Euroopan unionin
neuvosto

Bryssel, 5. marraskuuta 2018
(OR. en)

13711/18
ADD 1

Toimielinten välinen asia:
2018/0339 (NLE)

TRANS 488

ILMOITUS

Lähettäjä:	Neuvoston pääsihteeristö
Vastaanottaja:	Valtuuskunnat
Ed. asiak. nro:	ST 13711/18 TRANS 448
Kom:n asiak. nro:	ST 12727/18 TRANS 426 + ADD 1
Asia:	Neuvoston päätös kansainvälisessä maantieliikenteessä toimivien ajoneuvojen miehistöjen työstä tehtyä eurooppalaista sopimusta käsittelevässä Yhdistyneiden kansakuntien Euroopan talouskomission asiantuntijaryhmässä Euroopan unionin puolesta otettavasta kannasta

Liite edellä mainittuun neuvoston päätökseen.

Uusi lisäys AETR-sopimukseen

Lisäys 4

TACHOnet-järjestelmää koskevat yksityiskohtaiset tiedot

1. Soveltamisala ja tarkoitus

1.1. **Tässä lisäyksessä esitetään ehdot, jotka koskevat AETR-sopimuspuolten liittämistä TACHOnet-järjestelmään sähköisen eDelivery-jakelupalvelun välityksellä.**

1.2. **TACHOnet-järjestelmään sähköisen jakelupalvelun välityksellä liittyvien sopimuspuolten on noudatettava tässä lisäyksessä vahvistettuja säännöksiä.**

2. Määritelmät:

a) 'sopimuspuolella' tai 'osapuolella' tarkoitetaan mitä tahansa AETR-sopimuksen osapuolta;

b) 'sähköisellä jakelupalvelulla' (eDelivery) tarkoitetaan Euroopan komission kehittämää palvelua, jonka avulla tietoa voidaan siirtää sähköisesti kolmansien osapuolten välillä, joka antaa siirretyn tiedon käsittelyyn liittyviä todisteita, muun muassa vahvistuksen tietojen lähettämisestä ja vastaanottamisesta, ja joka suojaa siirretyt tiedot luvattomien muutosten riskiltä;

c) 'TACHOnet-järjestelmällä' tarkoitetaan asetuksen (EU) N:o 165/2014 31 artiklan 2 kohdassa tarkoitettua järjestelmää, jonka kautta sopimuspuolet vaihtavat keskenään sähköisesti tietoa kuljettajakorteista;

d) 'solmupisteellä' tarkoitetaan tietojärjestelmää, joka mahdollistaa TACHOnet-viestien reitittämisen pyytävän osapuolen ja vastaavan osapuolen välillä;

e) 'pyytävällä osapuolella' tarkoitetaan sitä sopimuspuolta, joka lähettää TACHOnet-pyynnön tai -ilmoituksen, joka reititetään asianmukaiselle vastaavalle osapuolelle solmupisteen kautta;

f) 'vastaavalla osapuolella' tarkoitetaan sopimuspuolta, jolle TACHOnet-pyyntö tai -ilmoitus on osoitettu;

g) 'kortin myöntävällä viranomaisella' tarkoitetaan tahoa, jonka sopimuspuoli on valtuuttanut myöntämään ja hallinnoimaan ajopiirturikortteja.

3. Yleiset velvollisuudet

3.1. **Kumpikaan sopimuspuoli ei voi tehdä sopimuksia pääsyn myöntämiseksi TACHOnet-järjestelmään toisen osapuolen puolesta eikä millään muulla tavoin edustaa toista sopimuspuolta tämän lisäyksen perusteella. Kumpikaan sopimuspuoli ei toimi toisen sopimuspuolen alihankkijana tässä lisäyksessä tarkoitetuissa toimissa.**

3.2. Sopimuspuolet tarjoavat pääsyn kansalliseen kuljettajakorttirekisteriinsä TACHOnet-järjestelmän välityksellä alalisäyksessä 4.6 tarkoitetulla tavalla ja tarkoitetun palvelutason mukaisesti.

3.3. Sopimuspuolet ilmoittavat toisilleen viipymättä, jos ne havaitsevat omalla vastuualueellaan sellaisia häiriöitä tai virheitä, jotka saattavat vaarantaa TACHOnet-järjestelmän normaalin toiminnan.

3.4. Kumpikin sopimuspuoli nimeää TACHOnet-järjestelmää varten yhteishenkilöt, jotka ilmoitetaan AETR-sihteeristölle. Yhteyshenkilöiden muutoksista on ilmoitettava AETR-sihteeristölle kirjallisesti.

4. Testit TACHOnet-järjestelmään liittymiseksi

4.1. Sopimuspuolen liittäminen TACHOnet-järjestelmään katsotaan vahvistetuksi sen jälkeen, kun on suoritettu onnistuneesti liitäntä-, integrointi- ja suorituskykytestit Euroopan komission ohjeiden mukaisesti ja sen valvonnassa.

4.2. Jos ennakkotestit epäonnistuvat, Euroopan komissio voi keskeyttää tilapäisesti testivaiheen. Testejä jatketaan sen jälkeen, kun sopimuspuoli on ilmoittanut Euroopan komissiolle sellaisten kansallisella tasolla tarvittavien teknisten parannusten hyväksymisestä, jotka mahdollistavat ennakkotestien onnistuneen suorittamisen.

4.3. Ennakkotestit saavat kestää enintään kuusi kuukautta.

5. Turva-arkkitehtuuri

5.1. TACHOnet-viestien luottamuksellisuus, eheys ja kiistämättömyys varmistetaan TACHOnet-järjestelmän turva-arkkitehtuurilla.

5.2. TACHOnet-järjestelmän turva-arkkitehtuuri perustuu Euroopan komission käyttöön ottamaan julkisen avaimen menetelmään (PKI), jota koskevat vaatimukset esitetään alalisäyksissä 4.8 ja 4.9.

5.3. TACHOnet-järjestelmän turva-arkkitehtuuriin osallistuvat seuraavat tahot:

a) varmenneviranomainen, joka vastaa niiden sähköisten varmenteiden luomisesta, jotka rekisteröintiviranomainen toimittaa sopimuspuolten kansallisille viranomaisille (niiden nimittämien luotettujen kuriirien välityksellä), sekä sähköisten varmenteiden myöntämistä, peruuttamista ja uusimista koskevan teknisen infrastruktuurin perustamisesta;

b) verkkotunnuksen omistaja, joka on vastuussa alalisäyksessä 4.1 tarkoitetun solmupisteen toiminnasta sekä TACHOnet-järjestelmän turva-arkkitehtuurin validoinnista ja koordinoinnista;

c) rekisteröintiviranomainen, joka kirjaa ja hyväksyy sähköisten varmenteiden myöntämistä, peruuttamista ja uusimista koskevat pyynnöt sekä tarkistaa luotettujen kuriirien henkilöllisyyden;

d) luotettu kuriiri, joka on kansallisten viranomaisten nimittämä henkilö ja joka vastaa julkisen avaimen luovuttamisesta rekisteröintiviranomaiselle ja varmenneviranomaisen luoman vastaavan varmenteen saamisesta;

e) sopimuspuolen kansallinen viranomainen, jonka tehtävänä on

i) luoda yksityiset avaimet ja niitä vastaavat julkiset avaimet, jotka sisällytetään varmenneviranomaisen luomiin varmenteisiin;

ii) pyytää varmenneviranomaiselta sähköiset varmenteet;

iii) nimittää luotettu kuriiri.

5.4. Varmenneviranomaisen ja rekisteröintiviranomaisen nimittää Euroopan komissio.

5.5. Kaikkien TACHOnet-järjestelmään liittyvien sopimuspuolten on pyydettävä sähköistä varmennetta alalisäyksen 4.9 mukaisesti, jotta sopimuspuoli voi allekirjoittaa ja salata TACHOnet-viestejä.

5.6. Varmenne voidaan peruuttaa alalisäyksen 4.9 mukaisesti.

6. Tietosuoja ja luottamuksellisuus

6.1. Tietosuojaa koskevien kansainvälisten ja kansallisten säädösten ja erityisesti yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyn yleissopimuksen mukaisesti osapuolet ottavat käyttöön kaikki tarvittavat tekniset ja organisaatiota koskevat toimenpiteet varmistaakseen TACHOnet-järjestelmässä olevien tietojen turvallisuuden ja estääkseen tietojen muuttamisen ja häviämisen sekä niiden luvattoman käsittelyn ja saannin (erityisesti varmistaakseen tietojen aitouden, luottamuksellisuuden, jäljitettävyyden, eheyden, saatavuuden ja kiistämättömyyden sekä viestien turvallisuuden).

6.2. Kunkin osapuolen on suojeltava kansallisia järjestelmiään laittomalta käytöltä, haittaohjelmilta, viruksilta, tietokonemurroilta, tietoturvaloukkauksilta, tietojen laittomalta peukaloinnilta ja muilta vastaavilta kolmansien osapuolen toimilta. Osapuolet sopivat toteuttavansa taloudellisesti kohtuullisia toimenpiteitä estääkseen virusten, aikapommien, tietokonematojen ja muiden vastaavien siirtymisen sekä kaikki sellaiset tietokone-ohjelmien toimet, jotka voivat haitata toisen osapuolen tietokonejärjestelmien toimintaa.

7. Kustannukset

7.1. Sopimuspuolet vastaavat omiin tietojärjestelmiinsä ja -menettelyihinsä liittyvistä kehittämis- ja toimintakustannuksista, jotka ovat tarpeen lisäyksessä asetettujen velvoitteiden täyttämiseksi.

7.2. Alalisäyksessä 4.1 määritellyt palvelut, joita tarjoaa solmupiste, ovat maksuttomia.

8. Alihankinta

8.1. Osapuolet voivat antaa alihankkijoiden tehtäväksi mitä tahansa palveluja, joista ne ovat vastuussa tämän lisäyksen mukaisesti.

8.2. Alihankinta ei kuitenkaan poista osapuolelle tämän lisäyksen mukaisesti kuuluvaa vastuuta, mukaan lukien vastuu alalisäyksessä 4.6 esitetyn asianmukaisen palvelutason varmistamisesta.

