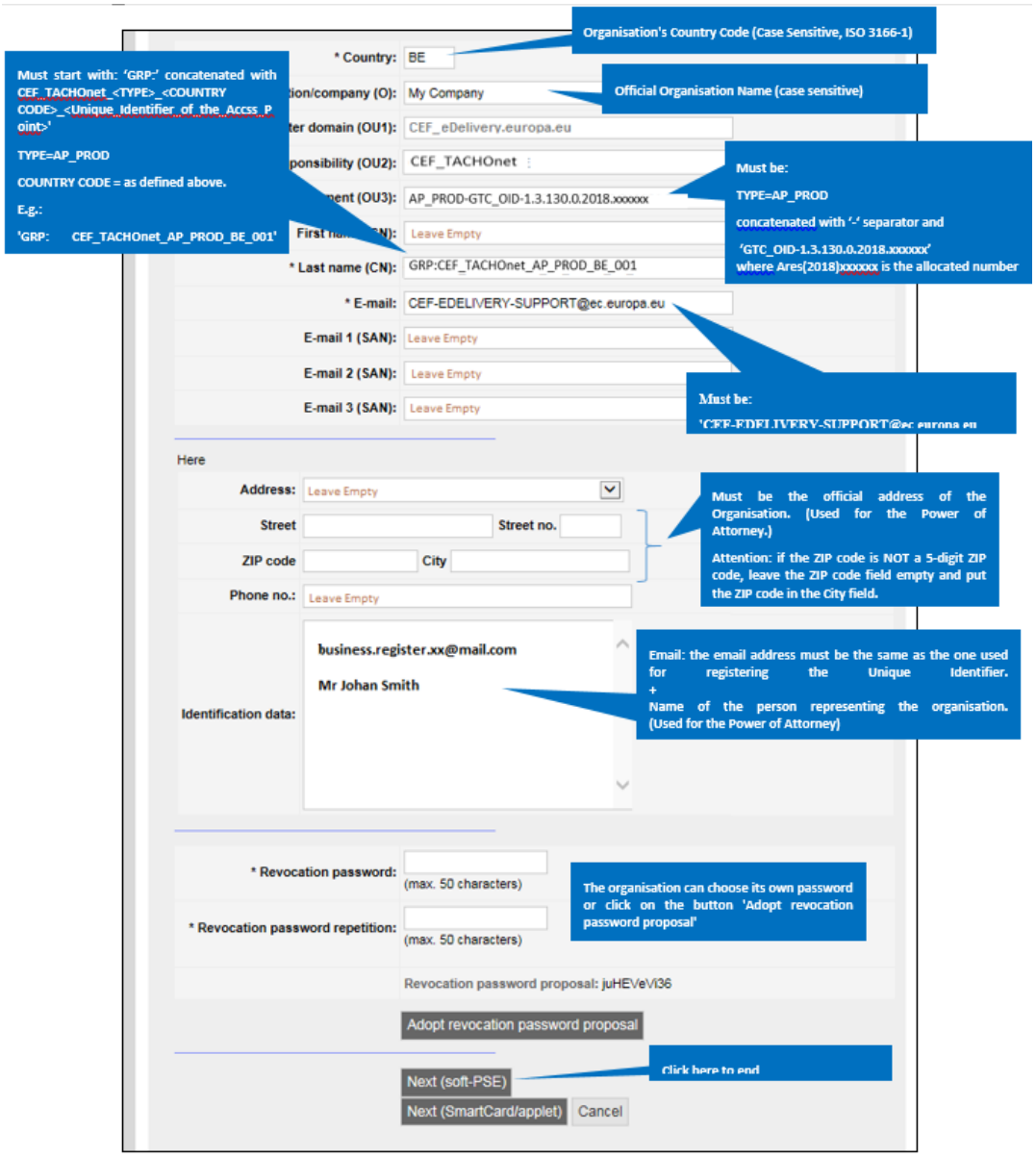


Joonis 2

b) Organisatsiooni esindaja klõpsab vasakpoolsel paneelil nupul „request“ (taotle) ja valib rippmenüüst „CEF_TACHOnet“.

Joonis 3

c) Organisatsiooni esindaja kannab tabelis 3 esitatud teabe joonisel 4 esitatud sertifikaadi taotlemise vormi, klõpsates protsessi lõpetamiseks nupul „Next (soft-PSE)“ (edasi).


Organisation's Country Code (Case Sensitive, ISO 3166-1)
Official Organisation Name (case sensitive)
Must start with: 'GRP:' concatenated with CEF_TACHOnet_<TYPE>_<COUNTRY CODE>_<Unique_Identifier_of_the_Accss_Point>'
TYPE=AP_PROD
COUNTRY CODE = as defined above.
E.g.:
'GRP: CEF_TACHOnet_AP_PROD_BE_001'
Must be:
TYPE=AP_PROD
concatenated with '-' separator and
'GTC_OID-1.3.130.0.2018.xxxxxx'
where Ares(2018)xxxxxx is the allocated number
Must be:
'CEF-EDELIVERY-SUPPORT@ec.europa.eu
Must be the official address of the Organisation. (Used for the Power of Attorney.)
Attention: if the ZIP code is NOT a 5-digit ZIP code, leave the ZIP code field empty and put the ZIP code in the City field.
Email: the email address must be the same as the one used for registering the Unique Identifier.
+
Name of the person representing the organisation. (Used for the Power of Attorney)
The organisation can choose its own password or click on the button 'Adopt revocation password proposal'
Click here to end
* Country: BE
My Company
CEF_eDelivery.europa.eu
CEF_TACHOnet
AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
Leave Empty
* Last name (CN): GRP:CEF_TACHOnet_AP_PROD_BE_001
* E-mail: CEF-EDELIVERY-SUPPORT@ec.europa.eu
E-mail 1 (SAN): Leave Empty
E-mail 2 (SAN): Leave Empty
E-mail 3 (SAN): Leave Empty
Here
Address: Leave Empty
Street
Street no.
ZIP code
City
Phone no.: Leave Empty
Identification data:
business.register.xx@mail.com
Mr Johan Smith
* Revocation password:
(max. 50 characters)
* Revocation password repetition:
(max. 50 characters)
Revocation password proposal: juHEVeVi36
Adopt revocation password proposal
Next (soft-PSE)
Next (SmartCard/applet)
Cancel

