



Eiropas Savienības
Padome

Briselē, 2018. gada 5. novembrī
(OR. en)

13711/18
ADD 1

Starpiestāžu lieta:
2018/0339(NLE)

TRANS 488

PIEZĪME

Sūtītājs:	Padomes Ģenerālsēkretariāts
Saņēmējs:	delegācijas
Iepri. dok. Nr.:	ST 13711/18 TRANS 448
K-jas dok. Nr.:	ST 12727/18 TRANS 426 + ADD 1
Temats:	Padomes Lēmums par nostāju, kas Eiropas Savienības vārdā jāieņem Apvienoto Nāciju Organizācijas Eiropas Ekonomikas komisijas Eiropas Nolīguma par transportlīdzekļu apkārpju darbu starptautiskajos autopārvadājumos ekspertu grupā

Pielikums minētajam Padomes Lēmumam.

Jauns *AETR* pielikums

4. papildinājums

***TACHOnet* specifikācijas**

1. Darbības joma un mērķis
 - 1.1. Šajā papildinājumā izklāstīti noteikumi un nosacījumi, kas attiecas uz *AETR* Līgumslēdzēju pušu savienojumu ar *TACHOnet*, izmantojot *eDelivery*.
 - 1.2. Līgumslēdzējas puses, kas veido savienojumu ar *TACHOnet*, izmantojot *eDelivery*, izpilda šajā papildinājumā izklāstītos noteikumus.
2. Definīcijas
 - (a) "Līgumslēdzēja puse" vai "puse" ir jebkura *AETR* Līgumslēdzēja puse;
 - (b) "*eDelivery*" ir Eiropas Komisijas izstrādāts pakalpojums, kas dod iespēju ar elektroniskiem līdzekļiem pārraidīt datus starp trešām personām, sniedz apliecinājumu par pārraidīto datu apstrādi, tostarp pierādījumu par datu nosūtīšanu un saņemšanu, un nodrošina pārraidīto datu aizsardzību pret jebkādas nesankcionētas sagrozīšanas risku;
 - (c) "*TACHOnet*" ir Regulas (ES) Nr. 165/2014 31. panta 2. punktā minētā sistēma, ar kuras palīdzību starp Līgumslēdzējām pusēm notiek elektroniska informācijas apmaiņa par vadītāja kartēm;
 - (d) "centrmezgls" ir informācijas sistēma, kas ļauj maršrutēt *TACHOnet* ziņojumus starp pieprasītāju pusi un atbildes sniedzēju pusi;
 - (e) "pieprasītāja puse" ir Līgumslēdzēja puse, kas izdod *TACHOnet* pieprasījumu vai paziņojumu, kuru pēc tam centrmezgls maršrutē, lai tas sasniegtu attiecīgo atbildes sniedzēju pusi;

- (f) "atbildes sniedzēja puse" ir Līgumslēdzēja puse, kurai *TACHOnet* pieprasījums vai paziņojums ir adresēts;
- (g) "kartes izdevējiestāde" vai "KII" ir struktūra, ko Līgumslēdzēja puse pilnvarojusi izdot un pārvaldīt tahogrāfa kartes.

3. Vispārēji pienākumi

- 3.1. Neviena Līgumslēdzēja puse nevar citas puses vārdā slēgt nolīgumus par piekļuvi *TACHOnet* vai jebkādā citā veidā pārstāvēt citu Līgumslēdzēju pusi, pamatojoties uz šo papildinājumu. Neviena Līgumslēdzēja puse nerīkojas kā citas Līgumslēdzējas puses apakšuzņēmēja šajā papildinājumā minētajās darbībās.
- 3.2. Līgumslēdzējas puses nodrošina piekļuvi savam valsts vadītāja karšu reģistram, izmantojot *TACHOnet*, 4.6. apakšpapildinājumā noteiktajā veidā un pakalpojuma līmenī.
- 3.3. Līgumslēdzējas puses nekavējoties paziņo cita citai par traucējumiem vai kļūdām, ko tās konstatējušas savā atbildības jomā un kas var apdraudēt *TACHOnet* normālu darbību.
- 3.4. Katra puse *AETR* Sekretariātam norāda kontaktpersonas saziņai par *TACHOnet*. Par visām kontaktpunktu izmaiņām *AETR* Sekretariātam paziņo rakstiski.

4. Testi savienojuma ar *TACHOnet* izveidei

- 4.1. Līgumslēdzējas puses savienojumu ar *TACHOnet* izveido pēc tam, kad saskaņā ar Eiropas Komisijas norādījumiem un tās uzraudzībā ir sekmīgi pabeigti savienojuma, integrācijas un veiktspējas testi.
- 4.2. Ja sākotnējie testi netiek izturēti, Eiropas Komisija testēšanas posmu drīkst uz laiku apturēt. Testus atsāk, kad Līgumslēdzēja puse ir Eiropas Komisijai paziņojusi, ka valsts līmenī ir pieņemti nepieciešamie tehniskie uzlabojumi, kas ļauj sekmīgi veikt sākotnējos testus.

- 4.3. Sākotnējo testu maksimālais ilgums ir seši mēneši.
5. Uzticamības arhitektūra
- 5.1. *TACHOnet* uzticamības arhitektūra nodrošina *TACHOnet* ziņojumu konfidencialitāti, integritāti un nenoliedzamību.
- 5.2. *TACHOnet* uzticamības arhitektūras pamatā ir publiskās atslēgas infrastruktūras (*PKI*) pakalpojums, ko izveidojusi Eiropas Komisija un kura prasības noteiktas 4.8. un 4.9. apakšpapildinājumā.
- 5.3. *TACHOnet* uzticamības arhitektūrā iesaistās šādi subjekti.
- a) Sertifikācijas iestāde, kas atbild par to digitālo sertifikātu ģenerēšanu, kurus reģistrācijas iestāde (ar tās norīkotu uzticamu kurjeru starpniecību) izsniedz Līgumslēdzēju pušu valsts iestādēm, kā arī par tehniskās infrastruktūras izveidi digitālo sertifikātu izdošanai, atsaukšanai un atjaunošanai.
 - b) Domēna īpašnieks, kas atbild par 4.1. apakšpapildinājumā minētā centrmezgla darbību un par *TACHOnet* uzticamības arhitektūras validēšanu un koordināciju.
 - c) Reģistrācijas iestāde, kas atbild par digitālo sertifikātu izdošanas, atsaukšanas un atjaunošanas pieprasījumu reģistrāciju un apstiprināšanu un par uzticamo kurjeru identitātes pārbaudi.
 - d) Uzticams kurjers ir valsts iestāžu norīkota persona, kas atbild par publiskās atslēgas nodošanu reģistrācijas iestādei un par attiecīgā sertifikācijas iestādes ģenerētā sertifikāta saņemšanu.
 - e) Līgumslēdzējas puses valsts iestāde, kas:
 - i) ģenerē privātās atslēgas un attiecīgās publiskās atslēgas, kas iekļaujamās sertifikācijas iestādes ģenerētajos sertifikātos;

- ii) pieprasa sertifikācijas iestādei digitālos sertifikātus;
- iii) norīko uzticamo kurjeru.

5.4. Sertifikācijas iestādi un reģistrācijas iestādi norīko Eiropas Komisija.

5.5. Lai varētu parakstīt un šifrēt *TACHOnet* ziņojumu, katrai Līgumslēdzējai pusei, kas veido savienojumu ar *TACHOnet*, jāpieprasa digitālais sertifikāts saskaņā ar 4.9. apakšpapildinājumu.

5.6. Sertifikātu var atsaukt saskaņā ar 4.9. apakšpapildinājumu.

6. Datu aizsardzība un konfidencialitāte

6.1. Puses atbilstīgi starptautiskajiem un valsts likumiem par datu aizsardzību un jo īpaši Konvencijai par personu aizsardzību attiecībā uz personas datu automātisko apstrādi veic visus tehniskos un organizatoriskos pasākumus nolūkā garantēt *TACHOnet* datu drošību un novērst šo datu sagrozīšanu vai zaudēšanu, to nesankcionētu apstrādi vai nesankcionētu piekļuvi tiem (jo sevišķi nodrošina autentiskumu, datu konfidencialitāti, izsekojamību, integritāti, pieejamību un nenoliedzamību un ziņojumu drošību).

6.2. Katra puse aizsargā savas valsts sistēmas pret neatļautu izmantošanu, ļaunkodu, vīrusiem, ielaušanos datorā, pārkāpumiem, nelikumīgām manipulācijām ar datiem un citām līdzīgām darbībām, ko veic trešās personas. Puses vienojas rīkoties komerciāli pamatoti, lai novērstu to, ka tiek pārsūtīti jebkādi vīrusi, laika bumbas, datortārpi vai līdzīgi elementi vai jebkādas datora rutīnprogrammas, kas var radīt traucējumus otras puses datorsistēmās.

7. Izmaksas

7.1. Līgumslēdzējas puses sedz izstrādes un darbības izmaksas, kas tām rodas saistībā ar pašu datu sistēmām un procedūrām un kas vajadzīgas, lai izpildītu šajā papildinājumā noteiktos pienākumus.

- 7.2. Šā papildinājuma 4.1. apakšpapildinājumā noteiktos pakalpojumus centrmezglis sniedz bez maksas.
8. Apakšuzņēmuma līguma slēgšana
- 8.1. Puses var slēgt apakšuzņēmuma līgumu attiecībā uz jebkuru pakalpojumu, par ko tā ir atbildīga saskaņā ar šo papildinājumu.
- 8.2. Šāda apakšuzņēmuma līguma slēgšana neatbrīvo pusi no šajā papildinājumā noteiktās atbildības, tostarp atbildības par attiecīgu pakalpojuma līmeni saskaņā ar 4.6. apakšpapildinājumu.