Alalisäys 4.1

TACHOnet-järjestelmää koskevia yleisiä näkökohtia

1. Yleiskuvaus

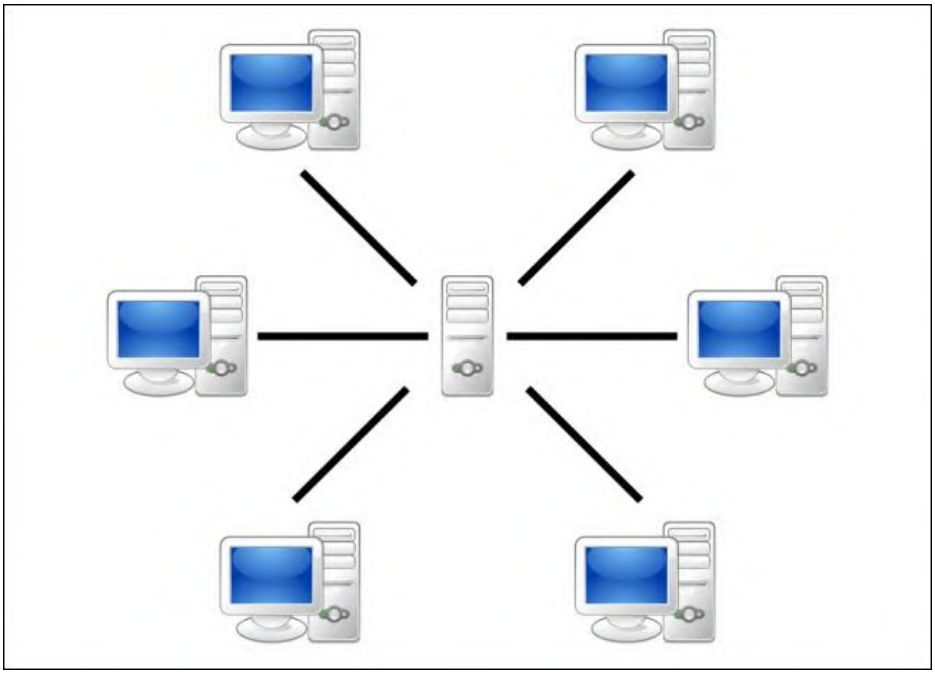
TACHOnet-järjestelmä on sähköinen järjestelmä, jonka kautta AETR-sopimuspuolet vaihtavat keskenään tietoa kuljettajakorteista. TACHOnet reitittää pyytävien osapuolten tietopyynnöt vastaaville osapuolille sekä jälkimmäisten vastaukset edellisille. TACHOnet-järjestelmään osallistuvien sopimuspuolten on liitettävä kansalliset kuljettajakorttirekisterinsä järjestelmään.

2. Arkkitehtuuri

TACHOnet-viestijärjestelmä koostuu seuraavista osista:

2.1. Solmupiste, jonka on voitava vastaanottaa pyyntö sen esittävältä osapuolelta, validoida se ja käsitellä se lähettämällä se edelleen vastaaville osapuolille. Solmupisteen on odotettava vastausta kultakin vastaavalta osapuolelta, koottava kaikki vastaukset ja toimitettava koottu vastaus eteenpäin pyynnön esittäneelle osapuolelle.

2.2. Osapuolten kansalliset järjestelmät varustettuina rajapinnalla, joka pystyy sekä lähettämään pyyntöjä solmupisteeseen että vastaanottamaan niiden vastaukset. Kansalliset järjestelmät voivat käyttää omistusoikeudellisia tai kaupallisia ohjelmistoja viestien lähettämiseen ja vastaanottamiseen solmupisteen välityksellä.



3. Hallinnointi

3.1. Solmupistettä hallinnoi Euroopan komissio, joka vastaa sen teknisestä toiminnasta ja ylläpidosta.

3.2. Solmupiste saa säilyttää tietoja enintään kuuden kuukauden ajan lukuun ottamatta alalisäyksessä 4.7 esitettyjä loki- ja tilastotietoja.

3.3. Solmupisteessä ei saa olla pääsyä henkilötietoihin muille kuin valtuutetulle Euroopan komission henkilöstölle tapauksissa, joissa tämä on tarpeen seurantaa, huoltoa ja vianetsintää varten.

3.4. Kukin sopimuspuoli on vastuussa seuraavista:

3.4.1. Kansallisten järjestelmien rakenne ja hallinnointi, myös niiden rajapinta solmupisteeseen.

3.4.2. Kansallisen järjestelmän käyttöönotto ja huolto, mihin sisältyvät sekä laitteisto että omistusoikeudelliset tai kaupalliset ohjelmistot.

3.4.3. Kansallisen järjestelmän moitteeton yhteentoimivuus solmupisteen kanssa, mukaan lukien solmupisteestä saatujen virheilmoitusten käsittely.

3.4.4. Kaikki toimenpiteet tietojen luottamuksellisuuden, eheyden ja saatavuuden varmistamiseksi.

3.4.5. Kansallisten järjestelmien toiminta alalisäyksessä 4.6 esitetyillä palvelutasoilla.

Alalisäys 4.2

TACHOnet-järjestelmän toiminnot

1. Seuraavat toiminnot on tarjottava TACHOnet-viestijärjestelmän välityksellä:

1.1. Kortin myöntämisen tarkastus (Check Issued Cards, CIC): Pyytävä osapuoli voi pyytää kortin myöntämisen tarkastusta joltakin tai kaikilta vastaavilta osapuolilta määrittääkseen, onko kortin hakijalla jo vastaavien osapuolten myöntämä kuljettajakortti. Vastaavien osapuolten on vastattava lähettämällä vastaus kortin myöntämistä koskevaan tarkastuspyyntöön.

1.2. Kortin tilan tarkastus (Check Card Status, CCS): Pyytävä osapuoli voi pyytää vastaavalta osapuolelta tietoja jälkimmäisen myöntämästä kortista lähettämällä kortin tilaa koskevan tarkastuspyynnön. Vastaavan osapuolen on vastattava lähettämällä vastaus kortin tilaa koskevaan tarkastuspyyntöön.

1.3. Kortin tilan muuttaminen (Modify Card Status, MCS): Pyytävä osapuoli voi ilmoittaa vastaavalle osapuolelle kortin tilan muuttamista koskevalla pyynnöllä, että jälkimmäisen myöntämän kortin tila on muuttunut. Vastaavan osapuolen on vastattava lähettämällä kortin tilan muuttamista koskeva kuittaus.

1.4. Ajokorttia vastaan myönnetty kortti (Issued Card Driving License, ICDL): Pyytävä osapuoli voi ilmoittaa vastaavalle osapuolelle ajokorttia vastaan myönnettyä korttia koskevalla pyynnöllä myöntäneensä kortin jälkimmäisen myöntämää ajokorttia vastaan. Vastaavan osapuolen on vastattava lähettämällä vastaus ajokorttia vastaan myönnettyä korttia koskevaan pyyntöön.

2. TACHOnet-järjestelmän on sisällettävä myös muita viestityyppejä, joiden katsotaan soveltuvan sen tehokkaaseen toimintaan, esimerkiksi virheilmoituksia.

3. Kansallisten järjestelmien on tunnistettava taulukossa 1 mainitut kortin tilat, kun käytetään 1 kohdassa kuvattuja toimintoja. Osapuolet eivät kuitenkaan ole velvollisia ottamaan käyttöön hallinnollista menettelyä, jossa käytetään kaikkia lisäyksessä mainittuja kortin tiloja.

4. Jos osapuoli vastaanottaa vastauksen tai ilmoituksen, jossa mainittu tila ei ole käytössä sen hallinnollisissa menettelyissä, kansallisen järjestelmän on muutettava vastaanotetussa viestissä mainittu tila soveltuvaksi arvoksi kyseisessä menettelyssä. Vastaava osapuoli ei saa hylätä viestiä, mikäli viestissä mainittu tila mainitaan taulukossa 1.

5. Taulukossa 1 mainittua kortin tilaa ei saa käyttää määritettäessä, onko kuljettajakortti voimassa ajamista varten. Jos osapuoli esittää kortin myöntäneen kansallisen viranomaisen rekisterille kysymyksen CCS-toiminnolla, vastauksessa on oltava erityinen kenttä "voimassa ajamista varten". Kansallisten hallinnollisten menettelyjen on oltava sellaisia, että CCS-vastauksissa on aina käytössä soveltuva "voimassa ajamista varten" -arvo.

Taulukko 1

Kortin tilat

Kortin tila	**Määritelmä**
Haussa	Kortin myöntävä viranomainen on vastaanottanut kuljettajakorttia koskevan hakemuksen. Kyseiset tiedot on rekisteröity ja tallennettu tietokantaan hakuavaimineen.
Hyväksytty	Kortin myöntävä viranomainen on hyväksynyt ajopiirturikorttia koskevan hakemuksen.
Hylätty	Kortin myöntävä viranomainen on jättänyt hakemuksen hyväksymättä.
Yksilöity	Ajopiirturikortti on yksilöllinen.
Lähetetty	Kansallinen viranomainen on lähettänyt kuljettajakortin asianomaiselle kuljettajalle tai välittäjätaholle.
Luovutettu	Kansallinen viranomainen on luovuttanut kuljettajakortin asianomaiselle kuljettajalle.
Takavarikoitu	Toimivaltainen viranomainen on määrännyt kuljettajakortin menetetyksi.
Voimassaolo keskeytetty	Kuljettajakortti on peruutettu kuljettajalta tilapäisesti.
Peruutettu	Kortin myöntänyt viranomainen on päättänyt peruuttaa kuljettajakortin. Kortti on pysyvästi mitätöity.
Palautettu	Ajopiirturikortti on palautettu kortin myöntäneelle viranomaiselle tarpeettomana.
Kadonnut	Ajopiirturikortti on ilmoitettu kadonneeksi kortin myöntäneelle viranomaiselle.
Varastettu	Ajopiirturikortti on ilmoitettu varastetuksi kortin myöntäneelle viranomaiselle. Varastettu kortti katsotaan kadonneeksi.
Viallinen	Ajopiirturikortti on ilmoitettu vialliseksi kortin myöntäneelle viranomaiselle.
Voimassaolo päättynyt	Ajopiirturikortin voimassaoloaika on päättynyt.
Korvattu	Kadonneeksi, varastetuksi tai vialliseksi ilmoitettu ajopiirturikortti on korvattu uudella kortilla. Kortissa olevat tiedot ovat samat lukuun ottamatta korvausnumeroa, jota on korotettu yhdellä.

Kortin tila	**Määritelmä**
Uusittu	Ajopiirturikortti on uusittu, koska hallinnolliset tiedot ovat muuttuneet tai voimassaoloaika on päättymässä. Uuden kortin numero on sama lukuun ottamatta uusintanumeroa, jota on korotettu yhdellä.
Vaihdettavana	Kuljettajakortin myöntänyt viranomainen on saanut ilmoituksen menettelyn aloittamisesta kortin vaihtamiseksi toisen osapuolen viranomaisen myöntämään kuljettajakorttiin.
Vaihdettu	Kuljettajakortin myöntänyt viranomainen on saanut ilmoituksen päätökseen saatetusta menettelystä kortin vaihtamiseksi toisen jäsenvaltion viranomaisen myöntämään kuljettajakorttiin.

Alalisäys 4.3

TACHOnet-järjestelmän viestejä koskevat säännökset

1. Yleiset tekniset vaatimukset

1.1. Solmupisteen on tarjottava sekä synkroninen että asynkroninen rajapinta viestinvaihtoa varten. Osapuolet voivat valita rajapinnaksi omiin sovelluksiinsa sopivimman teknologian.

1.2. Kaikkien solmukohdan ja kansallisten järjestelmien välisten viestien on oltava UTF-8-koodattuja.

1.3. Kansallisten järjestelmien on pystyttävä vastaanottamaan ja käsittelemään viestejä, jotka sisältävät kreikkalaisia tai kyrillisiä merkkejä.

2. XML-viestirakenne ja -skeemamäärittely (XSD)

2.1. XML-viestien yleisrakenteen on vastattava solmupisteen XSD-skeemoilla määriteltyä muotoa.

2.2. Solmupisteen ja kansallisten järjestelmien lähettämien ja vastaanottamien viestien on vastattava viestien XSD-skeemaa.

2.3. Kansallisten järjestelmien on voitava lähettää, vastaanottaa ja käsitellä kaikki alalisäyksessä 4.2 esitettyihin toimintoihin liittyvät viestit.