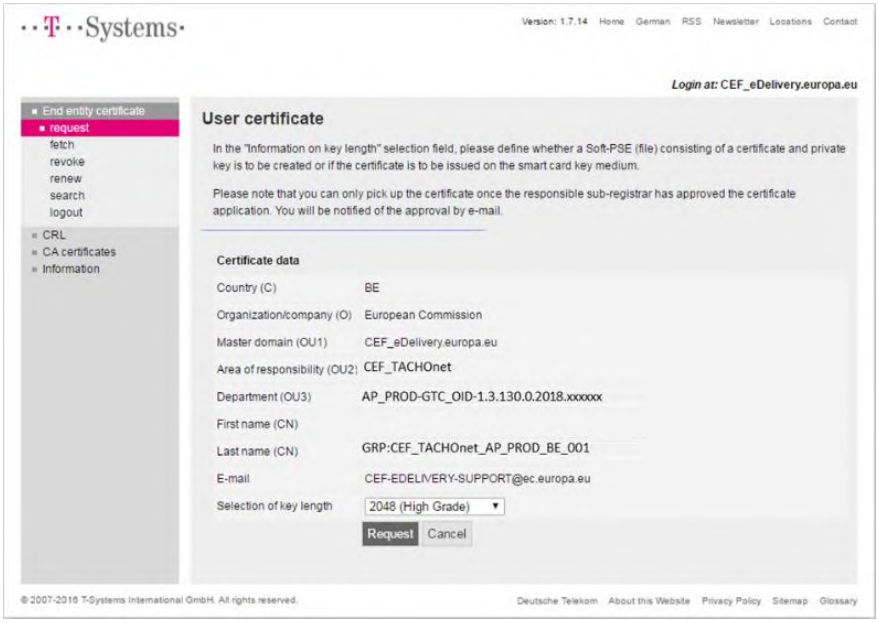
Joonis 4

Nõutud väljad	Kirjeldus
Country (Riik)	**C=riigi kood**, sertifikaadiomaniku asukoht, mida kontrollitakse avalikust kataloogist; Piirangud: 2 märki, vastavalt standardile ISO 3166-1, alpha-2, tõstutundlik; Näited: DE, BE, NL, Erijuhtumid: UK (Suurbritannia), EL (Kreeka)
Organisation/Company (O) (organisatsioon/äriühing)	**O=sertifikaadiomaniku organisatsiooni nimi**
Master domain (OU1) (põhivaldkond)	**OU=CEF_eDelivery.europa.eu**
Area of responsibility (OU2) (vastutusala)	**OU=CEF_TACHOnet**
Department (OU3) (osakond)	Välja „AREA OF RESPONSIBILITY“ kohustuslik väärtus Sertifikaadi taotlemisel peab sisu kontrollima ammendavast loetelust (valgest nimekirjast). Kui teave ei vasta loetelule, ei saa taotlust esitada. Vorming: **OU=<TYPE>-<GTC_NUMBER>** Milles „<TYPE>“ asendatakse järgmisega: AP_PROD: Access Point in Production environment (juurdepääsupunkt tootmiskeskkonnas). Ja milles <GTC_NUMBER> on **GTC_OID-1.3.130.0.2018.xxxxxx**, milles Ares(2018)xxxxxx on sõnumiedastussüsteemi TACHOnet projekti GTC number. Näiteks: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN) (eesnimi)	Peab olema täitmata
Last name (CN) (perekonnanimi)	Peab algama järgmisega: „GRP:“, millele järgneb tavanimetus. Vorming: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** Näiteks: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail (e-post)	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
E-mail 1 (SAN) (e-post 1)	Peab olema täitmata
E-mail 2 (SAN) (e-post 2)	Peab olema täitmata
E-mail 3 (SAN) (e-post 3)	Peab olema täitmata

Address (aadress)	Peab olema täitmata
Street (tänav)	Peab olema sertifikaadiomaniku organisatsiooni ametlik aadress. (Kasutatakse volikirjas.)
Street no.	Peab olema sertifikaadiomaniku organisatsiooni ametlik aadress. (Kasutatakse volikirjas.)
Zip Code (sihtnumber)	Peab olema sertifikaadiomaniku organisatsiooni ametlik aadress. (Kasutatakse volikirjas.) **Tähelepanu**: kui sihtnumber EI OLE viiekohaline, jätke sihtnumbri väli tühjaks ja kirjutage sihtnumber väljale City (linn).
City (linn)	Peab olema sertifikaadiomaniku organisatsiooni ametlik aadress. (Kasutatakse volikirjas.) **Tähelepanu**: kui sihtnumber EI OLE viiekohaline, jätke sihtnumbri väli tühjaks ja kirjutage sihtnumber väljale City (linn).
Phone no (tel nr)	Peab olema täitmata
Identification data (identimisandmed)	E-posti aadress peab olema sama, mida kasutati kordumatu tunnuse registreerimisel. + Peab olema organisatsiooni esindava isiku nimi. (Kasutatakse volikirjas.) + **Äriregistri number** (kohustuslik vaid eraõiguslike organisatsioonide puhul) **Esitatud ... kohalikule kohtule** (vajalik vaid Saksamaa ja Austria eraõiguslike organisatsioonide puhul)
Revocation password (tühistamissalasõna)	Kohustuslik väli, sisu valib taotleja
Revocation password repetition (tühistamissalasõna kordus)	Kohustuslik väli, sisu valib taotleja, kordus

Tabel 3. Kõigi nõutud väljade täielik selgitus

d) Võtme pikkuseks (Selection of key length) valitakse 2048(High Grade) (pikk).