4.1. apakšpapildinājums

TACHOnet vispārīgie aspekti

1. Vispārīgs apraksts

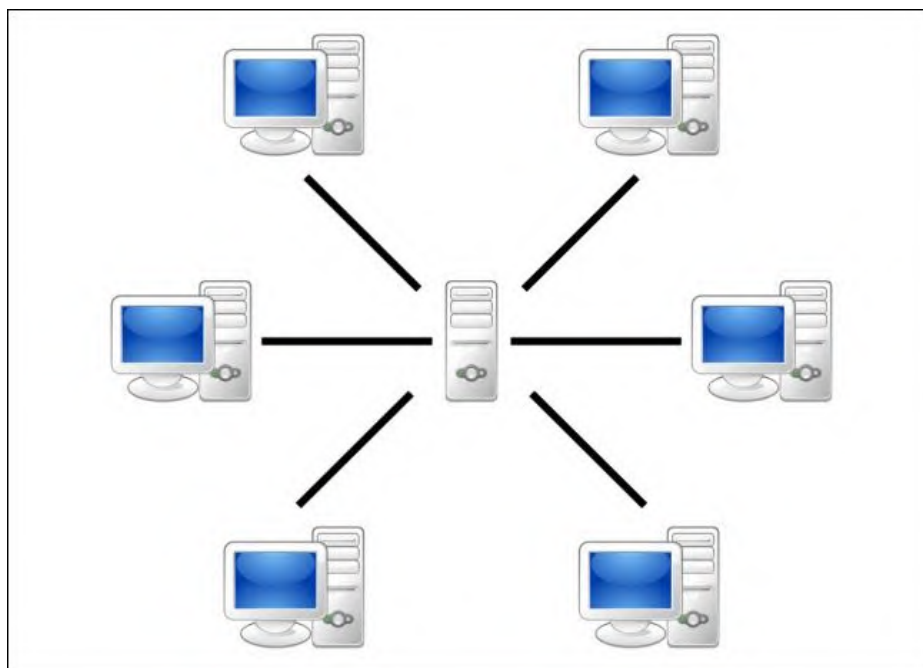
TACHOnet ir elektroniska sistēma, ar kuras palīdzību starp *AETR* Līgumslēdzējām pusēm notiek informācijas apmaiņa par vadītāja kartēm. *TACHOnet* maršrutē informācijas pieprasījumus no pieprasītājas puses atbildes sniedzējai pusei un atbildes pretējā virzienā. Līgumslēdzējām pusēm, kas ir *TACHOnet* dalībnieces, savi valsts vadītāja karšu reģistri jāsavieno ar sistēmu.

2. Arhitektūra

Ziņojumapmaiņas sistēma *TACHOnet* sastāv no šādām daļām.

2.1. Centrmezgls, kas spēj saņemt pieprasījumu no pieprasītājas puses, validēt un apstrādāt to, pārsūtot pieprasījumu atbildes sniedzējām pusēm. Centrmezgls sagaida katras atbildes sniedzējas puses atbildi, konsolidē visas atbildes un konsolidēto atbildi pārsūta pieprasītājai pusei.

2.2. Pušu valsts sistēmas, kas aprīkotas ar saskarni, kura spēj gan nosūtīt pieprasījumus centrmezglam, gan saņemt atbilstošās atbildes. Lai pārraidītu ziņojumus centrmezglam un saņemtu ziņojumus no centrmezgla, valstu sistēmas var izmantot īpašniekprogrammatūru vai komerciālu programmatūru.



- 3. Pārvaldība
 - 3.1. Centrmezglu pārvalda Eiropas Komisija, kas ir atbildīga par centrmezgla tehnisko darbību un uzturēšanu.
 - 3.2. Centrmezglā datus neglabā ilgāk kā sešus mēnešus, izņemot žurnālēšanas un statistikas datus, kas noteikti 4.7. apakšpapildinājumā.
 - 3.3. Centrmezgls nesniedz piekļuvi personas datiem, izņemot pilnvarotiem Eiropas Komisijas darbiniekiem, ja tas nepieciešams uzraudzībai, uzturēšanai un traucējummeklēšanai.
 - 3.4. Katras Līgumslēdzējas puses atbildībā ir šādi elementi.
 - 3.4.1. Savu valsts sistēmu, tostarp saskarnes ar centrmezglu, izveide un pārvaldība.
 - 3.4.2. Savas valsts sistēmas, proti, gan īpašnieka, gan komerciālas aparatūras un programmatūras, uzstādīšana un uzturēšana.
 - 3.4.3. Savas valsts sistēmas pareiza sadarbība ar centrmezglu, tostarp no centrmezgla saņemto kļūdas ziņojumu pārvaldība.
 - 3.4.4. Visu nepieciešamo pasākumu veikšana, lai nodrošinātu informācijas konfidencialitāti, integritāti un pieejamību.
 - 3.4.5. Valsts sistēmu darbība saskaņā ar pakalpojumu līmeni, kas noteikts 4.6. apakšpapildinājumā.

4.2. apakšpapildinājums

TACHOnet funkcijas

1. Ar ziņojumapmaiņas sistēmu *TACHOnet* nodrošina šādas funkcijas.
 - 1.1. "Check Issued Cards (CIC)" (izdoto karšu pārbaude): lai noteiktu, vai kartes pieteikuma iesniedzējam jau ir vadītāja karte, ko izdevusi kāda no atbildes sniedzējām pusēm, ļauj pieprasītājai pusei nosūtīt pieprasījumu "Check Issued Cards Request" vienai vai visām atbildes sniedzējām pusēm. Atbildes sniedzēja puse atbild uz pieprasījumu, nosūtot "Check Issued Cards Response".
 - 1.2. "Check Card Status (CCS)" (kartes statusa pārbaude): ļauj pieprasītājai pusei, nosūtot "Check Card Status Request", pieprasīt atbildes sniedzējai pusei sīkāku informāciju par atbildes sniedzējas puses izdotu karti. Atbildes sniedzēja puse atbild uz pieprasījumu, nosūtot "Check Card Status Response".
 - 1.3. "Modify Card Status (MCS)" (kartes statusa izmaiņas): ļauj pieprasītājai pusei ar pieprasījumu "Modify Card Status Request" informēt atbildes sniedzēju pusi par atbildes sniedzējas puses izdotās kartes statusa izmaiņām. Atbildes sniedzēja puse atbild ar apstiprinājumu "Modify Card Status Acknowledgement".
 - 1.4. "Issued Card Driving License (ICDL)" (kartes izdošana, pamatojoties uz vadītāja apliecību): ļauj pieprasītājai pusei ar pieprasījumu "Issued Card Driving Licence Request" informēt atbildes sniedzēju pusi par to, ka pieprasītāja puse ir izdevusi vadītāja karti, pamatojoties uz atbildes sniedzējas puses izdotu vadītāja apliecību. Atbildes sniedzēja puse atbild ar "Issued Card Driving Licence Response".
2. Iekļauj citus ziņojumu tipus, piemēram, kļūdas paziņojumus, ko uzskata par nepieciešamiem efektīvai *TACHOnet* darbībai.
3. Izmantojot jebkuru no 1. punktā aprakstītajām funkcijām, valstu sistēmas atpazīst kartes statusus, kas norādīti 1. tabulā. Taču pusēm nav jāīsteno administratīva procedūra, kas izmanto visus norādītos statusus.

4. Ja puse saņem atbildi vai paziņojumu, kurā norādīts statuss, ko tā neizmanto savās administratīvajās procedūrās, saņemtajā ziņojumā norādīto statusu valsts sistēma pārvērš par atbilstošu vērtību attiecīgajā procedūrā. Atbildes sniedzēja puse nenoraida ziņojumu, ja ziņojumā minētais statuss ir norādīts 1. tabulā.
5. Kartes statusu, kas norādīts 1. tabulā, neizmanto, lai noteiktu, vai vadītāja karte ir derīga transportlīdzekļa vadīšanai. Ja puse, izmantojot *CCS* funkciju, nosūta vaicājumu kartes izdevējas valsts iestādes reģistram, atbildē ietver īpašu lauku "valid for driving" (derīga transportlīdzekļa vadīšanai). Valsts administratīvās procedūras ir veidotas tā, ka *CCS* atbildēs vienmēr ir atbilstoša "valid for driving" vērtība.

1. tabula
Kartes statusi

Kartes statuss	Definīcija
"Application" (Pieteikums)	KII ir saņēmusi pieteikumu, kurā lūgts izdot vadītāja karti. Šī informācija ir reģistrēta un saglabāta datubāzē ar ģenerētajām meklēšanas atslēgām.
"Approved" (Apstiprināts)	KII ir apstiprinājusi pieteikumu, kurā lūgts izdot tahogrāfa karti.
"Rejected" (Noraidīts)	KII nav apstiprinājusi pieteikumu.
"Personalised" (Personalizēta)	Tahogrāfa karte ir personalizēta.
"Dispatched" (Nosūtīta)	Valsts iestāde ir nosūtījusi vadītāja karti attiecīgajam transportlīdzekļa vadītājam vai piegādātājam aģentūrai.
"Handed Over" (Nodota)	Valsts iestāde ir nodevusi vadītāja karti attiecīgajam transportlīdzekļa vadītājam.
"Confiscated" (Konfiscēta)	Kompetentā iestāde transportlīdzekļa vadītājam ir atņēmusi vadītāja karti.
"Suspended" (Apturēta)	Transportlīdzekļa vadītājam uz laiku ir atņemta vadītāja karte.
"Withdrawn" (Anulēta)	KII ir nolēmusi anulēt vadītāja karti. Karte ir neatgriezeniski padarīta par nederīgu.
"Surrendered" (Atdota)	Tahogrāfa karte ir atdota atpakaļ KII, un ir paziņots, ka tā vairs nav vajadzīga.
"Lost" (Pazaudēta)	KII ir paziņots, ka tahogrāfa karte ir pazaudēta.
"Stolen" (Nozagta)	KII ir paziņots, ka tahogrāfa karte ir nozagta. Nozagtu karti uzskata par pazaudētu.
"Malfunctioning" (Nedarbojas pareizi)	KII ir paziņots, ka tahogrāfa karte nedarbojas pareizi.
"Expired" (Beidzies termiņš)	Tahogrāfa kartes derīguma termiņš ir beidzies.
"Replaced" (Aizstāta)	Tahogrāfa karte, par kuru ir paziņots, ka tā ir pazaudēta, nozagta vai nedarbojas pareizi, ir aizstāta ar jaunu karti. Jaunās kartes dati ir tādi paši kā iepriekšējās kartes dati, izņemot kartes numura nomaiņas indeksu, kas ir par vienu vienību lielāks.

Kartes statuss	Definīcija
"Renewed" (Atjaunota)	Tahogrāfa karte ir atjaunota tāpēc, ka mainījušies administratīvie dati vai derīguma termiņš tuvojas beigām. Jaunās kartes numurs ir tāds pats kā iepriekšējās kartes numurs, izņemot kartes numura atjaunošanas indeksu, kas ir par vienu vienību lielāks.
"In Exchange" (Notiek apmaiņa)	Vadītāja karti izdevusī KII ir saņēmusi paziņojumu, ka ir sāкта procedūra, ar ko minēto karti apmaina pret citas puses KII izdotu vadītāja karti.
"Exchanged" (Apmainīta)	Vadītāja karti izdevusī KII ir saņēmusi paziņojumu, ka ir pabeigta procedūra, ar ko minēto karti apmaina pret citas puses KII izdotu vadītāja karti.

