Europos Sąjungos
Taryba

Briuselis, 2018 m. lapkričio 5 d.
(OR. en)

13711/18
ADD 1

Tarpinstitucinė byla:
2018/0339(NLE)

TRANS 488

PRANEŠIMAS

nuo:	Tarybos generalinio sekretoriato
kam:	Delegacijoms
Ankstesnio dokumento Nr.:	ST 13711/18 TRANS 448
Komisijos dok. Nr.:	ST 12727/18 TRANS 426 + ADD 1
Dalykas:	Tarybos sprendimas dėl pozicijos, kurios Europos Sąjungos vardu turi būti laikomasi Ekspertų grupėje, dėl Jungtinių Tautų Europos ekonomikos komisijos parengto Europos šalių susitarimo dėl kelių transporto priemonių ekipažų, važinėjančių tarptautiniais maršrutais, darbo

Pirmiau nurodyto Tarybos sprendimo priedas.

PRIEDAS

Naujas AETR priedėlis

4 priedėlis

„TACHOnet“ specifikacijos

1. Taikymo sritis ir tikslas

1.1. Šiame priedėlyje nustatomos AETR susitariančiųjų šalių prisijungimo prie „TACHOnet“ naudojantis e. pristatymo paslauga sąlygos.

1.2. Susitariančiosios šalys, kurios jungiasi prie „TACHOnet“ naudodamosi e. pristatymo paslauga, laikosi šio priedėlio nuostatų.

2. Apibrėžtys

a) susitariančioji šalis arba šalis – bet kuri AETR susitariančioji šalis;

b) e. pristatymas – Europos Komisijos sukurta paslauga, užtikrinanti galimybę trečiosioms šalims tarpusavyje perduoti duomenis, suteikianti su perduodamų duomenų tvarkymu susijusių įrodymų, įskaitant duomenų išsiuntimo ir gavimo įrodymą, ir apsauganti perduodamus duomenis nuo bet kokio neteisėto pakeitimo rizikos;

c) „TACHOnet“ – Reglamento (ES) Nr. 165/2014 31 straipsnio 2 dalyje nurodyta pranešimų sistema, kuria naudodamosi susitariančiosios šalys tarpusavyje keičiasi informacija apie vairuotojų korteles;

d) duomenų centras – informacinė sistema, užtikrinanti galimybę persiųsti užklausas teikiančių ir atsakančių šalių siunčiamus „TACHOnet“ pranešimus;

e) užklausą teikianti šalis – susitariančioji šalis, teikianti „TACHOnet“ užklausą arba pranešimą, kurį (kurią) duomenų centras persiunčia atitinkamai atsakančiai šaliai;

f) atsakanti šalis – susitariančioji šalis, kuriai skirta „TACHOnet“ užklausa ar pranešimas;

g) korteles išduodančioji institucija (KII) – subjektas, kurį susitariančioji šalis yra įgaliojusi išduoti ir tvarkyti tachografų korteles.

3. Bendrosios pareigos

3.1. Jokia susitariančioji šalis negali kitos šalies vardu sudaryti susitarimo dėl prieigos prie „TACHOnet“ ar kitaip atstovauti kitai susitariančiajai šaliai remiantis šiuo priedėliu. Jokia susitariančioji šalis negali veikti kaip kitos susitariančiosios šalies šiame priedėlyje nurodytų operacijų subrangovė.

3.2. Susitariančiosios šalys teikia prieigą prie savo nacionalinių vairuotojų kortelių registrų per „TACHOnet“ 4.6 papildomame priedėlyje nustatytu būdu ir užtikrindamos jame nustatytą paslaugos lygį.

3.3. Pastebėjusios savo atsakomybės srities trikčių ar klaidų, dėl kurių gali kilti pavojus įprastam „TACHOnet“ veikimui, susitariančiosios šalys nedelsdamos apie tai informuoja viena kitą.

3.4. Kiekviena šalis paskiria ir AETR sekretoriatui praneša „TACHOnet“ kontaktinius asmenis. Apie visus kontaktinių asmenų pasikeitimus AETR sekretoriatui turi būti pranešama raštu.