Joonis 5

e) Organisatsiooni esindaja märgib sertifikaadi kättesaamiseks üles selle viitenumbri.

Joonis 6

f) Euroopa ühendamise rahastu tugimeeskond kontrollib, kas on saabunud uusi sertifikaaditaotlusi ja seda, kas neis esitatud teave on õige, st see vastab sertifikaatidele nimeandmise põhimõtteid käsitlevas liites 5.1 sätestatud põhimõtetele.

g) Euroopa ühendamise rahastu tugimeeskond kontrollib, et taotlusse kantud teave oleks õiges vormingus.

h) Kui kas eespool punktis 5 või 6 osutatud kontroll ebaõnnestub, saadab Euroopa ühendamise rahastu tugimeeskond taotlusvormi sektsioonis „Identification data“ (identimisandmed) esitatud e-posti aadressil e-kirja (pannes koopiasse domeeni omaniku), milles palutakse organisatsiooni esindajal protsessi taasalustada. Ebaõnnestunud sertifikaaditaotlus katkestatakse.

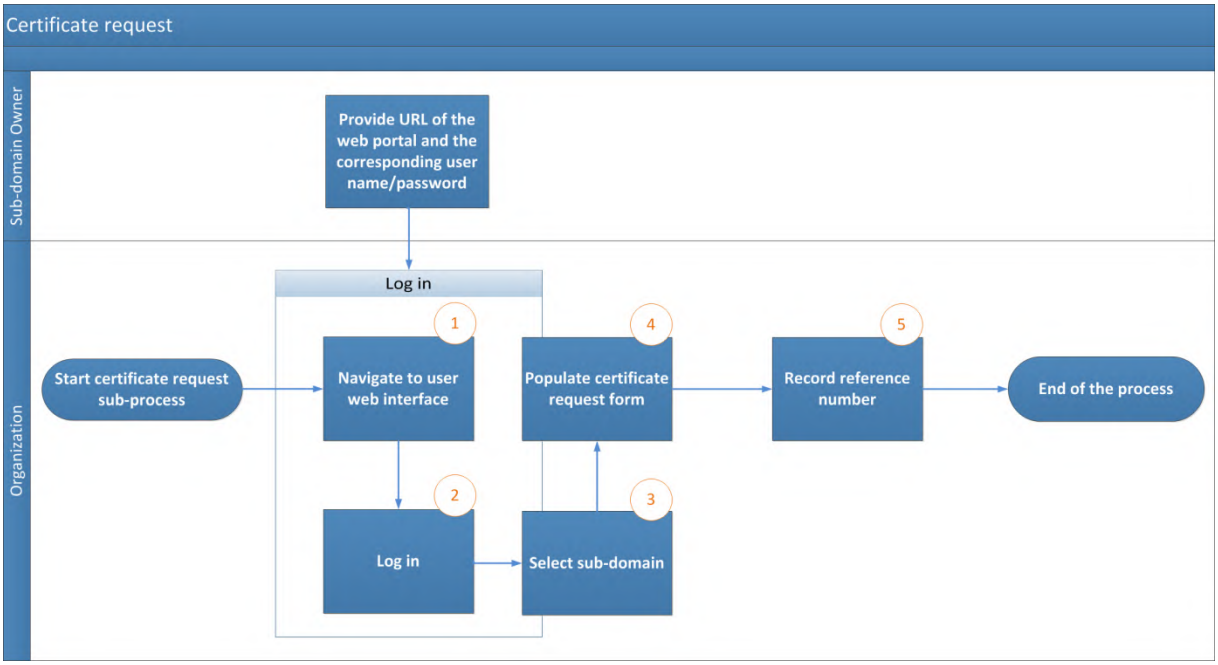
i) Euroopa ühendamise rahastu tugimeeskond saadab registripidajale taotluse kehtivust käsitleva e-kirja. E-kirjas märgitakse ära järgmine:

   (1) organisatsiooni nimi sertifikaaditaotluse väljalt „Organisation (O)“ (organisatsioon);

   (2) sertifikaati käsitlevad andmed, sh juurdepääsupunkti nimi, kellele sertifikaat välja antakse, sertifikaaditaotluse väljalt „Last Name (CN)“ (perekonnanimi);

   (3) sertifikaadi viitenumber;

   (4) organisatsiooni aadress, e-posti aadress ja esindaja nimi.



Joonis 7 – Sertifikaadi taotlemise protsess

2.2.4. 3. etapp: registreerimine registripidaja juures (sertifikaadi heakskiitmine)

2.2.4.1. Volitatud kuller või kontaktpunkt lepib registripidajaga e-posti teel kokku kohtumise, nimetades volitatud kulleri, kes sellel isiklikult osaleb.

2.2.4.2. Organisatsiooni esindaja koostab dokumendikausta, millesse kuuluvad:

a) täidetud ja allkirjastatud volikiri;

b) kohtumisel isiklikult osaleva volitatud kulleri kehtiva passi koopia. Koopia peab allkirjastama mõni 1. etapis identifitseeritud organisatsiooni kontaktpunktidest;

c) pabervormil sertifikaaditaotlus, mille on allkirjastanud mõni organisatsiooni kontaktpunktidest.