4.3. apakšpapildinājums

Noteikumi par *TACHOnet* ziņojumiem

1. Vispārīgās tehniskās prasības
 - 1.1. Centrmezgls nodrošina gan sinhronās, gan asinhronās saskarnes ziņojumapmaiņai. Puses var izvēlēties vispiemērotāko tehnoloģiju saskarnei ar savām lietojumprogrammām.
 - 1.2. Visus ziņojumus, ar kuriem notiek apmaiņa starp centrmezglu un valstu sistēmām, kodē *UTF-8* kodējumā.
 - 1.3. Valstu sistēmas spēj saņemt un apstrādāt ziņojumus, kas satur grieķu un kirilicas alfabēta rakstzīmes.
2. *XML* ziņojumu struktūra un shēmas definīcija (*XSD*)
 - 2.1. *XML* ziņojumu vispārējā struktūrā ievēro formātu, kas noteikts *XSD* shēmās, kuras instalētas centrmezglā.
 - 2.2. Centrmezgls un valstu sistēmas pārraida un saņem ziņojumus, kas atbilst ziņojuma *XSD* shēmai.
 - 2.3. Valstu sistēmas spēj nosūtīt, saņemt un apstrādāt visus ziņojumus, kas atbilst kādai no 4.2. apakšpapildinājumā noteiktajām funkcijām.
 - 2.4. *XML* ziņojumu saturs atbilst vismaz minimālajām prasībām, kas noteiktas 2. tabulā.

2. tabula

Minimālās prasības attiecībā uz XML ziņojumu saturu

Kopējā galvene		Obligāti
"Version" (Versija)	<i>XML</i> specifikāciju oficiālo versiju norāda, izmantojot nosaukumvietu, kas definēta ziņojuma <i>XSD</i> un ikviena <i>XML</i> ziņojuma galvenes elementa " <i>version</i> " atribūtā. Versijas numuru ("n.m") definē kā fiksētu vērtību katrā <i>XML</i> shēmas definīcijas datnes (<i>xsd</i>) laidienā.	Jā
"Test Identifier" (Testa identifikators)	Fakultatīvs identifikators testēšanai. Testa iniciators aizpilda identifikatoru, un visi darbplūsmas dalībnieki pārsūta/atsūta atpakaļ to pašu identifikatoru. Eksploatācijā to ignorē un, ja tas ir sniegts, to neizmanto.	Nē
"Technical Identifier" (Tehniskais identifikators)	Vispārēji unikāls identifikators (<i>UUID</i>), kas unikāli identificē katru atsevišķu ziņojumu. Sūtītājs ģenerē <i>UUID</i> un aizpilda šo atribūtu. Šos datus neizmanto komercdarbību veikšanai.	Jā
"Workflow Identifier" (Darbplūsmas identifikators)	Darbplūsmas identifikators ir <i>UUID</i> , un to ģenerē pieprasītāja puse. Pēc tam šo identifikatoru izmanto visos ziņojumos darbplūsmas korelēšanai.	Jā
"Sent At" (Nosūtīšanas laiks)	Ziņojuma nosūtīšanas datums un laiks (<i>UTC</i>).	Jā
"Timeout" (Noildze)	Šis ir fakultatīvs datuma un laika (<i>UTC</i> formātā) atribūts. Šo vērtību iestata tikai centrmezgls pārsūtītiem pieprasījumiem. Tā informē atbildes sniedzēju pusi par pieprasījuma noildzes iestāšanās laiku. Šo vērtību neprasa "MS2TCN_<x>_Req", un atbildes ziņojumos to neizmanto. Tā ir fakultatīva tālab, lai vienu un to pašu galvenes definīciju varētu izmantot visiem ziņojumu veidiem neatkarīgi no tā, vai ir prasīts "timeoutValue" atribūts.	Nē
"From" (Sūtītājs)	Ziņojuma sūtītājas puses ISO 3166-1 <i>Alpha 2</i> kods vai "EU".	Jā
"To" (Saņēmējs)	Ziņojuma saņēmējas puses ISO 3166-1 <i>Alpha 2</i> kods vai "EU".	Jā

4.4. apakšpapildinājums

Transliterācija un *NYSIIS* (*New York State Identification and Intelligence System*) pakalpojumi

1. Visu transportlīdzekļa vadītāju vārdu un uzvārdu kodēšanai valsts reģistrā izmanto centrmezglā *NYSIIS* algoritmu.
2. Meklējot karti ar *CIC* funkciju, kā galveno meklēšanas mehānismu izmanto *NYSIIS* atslēgas.
3. Turklāt puses var izmantot pielāgotu algoritmu papildu rezultātu gūšanai.
4. Meklēšanas rezultātos norāda meklēšanas mehānismu (*NYSIIS* vai pielāgots algoritms), kas tika izmantots, lai atrastu ierakstu.
5. Ja puse izvēlas reģistrēt *ICDL* paziņojumus, tad paziņojumā ietvertās *NYSIIS* atslēgas reģistrē kā daļu no *ICDL* datiem. Veicot meklēšanu *ICDL* datos, puse izmanto pieteikuma iesniedzēja vārda un uzvārda *NYSIIS* atslēgas.

4.5. apakšpapildinājums

Drošības prasības

1. Ziņojumapmaiņai starp centrmezglu un valstu sistēmām izmanto *HTTPS*.
2. Lai droši pārraidītu ziņojumus starp valsts sistēmu un centrmezglu, valstu sistēmas izmanto 4.8. un 4.9. apakšpapildinājumā minētos digitālos sertifikātus.
3. Valstu sistēmas piemēro vismaz sertifikātus, kuri izmanto *SHA-2 (SHA-256)* paraksta jaucējalgoritmu (*signature hash algorithm*), un 2048 bitu publiskās atslēgas garumu.

4.6. apakšpapildinājums

Pakalpojumu līmenis

1. Valstu sistēmas nodrošina šādu minimālo pakalpojumu līmeni.
- 1.1. Tās ir izmantojamas 24 stundas diennaktī, 7 dienas nedēļā.
- 1.2. To izmantojamību uzrauga ar periodisko kontrolziņojumu, ko sniedz centrmezglis.
- 1.3. To izmantojamības rādītājs ir 98 % saskaņā ar turpmāko tabulu (skaitļi ir noapaļoti līdz vienam ciparam aiz komata):

Izmantojamība	nozīmē neizmantojamību		
	dienā	mēnesī	gadā
98 %	0,5 stundas	15 stundas	7,5 dienas

Puses tiek mudinātas ievērot dienas izmantojamības rādītāju, tomēr ir atzīts, ka dažas nepieciešamas darbības, piemēram, sistēmas apkope, rada zaudlaiku, kas ir ilgāks nekā 30 minūtes. Tomēr mēneša un gada izmantojamības rādītājs ir jāievēro obligāti.

- 1.4. Tās atbild uz vismaz 98 % pieprasījumu, kas pārsūtīti vienā kalendārajā mēnesī.
- 1.5. Tās atbild uz pieprasījumiem 10 sekunžu laikā.
- 1.6. Vispārējā pieprasījuma noildze (laiks, kurā pieprasītājs var gaidīt atbildi) nepārsniedz 20 sekundes.
- 1.7. Tās spēj apstrādāt pieprasījumus ar ātrumu 6 ziņojumi sekundē.
- 1.8. Valstu sistēmas nedrīkst sūtīt pieprasījumus *TACHOnet* centrmezglam ar ātrumu, kas pārsniedz 2 pieprasījumus sekundē.

1.9. Katras valsts sistēma spēj pārvarēt centrmezgla vai citu pušu valsts sistēmu iespējamās tehniskās problēmas. Tās var būt šādas (saraksts nav izsmeļošs):

- a) zaudēts savienojums ar centrmezglu;
- b) nav atbildes uz pieprasījumu;
- c) atbilžu saņemšana pēc ziņojuma noildzes;
- d) nevēlamu ziņojumu saņemšana;
- e) nederīgu ziņojumu saņemšana.

2. Centrmezgls:

2.1. nodrošina izmantojamības rādītāju 98 %;

2.2. nosūta valstu sistēmām paziņojumus par kļūdām, vai nu izmantojot atbildes ziņojumu, vai ar īpašu kļūdas ziņojumu. Valstu sistēmas savukārt saņem šos īpašos kļūdas ziņojumus un nodrošina darbplūsmas eskalāciju, lai veiktu visus vajadzīgos pasākumus paziņotās kļūdas labošanai.

3. Apkope

Ja tas ir tehniski iespējams, puses, izmantojot tīmekļa lietojumprogrammu, informē citas puses un Eiropas Komisiju par kārtējām apkopēm vismaz vienu nedēļu pirms šo darbību sākšanas.

4.7. apakšpapildinājums

Centrmezglā savāktu datu žurnalēšana un statistika

1. Lai nodrošinātu privātumu, statistikas vajadzībām savāktie dati ir anonīmi. Konkrētas kartes, vadītāja apliecības vai vadītāja identifikācijas dati nav pieejami statistikas vajadzībām.
2. Žurnalēšanas informācijā reģistrē visas transakcijas – pārraudzīšanas un atklūdošanas vajadzībām un tālab, lai varētu ģenerēt statistiku par šīm transakcijām.
3. Personas datus žurnālos nesaglabā ilgāk kā 6 mēnešus. Statistikas informāciju saglabā uz nenoteiktu laiku.
4. Ziņošanai izmantotie statistikas dati ietver šādu informāciju:
 - a) pieprasītāja puse;
 - b) atbildes sniedzēja puse;
 - c) ziņojuma veids;
 - d) atbildes statusa kods;
 - e) ziņojumu datums un laiks;
 - f) atbildes laiks.

4.8. apakšpapildinājums

Vispārīgi noteikumi par *TACHOnet* digitālajām atslēgām un sertifikātiem

1. Eiropas Komisijas Informātikas ģenerāldirektorāts (DIGIT) dara pieejamu *AETR* Līgumslēdzējām pusēm, kuras veido savienojumu ar *TACHOnet* (turpmāk "valsts iestādes"), *PKI* pakalpojumu ¹ (turpmāk "*CEF PKI* pakalpojums"), izmantojot *eDelivery*.
2. Digitālo sertifikātu pieprasīšanas un atsaukšanas procedūra, kā arī detalizēti to izmantošanas noteikumi un nosacījumi ir izklāstīti papildinājumā.
3. Sertifikātu izmantošana
- 3.1. Pēc sertifikāta saņemšanas valsts iestāde ² sertifikātu izmanto tikai *TACHOnet* kontekstā. Sertifikātu var izmantot, lai:
 - a) autentificētu datu izcelsmi;
 - b) šifrētu datus;
 - c) nodrošinātu datu integritātes pārkāpumu atklāšanu.
- 3.2. Aizliegts sertifikātu izmantot jebkādā veidā, kas nav skaidri atļauts kā kāds no pieļaujamajiem izmantojumiem.
4. Līgumslēdzējas puses:
 - a) aizsargā savu privāto atslēgu pret nesankcionētu izmantošanu;
 - b) atturas nodot vai izpaust savu privāto atslēgu trešām personām, pat kā pārstāvjiem;

¹ *PKI* (publiskās atslēgas infrastruktūra) ir lomu, politikas, procedūru un sistēmu kopums, kas vajadzīgs, lai izveidotu, pārvaldītu, izplatītu un atsauktu digitālos sertifikātus.