2.4. XML-viestien sisältöä koskevat vähimmäisvaatimukset esitetään taulukossa 2.

Taulukko 2

XML-viestien sisältöä koskevat vähimmäisvaatimukset

Yhteinen otsikkoelementti ("Common header")		**Pakollinen**
Versio	XML-eritelmien virallinen versio määritellään viestin XSD:n nimiavaruusmäärittelyllä (namespace) ja minkä tahansa XML-viestin otsikkoelementin versio-attribuutin nimiavaruusmäärittelyllä. Version numero ("n.m") määritetään vakioarvona XML-skeemamäärittelyn (xsd) kussakin julkaisussa.	Kyllä
"Test Identifier" (Testitunniste)	Vapaaehtoinen tunniste testausta varten. Testin alullepanija täydentää tunnisteen, ja kaikki työnkulkuun osallistuvat lisäävät sen edelleen/takaisin. Tuotannossa se jätetään huomiotta ja käyttämättä, jos se on toimitettu.	Ei
"Technical Identifier" (Tekninen tunniste)	Kunkin yksittäisen viestin ainutkertaisesti yksilöivä UUID. Lähettäjä luo UUID-tunnisteen ja täydentää tämän attribuutin. Näitä tietoja ei käytetä liiketoiminnallisissa yhteyksissä.	Kyllä
"Workflow Identifier" (Työnkulun tunniste)	Työnkulun tunniste on UUID, joka pyytävän osapuolen olisi luotava. Tätä tunnistetta käytetään sen jälkeen kaikissa työnkulkuun kytkeytyvissä viesteissä.	Kyllä
"Sent At" (Lähettämisajankohta)	Viestin lähettämispäivä ja -aika (UTC).	Kyllä
"Timeout" (Aikakatkaisu)	Tämä on valinnainen aika-attribuutti (päivämäärä ja kellonaika UTC-muodossa). Solmupiste antaa tämän arvon vain edelleenlähetetyille pyynnöille. Se ilmoittaa vastaavalle osapuolelle ajan, jonka jälkeen pyynnön toimitus katkaistaan. Tätä arvoa ei vaadita MS2TCN_<x>_Req:issä eikä vastausviesteissä. Se on valinnainen, joten samaa otsikkomääritelmää voidaan käyttää kaikissa viestityypeissä riippumatta siitä, vaaditaanko attribuutti aikakatkaisulle.	Ei
"From" (Lähettäjä)	Standardin ISO 3166-1 alpha-2 mukainen lähettävän osapuolen kaksimerkkinen koodi tai "EU".	Kyllä
"To" (Vastaanottaja)	Standardin ISO 3166-1 alpha-2 mukainen vastaanottavan osapuolen kaksimerkkinen koodi tai "EU".	Kyllä

Alalisäys 4.4

Translitterointi ja NYSIIS-palvelut (New York State Identification and Intelligence System)

1. Solmupisteessä käyttöön otettavaa NYSIIS-algoritmia käytetään kaikkien kansallisessa rekisterissä olevien kuljettajien nimien koodaamiseen.

2. Haettaessa korttia CIC-toiminnolla ensisijaisena hakumekanismina käytetään NYSIIS-avaimia.

3. Lisäksi osapuolet voivat käyttää tarkoitukseen laadittua algoritmia lisätulosten saamiseksi täsmähaulla.

4. Hakutuloksissa ilmoitetaan kirjauksen löytämiseen käytetty hakumekanismi, joko NYSIIS-haku tai täsmähaku.

5. Jos osapuoli päättää kirjata ICDL-ilmoituksia, ilmoitukseen sisältyvät NYSIIS-avaimet kirjataan osana ICDL-tietoja. ICDL-tietoja hakiessaan osapuolen on käytettävä hakijan nimen NYSIIS-avaimia.

Alalisäys 4.5

Turvallisuusvaatimukset

1. Solmupisteen ja kansallisten järjestelmien välisten viestien vaihtoon käytetään https-protokollaa.

2. Kansallisten järjestelmien on suojattava kansallisen järjestelmän ja solmupisteen väliset viestit alalisäyksissä 4.8 ja 4.9 tarkoitetuilla sähköisillä varmenteilla.

3. Kansallisten järjestelmien on käytettävä vähintään varmenteita, joissa allekirjoittamiseen käytetään SHA-2 (SHA-256) -algoritmia ja 2048-bittistä julkista avainta.

Alalisäys 4.6

Palvelutasot

1. Kansallisten järjestelmien on oltava vähintään seuraavalla palvelutasolla:

1.1. Ne ovat käytettävissä 24 tuntia vuorokaudessa jokaisena viikonpäivänä.

1.2. Niiden käytettävyyttä valvotaan solmupisteestä tulevalla heartbeat-viestillä.

1.3. Niiden käytettävyysaste on 98 prosenttia seuraavan taulukon mukaisesti (luvut on pyöristetty lähimpään sopivaan yksikköön):

Käytettävyyden ollessa	järjestelmä on poissa käytössä		
	viikoittain	kuukausittain	vuosittain
98 %	0,5 tuntia	15 tuntia	7,5 päivää

Osapuolia kannustetaan noudattamaan päivittäistä käytettävyysastetta, mutta on kuitenkin huomattava, että tietyt välttämättömät toimet, kuten järjestelmän ylläpito, edellyttävät yli 30 minuutin toimintakatkoa. Kuukausittainen ja vuosittainen käytettävyysaste pysyvät pakollisina.

1.4. Ne vastaavat vähintään 98 prosenttiin niille kalenterikuukauden aikana toimitetuista pyynnöistä.

1.5. Ne reagoivat pyyntöihin 10 sekunnin kuluessa.

1.6. Pyynnön aikakatkaisu (aika, jonka pyynnön esittäjä voi odottaa vastausta) on enintään 20 sekuntia.

1.7. Pyyntöjen esittämistiheys voi olla 6 viestiä sekunnissa.

1.8. Kansalliset järjestelmät eivät voi lähettää TACHOnet-solmupisteeseen yli 2 pyyntöä sekunnissa.

1.9. Jokaisen kansallisen järjestelmän on kyettävä selviytymään mahdollisista solmupisteessä ja muiden osapuolten kansallisissa järjestelmissä esiintyvistä teknisistä ongelmista. Näitä ovat muun muassa seuraavat:

a) yhteyden katkeaminen solmupisteeseen;

b) vastauksen jääminen saamatta pyyntöön;

c) vastauksien tuleminen pyynnön aikakatkaisun jälkeen;

d) ei-toivottujen viestien vastaanottaminen;

e) virheellisten viestien vastaanottaminen.

2. Solmupisteen on:

2.1. oltava käytettävissä 98 prosentin käytettävyysasteella;

2.2. annettava kansallisille järjestelmille ilmoitukset mahdollisista virheistä joko vastausviestillä tai erityisellä virheilmoituksella. Nämä virheilmoitukset vastaanotetaan kansallisissa järjestelmissä, joissa on käytössä eskaloiva työnkulku asianmukaisiin toimiin ryhtymiseksi ilmoitetun virheen korjaamista varten.

3. Huolto

Osapuolten on ilmoitettava muille osapuolille ja Euroopan komissiolle kaikesta rutiinihuollosta verkkosovelluksen välityksellä vähintään viikkoa ennen ylläpidon alkamista, jos se on teknisesti mahdollista.

Alalisäys 4.7

Solmupisteessä kerättävien tietojen tilastointi ja lokitiedot

1. Tilastointitarkoituksiin käytettävän tiedon on yksityisyyden suojan varmistamiseksi oltava anonyymiä. Yksittäisten korttien, kuljettajien tai ajokorttien tunnistetietoja ei saa käyttää tilastollisiin tarkoituksiin.

2. Lokitiedoissa on pidettävä kirjaa kaikista järjestelmän käyttötapahtumista seurantaa ja ohjelmistovirheiden korjaamista varten ja jotta tapahtumista voidaan laatia tilastoja.

3. Henkilötietoja saa säilyttää lokeissa enintään 6 kuukauden ajan. Tilastotiedot on säilytettävä toistaiseksi.

4. Raportointiin käytettäviin tilastotietoihin sisältyvät seuraavat:

   a) pyytävä osapuoli;

   b) vastaava osapuoli;

   c) viestin tyyppi;

   d) vastauksen tilakoodi;

   e) viestien päivämäärä ja kellonaika;

   f) vastausaika.

Alalisäys 4.8

TACHOnet-järjestelmässä käytettäviä digitaalisia avaimia ja sähköisiä varmenteita koskevat yleiset säännökset

1. Komission tietotekniikan pääosasto (DIGIT) antaa TACHOnet-järjestelmään liittyvien AETR-sopimuspuolten käyttöön julkisen avaimen menetelmään (PKI) perustuvan palvelun[1] ('CEF PKI -palvelu') sähköisen jakelupalvelun (eDelivery) kautta.

2. Sähköisten varmenteiden pyytämisessä ja peruuttamisessa käytettävä menetelmä sekä sen käyttöä koskevat yksityiskohtaiset ehdot esitetään lisäyksessä.

3. Varmenteiden käyttö

3.1. Kun varmenne on myönnetty, kansallinen viranomainen[2] saa käyttää sitä pelkästään TACHOnet-järjestelmän yhteydessä. Varmennetta voidaan käyttää

a) tietojen alkuperän todentamiseen;

b) tietojen salaamiseen;

c) varmistamaan, että tietojen eheyteen vaikuttavat tietoturvaloukkaukset havaitaan.

3.2. Kaikki sellainen varmenteen käyttö, joka ei ole erikseen sallittua sallittujen käyttötarkoitusten yhteydessä, on kiellettyä.

4. Sopimuspuolten on

a) suojattava yksityistä avaintaan luvattomalta käytöltä;

b) pidättäydyttävä siirtämästä tai paljastamasta yksityistä avaintaan kolmansille osapuolille, edes edustajina;

---

1 Julkisen avaimen menetelmä on kokoelma tehtäviä, toimintatapoja, menettelyjä ja järjestelmiä, jotka ovat tarpeen sähköisten varmenteiden luomiseksi, hallinnoimiseksi, jakamiseksi ja peruuttamiseksi.

2 Kansallisen viranomaisen tunnistaa myönnetyn varmenteen DN-nimessä olevan attribuutin "O=" arvosta.

c) varmistettava TACHOnet-järjestelmää varten luotujen, tallennettujen ja käytettyjen yksityisten avainten luottamuksellisuus, eheys ja saatavuus;

d) pidättäydyttävä yksityisen avaimen käytön jatkamisesta varmenteen voimassaoloajan päätyttyä tai varmenteen peruuttamisen jälkeen muuta tarkoitusta kuin salattujen tietojen katselua varten (esim. sähköpostien salauksen purku). Avaimet, joiden voimassaolo on päättynyt, on joko tuhottava tai niitä on säilytettävä siten, että niiden käyttö voidaan estää;

e) ilmoitettava rekisteröintiviranomaiselle niiden valtuutettujen edustajien henkilöllisyydet, joilla on lupa pyytää organisaatiolle myönnettyjen varmenteiden peruuttamista (peruuttamispyynnöissä on esitettävä asianomainen salasana ja tarkat tiedot peruuttamiseen johtaneista syistä);

f) estettävä yksityisen avaimen väärinkäyttö pyytämällä niihin liittyvän julkisen avaimen varmenteen peruuttamista, mikäli yksityinen avain tai sitä koskevat aktivointitiedot ovat vaarantuneet;

g) oltava vastuussa ja noudatettava velvollisuutta pyytää varmenteen peruuttamista varmenneviranomaisen varmennepolitiikoissa ja varmennuskäytännössä (CPS) määritellyissä olosuhteissa;

h) ilmoitettava rekisteröintiviranomaiselle viipymättä TACHOnet-järjestelmän yhteydessä käytettävien AETR-avainten katoamisesta, varkaudesta tai mahdollisesta vaarantumisesta.