4. Prisijungimo prie „TACHOnet“ bandymai

4.1. Susitariančiosios šalies jungtis su „TACHOnet“ sukuriama sėkmingai atlikus prisijungimo, integravimo ir veikimo bandymus, kurių nurodymus duoda ir kuriuos prižiūri Europos Komisija.

4.2. Jei parengiamųjų bandymų rezultatas neigiamas, Europos Komisija gali laikinai sustabdyti bandymų etapą. Bandymai tęsiami, kai susitariančioji šalis Europos Komisijai praneša padariusi būtinus nacionalinio lygmens techninius patobulinimus, kad parengiamuosius bandymus būtų galima atlikti sėkmingai.

4.3. Ilgiausia parengiamųjų bandymų trukmė – šeši mėnesiai.

5. Pasitikėjimo architektūra

5.1. „TACHOnet“ pranešimų konfidencialumą, vientisumą ir nepaneigiamumą užtikrina „TACHOnet“ pasitikėjimo architektūra.

5.2. „TACHOnet“ pasitikėjimo architektūra grindžiama Europos Komisijos sukurta viešojo rakto infrastruktūros (PKI) paslauga, kurios reikalavimai nustatyti 4.8 ir 4.9 papildomuose priedėliuose.

5.3. „TACHOnet“ pasitikėjimo architektūroje veikia šie subjektai:

a) sertifikavimo institucija, atsakinga už skaitmeninių sertifikatų, kuriuos registravimo institucija pristato susitariančiųjų šalių nacionalinėms institucijoms (per jų paskirtus patikimus kurjerius), kūrimą ir skaitmeninių sertifikatų išdavimo, panaikinimo ir atnaujinimo techninės infrastruktūros sukūrimą;

b) domeno savininkas, atsakingas už 4.1 papildomame priedėlyje nurodyto duomenų centro valdymą ir „TACHOnet“ pasitikėjimo architektūros patvirtinimą ir koordinavimą;

c) registravimo institucija, atsakinga už prašymų išduoti, panaikinti ir atnaujinti skaitmeninius sertifikatus registravimą ir patvirtinimą bei patikimų kurjerių tapatybės patikrinimą;

d) patikimas kurjeris, t. y. nacionalinės institucijos paskirtas asmuo, atsakingas už viešojo rakto perdavimą registravimo institucijai ir sertifikavimo institucijos sugeneruoto atitinkamo sertifikato gavimą;

e) susitariančiosios šalies nacionalinė institucija, kuri:

i) generuoja privačiuosius raktus ir atitinkamus viešuosius raktus, įtrauktinus į sertifikavimo institucijos generuojamus sertifikatus;

ii) užsako skaitmeninius sertifikatus iš sertifikavimo institucijos;

iii) paskiria patikimą kurjerį.

5.4. Sertifikavimo instituciją ir registravimo instituciją skiria Europos Komisija.

5.5. Kiekviena prie „TACHOnet“ prisijungianti susitariančioji šalis privalo prašyti pagal 4.9 papildomą priedėlį išduoti skaitmeninį sertifikatą, kad galėtų pasirašyti ir užšifruoti „TACHOnet“ pranešimus.

5.6. Sertifikatas gali būti panaikintas pagal 4.9 papildomą priedėlį.

6. Duomenų apsauga ir konfidencialumas

6.1. Šalys, laikydamosi tarptautinių ir nacionalinių duomenų apsaugos teisės aktų, visų pirma Konvencijos dėl asmenų apsaugos ryšium su asmens duomenų automatizuotu tvarkymu, imasi visų būtinų techninių ir organizacinių priemonių, kad užtikrintų „TACHOnet“ duomenų saugumą ir išvengtų jų pakeitimo, praradimo, neleistino jų apdorojimo ar prieigos prie jų (ypač pranešimų autentiškumą, duomenų konfidencialumą, atsekamumą, vientisumą, prieinamumą, nepaneigiamumą ir saugumą).