² Identificēta ar "O=" atribūtvērtību izdotā sertifikāta subjekta atšķiramajā nosaukumā (*Subject Distinguished Name*).

- c) nodrošina *TACHOnet* vajadzībām ģenerēto, saglabāto un izmantoto privāto atslēgu konfidencialitāti, integritāti un izmantojamību;
- d) atturas turpināt privātās atslēgas izmantošanu pēc sertifikāta derīguma termiņa beigām vai atsaukšanas citādā veidā nekā šifrētu datu skatīšanai (piemēram, e-vēstuļu atšifrēšanai). Atslēgas, kuru derīguma termiņš ir beidzies, vai nu iznīcina, vai saglabā tādā veidā, kas novērš to izmantošanu;
- e) informē reģistrācijas iestādi par to pilnvaroto pārstāvju identitāti, kuri ir pilnvaroti pieprasīt organizācijai izdoto sertifikātu atsaukšanu (atsaukšanas pieprasījumos ietver atsaukšanas pieprasījuma paroli un sīku informāciju par notikumiem, kuru rezultātā tiek prasīta atsaukšana);
- f) novērš privātās atslēgas ļaunprātīgu izmantošanu un šādā nolūkā pieprasa atsaukt attiecīgo publiskās atslēgas sertifikātu, ja noticis privātās atslēgas vai privātās atslēgas aktivizēšanas datu kompromitējums;
- g) atbild par sertifikāta atsaukšanas pieprasīšanu un izpilda šo pienākumu apstākļos, kas norādīti sertifikācijas iestādes sertifikācijas politikā (*certification policies (CP)*) un paziņojumā par sertifikācijas praksi (*certification practices statement (CPS)*);
- h) nekavējoties paziņo reģistrācijas iestādei par jebkuras *TACHOnet* kontekstā izmantotas *AETR* atslēgas nozaudēšanu, zādzību vai iespējamu kompromitējumu.

5. Atbildība

Neskarot Eiropas Komisijas atbildību pretēji jebkurām prasībām, kas ir noteiktas piemērojamajos valstu tiesību aktos, vai attiecībā uz atbildību tajās jomās, kurās jāuzņemas atbildība saskaņā ar minētajiem tiesību aktiem, Eiropas Komisija nav atbildīga par:

- a) sertifikāta saturu, jo tas ir sertifikāta īpašnieka ekskluzīvā atbildībā. Sertifikāta īpašnieks atbild par sertifikāta satura pareizības pārbaudi;
- b) to, kā sertifikāta īpašnieks izmanto sertifikātu.

4.9. apakšpapildinājums

TACHOnet vajadzībām izmantojamā PKI pakalpojuma apraksts

1. Ievads

PKI (publiskās atslēgas infrastruktūra) ir lomu, politikas, procedūru un sistēmu kopums, kas vajadzīgs, lai izveidotu, pārvaldītu, izplatītu un atsauktu digitālos sertifikātus ³. *eDelivery CEF PKI* pakalpojums ļauj izdot un pārvaldīt digitālos sertifikātus, ko izmanto, lai nodrošinātu starp piekļuves punktiem apmaināmās informācijas konfidencialitāti, integritāti un nenoliedzamību.

eDelivery PKI pakalpojuma pamatā ir *Trust Center Services TeleSec Shared Business CA* (sertifikācijas iestāde), uz ko attiecas *T-Systems International GmbH TeleSec Shared-Business-CA* sertifikācijas politika (*CP*)/paziņojums par sertifikācijas praksi (*CPS*) ⁴.

PKI pakalpojums izdod sertifikātus, kas ir piemēroti, lai uzņēmumos, organizācijās, publiskās iestādēs un institūcijās un ārpus tām gādātu par drošību dažādos darbības procesos, kam vajadzīgs vidējs drošības līmenis, nolūkā pierādīt galasubjekta autentiskumu, integritāti un uzticamību.

2. Sertifikāta pieprasīšanas process

2.1. Lomas un pienākumi

2.1.1. "Organizācija" vai "valsts iestāde", kas pieprasa sertifikātu

2.1.1.1. Valsts iestāde pieprasa sertifikātus *TACHOnet* projekta kontekstā.

2.1.1.2. Valsts iestāde:

- (a) pieprasa sertifikātus no *CEF PKI* pakalpojuma;

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

⁴ *CP* un *CPS* jaunāko versiju var lejupielādēt vietnē <https://www.telesec.de/en/sbca-en/support/download-area/>

- (b) ģenerē privātās atslēgas un attiecīgās publiskās atslēgas, kas iekļaujamās sertifikācijas iestādes izdotajos sertifikātos;
- (c) lejupielādē sertifikātu pēc tā apstiprināšanas;
- (d) paraksta un nosūta atpakaļ reģistrācijas iestādei:
 - (i) kontaktpersonu un uzticamo kurjeru identifikācijas veidlapu,
 - (ii) parakstītu individuālu pilnvaru ⁵.

2.1.2. Uzticamais kurjers

2.1.2.1. Valsts iestāde norīko uzticamo kurjeru.

2.1.2.2. Uzticamais kurjers:

- (a) nodod reģistrācijas iestādei publisko atslēgu klātienē veiktā identifikācijas un reģistrācijas procesā;
- (b) saņem no reģistrācijas iestādes attiecīgo sertifikātu.

2.1.3. Domēna īpašnieks

2.1.3.1. Domēna īpašnieks ir Mobilitātes un transporta ģenerāldirektorāts (MOVE ĢD).

2.1.3.2. Domēna īpašnieks:

- (a) validē un koordinē tīklu *TACHOnet* un *TACHOnet* uzticamības arhitektūru, tostarp validē sertifikātu izdošanas procedūras;
- (b) ekspluatē *TACHOnet* centrmezglu un koordinē pušu darbību attiecībā uz *TACHOnet* funkcionēšanu;
- (c) kopā ar valstu iestādēm testē savienojumu ar *TACHOnet*.

⁵ Pilnvara ir juridisks dokuments, ar kuru organizācija piešķir Eiropas Komisijai, ko pārstāv identificēts ierēdnis, kurš atbild par *CEF PKI* pakalpojumu, pilnvaras organizācijas vārdā pieprasīt *T-Systems International GmbH TeleSec Shared Business CA* ģenerēt sertifikātu. Sk. arī 6. punktu.

2.1.4. Reģistrācijas iestāde

2.1.4.1. Kopīgais pētniecības centrs (*JRC*) ir reģistrācijas iestāde.

2.1.4.2. Reģistrācijas iestāde atbild par uzticamā kurjera identitātes pārbaudi un par digitālo sertifikātu izdošanas, atsaukšanas un atjaunošanas pieprasījumu reģistrāciju un apstiprināšanu.

2.1.4.3. Reģistrācijas iestāde:

- (a) piešķir valsts iestādei unikālu identifikatoru;
- (b) autentificē valsts iestādes, tās kontaktpunktu un uzticamo kurjeru identitāti;
- (c) sazinās ar *CEF* atbalsta dienestu par valsts iestādes, tās kontaktpunktu un uzticamo kurjeru autentiskumu;
- (d) informē valsts iestādi par sertifikāta apstiprināšanu vai atteikšanu.

2.1.5. Sertifikācijas iestāde

2.1.5.1. Sertifikācijas iestāde atbild par tehniskās infrastruktūras nodrošināšanu digitālo sertifikātu pieprasīšanai, izdošanai un atsaukšanai.

2.1.5.2. Sertifikācijas iestāde:

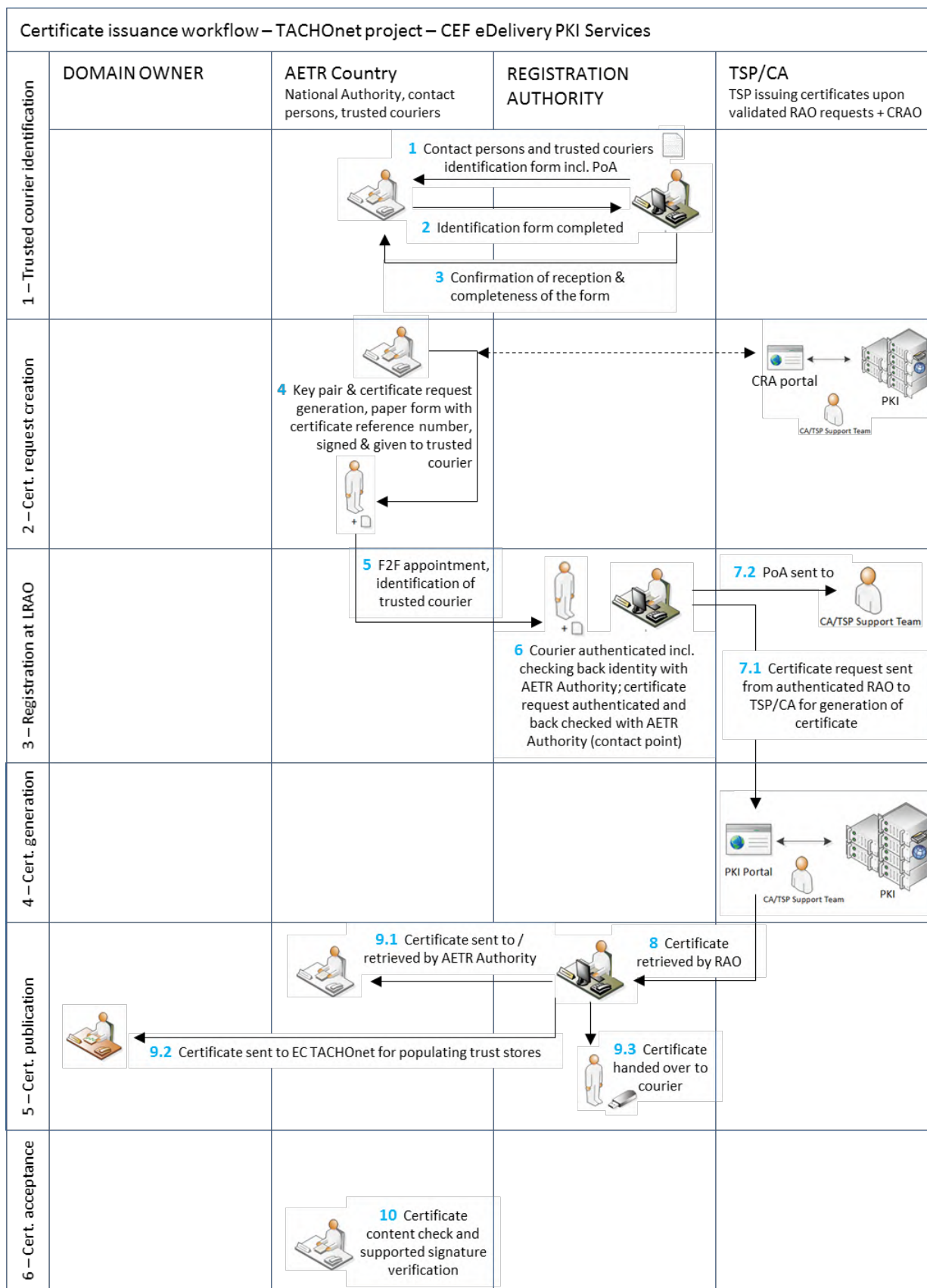
- (a) nodrošina tehnisko infrastruktūru valstu iestāžu sertifikātu pieprasījumiem;
- (b) apstiprina vai noraida sertifikāta pieprasījumu;
- (c) vajadzības gadījumā sazinās ar reģistrācijas iestādi par pieprasījumu iesniegušās organizācijas identitātes verifikāciju.