5. Vastuu

Rajoittamatta Euroopan komission vastuuta vastoin sovellettavan kansallisen lain vaatimuksia tai poistaa komission vastuuta seikoista, joiden osalta vastuuta ei sovellettavan kansallisen lain mukaan voida poistaa, Euroopan komissio ei ole vastuussa

a) varmenteen sisällöstä, sillä siitä vastaa yksinomaan varmenteen haltija. Varmenteen haltijan velvollisuus on tarkistaa, että varmenteen sisältö pitää paikkansa;

b) siitä, miten varmenteen haltija käyttää varmennetta.

Alalisäys 4.9

TACHOnet-järjestelmässä käytettävän, julkisen avaimen menetelmään perustuvan palvelun kuvaus

1. Johdanto

Julkisen avaimen menetelmä on kokoelma tehtäviä, toimintatapoja, menettelyjä ja järjestelmiä, jotka ovat tarpeen sähköisten varmenteiden luomiseksi, hallinnoimiseksi, jakamiseksi ja peruuttamiseksi.[3] Sähköisen jakelupalvelun CEF PKI -palvelu mahdollistaa sellaisten sähköisten varmenteiden myöntämisen ja hallinnoinnin, joiden avulla varmistetaan liityntäpisteiden välillä vaihdettavien tietojen luottamuksellisuus, eheys ja kiistämättömyys.

Sähköisen jakelupalvelun (eDelivery) PKI-palvelu perustuu varmenneviranomaisena toimivan TeleSec Shared Business CA:n tarjoamiin valvontakeskuspalveluihin (Trust Center), joihin sovelletaan yrityksen T-Systems International GmbH[4] varmenneviranomaisen (TeleSec Shared-Business-CA) varmennepolitiikkaa ja varmennuskäytäntöä.

PKI-palvelu myöntää varmenteita, jotka soveltuvat erilaisten liiketoimintaprosessien turvaamiseen yritysten, organisaatioiden, viranomaisten ja instituutioiden sisällä ja ulkopuolella silloin, kun on todistettava loppukäyttäjän aitous, eheys ja luotettavuus ja tavoitteena on keskimääräinen turvallisuustaso.

2. Varmenteen pyytämismenettely

2.1. Tehtävät ja vastuualueet

2.1.1. Varmennetta pyytävä "organisaatio" tai "kansallinen viranomainen"

2.1.1.1. Kansallisen viranomaisen on pyydettävä varmenteita TACHOnet-hankkeen yhteydessä.

2.1.1.2. Kansallisen viranomaisen on

a) pyydettävä varmenteita CEF PKI -palvelulta;

---

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

4 Varmennepolitiikan ja varmennuskäytännön uusimman version voi ladata osoitteesta https://www.telesec.de/en/sbca-en/support/download-area/

b) luotava yksityiset avaimet ja vastaavat julkiset avaimet, jotka on sisällytettävä varmenneviranomaisen myöntämiin varmenteisiin;

c) ladattava varmenne sen jälkeen kun se on hyväksytty;

d) allekirjoitettava ja lähetettävä takaisin rekisteröintiviranomaiselle

i) yhteyshenkilöille ja luotetuille kuriireille tarkoitettu yksilöintilomake,

ii) allekirjoitettu valtakirja[5].

2.1.2. Luotettu kuriiri

2.1.2.1. Kansallinen viranomainen nimittää luotetun kuriirin.

2.1.2.2. Luotetun kuriirin on

a) luovutettava julkinen avain rekisteröintiviranomaiselle henkilökohtaisen tunnistus- ja rekisteröintiprosessin aikana;

b) saatava vastaava varmenne rekisteröintiviranomaiselta.

2.1.3. Verkkotunnuksen omistaja

2.1.3.1. Verkkotunnuksen omistaja on liikenteen ja liikkumisen pääosasto.

2.1.3.2. Verkkotunnuksen omistajan on

a) validoitava ja koordinoitava TACHOnet-järjestelmää ja sen turva-arkkitehtuuria, varmenteiden myöntämismenettelyjen validointi mukaan luettuna;

b) vastattava TACHOnet-järjestelmän solmupisteen toiminnasta ja koordinoitava osapuolten toimia, jotka koskevat TACHOnet-järjestelmän toimintaa;

c) tehtävä kansallisten viranomaisten ohella testejä, jotka koskevat liittymistä TACHOnet-järjestelmään.

[5] Valtakirja on oikeudellinen asiakirja, jolla organisaatio valtuuttaa Euroopan komission, jota edustaa CEF PKI -palvelusta vastaava nimeltä mainittu virkamies, pyytämään puolestaan varmenteen luomista T-Systems International GmbH:n varmenneviranomaiselta TeleSec Shared Business CA:lta. Ks. myös 6 kohta.

2.1.4. Rekisteröintiviranomainen

2.1.4.1. Rekisteröintiviranomaisena toimii Yhteinen tutkimuskeskus (JRC).

2.1.4.2. Rekisteröintiviranomainen on vastuussa luotetun kuriirin henkilöllisyyden tarkistamisesta sekä sähköisten varmenteiden myöntämistä, peruuttamista ja uusimista koskevien pyyntöjen kirjaamisesta ja hyväksymisestä.

2.1.4.3. Rekisteröintiviranomaisen on

a) annettava kansalliselle viranomaiselle yksilöllinen tunniste;

b) todennettava kansallisen viranomaisen, sen yhteyspisteiden ja luotettujen kuriirien henkilöllisyys;

c) viestittävä Verkkojen Eurooppa -välineen tukipalvelun (jäljempänä 'CEF-tukitiimi') kanssa kansallisen viranomaisen, sen yhteyspisteiden ja luotettujen kuriirien aitoudesta;

d) ilmoitettava kansalliselle viranomaiselle varmenteen hyväksymisestä tai hylkäämisestä.

2.1.5. Varmenneviranomainen

2.1.5.1. Varmenneviranomainen on vastuussa sähköisten varmenteiden pyytämistä, myöntämistä ja peruuttamista koskevan teknisen infrastruktuurin tarjoamisesta.

2.1.5.2. Varmenneviranomaisen on

a) tarjottava tekninen infrastruktuuri kansallisten viranomaisten varmennepyyntöjä varten;

b) validoitava tai hylättävä varmennepyyntö;

c) viestittävä tarvittaessa rekisteröintiviranomaisen kanssa pyytävän organisaation identiteetin tarkistamiseksi.

2.2. Varmenteen myöntäminen

2.2.1. Varmenne myönnetään noudattaen seuraavia kuviossa 1 esitettyjä vaiheita, jotka on suoritettava järjestyksessä.

a) Vaihe 1: luotetun kuriirin tunnistaminen

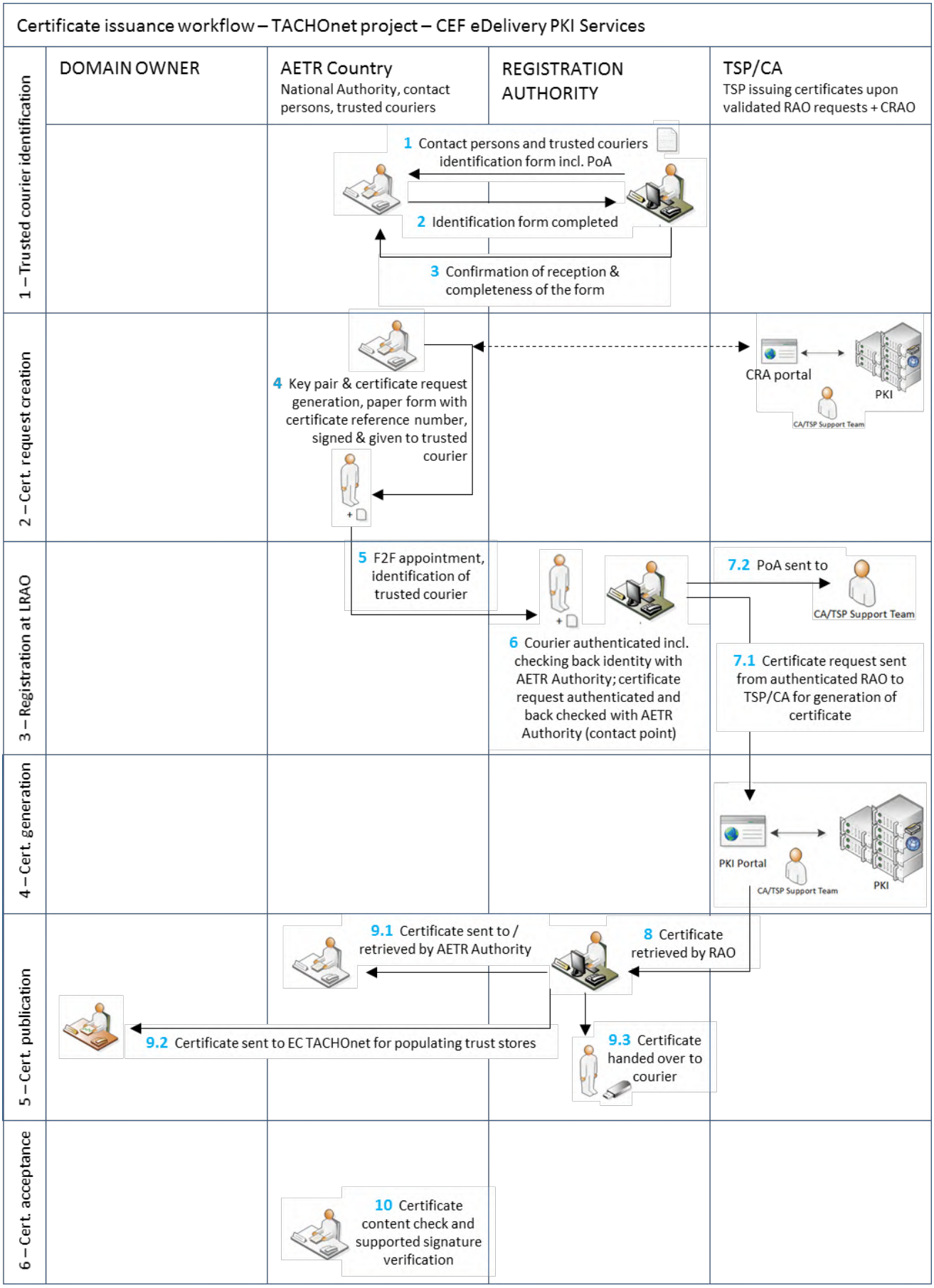
b) **Vaihe 2: varmennepyynnön luominen**

c) Vaihe 3: rekisteröintiviranomaisen suorittama rekisteröiminen

d) Vaihe 4: varmenteen luominen

e) Vaihe 5: varmenteen julkaiseminen

f) Vaihe 6: varmenteen hyväksyminen.