6.2. Kiekviena šalis apsaugo savo nacionalines sistemas nuo neteisėto naudojimo, kenkėjiško programos kodo, kompiuterių virusų, kompiuterinių įsilaužimų, pažeidimų ir neteisėto duomenų keitimo, taip pat kitų panašių trečiųjų šalių veiksmų. Šalys sutinka dėti komerciškai pagrįstas pastangas, kad būtų išvengta kompiuterių virusų, tam tikru metu pradedančių veikti kenkėjiškų programų, kirminų ar panašių dalykų, taip pat bet kokių programų, galinčių sutrikdyti kitos šalies kompiuterių sistemų veikimą, perdavimo.

7. Išlaidos

7.1. Susitariančiosios šalys pačios padengia su savo duomenų sistemomis ir procedūromis, kurių reikia įsipareigojimams pagal šį priedėlį įvykdyti, susijusias kūrimo ir naudojimo išlaidas.

7.2. 4.1 papildomame priedėlyje nustatytos duomenų centro paslaugos yra nemokamos.

8. Subranga

8.1. Šalys gali bet kurią paslaugą, už kurią yra atsakingos pagal šį priedėlį, perduoti vykdyti subrangovui.

8.2. Tokia subranga neatleidžia šalies nuo atsakomybės pagal šį priedėlį, įskaitant atsakomybę užtikrinti tinkamą paslaugos lygį pagal 4.6 papildomą priedėlį.

4.1 papildomas priedėlis

„TACHOnet“ bendrieji aspektai

1. Bendras aprašymas

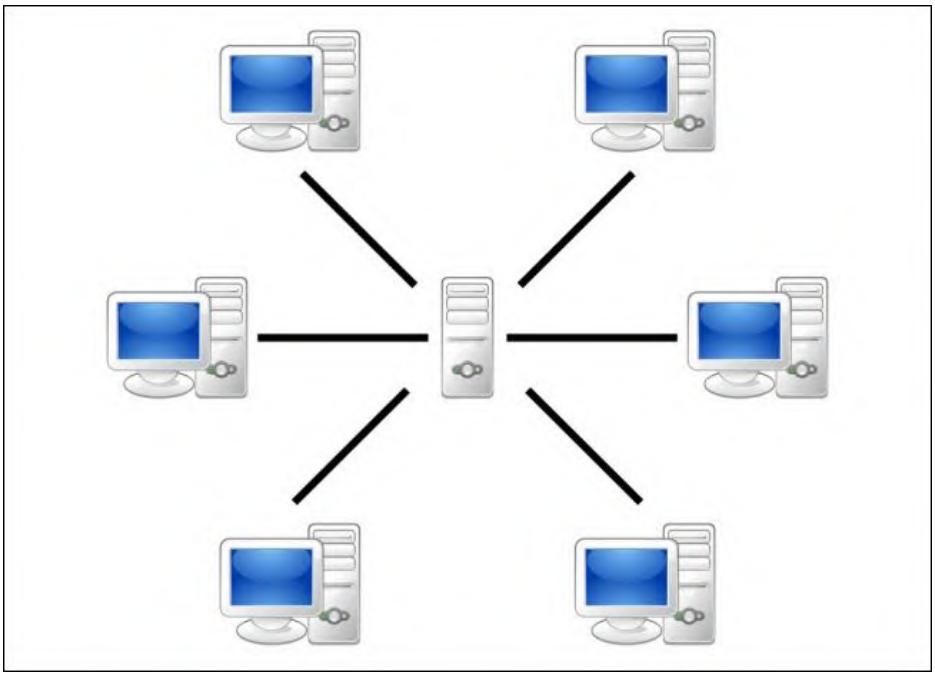
„TACHOnet“ – elektroninė pranešimų sistema, skirta AETR susitariančiosioms šalims tarpusavyje keistis informacija apie vairuotojų korteles. „TACHOnet“ nukreipia užklausas teikiančių šalių užklausas atitinkamoms šalims ir pastarųjų atsakymus pirmosioms. Susitariančiosios šalys, naudojančios „TACHOnet“, privalo prijungti savo nacionalinius vairuotojų kortelių registrus prie sistemos.