2.2. Sertifikāta izdošana

2.2.1. Sertifikāta izdošana notiek turpmāk izklāstītos secīgos posmos, kas attēloti 1. attēlā.

- (a) **1. posms:** uzticamā kurjera identifikācija;

- (b) **2. posms:** sertifikāta pieprasījuma izveide;
- (c) **3. posms:** reģistrēšana reģistrācijas iestādē;
- (d) **4. posms:** sertifikāta ģenerēšana;
- (e) **5. posms:** sertifikāta publicēšana;
- (f) **6. posms:** sertifikāta pieņemšana.



1. attēls. Sertifikāta izdošanas darbplūsmā

2.2.2. 1. posms: uzticamā kurjera identifikācija

Uzticamā kurjera identifikācijai īsteno šādu procesu.

- (a) Reģistrācijas iestāde nosūta valsts iestādei kontaktpersonu un uzticamo kurjeru identifikācijas veidlapu⁶. Šī veidlapa ietver arī pilnvaru, ko paraksta organizācija (*AETR* iestāde).
- (b) Valsts iestāde nosūta atpakaļ reģistrācijas iestādei aizpildīto veidlapu un parakstīto pilnvaru.
- (c) Reģistrācijas iestāde apstiprina, ka veidlapa ir sekmīgi saņemta un pilnīgi aizpildīta.
- (d) Reģistrācijas iestāde nosūta domēna īpašniekam atjauninātā kontaktpersonu un uzticamo kurjeru saraksta kopiju.

2.2.3. 2. posms: sertifikāta pieprasījuma izveide

2.2.3.1. Sertifikāta pieprasīšanu un izguvi veic no viena un tā paša datora, izmantojot vienu un to pašu pārlūku.

2.2.3.2. Sertifikāta pieprasījuma izveidei īsteno šādu procesu.

- (a) Organizācija navigē uz lietotāja tīmekļa saskarni, lai pieprasītu sertifikātu tīmekļa adresē <https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en;> un ievada lietotājvārdu "**sbca/CEF_eDelivery.europa.eu**" un paroli "**digit.333**".

⁶ Sk. 5. punktu.

Version: 1.5.5 Home German RSS Newsletter Locations Contact

end entity certificate
request
fetch
revoke
renew
search
login
CRL
CA certificates
Informations

Login

All actions in the "User certificate" menu option are security critical and require login. The "informations | documents" section can also only be entered after login.

You will receive the relevant login data from your responsible sub-registrar.

login:

password:

Login cancel

© 2007-2013 T-Systems International GmbH. All rights reserved. Deutsche Telekom About this Website Privacy Policy Sitemap Glossary

2. attēls

- (b) Organizācija noklikšķina uz "request" ("pieprasīt") paneļa kreisajā pusē un nolaižamajā sarakstā izvēlas "CEF_TACHOnet".

End entity certificate
request
fetch
revoke
renew
search
logout
CRL
CA certificates
Information

User certificate

To issue a certificate for a user, please fill in the following certificate application.

Please fill in at least the input fields marked with an asterisk (*) (mandatory fields). Here, you can enter additional data that is not included in the certificate but which is used by the registration authority to identify the applicant.

Subdomain: CEF_ELRC-SHARE

3. attēls

- (c) Organizācija 4. attēlā norādīto sertifikāta pieprasījuma veidlapu aizpilda ar 3. tabulā norādīto informāciju un noklikšķina uz "Next (soft-PSE)", lai pabeigtu procesu.

Must start with: 'GRP:' concatenated with CEF_TACHOnet_<TYPE>_<COUNTRY CODE>_<Unique_Identifier_of_the_Accss_P oint>'
E.g.:
'GRP: CEF_TACHOnet_AP_PROD_BE_001'

Organisation's Country Code (Case Sensitive, ISO 3166-1)

Official Organisation Name (case sensitive)

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

Next (soft-PSE)
Next (SmartCard/applet) Cancel

Country: BE

Organisation/company (O): My Company

Internet domain (OU1): CEF_eDelivery.europa.eu

Responsibility (OU2): CEF_TACHOnet

Unique Identifier (OU3): AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx

First name (CN): 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

Address: Leave Empty

Street: Street no.

ZIP code: City

Phone no.: Leave Empty

business.register.xx@mail.com

Mr Johan Smith

Revocation password: (max. 50 characters)

Revocation password repetition: (max. 50 characters)

Revocation password proposal: juHEVeV136

Adopt revocation password proposal

4. attēls

Prasītie lauki	Apraksts
"Country" (valsts)	C=Valsts kods , sertifikāta īpašnieka atrašanās vieta, ko pārbauda, izmantojot publisku adresu grāmatu; Ierobežojumi: 2 rakstzīmes, saskaņā ar ISO 3166-1, <i>alpha-2</i> , reģistrējams Piemēri: DE, BE, NL Īpašie gadījumi: UK (Lielbritānija), EL (Grieķija)
"Organisation/Company (O)" (organizācija/uzņēmums)	O=sertifikāta īpašnieka organizācijas nosaukums
"Master domain (OU1)" (galvenais domēns)	OU=CEF_eDelivery.europa.eu
"Area of responsibility (OU2)" (atbildības joma)	OU=CEF_TACHOnet
"Department (OU3)" (nodaļa)	"AREA OF RESPONSIBILITY" obligāta vērtība Kad ir pieprasīts sertifikāts, saturs jāpārbauda, izmantojot pozitīvo sarakstu (balto sarakstu). Ja informācija neatbilst sarakstam, pieprasījumu neļauj veikt. Formāts: OU=<TYPE>-<GTC_NUMBER> kur "<TYPE>" aizstāj ar AP_PROD: piekļuves punkts ekspluatācijas vidē un kur <GTC_NUMBER> ir GTC_OID-1.3.130.0.2018.xxxxxx , kur Ares(2018)xxxxxx ir GTC numurs <i>TACHOnet</i> projektam, piem.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
"First name (CN)" (vārds)	Jābūt tukšam
"Last name (CN)" (uzvārds)	Jāsākas ar "GRP", pēc kura norāda kopējo nosaukumu ("common name"). Formāts: CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER> piem.: GRP:CEF_TACHOnet_AP_PROD_BE_001
"E-mail" (e-pasta adrese)	E=CEF-EDELIVERY-SUPPORT@ec.europa.eu
"E-mail 1 (SAN)"	Jābūt tukšam
"E-mail 2 (SAN)"	Jābūt tukšam
"E-mail 3 (SAN)"	Jābūt tukšam

"Address" (adrese)	Jābūt tukšam
"Street" (iela)	Jānorāda sertifikāta īpašnieka organizācijas oficiālā adrese (kas izmantota pilnvarā)
"Street no." (ēkas numurs)	Jānorāda sertifikāta īpašnieka organizācijas oficiālā adrese (kas izmantota pilnvarā)
"Zip Code" (pasta indekss)	Jānorāda sertifikāta īpašnieka organizācijas oficiālā adrese (kas izmantota pilnvarā) <u>Uzmanību:</u> ja pasta indekss NAV piecciparu kods, pasta indeksam paredzēto lauku atstāj tukšu un pasta indeksu ieraksta pilsētas nosaukumam paredzētajā laukā.
"City" (pilsēta)	Jānorāda sertifikāta īpašnieka organizācijas oficiālā adrese (kas izmantota pilnvarā) <u>Uzmanību:</u> ja pasta indekss NAV piecciparu kods, pasta indeksam paredzēto lauku atstāj tukšu un pasta indeksu ieraksta pilsētas nosaukumam paredzētajā laukā.
"Phone no" (tālrunis)	Jābūt tukšam
"Identification data" (identifikācijas dati)	E-pasta adrese jābūt tai pašai, kas izmantota, reģistrējot unikālo identifikatoru + jābūt organizāciju pārstāvošās personas vārdam un uzvārdam (kas izmantots pilnvarā) + komercrēģistra numurs (obligāts tikai privātām organizācijām) reģistrēts [vietas nosaukums] pirmās instances tiesā (prasīts tikai Vācijas un Austrijas privātajām organizācijām)
"Revocation password" (atsaukšanas parole)	Obligāts lauks, ko izvēlas pieprasītājs
"Revocation password repetition" (atsaukšanas paroles atkārtojums)	Obligāts lauks, ko izvēlas pieprasītājs, atkārtoti

3. tabula. Pilnīga informācija par katru prasīto lauku

(d) Izvēlas atslēgas garumu "2048(High Grade)".

The screenshot shows the T-Systems website interface for requesting a user certificate. The page title is "User certificate". On the left, there is a sidebar menu with options: "End entity certificate", "request" (highlighted), "fetch", "revoke", "renew", "search", "logout", "CRL", "CA certificates", and "Information". The main content area contains instructions and a form for certificate data. The form fields are: Country (C) BE, Organization/company (O) European Commission, Master domain (OU1) CEF_eDelivery.europa.eu, Area of responsibility (OU2) CEF_TACHOnet, Department (OU3) AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx, First name (CN), Last name (CN) GRP:CEF_TACHOnet_AP_PROD_BE_001, E-mail CEF-EDELIVERY-SUPPORT@ec.europa.eu, and Selection of key length 2048 (High Grade). There are "Request" and "Cancel" buttons at the bottom of the form. The footer includes copyright information and links to Deutsche Telekom, About this Website, Privacy Policy, Sitemap, and Glossary.