2.2.4.3. Registripidaja võtab volitatud kulleri vastu pärast isikusamasuse tuvastamist hoone vastuvõtus. Registripidaja läbib sertifikaaditaotluse isiklikuks registreerimiseks järgmised etapid:

a) volitatud kulleri identifitseerimine ja autentimine;

b) volitatud kulleri füüsilise välimuse võrdlemine fotoga tema poolt esitatud passis;

c) volitatud kulleri poolt esitatud passi kehtivusaja kontrollimine;

d) volitatud kulleri poolt esitatud valideeritud passi võrdlemine tema kehtiva passi koopiaga, mille on allkirjastanud mõni organisatsiooni kindlaksmääratud kontaktpunktidest. Allkirja võrreldakse „kontaktisikuid ja volitatud kullereid käsitlevale teabevormile“ kirjutatud originaalallkirjaga;

e) täidetud ja allkirjastatud volikirja kontrollimine;

f) pabervormil sertifikaaditaotluse ja sellele kirjutatud allkirja võrdlemine „kontaktisikuid ja volitatud kullereid käsitlevale teabevormile“ kirjutatud originaalallkirjaga;

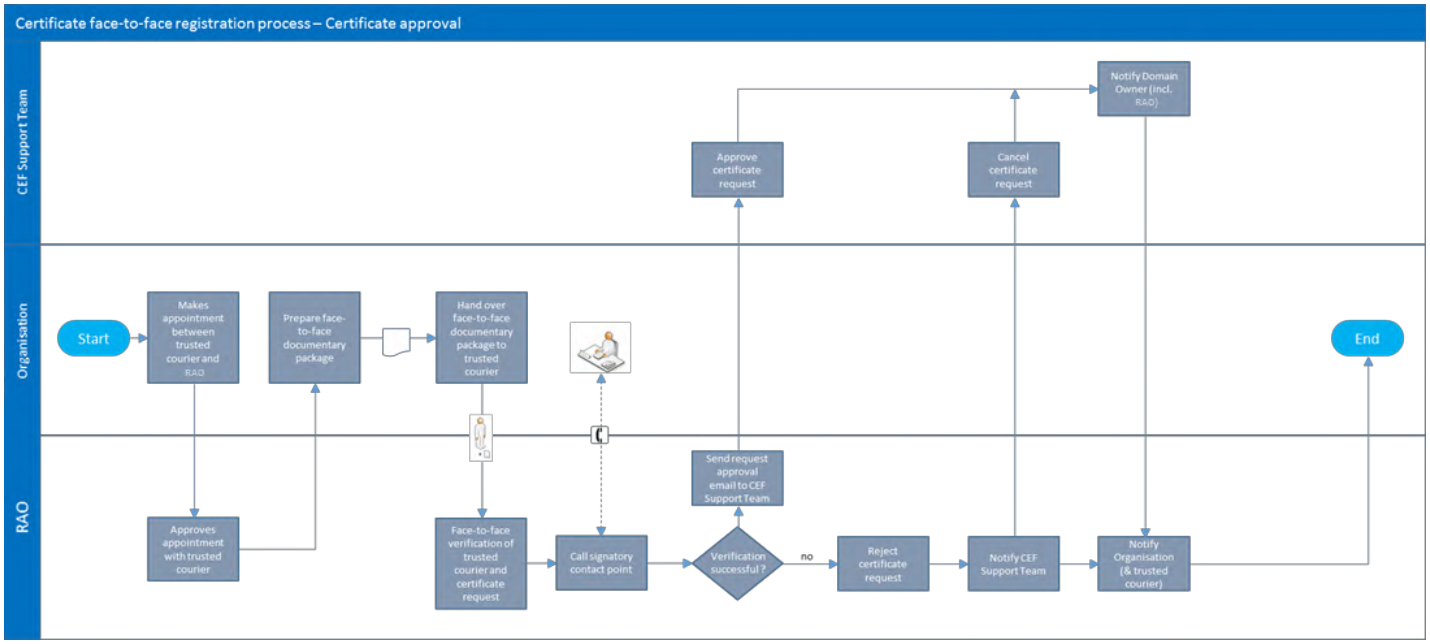
g) allkirjastaja kontaktpunktile helistamine, et üle kontrollida volitatud kulleri isik ja sertifikaaditaotluse sisu.

2.2.4.4. Registripidaja kinnitab Euroopa ühendamise rahastu tugimeeskonnale, et riigi ametiasutus on tõepoolest volitatud haldama komponente, milleks ta sertifikaate taotleb, ning et vastavisiklik registreerimisprotsess oli edukas. „CommiSign“-sertifikaadiga turvalise e-kirja teel saadetakse kinnituskiri, millele lisatakse skaneeritud koopiad isiklikult autenditud dokumentide kaustast ja registripidaja läbiviidud menetluse allkirjastatud kontrollnimekirjast.

2.2.4.5. Kui registripidaja kinnitab taotluse kehtivust, jätkub menetlus vastavalt punktides 2.2.4.6 ja 2.2.4.7 kirjeldatule. Vastupidisel juhul lükatakse sertifikaadi väljaandmine tagasi ja sellest teatatakse organisatsioonile.