2. Architektūra

Pranešimų mainų sistemą „TACHOnet“ sudaro toliau nurodytos dalys.

2.1. Duomenų centras, galintis priimti užklausą teikiančios šalies užklausą, ją patvirtinti ir persiųsti atsakančioms šalims. Duomenų centras laukia, kol kiekviena atsakanti šalis atsakys, sujungia visus atsakymus ir jungtinį atsakymą nusiunčia užklausą pateikusiai šaliai.

2.2. Šalių nacionalinės sistemos, kuriose įrengiama sąsaja, per kurią būtų galima siųsti užklausas į duomenų centrą ir gauti atitinkamus atsakymus. Nacionalinių sistemų pranešimams į duomenų centrą perduoti ir iš jo priimti gali būti naudojama nuosavybinė arba komercinė programinė įranga.



3. Valdymas

3.1. Duomenų centrą valdo ir jo techninį veikimą bei priežiūrą užtikrina Europos Komisija.

3.2. Duomenų centre duomenys, išskyrus 4.7 papildomame priedėlyje nustatytus registravimo ir statistinius duomenis, saugomi ne ilgiau kaip šešis mėnesius.

3.3. Duomenų centras neteikia prieigos prie asmens duomenų, išskyrus prieigą įgaliotiesiems Europos Komisijos darbuotojams, kai tai būtina stebėsenos, techninės priežiūros ir gedimų šalinimo tikslais.

3.4. Kiekvienos susitariančiosios šalies pareigos

3.4.1. Savo nacionalinės sistemos ir jos sąsajos su duomenų centru sukūrimas ir valdymas.

3.4.2. Savo nacionalinės sistemos – techninės ir programinės įrangos (nuosavybinės arba komercinės) – įdiegimas ir techninė priežiūra.

3.4.3. Tinkamos savo nacionalinės sistemos sąveikos su duomenų centru užtikrinimas ir iš jo gautų klaidų pranešimų tvarkymas.

3.4.4. Visų priemonių, būtinų, kad būtų užtikrintas informacijos konfidencialumas, vientisumas ir prieinamumas, taikymas.

3.4.5. Nacionalinės sistemos naudojimas užtikrinant 4.6 papildomame priedėlyje nustatytus paslaugų lygius.

4.2 papildomas priedėlis

„TACHOnet“ funkcijos

1. Pranešimų mainų sistemoje „TACHOnet“ užtikrinamos toliau nurodytos funkcijos.

1.1. Check Issued Cards (CIC) (patikrinti išduotas korteles) – užklausą teikiančiai šaliai suteikia galimybę siųsti CIC užklausą vienai arba visoms atsakančioms šalims, kad būtų galima nustatyti, ar prašymo išduoti kortelę teikėjas jau turi vairuotojo kortelę, išduotą kurioje nors iš atsakančių šalių. Atsakančios šalys į užklausą atsako išsiųsdamos CIC atsakymą.

1.2. Check Card Status (CCS) (patikrinti kortelės statusą) – užklausą teikiančiai šaliai suteikia galimybę išsiųsti CCS užklausą ir taip paprašyti atsakančios šalies pateikti daugiau informacijos apie pastarosios išduotą kortelę. Atsakanti šalis į užklausą atsako išsiųsdama CCS atsakymą.

1.3. Modify Card Status (MCS) (pakeisti kortelės statusą) – užklausą teikiančiai šaliai suteikia galimybę išsiųsti MCS užklausą ir taip pranešti atsakančiai šaliai, kad pastarosios išduotos kortelės statusas pasikeitė. Atsakanti šalis į užklausą atsako išsiųsdama MCS patvirtinimą.

1.4. Issued Card Driving License (ICDL) (kortelė išduota remiantis vairuotojo pažymėjimu) – užklausą teikiančiai šaliai suteikia galimybę išsiųsti ICDL užklausą ir taip pranešti atsakančiai šaliai, kad remdamasi pastarosios išduotu vairuotojo pažymėjimu ji išdavė kortelę. Atsakanti šalis į užklausą atsako išsiųsdama ICDL atsakymą.