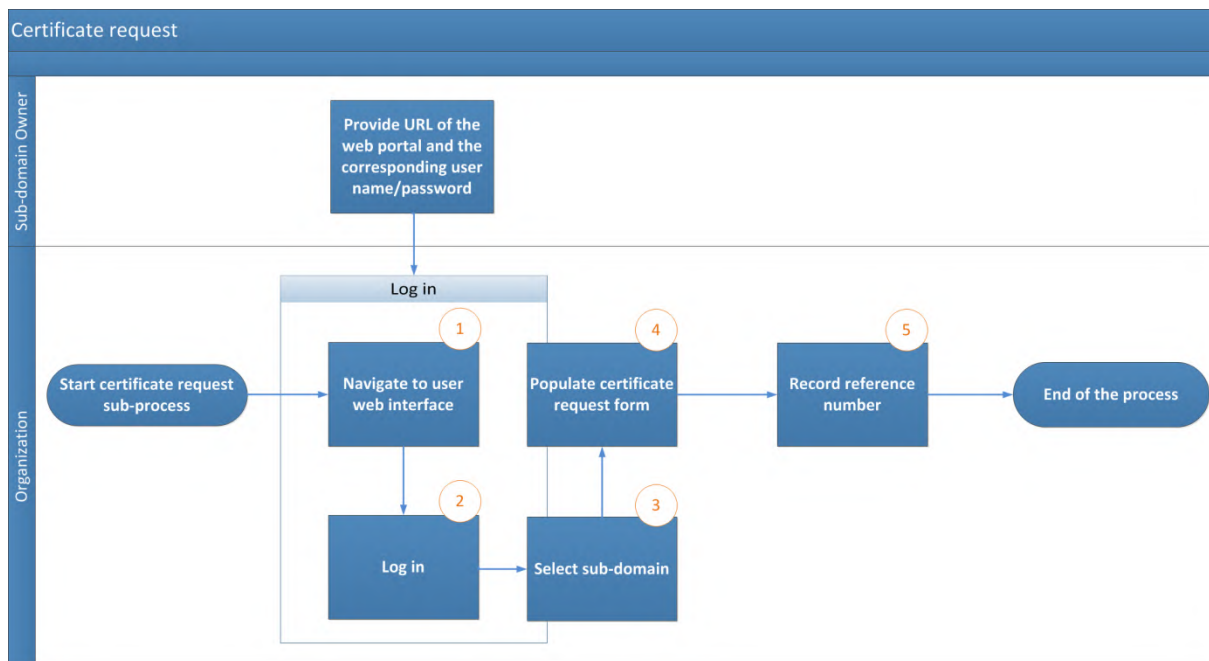
5. attēls

(e) Organizācija reģistrē atsaucē numuru sertifikāta izgūvei.

The screenshot shows the T-Systems website interface after a user certificate request has been submitted. The page title is "User certificate". The main content area displays the message: "The certificate was requested. Your request was stored with reference number 776002." Below this, it states: "Please note that you can only pick up the certificate once the responsible sub-registrar has approved the certificate application. You will be notified of the approval by e-mail." A blue callout box with the text "Certificate Reference Number" points to the reference number 776002. The sidebar menu and footer are identical to the previous screenshot.

6. attēls

- (f) *CEF* atbalsta dienests seko līdzī tam, vai ir saņemti jauni sertifikāta pieprasījumi, un pārbauda, vai sertifikāta pieprasījumā ietvertā informācija ir derīga, proti, atbilst 5.1. papildinājumā "Sertifikāta nosaukumdošanas metode" noteiktajai nosaukumdošanas metodei.
- (g) *CEF* atbalsta dienests pārbauda, vai pieprasījumā ietvertā informācija ir derīgā formātā.
- (h) Ja kāda no 5. un 6. punktā minētajām pārbaudēm nedod pozitīvu rezultātu, *CEF* atbalsta dienests uz e-pasta adresi, kas norādīta pieprasījuma veidlapas laukā "Identification data", nosūta e-vēstuli ar kopiju domēna īpašniekam, kurā organizācijai prasa sākt procesu no jauna. Neizdevušos sertifikāta pieprasījumu atceļ.
- (i) *CEF* atbalsta dienests nosūta reģistrācijas iestādei e-vēstuli par pieprasījuma derīgumu. E-vēstulē ietver:
 - (1) organizācijas nosaukumu, kas norādīts sertifikāta pieprasījuma laukā "Organisation (O)";
 - (2) sertifikāta datus, tostarp sertifikāta pieprasījuma laukā "Last Name (CN)" norādīto tā piekļuves punkta nosaukumu, kam pieprasīts sertifikāts;
 - (3) sertifikāta atsauces numuru;
 - (4) organizācijas adresi, tās e-pasta adresi un organizāciju pārstāvošās personas vārdu un uzvārdu.



7. attēls. Sertifikāta pieprasīšanas process

2.2.4. 3. posms: reģistrēšana reģistrācijas iestādē (sertifikāta apstiprināšana)

2.2.4.1. Uzticamais kurjers vai kontaktpunkts, apmainoties e-vēstulēm ar reģistrācijas iestādi, vienojas par tikšanos un norāda uzticamo kurjeru, kurš ieradīsies reģistrācijas iestādē uz tikšanos klātienē.

2.2.4.2. Organizācija sagatavo dokumentu paketi, kurā ir:

- (a) aizpildīta un parakstīta pilnvara;
- (b) uzticamā kurjera, kurš ieradīsies uz tikšanos klātienē, derīgas pases kopija. Šī kopija jāparaksta kādam no 1. posmā norādītajiem organizācijas kontaktpunktiem;
- (c) sertifikāta pieprasījums papīra formātā, ko parakstījis kāds no organizācijas kontaktpunktiem.

2.2.4.3. Reģistrācijas iestāde pieņem uzticamo kurjeru pēc identitātes pārbaudes ēkas reģistratūrā. Reģistrācijas iestāde klātienē reģistrē sertifikāta pieprasījumu, šādā nolūkā:

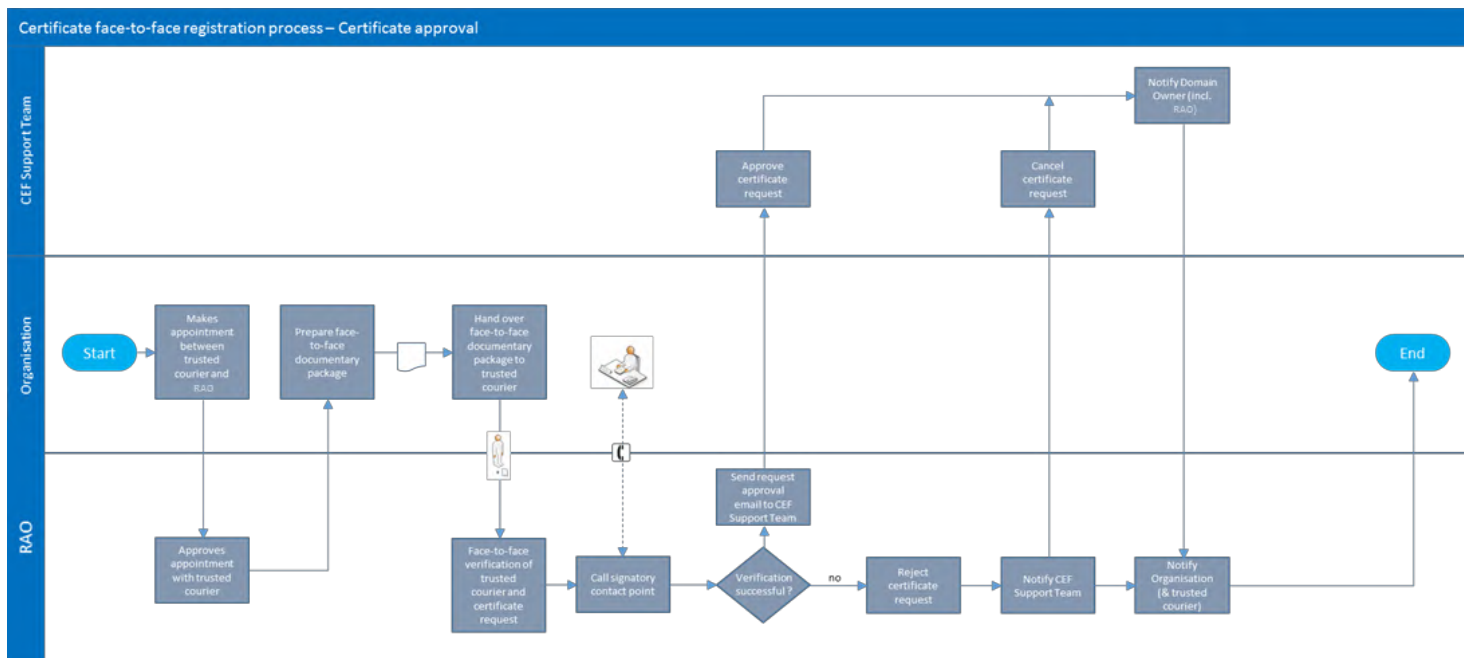
- (a) identificējot un autentificējot uzticamo kurjeru;
- (b) pārbaudot uzticamā kurjera izskatu salīdzinājumā ar uzticamā kurjera uzrādīto pasi;
- (c) pārbaudot uzticamā kurjera uzrādītās pases derīgumu;
- (d) pārbaudot uzticamā kurjera uzrādīto derīgo pasi salīdzinājumā ar uzticamā kurjera derīgās pases kopiju, ko parakstījis kāds no organizācijas norādītajiem kontaktpunktiem. Parakstu autentificē salīdzinājumā ar uzticamo kurjeru un kontaktpunktu identifikācijas veidlapas oriģinālu;
- (e) pārbaudot aizpildīto un parakstīto pilnvaru;
- (f) pārbaudot sertifikāta pieprasījumu papīra formātā un parakstu uz tā salīdzinājumā ar uzticamo kurjeru un kontaktpunktu identifikācijas veidlapas oriģinālu;
- (g) pa tālruni sazinoties ar parakstītāju kontaktpunktu un vēlreiz pārbaudot uzticamā kurjera identitāti un sertifikāta pieprasījuma saturu.

2.2.4.4. Reģistrācijas iestāde *CEF* atbalsta dienestam apstiprina, ka valsts iestāde tiešām ir pilnvarota ekspluatēt komponentus, kuriem tā prasa sertifikātus, un ka attiecīgā reģistrācija klātienē ir noritējusi sekmīgi. Apstiprinājumu nosūta pa drošu e-pastu, izmantojot sertifikātu "CommiSign", un pievieno šādu dokumentu skenētu kopiju: autentificēta klātienē tikšanās dokumentu pakete un parakstīts reģistrācijas iestādes veiktā procesa kontrolsaraksts.

2.2.4.5. Ja reģistrācijas iestāde apstiprina pieprasījuma derīgumu, process turpinās, kā noteikts 2.2.4.6. un 2.2.4.7. punktā. Pretējā gadījumā sertifikāta izdošana tiek atteikta un organizācija — attiecīgi informēta.

2.2.4.6. CEF atbalsta dienests apstiprina sertifikāta pieprasījumu un paziņo reģistrācijas iestādei par sertifikāta apstiprināšanu.