Kuvio 1 – Varmenteen myöntäminen (työnkulku)

2.2.2. Vaihe 1: Luotetun kuriirin tunnistaminen

Luotetun kuriirin tunnistamisessa on noudatettava seuraavaa menettelyä:

a) Rekisteröintiviranomainen lähettää kansalliselle viranomaiselle yhteyshenkilöiden ja luotettujen kuriirien yksilöintilomakkeen[6]. Lomakkeeseen on sisällyttävä myös valtakirja, joka organisaation (AETR-viranomaisen) on allekirjoitettava.

b) Kansallisen viranomaisen on lähetettävä täytetty lomake ja allekirjoitettu valtakirja takaisin rekisteröintiviranomaiselle.

c) Rekisteröintiviranomaisen on vahvistettava, että se on vastaanottanut lomakkeen ja että lomake on täydellinen.

d) Rekisteröintiviranomaisen on toimitettava päivitetty jäljennös yhteyshenkilöiden ja luotettujen kuriirien luettelosta verkkotunnuksen omistajalle.

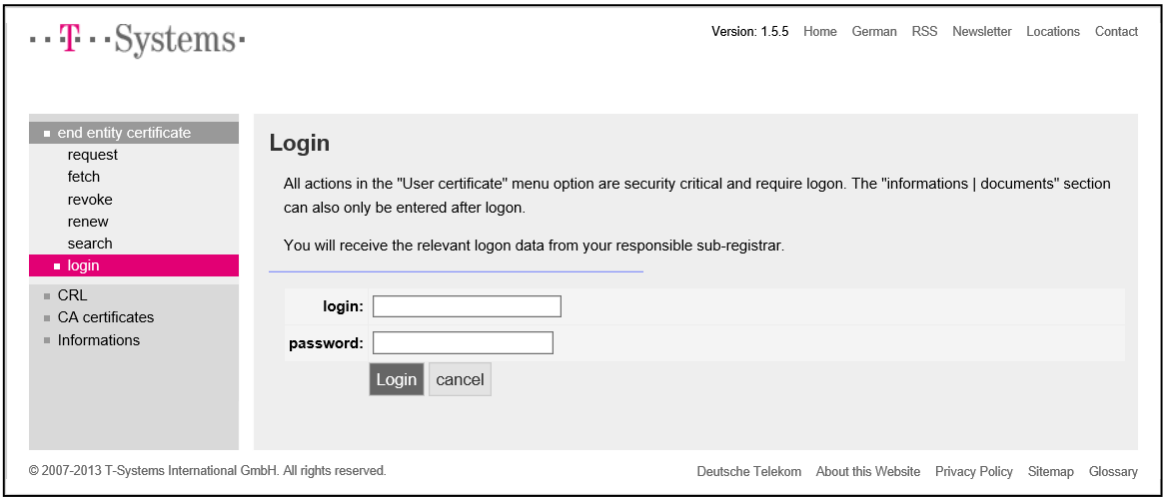
2.2.3. Vaihe 2: Varmennepyynnön luominen

2.2.3.1. Varmennetta on pyydettävä ja se on noudettava samaa tietokonetta ja samaa selainta käyttäen.

2.2.3.2. Varmennepyynnön luomisessa on noudatettava seuraavaa menettelyä:

a) Organisaation on pyydettävä varmennetta verkossa olevan käyttöliittymän kautta URL-osoitteessa https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: ja kirjoitettava sinne käyttäjänimi '**sbca/CEF_eDelivery.europa.eu'** ja salasana '**digit.333**'

[6] Ks. 5 kohta.

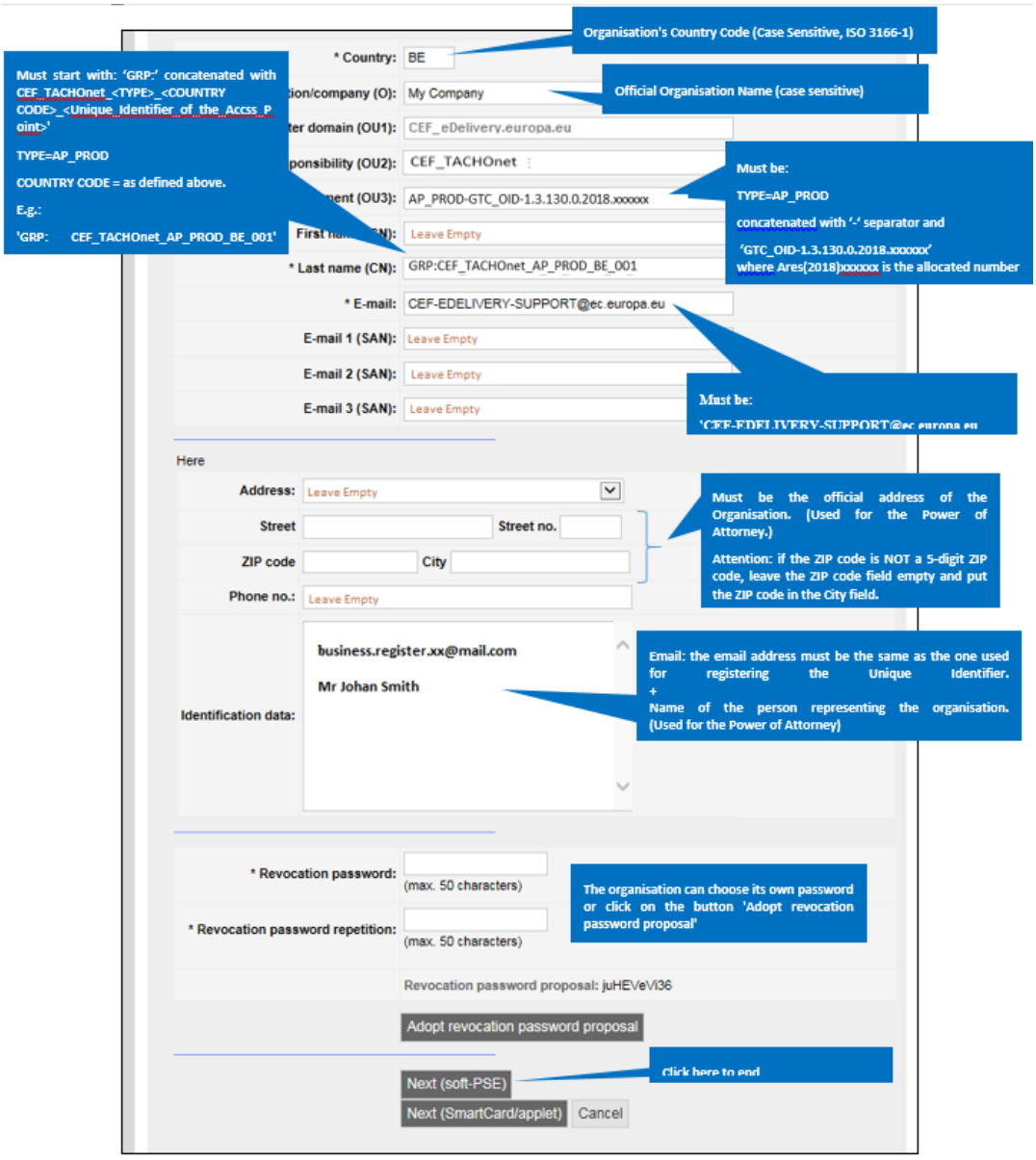


Kuvio 2

b) Organisaation on napsautettava näkymässä vasemmalla olevaa kohtaa 'request' (pyyntö) ja valittava pudotusvalikosta 'CEF_TACHOnet'.

Kuvio 3

c) Organisaation on täytettävä kuviossa 4 oleva varmennepyyntölomake taulukon 3 tiedoilla ja napsautettava kohtaa 'Next (soft-PSE)', kun lomake on valmis.


Organisation's Country Code (Case Sensitive, ISO 3166-1)
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'
* Country: BE
Official Organisation Name (case sensitive)
My Company
CEF_eDelivery.europa.eu
CEF_TACHOnet
AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
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
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
Must be:
Here
Address: Leave Empty
Street
Street no.
ZIP code
City
Phone no.: Leave Empty
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.
Identification data:
business.register.xx@mail.com
Mr Johan Smith
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)
* Revocation password:
(max. 50 characters)
* Revocation password repetition:
(max. 50 characters)
The organisation can choose its own password or click on the button 'Adopt revocation password proposal'
Revocation password proposal: juHEVeVi36
Adopt revocation password proposal
Next (soft-PSE)
Next (SmartCard/applet)
Cancel

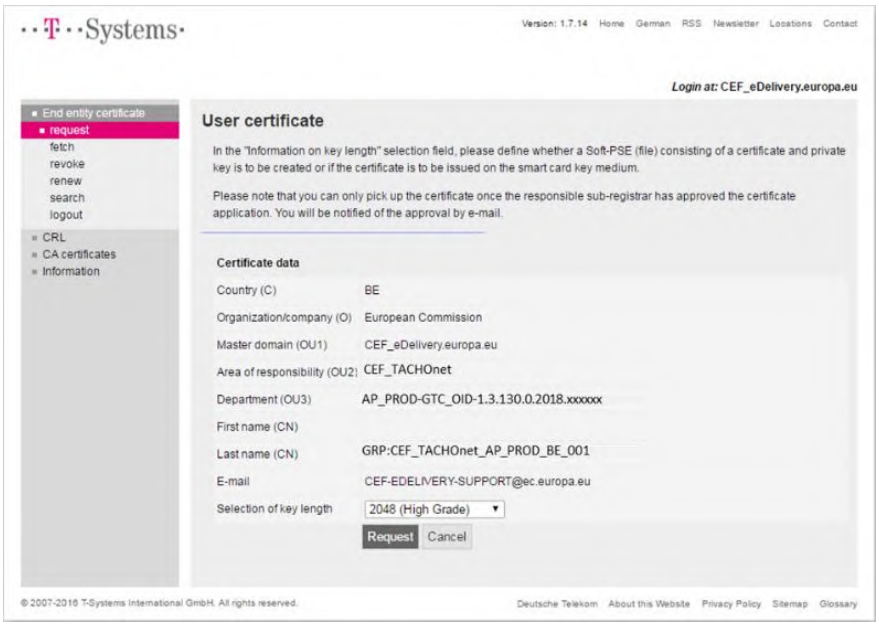
Kuvio 4

Pyydetyt kentät	Kuvaus
"Country" (Maa)	**C=maatunnus**; varmenteen haltijan sijainti, joka on varmennettu julkisen hakemiston avulla Rajoitukset: 2 merkkiä standardin ISO 3166-1, alpha-2 mukaisesti; aakkoskoon tunnistava; Esimerkkejä: DE, BE, NL Erityistapaukset: UK (Yhdistynyt kuningaskunta), EL (Kreikka)
"Organisation/Company" (Organisaatio/yhtiö) (O)	**O=Varmenteen haltijana toimivan organisaation nimi**
"Master domain" (OU1)	**OU=CEF_eDelivery.europa.eu**
"Area of responsibility" (OU2) (vastuualue)	**OU=CEF_TACHOnet**
"Department" (OU3) (yksikkö)	Pakollinen arvo, joka liittyy kohtaan "AREA OF RESPONSIBILITY". Sisältö on tarkistettava sallittujen yksiköiden luettelosta silloin kun varmennetta pyydetään. Jos tiedot eivät vastaa luetteloa, pyyntö estetään. Muoto: **OU=<TYPE>-<GTC_NUMBER>** jossa osan "<TYPE>" korvaa "AP_PROD": liityntäpiste tuotantoympäristössä ja jossa <GTC_NUMBER> on **GTC_OID-1.3.130.0.2018.xxxxxx**, jossa Ares(2018)xxxxxx on TACHOnet-hankkeen GTC-numero. Esim.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
"First name" (CN) (etunimi)	Jätettävä tyhjäksi
"Last name" (CN) sukunimi	Alkuun tulee lyhenne "GRP", jonka jälkeen lisätään yleisnimi. Muoto: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** Esim.: GRP:CEF_TACHOnet_AP_PROD_BE_001
"E-mail" (sähköposti)	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
"E-mail 1" (SAN)	Jätettävä tyhjäksi
"E-mail 2" (SAN)	Jätettävä tyhjäksi
"E-mail 3" (SAN)	Jätettävä tyhjäksi