2.2.4.6. Euroopa ühendamise rahastu tugimeeskond kiidab sertifikaaditaotluse heaks ja teatab sellest registripidajale.

2.2.4.7. Registripidaja teatab organisatsioonile, et sertifikaadi saab kätte kasutajaportaali kaudu.



Joonis 8 – Sertifikaadi heakskiitmine

2.2.5. 4. etapp: sertifikaadi genereerimine

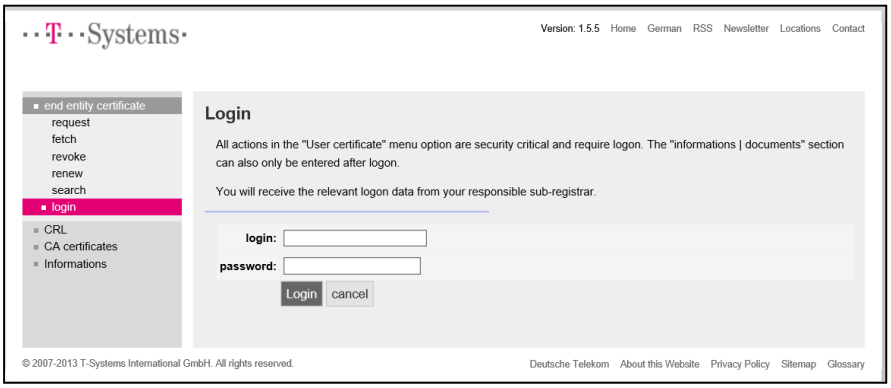
Sertifikaaditaotluse heakskiitmisel genereeritakse sertifikaat.

2.2.6. 5. etapp: sertifikaadi avaldamine ja kättesaamine

2.2.6.1. Sertifikaaditaotluse heakskiitmise järel saab registripidaja sertifikaadi kätte ja annab selle koopia üle volitatud kullerile.

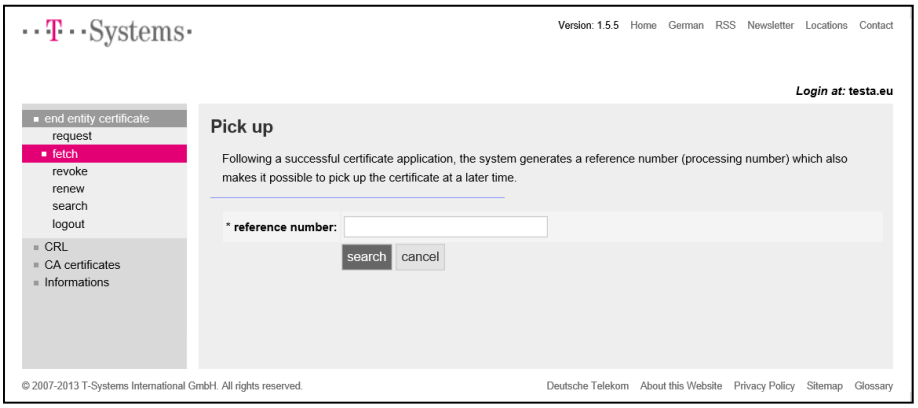
2.2.6.2. Organisatsioon saab registripidajalt teate, et sertifikaadid on kättesaadavad.

2.2.6.3. Organisatsiooni esindaja läheb kasutajaportaali veebisaidile aadressil https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en ja logib sisse kasutajanime „**sbca/CEF_eDelivery.europa.eu**“ ja salasõnaga „**digit.333**“.



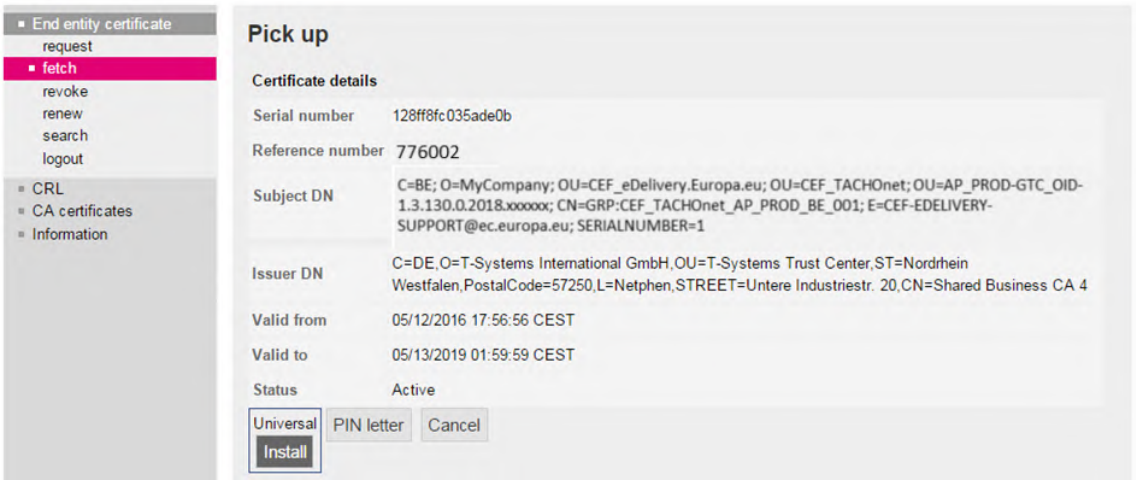
Joonis 9

2.2.6.4. Organisatsiooni esindaja klõpsab vasakpoolsel paneelil nupul „fetch“ (võtt) ja sisestab sertifikaadi taotlemise protsessi käigus ülesmärgitud viitenumbri;