2.2.4.7. Reģistrācijas iestāde paziņo organizācijai, ka sertifikātu var izgūt lietotāju portālā.



8. attēls. Sertifikāta apstiprināšana

2.2.5. 4. posms: sertifikāta ģenerēšana

Pēc sertifikāta pieprasījuma apstiprināšanas ģenerē sertifikātu.

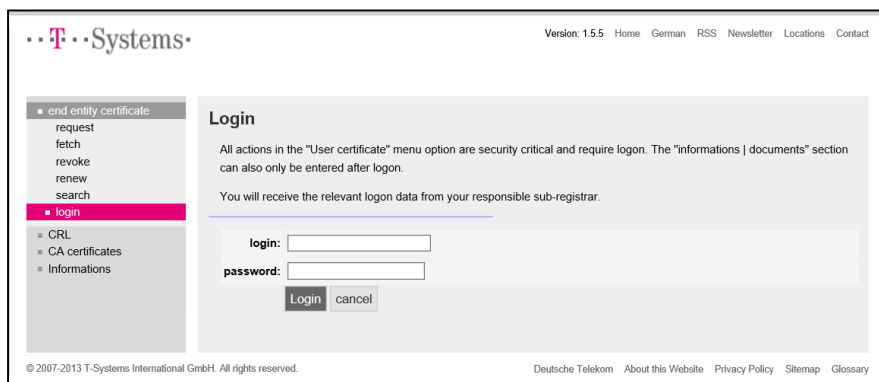
2.2.6. 5. posms: sertifikāta publicēšana un izguve

2.2.6.1. Pēc sertifikāta pieprasījuma apstiprināšanas reģistrācijas iestāde izgūst sertifikātu un tā kopiju nodod uzticamajam kurjeram.

2.2.6.2. Organizācija saņem no reģistrācijas iestādes paziņojumu par to, ka sertifikātus var izgūt.

2.2.6.3. Organizācija navigē uz lietotāju portālu adresē

<https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en> un piesakās ar lietotājvārdu "**sbca/CEF_eDelivery.europa.eu**" un paroli "**digit.333**".



..T..Systems·

Version: 1.5.5 Home German RSS Newsletter Locations Contact

- end entity certificate
 - request
 - fetch
 - revoke
 - renew
 - search
- login
- CRL
- CA certificates
- Informations

Login

All actions in the "User certificate" menu option are security critical and require login. The "informations | documents" section can also only be entered after login.

You will receive the relevant login data from your responsible sub-registrar.

login:

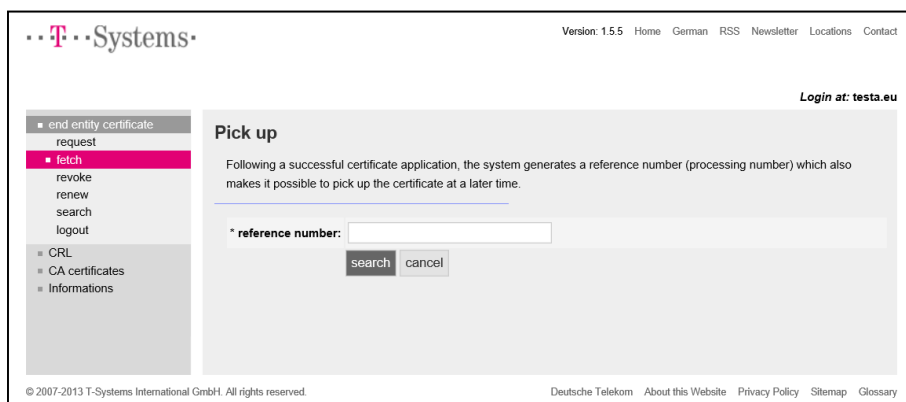
password:

Login cancel

© 2007-2013 T-Systems International GmbH. All rights reserved. Deutsche Telekom About this Website Privacy Policy Sitemap Glossary

9. attēls

2.2.6.4. Organizācija noklikšķina uz pogas "fetch" ("paņemt") paneļa kreisajā pusē un norāda sertifikāta pieprasīšanas procesā reģistrēto atsauces numuru.



..T..Systems·

Version: 1.5.5 Home German RSS Newsletter Locations Contact

Login at: testa.eu

- end entity certificate
 - request
 - fetch
 - revoke
 - renew
 - search
 - logout
- CRL
- CA certificates
- Informations

Pick up

Following a successful certificate application, the system generates a reference number (processing number) which also makes it possible to pick up the certificate at a later time.

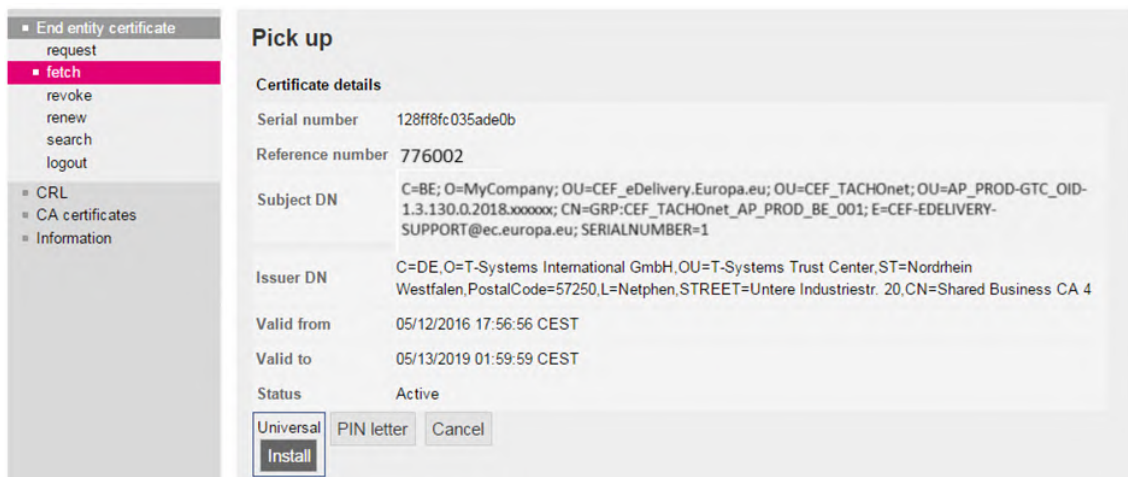
* reference number:

search cancel

© 2007-2013 T-Systems International GmbH. All rights reserved. Deutsche Telekom About this Website Privacy Policy Sitemap Glossary

10. attēls

2.2.6.5. Organizācija instalē sertifikātus, noklikšķinot uz pogas "install".

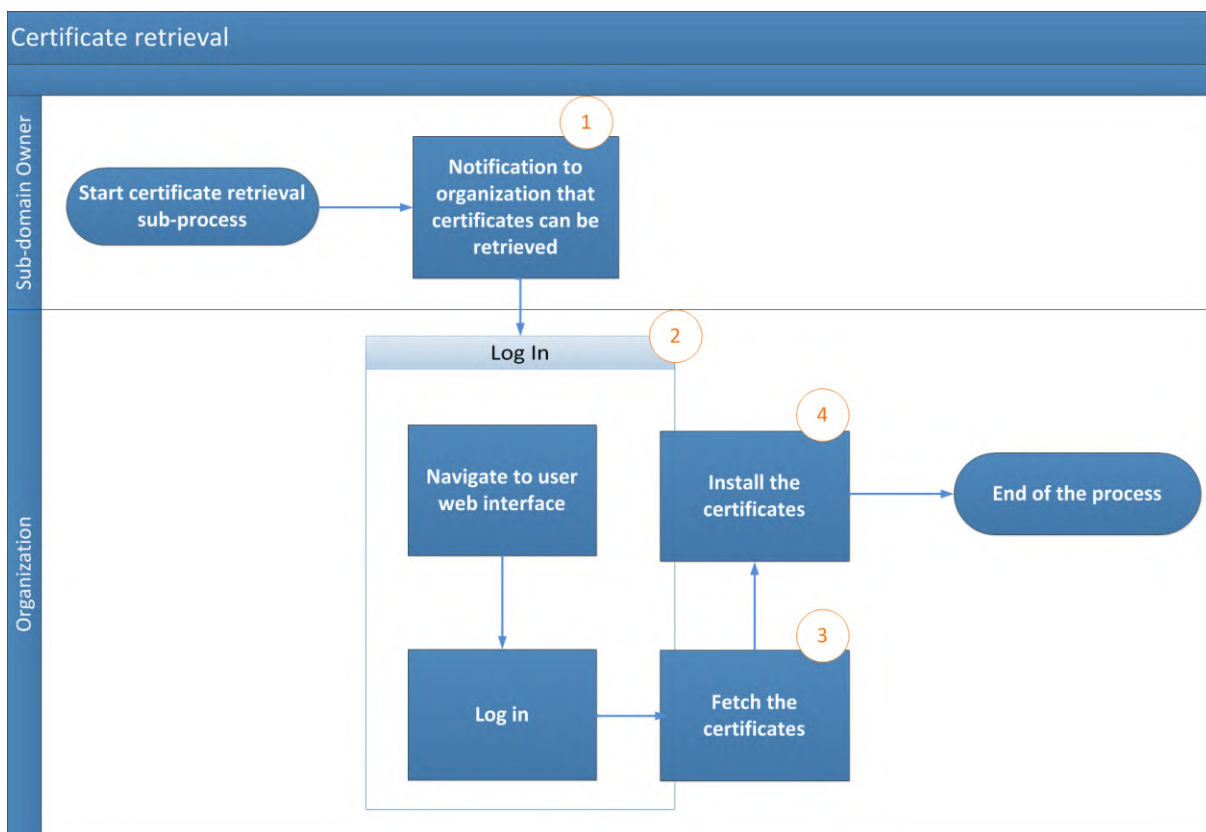


11. attēls

2.2.6.6. Sertifikātu instalē piekļuves punktā. Tā kā instalēšana ir atkarīga no īstenošanas procesa, organizācija lūdz piekļuves punkta nodrošinātājam šā procesa aprakstu.

2.2.6.7. Lai sertifikātu instalētu piekļuves punktā, jāveic šādas darbības:

- (a) jāeksportē privātā atslēga un sertifikāts;
- (b) jāizveido krātuves "keystore" un "truststore";
- (c) jāinstalē krātuves "keystore" un "truststore" piekļuves punktā.