"Address" (osoite)	Jätettävä tyhjäksi
"Street" (katu)	Varmenteen haltijana toimivan organisaation virallinen osoite (sama kuin valtakirjassa).
"Street no." (talon numero)	Varmenteen haltijana toimivan organisaation virallinen osoite (sama kuin valtakirjassa).
"Zip Code" (postinumero)	Varmenteen haltijana toimivan organisaation virallinen osoite (sama kuin valtakirjassa). **Huomio**: Jos postinumero EI ole viisinumeroinen, postinumerokenttä on jätettävä tyhjäksi ja postinumero on lisättävä kaupunkia koskevaan kenttään.
"City" (kaupunki)	Varmenteen haltijana toimivan organisaation virallinen osoite (sama kuin valtakirjassa). **Huomio**: Jos postinumero EI ole viisinumeroinen, postinumerokenttä on jätettävä tyhjäksi ja postinumero on lisättävä kaupunkia koskevaan kenttään.
"Phone no" (puhelinnumero)	Jätettävä tyhjäksi
"Identification data" (tunnistetiedot)	Sähköpostiosoitteen on oltava sama, jota on käytetty yksilöllisen tunnisteen kirjaamisessa. + Sen on oltava organisaatiota edustavan henkilön nimi (sama kuin valtakirjassa). + **Kaupparekisterinumero** (pakollinen vain yksityisten organisaatioiden kohdalla) **Merkitty seuraavan paikkakunnan paikallistuomioistuimeen:** (koskee vain saksalaisia ja itävaltalaisia yksityisiä organisaatioita)
"Revocation password" (peruuttamiseen vaadittava salasana)	Pakollinen kenttä, jonka arvon varmenteen pyytäjä itse valitsee
"Revocation password repetition" (toistetaan peruuttamiseen vaadittava salasana)	Toistettava pakollinen kenttä, jonka arvon varmenteen pyytäjä itse valitsee

Taulukko 3. Kunkin pyydetyn kentän täydelliset tiedot

d) Valittu avaimen pituus on 2048 bittiä (vahva salaus).



Kuvio 5

e) Organisaation on kirjattava muistiin viitenumero varmenteen noutamista varten.

Kuvio 6

f) CEF-tukitiimi tarkistaa, onko uusia varmennepyyntöjä esitetty ja pitävätkö varmennepyynnössä mainitut tiedot paikkansa, eli vastaavatko ne lisäyksessä 5.1 esitettyä varmenteiden nimeämiskäytäntöä.

g) CEF-tukitiimi tarkistaa, että pyynnössä olevat tiedot ovat oikeassa muodossa.

h) Jos joko 5 tai 6 kohdassa tarkoitetun tarkistuksen tulos on kielteinen, CEF-tukitiimin on lähetettävä varmennepyynnön kentässä "Identification data" ilmoitettuun sähköpostiosoitteeseen sähköpostiviesti, jossa organisaatiota pyydetään käynnistämään menettely uudelleen ja jossa viestin kopion vastaanottajiin lisätään verkkotunnuksen omistaja. Epäonnistunut varmennepyyntö peruutetaan.

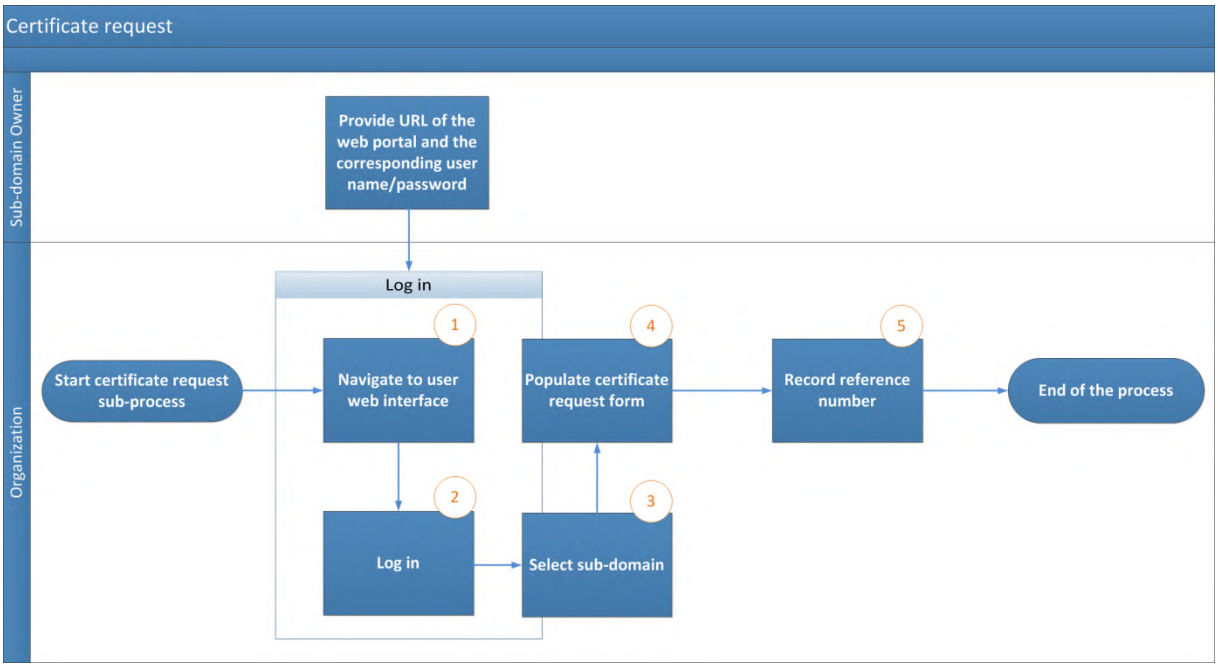
i) CEF-tukitiimi lähettää rekisteröintiviranomaiselle sähköpostiviestin siitä, onko pyyntö oikeassa muodossa. Sähköpostiviestin on sisällettävä

    1) organisaation nimi, joka mainitaan varmennepyynnön kentässä "Organisation (O)";

    2) varmenteen tiedot, mukaan lukien sen liityntäpisteen nimi, jota varten varmenne myönnetään; tämä on saatavilla varmennepyynnön kentässä "Last Name (CN)";

    3) varmenteen viitenumero;

    4) organisaation osoite, sähköpostiosoite ja organisaatiota edustavan henkilön nimi.



Kuvio 7 – Varmenteen pyytämismenettely

2.2.4. Vaihe 3: Rekisteröintiviranomaisen luona tapahtuva rekisteröinti (varmenteen hyväksyminen)

2.2.4.1. Luotettu kuriiri tai yhteyspiste sopii rekisteröintiviranomaisen kanssa sähköpostitse tapaamisen ja nimeää luotetun kuriirin, jonka on määrä osallistua henkilökohtaiseen tapaamiseen.

2.2.4.2. Organisaatio laatii asiakirjapaketin, johon sisältyy

a) täytetty ja allekirjoitettu valtakirja;

b) kopio henkilökohtaiseen tapaamiseen osallistuvan luotetun kuriirin voimassa olevasta passista. Kopiossa on oltava ainakin yhden vaiheessa 1 määritellyn organisaation yhteyspisteen allekirjoitus;

c) paperimuodossa oleva varmennepyyntö, jonka on allekirjoittanut yksi organisaation yhteyspisteistä.

2.2.4.3. Rekisteröintiviranomainen vastaanottaa luotetun kuriirin sen jälkeen, kun tämän henkilöllisyys on varmistettu rakennuksen vastaanotossa. Rekisteröintiviranomaisen on suoritettava varmennepyynnön rekisteröinti henkilökohtaisessa tapaamisessa

a) tunnistamalla ja todentamalla luotettu kuriiri;

b) tarkistamalla, että luotetun kuriirin ulkonäkö vastaa tämän esittämässä passissa olevaa kuvaa;

c) tarkistamalla, että luotetun kuriirin esittämä passi on voimassa;

d) tarkistamalla luotetun kuriirin esittämä voimassa oleva passi vertaamalla sitä luotetun kuriirin voimassa olevan passin kopioon, jonka yksi organisaation yhteyspisteistä on allekirjoittanut. Allekirjoitus todennetaan vertaamalla sitä alkuperäisessä luotettujen kuriirien ja yhteyshenkilöiden yksilöintilomakkeessa olevaan allekirjoitukseen;

e) tarkistamalla täytetty ja allekirjoitettu valtakirja;

f) tarkistamalla paperimuodossa oleva varmennepyyntö ja sen allekirjoitus vertaamalla sitä alkuperäiseen luotettujen kuriirien ja yhteyshenkilöiden yksilöintilomakkeeseen;

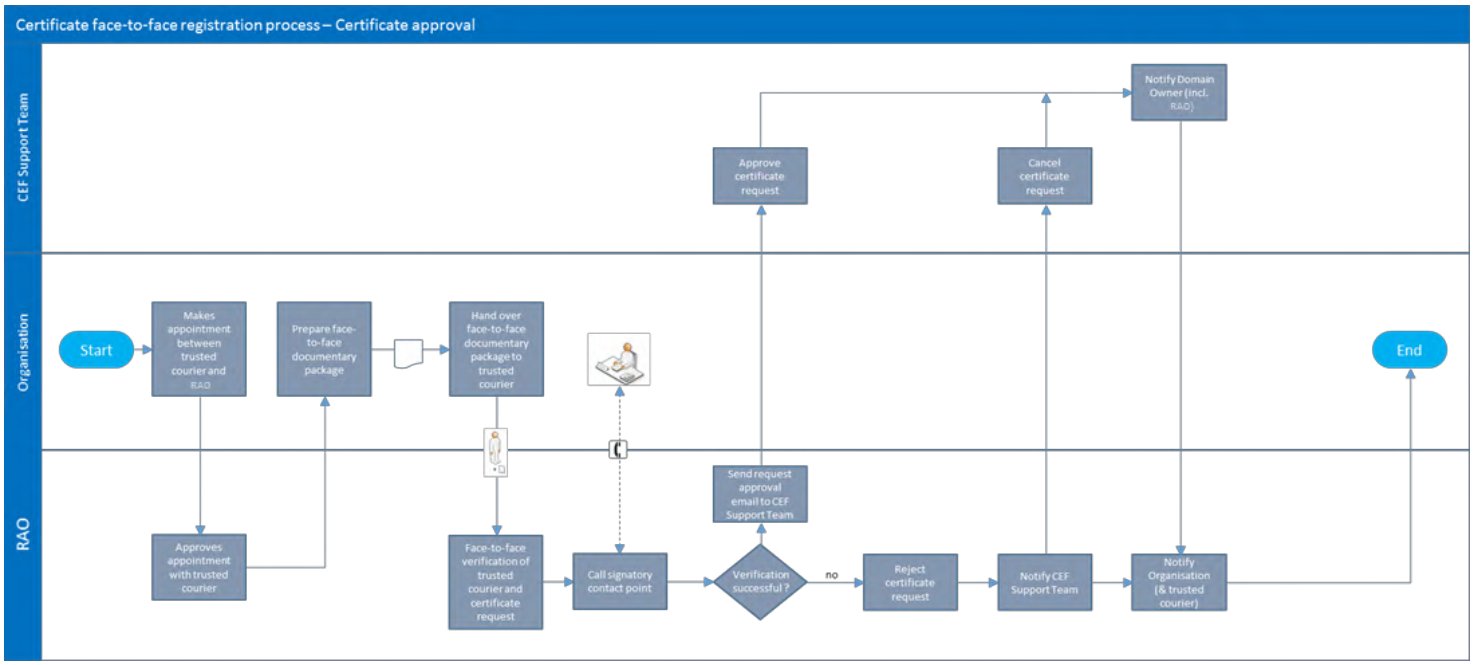
g) soittamalla allekirjoittajan yhteyspisteeseen luotetun kuriirin henkilöllisyyden ja varmennepyynnön sisällön tarkistamiseksi uudelleen.