Joonis 10

2.2.6.5. Organisatsiooni esindaja installeerib sertifikaadid, klõpsates nupul „Install“ (installeeri);



Joonis 11

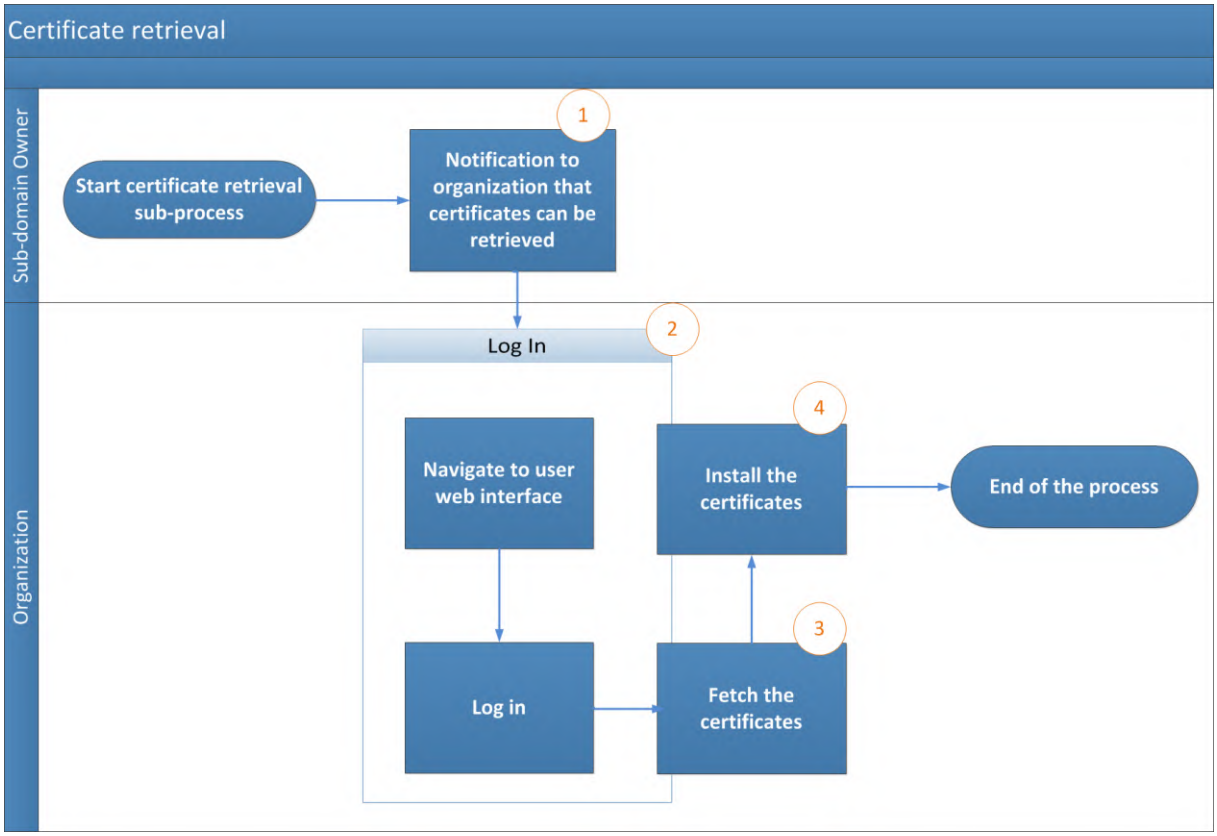
2.2.6.6. Sertifikaat installeeritakse juurdepääsupunktis. Kuna protsess on rakendusespetsiifiline, pöördub organisatsiooni esindaja selle protsessi kirjelduse saamiseks oma juurdepääsupunkti pakkuja poole.

2.2.6.7. Juurdepääsupunktis sertifikaadi installeerimiseks tuleb läbida järgmised etapid:

a) privaatvõtme ja sertifikaadi eksportimine,

b) võtmehoidla ja usaldushoidla loomine,

c) võtmehoidla ja usaldushoidla installeerimine juurdepääsupunktis.

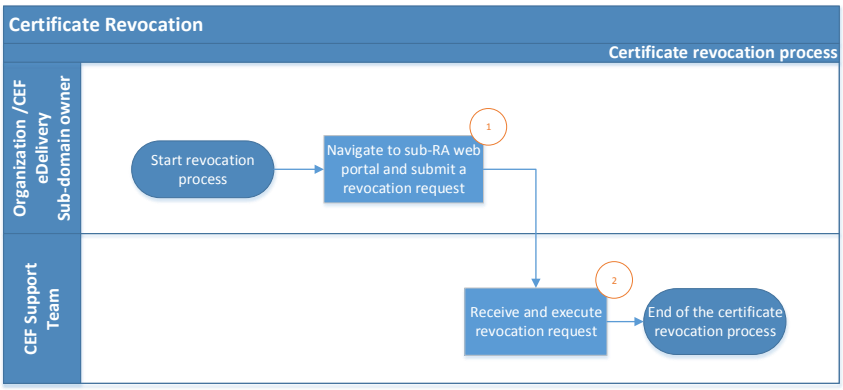


Joonis 12 – Sertifikaadi kättesaamine

3. Sertifikaadi tühistamise protsess

3.1. Organisatsioon esitab tühistamistaotluse kasutajaportaali kaudu;

3.2. Euroopa ühendamise rahastu tugimeeskond tühistab sertifikaadi.



Joonis 13 – Sertifikaadi tühistamine

4. Euroopa ühendamise rahastu PKI teenuse üldtingimused

4.1. Taust

Euroopa ühendamise rahastu platvormi eDelivery lahendusepakkujana osutab Euroopa Komisjoni informaatika peadirektoraat (DIGIT) AETRi osalistele PKI teenust[7] (edaspidi „Euroopa ühendamise rahastu PKI teenus“). Euroopa ühendamise rahastu PKI teenust kasutavad sõnumiedastussüsteemi TACHOnet kasutavad riikide ametiasutused (edaspidi „lõppkasutajad“).