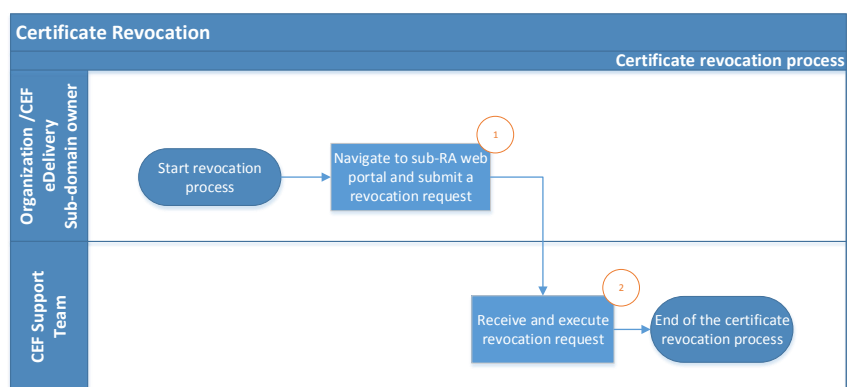


12. attēls. Sertifikāta izguve

3. Sertifikāta atsaukšanas process

3.1. Organizācija lietotāju tīmekļa portālā iesniedz atsaukšanas pieprasījumu.

3.2. CEF atbalsta dienests atsauc sertifikātu.



13. attēls. Sertifikāta atsaukšana

4. CEF PKI pakalpojuma vispārīgie noteikumi un nosacījumi

4.1. Konteksts

DIGIT kā Eiropas infrastruktūras savienošanas instrumenta *eDelivery* moduļa risinājumu nodrošinātājs darīs PKI pakalpojumu ⁷ ("*CEF PKI* pakalpojums") pieejamu *AETR* Līgumslēdzējām pusēm. *CEF PKI* pakalpojumu izmanto valstu iestādes ("tiešie lietotāji"), kuras piedalās *TACHOnet*.

DIGIT ir PKI nomnieks risinājumā *TeleSec Shared-Business-CA* ("*SBCA*"), kura darbību nodrošina *T-Systems International GmbH* ("*T-Systems*" ⁸) grupu nodaļas drošības kontroles centrs. DIGIT ir *SBCA* domēna "*CEF_eDelivery.europa.eu*" galvenais reģistrētājs. Šajā lomā DIGIT domēnā "*CEF_eDelivery.europa.eu*" veido apakšdomēnus katram projektam, kas izmanto *CEF PKI* pakalpojumu.

Šajā dokumentā sniegta sīkāka informācija par apakšdomēna *TACHOnet* noteikumiem un nosacījumiem. DIGIT ir šā apakšdomēna apakšreģistrētājs. Šajā statusā tas izdod, atsauc un atjaunina šā projekta sertifikātus.

4.2. Atbildības ierobežojuma atruna

Eiropas Komisija neuzņemas nekādu atbildību par sertifikāta saturu, jo tas ir sertifikāta īpašnieka ekskluzīvā atbildībā. Sertifikāta īpašnieks atbild par sertifikāta satura pareizības pārbaudi.

Eiropas Komisija neuzņemas nekādu atbildību par to, kā sertifikāta īpašnieks izmanto sertifikātu, jo īpašnieks ir trešā juridiskā persona ārpus Eiropas Komisijas.

⁷ PKI (publiskās atslēgas infrastruktūra) ir lomu, politikas, procedūru un sistēmu kopums, kas vajadzīgs, lai izveidotu, pārvaldītu, izplatītu un atsauktu digitālos sertifikātus.

⁸ Drošības kontroles centra operatora uzticamības loma; atrodas *T-Systems* drošības kontroles centrā; veic arī iekšējās reģistrācijas iestādes uzdevumu.

Šīs atrunas mērķis nav ierobežot Eiropas Komisijas atbildību pretēji jebkurām prasībām, kas ir noteiktas piemērojamajos valstu tiesību aktos, vai atbrīvot to no atbildības tajās jomās, kurās jāuzņemas atbildība saskaņā ar tiesību aktiem.

4.3. Atļauts/aizliegts sertifikātu izmantojums

4.3.1. Pieļaujams sertifikātu izmantojums

Pēc sertifikāta saņemšanas sertifikāta īpašnieks ⁹ sertifikātu izmanto tikai *TACHOnet* kontekstā. Šajā kontekstā sertifikātu var izmantot, lai:

- autentificētu datu izcelsmi;
- šifrētu datus;
- nodrošinātu datu integritātes pārkāpumu atklāšanu.

4.3.2. Aizliegts sertifikātu izmantojums

Aizliegts sertifikātu izmantot jebkādā veidā, kas nav skaidri atļauts kā kāds no pieļaujamajiem izmantojumiem.

4.4. Sertifikāta īpašnieka papildpienākumi

Detalizētus *SBCA* noteikumus un nosacījumus *T-Systems* nosaka *SBCA* pakalpojuma sertifikācijas politikā (*CP*)/paziņojumā par sertifikācijas praksi (*CPS*) ¹⁰. Šajā dokumentā ietvertas drošības specifikācijas un vadlīnijas, kas attiecas uz tehniskiem un organizatoriskiem aspektiem, un aprakstīta drošības kontroles centra operatora darbība šādās lomās: sertifikācijas iestāde (*CA*) un reģistrācijas iestāde (*RA*), kā arī trešās personas deleģēta reģistrācijas iestāde (*RA*).

Sertifikātu drīkst pieprasīt tikai subjekti, kam atļauts piedalīties *TACHOnet*.

⁹ Identificēts ar "O=" atribūtvērtību izdotā sertifikāta subjekta atšķiramajā nosaukumā (*Subject Distinguished Name*).

¹⁰ *T-Systems SBCA CP/CPS* jaunākā versija pieejama vietnē <https://www.telesec.de/en/sbca-en/support/download-area/>.

Attiecībā uz sertifikāta pieņemšanu piemēro *SBCA* sertifikācijas politikas un paziņojuma par sertifikācijas praksi ("*CP/CPS*") 4.4.1. punktu, turklāt uzskata, ka organizācija, kurai sertifikāts izdots ("O="), ir pieņēmusi šajā dokumentā aprakstītos izmantošanas noteikumus tad, kad tā pirmoreiz izmantojusi sertifikātu.

Attiecībā uz sertifikāta publicēšanu piemēro *SBCA CP/CPS* 2.2. punktu.

Visi sertifikātu īpašnieki izpilda šādas prasības:

- (1) aizsargā savu privāto atslēgu pret nesankcionētu izmantošanu;
- (2) atturas nodot vai izpaust savu privāto atslēgu trešām personām, pat kā pārstāvjiem;
- (3) atturas turpināt privātās atslēgas izmantošanu pēc sertifikāta derīguma termiņa beigām vai atsaukšanas citādā veidā nekā šifrētu datu skatīšanai (piemēram, e-vēstuļu atšifrēšanai);
- (4) sertifikāta īpašnieks atbild par atslēgas kopēšanu vai pārsūtīšanu galasubjektam vai galasubjektiem;
- (5) sertifikāta īpašniekam jāuzliek galasubjektam/visiem galasubjektiem pienākums nodrošināt atbilstību šiem noteikumiem un nosacījumiem, tostarp *SBCA CP/CPS*, kad tie rīkojas ar privāto atslēgu;
- (6) sertifikāta īpašnieka pienākums ir sniegt informāciju par to pilnvaroto pārstāvju identitāti, kuri ir pilnvaroti pieprasīt organizācijai izdoto sertifikātu atsaukšanu, un izklāstīt sīku informāciju par notikumiem, kas izraisījuši atsaukšanu, kā arī norādīt atsaukšanas paroli;
- (7) attiecībā uz sertifikātiem, kas saistīti ar fizisku personu un funkciju grupām un/vai juridiskām personām, sertifikāta īpašniekam pēc tam, kad fiziska persona aizgājusi no galasubjektu grupas (piem., darba attiecību izbeigšanas gadījumā), jānovērš privātās atslēgas ļaunprātīga izmantošana, šādā nolūkā atsaucot sertifikātu;
- (8) sertifikāta īpašnieks atbild par sertifikāta atsaukšanu un pieprasa to *SBCA CP/CPS* 4.9.1. punktā minētajos apstākļos.

Attiecībā uz sertifikātu atjaunošanu vai jaunas atslēgas piešķiršanu piemēro *SBCA CP/CPS* 4.6. vai 4.7. punktu.

Attiecībā uz sertifikāta grozījumiem piemēro *SBCA CP/CPS* 4.8. punktu.

Attiecībā uz sertifikāta atsaukšanu piemēro *SBCA CP/CPS* 4.9. punktu.

5. Kontaktpersonu un uzticamo kurjeru identifikācijas veidlapa (paraugs)

Es, [organizācijas pārstāvja vārds, uzvārds un adrese], apliecinu, ka turpmāk norādītā informācija tiks izmantota *TACHOnet* piekļuves punktu publiskās atslēgas digitālo sertifikātu pieprasīšanas, ģenerēšanas un izguves kontekstā *TACHOnet* ziņojumu konfidencialitātes, integritātes un nenoliedzamības atbalstam.

– Informācija par kontaktpersonu

– 1. kontaktpersona	– 2. kontaktpersona
– Uzvārds:	– Uzvārds:
– Vārds(-i):	– Vārds(-i):
– Mobilais tālrunis:	– Mobilais tālrunis:
– Tālrunis:	– Tālrunis:
– E-pasts:	– E-pasts:
– Ar roku rakstīta paraksta paraugs: –	– Ar roku rakstīta paraksta paraugs: – – –

– Informācija par uzticamo kurjeru

– 1. uzticamais kurjers	– 2. uzticamais kurjers
– Uzvārds:	– Uzvārds:
– Vārds(-i):	– Vārds(-i):
– Mobilais tālrunis:	– Mobilais tālrunis:
– E-pasts:	– E-pasts:
– Pases izdevējvalsts:	– Pases izdevējvalsts:
– Pases numurs:	– Pases numurs:
– Pases derīguma termiņa beigu datums:	– Pases derīguma termiņa beigu datums:

Vieta, laiks, uzņēmuma spiedogs vai organizācijas zīmogs:

Pilnvarotā pārstāvja paraksts:

6. Dokumenti

6.1. Individuāla pilnvara (paraugs)

Individuālas pilnvaras, kam jābūt parakstītai un kas uzticamajam kurjeram jāuzrāda, kad notiek reģistrācija klātienē reģistrācijas iestādē, paraugs ir šāds.

*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 FERAL**

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):

☒ user¹: e.g. mail security (signature, encryption), virtual private network (VPN), TLS/SSL client

☐ server²: 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-Gateway³: 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 months²** 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 month²** 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. Sertifikāta pieprasījums papīra formātā (paraugs)

Sertifikāta pieprasījuma papīra formātā, kam jābūt parakstītam un kas uzticamajam kurjeram jāuzrāda, kad notiek reģistrācija klātienē reģistrācijas iestādē, paraugs ir šāds.

7. Glosārijs

Galvenie šajā apakšpapildinājumā izmantotie termini definēti *CEF* digitālā vienotā tīmekļa portāla *CEF* definīciju iedaļā:

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

Galvenie šajā apakšpapildinājumā izmantotie akronīmi definēti *CEF* digitālā vienotā tīmekļa portāla *CEF* glosārijā:

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