2.2.4.4. Rekisteröintiviranomaisen on vahvistettava CEF-tukitiimille, että kansallisella viranomaisella on todella valtuudet käyttää niitä järjestelmän osia, joita varten varmenteita pyydetään, ja että pyyntöä vastaava henkilökohtainen rekisteröintimenettely on suoritettu onnistuneesti. Vahvistus on lähetettävä käyttäen "CommiSign"-varmenteella turvattua sähköpostia, johon on liitettävä skannattu kopio todennetusta henkilökohtaiseen tapaamiseen tarkoitetusta asiakirjapaketista ja allekirjoitetusta rekisteröintiviranomaisen suorittamassa menettelyssä käytetystä tarkistuslistasta.

2.2.4.5. Jos rekisteröintiviranomainen vahvistaa pyynnön aitouden, menettelyä jatketaan 2.2.4.6 ja 2.2.4.7 kohdan mukaisesti. Muutoin varmenteen myöntäminen hylätään ja asiasta ilmoitetaan organisaatiolle.

2.2.4.6. CEF-tukitiimi hyväksyy varmennepyynnön ja ilmoittaa rekisteröintiviranomaiselle varmenteen hyväksymisestä.

2.2.4.7. Rekisteröintiviranomainen ilmoittaa organisaatiolle, että varmenne on noudettavissa käyttäjäportaalin kautta.



Kuvio 8 – Varmenteen hyväksyminen

2.2.5. Vaihe 4: Varmenteen luominen

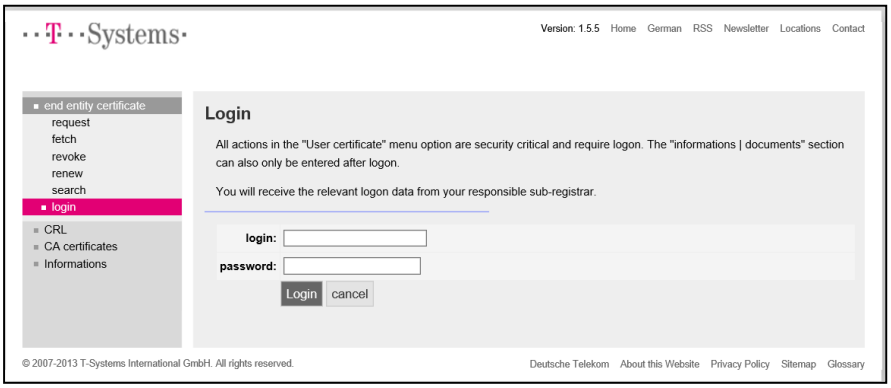
Varmenne luodaan heti, kun varmennepyyntö on hyväksytty.

2.2.6. Vaihe 5: Varmenteen julkaiseminen ja noutaminen

2.2.6.1. Kun varmennepyyntö on hyväksytty, rekisteröintiviranomaisen on noudettava varmenne ja annettava siitä kopio luotetulle kuriirille.

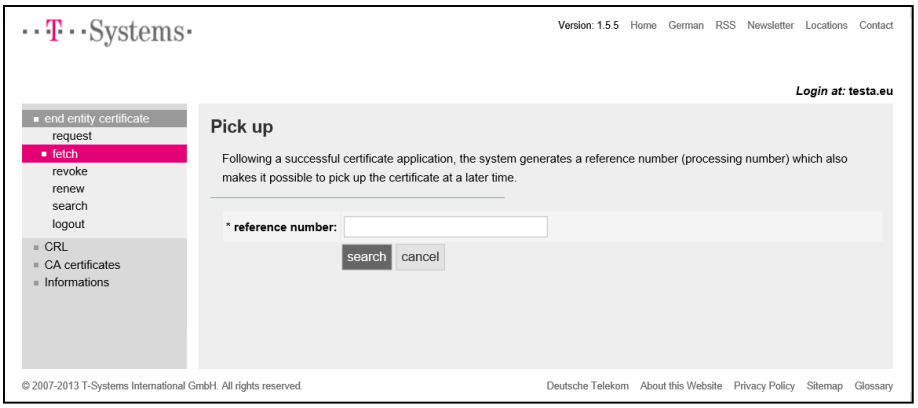
2.2.6.2. Rekisteröintiviranomaisen on ilmoitettava organisaatiolle, että varmenne on noudettavissa.

2.2.6.3. Organisaation on mentävä käyttäjäportaaliin osoitteessa https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en ja kirjauduttava sisään käyttäjänimellä "**sbca/CEF_eDelivery.europa.eu**" ja salasanalla "**digit.333**".



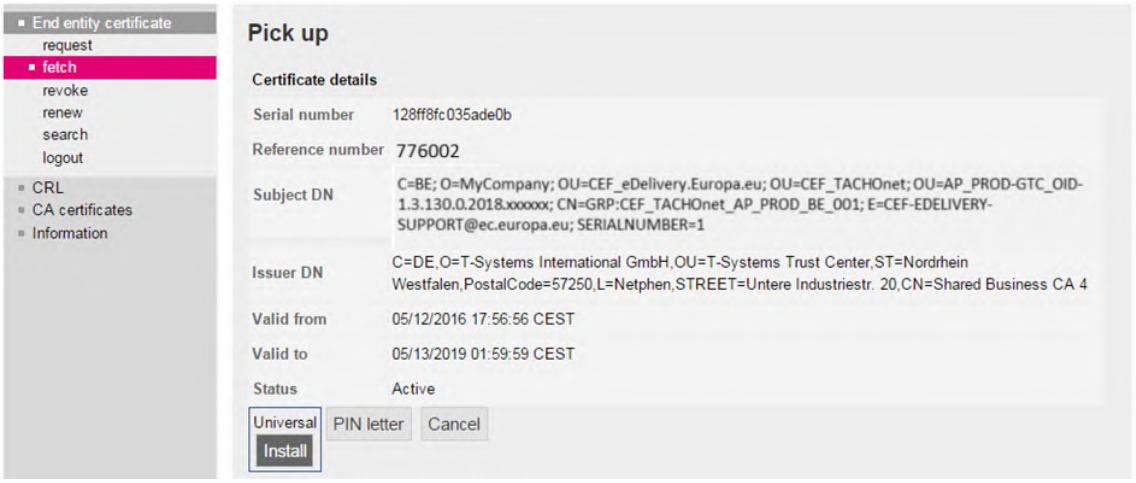
Kuvio 9

2.2.6.4. Organisaation on napsautettava vasemmalla olevaa painiketta "fetch" (hae) ja annettava varmenteen pyytämismenettelyn aikana muistiin kirjattu viitenumero.



Kuvio 10

2.2.6.5. Organisaation on asennettava varmenteet napsauttamalla painiketta "install" (asenna).



Kuvio 11

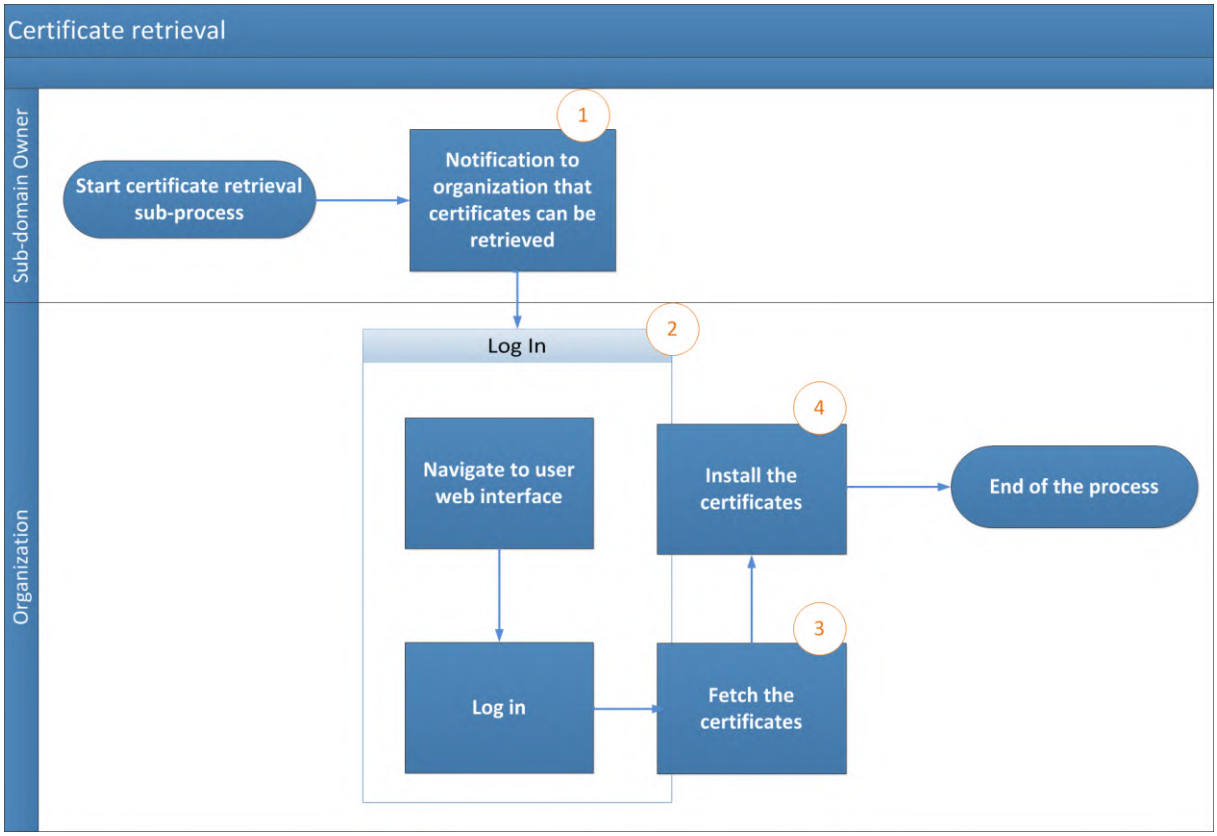
2.2.6.6. Varmenne on asennettava liityntäpisteeseen. Koska liityntäpiste on toteutuskohtainen, organisaation on otettava yhteyttä liityntäpisteen tarjoajaan saadakseen menettelyn kuvauksen.

2.2.6.7. Seuraavat vaihteet ovat tarpeen, jotta varmenne voidaan asentaa liityntäpisteeseen:

a) siirretään yksityinen avain ja varmenne,

b) luodaan keystore ja truststore,

c) asennetaan keystore ja truststore liityntäpisteeseen.