DIGIT rendib PKId TeleSec Shared-Business-CA lahenduses (edaspidi „SBCA“), mida käitatakse ettevõtja T-Systems International GmbH (edaspidi „T-Systems“[8]) rühmaüksuse usalduskeskuses. DIGIT täidab SBCA domeeni „CEF_eDelivery.europa.eu“ pearegistripidaja rolli. Selles rollis loob DIGIT domeenis „CEF_eDelivery.europa.eu“ alamdomeenid kõigile Euroopa ühendamise rahastu PKI teenust kasutavatele projektidele.

Käesolevas dokumendis on esitatud sõnumiedastussüsteemi TACHOnet alamdomeeni üksikasjalikud tingimused. DIGIT täidab kõnealuse alamdomeeni alamregistripidaja rolli. Selle ülesande täitmisel annab ta välja, tühistab ja uuendab kõnealuse projekti sertifikaate.

4.2. Vastutuse välistamine

Euroopa Komisjon ei võta mingit vastutust sertifikaadi sisu eest, mille eest vastutab ainult selle omanik. Sertifikaadi sisu õigsuse kontrollimise eest vastutab sertifikaadi omanik.

Euroopa Komisjon ei võta mingit vastutust sertifikaadi kasutamise eest selle omaniku poolt, kes on Euroopa Komisjoni väline kolmas juriidiline isik.

---

7 PKI on kogum rolle, poliitikaid, menetlusi ja süsteeme, mis on vajalikud digisertifikaatide loomiseks, haldamiseks, levitamiseks ja tühistamiseks.

8 Ettevõtja T-Systems usalduskeskuses asuv usalduskeskuse käitaja täidab talle usaldatavas rollis ka sisemise registripidaja ülesandeid.

Vastutuse välistamise klausli eesmärk ei ole piirata komisjoni vastutust vastuolus kohaldatavas siseriiklikus õiguses sätestatud mis tahes nõuetega ega välistada vastutust nendel juhtudel, kui asjaomase õiguse alusel vastutust välistada ei saa.

4.3. Sertifikaatide lubatud/keelatud kasutusviisid

4.3.1. Sertifikaatide lubatud kasutusviisid

Sertifikaadi omanik[9] kasutab väljaantud sertifikaati üksnes sõnumiedastussüsteemi TACHOnet raames. Sertifikaati võib sõnumiedastussüsteemi TACHOnet raames kasutada järgmistel eesmärkidel:

- andmete päritolu autentimine;
- andmete krüpteerimine;
- andmete tervikluse rikkumiste avastamise tagamine.

4.3.2. Sertifikaatide keelatud kasutusviisid

Kõik kasutusviisid, mis ei ole lubatud kasutusviisidena sõnaselgelt lubatud, on keelatud.

4.4. Sertifikaadiomaniku täiendavad kohustused

T-Systems on SBCA üksikasjalikud tingimused kindlaks määranud SBCA teenuse sertifitseerimispoliitikas ja -tavades[10]. Kõnealune dokument hõlmab turvaspetsifikatsioone ning tehnilisi ja korralduslikke aspekte käsitlevaid suuniseid ja selles kirjeldatakse usalduskeskuse käitaja tegevust sertifitseerimisasutuse ja registripidajana, samuti registripidaja volitatud kolmanda isikuna.

Sertifikaate võivad taotleda ainult sõnumiedastussüsteemis TACHOnet osalema volitatud üksused.

---

9 Identifitseeritakse atribuudi väärtusega „O=“ väljaantud sertifikaadi teema eraldusnimes.

10 Ettevõtja T-Systems SBCA teenuse sertifitseerimispoliitika ja -tavade ajakohaseim versioon on kättesaadav aadressil https://www.telesec.de/en/sbca-en/support/download-area/.

Sertifikaadi heakskiitmise suhtes kohaldatakse SBCA teenuse sertifitseerimispoliitika ja -tavade punkti 4.4.1, lisaks loetakse käesolevas dokumendis kirjeldatud kasutustingimused ja -sätted sertifikaadi esmakordsel kasutamisel selle saanud organisatsiooni („O=“) poolt heakskiidetuks.

Sertifikaadi avaldamise suhtes kohaldatakse SBCA teenuse sertifitseerimispoliitika ja -tavade punkti 2.2.

Kõik sertifikaadiomanikud peavad täitma järgmisi nõudeid:

(1) kaitsevad oma privaatvõtmeid loata kasutamise eest;

(2) hoiduvad privaatvõtmete kolmandatele isikutele edastamisest või avaldamisest, ka esindajatena;

(3) hoiduvad pärast sertifikaadi kehtivuse lõppu või selle tühistamist privaatvõtme kasutamise jätkamisest, v.a krüpteeritud andmete vaatamiseks (nt e-kirjade dekrüpteerimiseks).

(4) sertifikaadiomanik vastutab võtme kopeerimise või lõppkasutaja(te)le edasisaatmise eest;

(5) sertifikaadiomanik peab kohustama lõppkasutajat / kõiki lõppkasutajaid täitma privaatvõtmete kasutamisel käesolevaid tingimusi, sealhulgas SBCA teenuse sertifitseerimispoliitikat ja -tavasid;

(6) sertifikaadiomanik peab esitama nende volitatud esindajate nimed, kes on volitatud taotlema organisatsioonile väljastatud sertifikaatide tühistamist, märkides üksikasjad sündmuste kohta, mille tõttu tühistamine on vajalik, ja tühistamissalasõna;

(7) isikute rühmade ja ametikohtade ja/või juriidiliste isikutega seotud sertifikaatide puhul peab sertifikaadiomanik pärast isiku lõppkasutajate rühmast lahkumist (nt seoses töösuhte lõpetamisega) vältima privaatvõtme kuritarvitamist, tühistades sertifikaadi;

(8) sertifikaadiomanik vastutab sertifikaadi tühistamise eest SBCA teenuse sertifitseerimispoliitika ja -tavade punktis 4.9.1 osutatud asjaolude ilmnemisel, ja taotleb seda.