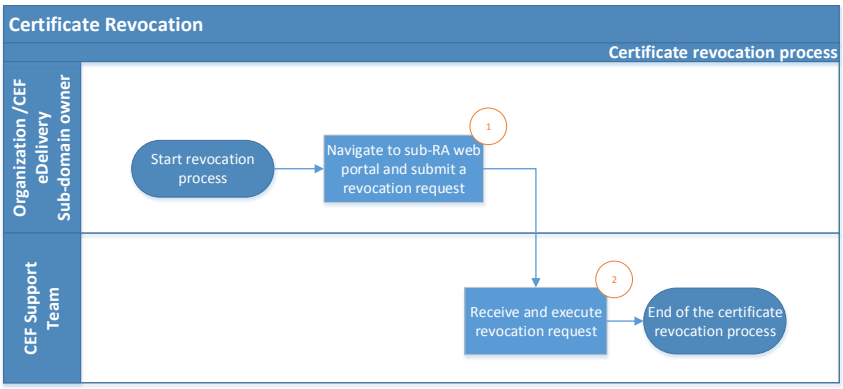


Kuvio 12 – Varmenteen noutaminen

3. Varmenteen peruuttamismenettely

3.1. Organisaation on esitettävä peruuttamispyyntö verkossa olevan käyttöliittymän kautta.

3.2. CEF-tukitiimin on toteutettava varmenteen peruuttaminen.



Kuvio 13 – Varmenteen peruuttaminen

4. CEF PKI -palvelun yleiset ehdot

4.1. Taustaa

Tietotekniikan pääosasto toimii Verkkojen Eurooppa -välineeseen kuuluvan sähköisen jakelupalvelun (eDelivery) ratkaisujen tarjoajana, ja sen tehtävänä on tarjota PKI-palvelu[7] (CEF PKI -palvelu) AETR-sopimuspuolille. CEF PKI -palvelua käyttävät TACHOnet-järjestelmään osallistuvat kansalliset viranomaiset (loppukäyttäjät).

Tietotekniikan pääosasto saa PKI-käyttäjäpalvelut TeleSec Shared-Business-CA:lta ('SBCA'), joka toimii T-Systems International GmbH:n ('T-Systems'[8]) valvontakeskuksessa. Pääosasto toimii SBCA:n verkkotunnuksen CEF_eDelivery.europa.eu päärekisterinpitäjänä. Tässä tehtävässä tietotekniikan pääosasto luo verkkotunnuksen CEF_eDelivery.europa.eu alle aliverkkotunnuksen kullekin hankkeelle, jossa käytetään CEF PKI -palvelua.

Tässä asiakirjassa esitetään TACHOnet-aliverkkotunnuksen ehdot. Tietotekniikan pääosasto toimii kyseisen aliverkkotunnuksen rekisterinpitäjänä. Tässä ominaisuudessa se myöntää, peruuttaa ja uusii hankkeeseen liittyviä varmenteita.

4.2. Vastuunrajoitus

Euroopan komissio ei ole vastuussa varmenteen sisällöstä, vaan sisällöstä vastaa yksinomaan varmenteen haltija. Varmenteen haltijan velvollisuus on tarkistaa, että varmenteen sisältö pitää paikkansa.

Euroopan komissio ei ole vastuussa siitä, miten varmenteen haltija käyttää varmennetta, sillä varmenteen haltija on Euroopan komission ulkopuolinen oikeushenkilö.

---

7 Julkisen avaimen menetelmä on kokoelma tehtäviä, toimintatapoja, menettelyjä ja järjestelmiä, jotka ovat tarpeen sähköisten varmenteiden luomiseksi, hallinnoimiseksi, jakamiseksi ja peruuttamiseksi.

8 T-Systemsin valvontakeskuksessa sijaitsevan valvontakeskusoperaattorin rooliin kuuluu myös toimia sisäisenä rekisteröintiviranomaisena.

Tämän vastuuvapauslausekkeen tarkoituksena ei ole rajoittaa Euroopan komission vastuuta vastoin sovellettavan kansallisen lain vaatimuksia tai poistaa komission vastuuta seikoista, joiden osalta vastuuta ei voida poistaa sovellettavan kansallisen lain mukaan.

4.3. Varmenteiden sallitut/kielletyt käyttötarkoitukset

4.3.1. Varmenteiden sallittu käyttö

Kun varmenne on myönnetty, varmenteen haltija[9] saa käyttää sitä pelkästään TACHOnet-järjestelmän yhteydessä. Varmennetta voidaan tässä yhteydessä käyttää

- tietojen alkuperän todentamiseen
- tietojen salaamiseen
- varmistamaan, että tietojen eheyteen vaikuttavat tietoturvaloukkaukset havaitaan.

4.3.2. Varmenteiden kielletty käyttö

Kaikki sellainen varmenteen käyttö, joka ei ole erikseen sallittua sallittujen käyttötarkoitusten yhteydessä, on kiellettyä.

4.4. Varmenteen haltijan muut velvoitteet

T-Systems määrittelee SBCA:n yksityiskohtaiset ehdot SBCA-palvelun varmennepolitiikassa/varmennuskäytännössä[10]. Kyseisessä asiakirjassa esitetään muun muassa turvallisuuseritelmät ja -ohjeet, jotka koskevat teknisiä ja organisaatioon liittyviä näkökohtia, ja kuvataan valvontakeskusoperaattorin toimintaa varmenneviranomaisena ja rekisteröintiviranomaisena sekä rekisteröintiviranomaisen valtuuttamaa kolmatta osapuolta.

Ainoastaan tahot, joilla on valtuudet osallistua TACHOnet-järjestelmään, voivat pyytää varmennetta.

---

9 Varmenteen haltijan tunnistaa myönnetyn varmenteen DN-nimessä olevan attribuutin "O=" arvosta.

10 T-Systemsin SBCA:n varmennepolitiikan/varmennuskäytännön uusin versio on saatavilla osoitteessa https://www.telesec.de/en/sbca-en/support/download-area/

Varmenteiden hyväksymisen osalta sovelletaan SBCA:n varmennepolitiikan/varmennuskäytännön 4.4.1 kohtaa, ja organisaation, jolle varmenne myönnetään ("O="), katsotaan hyväksyneen tässä asiakirjassa esitetyt ehdot ja määräykset silloin, kun varmennetta käytetään ensimmäistä kertaa.

Varmenteen julkaisemisen osalta sovelletaan SBCA:n varmennepolitiikan/varmennuskäytännön 2.2 kohtaa.

Kaikkien varmenteiden haltijoiden on täytettävä seuraavat vaatimukset:

1) Varmenteen haltijoiden on suojattava yksityistä avaintaan luvattomalta käytöltä.

2) Varmenteen haltijoiden on pidättäydyttävä siirtämästä tai paljastamasta yksityistä avaintaan kolmansille osapuolille, edes edustajina.

3) Varmenteen haltijoiden on pidättäydyttävä yksityisen avaimen käytön jatkamisesta varmenteen voimassaoloajan päätyttyä tai varmenteen peruuttamisen jälkeen muuta tarkoitusta kuin salattujen tietojen katselua varten (esim. sähköpostien salauksen purku).

4) Varmenteen haltija on vastuussa avaimen jäljentämisestä tai toimittamisesta loppukäyttäjälle (loppukäyttäjille).

5) Varmenteen haltijan on velvoitettava loppukäyttäjä / kaikki loppukäyttäjät noudattamaan näitä ehtoja, mukaan lukien SBCA:n varmennepolitiikkaa/varmennuskäytäntöä, kun ne käyttävät yksityistä avainta.

6) Varmenteen haltijan on huolehdittava niiden valtuutettujen edustajien tunnistamisesta, joilla on lupa pyytää organisaatiolle myönnettyjen varmenteiden peruuttamista esittämällä tarkat tiedot peruuttamiseen johtaneista syistä ja peruuttamista varten vaadittava salasana.

7) Silloin kun varmenteita on myönnetty henkilö- tai tehtäväryhmille ja/tai oikeushenkilöille ja joku henkilöistä poistuu loppukäyttäjien ryhmästä (esim. työsuhteen päättyessä), varmenteen haltijan on estettävä yksityisen avaimen väärinkäyttö peruuttamalla varmenne.

8) Varmenteen haltija on vastuussa varmenteen peruuttamispyynnön esittämisestä SBCA:n varmennepolitiikan/varmennuskäytännön 4.9.1 kohdassa tarkoitetuissa tapauksissa.

9) Varmenteen uusimisen tai varmenteen avaimen uusimisen osalta sovelletaan SBCA:n varmennepolitiikan/varmennuskäytännön 4.6 tai 4.7 kohtaa.

Varmenteen muuttamisen osalta sovelletaan SBCA:n varmennepolitiikan/varmennuskäytännön 4.8 kohtaa.

Varmenteen peruuttamisen osalta sovelletaan SBCA:n varmennepolitiikan/varmennuskäytännön 4.9 kohtaa.

5. Yhteyshenkilöille ja luotetuille kuriireille tarkoitettu yksilöintilomake (esimerkki)

Allekirjoittanut, *[organisaation edustajan nimi ja osoite]***, vakuuttaa, että seuraavia tietoja käytetään silloin kun pyydetään, luodaan ja noudetaan julkisen avaimen sähköisiä varmenteita TACHOnet-liityntäpisteitä varten TACHOnet-viestien luottamuksellisuuden, eheyden ja kiistämättömyyden varmistamiseksi:**

Yhteyshenkilöä koskevat tiedot:

Yhteyshenkilö 1	**Yhteyshenkilö 2**
Nimi:	Nimi:
Etunimi (etunimet):	Etunimi (etunimet):
Matkapuhelin:	Matkapuhelin:
Puhelin:	Puhelin:
Sähköposti:	Sähköposti:
Allekirjoitusnäyte:	Allekirjoitusnäyte:

Luotetun kuriirin tiedot:

Luotettu kuriiri 1	**Luotettu kuriiri 2**
Nimi:	Nimi:
Etunimi (etunimet):	Etunimi (etunimet):
Matkapuhelin:	Matkapuhelin:
Sähköposti:	Sähköposti:
Passin myöntänyt maa:	Passin myöntänyt maa:
Passin nro:	Passin nro:
Passin voimassaolo päättyy:	Passin voimassaolo päättyy:

Paikka ja aika sekä organisaation leima:

Valtuutetun edustajan allekirjoitus:

6. Asiakirjat

6.1. Valtakirja (esimerkki)

Seuraavassa on esimerkki valtakirjasta, joka luotetun kuriirin on allekirjoitettava ja esitettävä henkilökohtaisessa tapaamisessa rekisteröintiviranomaisen luona:

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. Paperimuodossa oleva varmennepyyntö (esimerkki)

Seuraavassa on esimerkki paperimuodossa olevasta varmennepyynnöstä, joka luotetun kuriirin on allekirjoitettava ja esitettävä henkilökohtaisessa tapaamisessa rekisteröintiviranomaisen luona:

7. Sanasto

Tässä alalisäyksessä käytetyt keskeiset termit määritellään Verkkojen Eurooppa -välineen digitaaliosion (CEF Digital) verkkoportaalin määritelmät käsittävässä osiossa:

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

Tässä komponenttien kuvauksessa käytetyt keskeiset lyhenteet määritellään CEF Digital -palvelun verkkoportaalin CEF-sanastossa:

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