Sertifikaadi uuendamise või uute võtmete väljastamise suhtes kohaldatakse SBCA teenuse sertifitseerimispoliitika ja -tavade punkti 4.6 või 4.7.

Sertifikaadi muutmise suhtes kohaldatakse SBCA teenuse sertifitseerimispoliitika ja -tavade punkti 4.8.

Sertifikaadi tühistamise suhtes kohaldatakse SBCA teenuse sertifitseerimispoliitika ja -tavade punkti 4.9.

5. Kontaktisikuid ja volitatud kullereid käsitlev teabevorm (näidis)

Mina, [organisatsiooni esindaja nimi ja aadress], **kinnitan, et järgnevat teavet võib kasutada seoses sõnumiedastussüsteemi TACHOnet juurdepääsupunktidele avaliku võtme digisertifikaatide taotlemise, genereerimise ja kättesaamisega ning sellega toetatakse sõnumiedastussüsteemi TACHOnet teadete konfidentsiaalsust, terviklust ja salgamise vääramist:**

Kontaktisikute andmed

– **Kontaktisik #1**	– **Kontaktisik #2**
– Nimi:	– Nimi:
– Eesnimed:	– Eesnimed:
– Mobiiltelefon:	– Mobiiltelefon:
– Telefon:	– Telefon:
– E-post:	– E-post:
– Omakäeline allkirjanäidis: –	– Omakäeline allkirjanäidis: – – –

Volitatud kullerite andmed

– **Volitatud kuller #1**	– **Volitatud kuller #2**
– Nimi:	– Nimi:
– Eesnimed:	– Eesnimed:
– Mobiiltelefon:	– Mobiiltelefon:
– E-post:	– E-post:
– Passi väljaandnud riik:	– Passi väljaandnud riik:
– Passi number:	– Passi number:
– Passi kehtivuse lõppkuupäev:	– Passi kehtivuse lõppkuupäev:

Koht, kuupäev, äriühingu tempel või organisatsiooni pitser:

Volitatud esindaja allkiri:

6. Dokumendid

6.1. Ühekordne volikiri (näidis)

Järgnevalt on esitatud ühekordse volikirja näidis, mille volitatud kuller peab allkirjastama ja esitama isiklikul registreerimisel registripidajaga:

Please print the text of this document on your letterhead, add your company stamp and have it signed by the administrative contact or admin-c of the domain.
The power of attorney must be signed by an authorized representative of the organization (principal).

The Shared-Business-CA customer will then submit this document together with the order document to the T-Systems International GmbH Trust Center.

Individual power of attorney / Power of attorney granted to one person

I, ***[name and address of the end-user]***, empower as an authorized person of this organization *

[name of the company receiving the certificate]

(e. g. sample company, sample authority, to be registered in the O-field of the certificate *)

following company and/or person:

Company: **European Commission**
Address: **DG DIGIT, 28 rue Belliard, 1000 Brussels**
Represented by Mr/Mrs/Ms: **Adrien FERIAL**

On my behalf, by complying with all and any regulations and formalities (particularly Certificate Policy (CP) / Certification Practice Statement (CPS)), for authorisation to manage (i.e. issue, revoke, renew) X.509v3-certificates, including the complete key-material, issued by the certification authority „TeleSec Shared-Business-CA", in respect of the domain as above mentioned.

This power of attorney relates to issuing and management of the following certificate types (the applicable type has to be marked):

☒ user [1]: e.g. mail security (signature, encryption), virtual private network (VPN), TLS/SSL client

☐ server [2]: e.g. identity of web server, TLS/SSL client server authentication
Please enter additionally the country, organization, locality, state or province name of the server:
_____

☐ eMail-Gateway [3]: e.g. identity of eMail gateways / eMail-Appliance, virtual mail-administrating centre.

Validity

☒ The power of attorney is valid until further notice, but up to a **maximum of 27 months** [2] or **maximum of 36 months** [1,3] from date of issuance.

☐ The power of attorney is valid until _____ (mm.dd.yyyy), but up to a **maximum of 27 month** [2] months or **maximum of 36 months** [1,3] from date of issuance.

Please note that a time limit on the power of attorney can cause that a request for certificate order, renewal or revocation may not be possible because the validity period of the authorization has been exceeded!

Place, date, company stamp or seal of the organisation (principal)

Signature of the authorized representative

6.2. Sertifikaaditaotluse pabervorm

Järgnevalt on esitatud sertifikaaditaotluse pabervormi näidis, mille volitatud kuller peab allkirjastama ja esitama isiklikul registreerimisel registripidajaga:

7. Sõnastik

Käesolevas alamliites kasutatud põhimõisted on määratletud Euroopa ühendamise rahastu digitaalse ühtse veebiportaali Euroopa ühendamise rahastu mõistete osas:

https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/CEF+Definitions

Käesolevas komponentide pakkumise kirjelduses kasutatud põhiakronüümid on määratletud Euroopa ühendamise rahastu digitaalse ühtse veebiportaali Euroopa ühendamise rahastu sõnastiku osas:

https://ec.europa.eu/cefdigital/wiki/pages/viewpage.action?spaceKey=CEFDIGITAL&title=CEF+Glossary