2. Įtraukiami ir kitų tipų pranešimai, kurių reikia efektyviam „TACHOnet“ veikimui užtikrinti, pvz., klaidų pranešimai.

3. Nacionalinės sistemos, naudodamosi bet kuria iš 1 punkte išvardytų funkcijų, turi atpažinti 1 lentelėje išvardytas kortelės statuso reikšmes. Tačiau šalys neprivalo įgyvendinti administracinės procedūros, pagal kurią būtų panaudojamos visos išvardytos statuso reikšmės.

4. Kai šalis gauna pranešimą arba atsakymą, kuriame nurodyta jos administracinėse procedūrose nenaudojama statuso reikšmė, nacionalinė sistema gautame pranešime nurodytą statusą konvertuoja į atitinkamą toje procedūroje naudojamą reikšmę. Jei pranešime nurodyta statuso reikšmė yra 1 lentelėje pateiktame sąraše, atsakanti šalis pranešimo neatmeta.

5. 1 lentelėje išvardytos kortelės statuso reikšmės nenaudojamos siekiant nustatyti, ar vairuotojo kortelė yra galiojanti. Kai šalis pateikia kortelę išdavusios nacionalinės institucijos registro užklausą naudodama CCS funkciją, atsakyme turi būti specialus laukas „valid for driving“ (galiojanti). Nacionalinės administracinės procedūros turi būti tokios, kad CCS atsakymuose visada būtų pateikiama atitinkama „valid for driving“ reikšmė.

1 lentelė

Kortelės statuso reikšmės

Kortelės statusas	**Apibrėžtis**
Application (pateiktas prašymas)	KII gavo prašymą išduoti vairuotojo kortelę. Ši informacija užregistruota ir saugoma duomenų bazėje su paieškos reikšminiais žodžiais.
Approved (prašymas patvirtintas)	KII patvirtino prašymą išduoti tachografo kortelę.
Rejected (prašymas atmestas)	KII nepatvirtino prašymo.
Personalised (asmeninė)	Tachografo kortelė skirta konkrečiam asmeniui.
Dispatched (išsiųsta)	Nacionalinė institucija išsiuntė vairuotojo kortelę atitinkamam vairuotojui arba perdavė pristatymo agentūrai.
Handed Over (perduota)	Nacionalinė institucija perdavė vairuotojo kortelę atitinkamam vairuotojui.
Confiscated (konfiskuota)	Kompetentinga institucija atėmė vairuotojo kortelę iš vairuotojo.
Suspended (galiojimas sustabdytas)	Vairuotojo kortelė iš vairuotojo laikinai atimta.
Withdrawn (panaikinta)	KII nusprendė panaikinti vairuotojo kortelę. Kortelė galutinai pripažinta negaliojančia.
Surrendered (grąžinta)	Tachografo kortelė grąžinta KII ir pareikšta, kad jos nebereikia.
Lost (prarasta)	KII pranešta, kad tachografo kortelė prarasta.
Stolen (pavogta)	KII pranešta, kad tachografo kortelė pavogta. Pavogta kortelė laikoma prarasta.
Malfunctioning (neveikianti)	KII pranešta, kad tachografo kortelė neveikia.
Expired (nebegaliojanti)	Tachografo kortelės galiojimo laikotarpis pasibaigęs.
Replaced (pakeista)	Prarasta, pavogta arba neveikianti tachografo kortelė pakeista nauja kortele. Naujoje kortelėje nurodyti tie patys duomenys, išskyrus kortelės numerio pakeitimo indeksą, kuris padidintas vienetu.

Renewed (atnaujinta)	Tachografo kortelė atnaujinta, nes pasikeitė administraciniai duomenys arba baigėsi jos galiojimo laikotarpis. Naujos kortelės numeris yra tas pats, o kortelės numerio atnaujinimo indeksas padidintas vienetu.
In Exchange (keičiama kita kortele)	Vairuotojo kortelę išdavusi KII gavo pranešimą, kad buvo pradėta tos kortelės pakeitimo kitos šalies KII išduota vairuotojo kortele procedūra.
Exchanged (pakeista kita kortele)	Vairuotojo kortelę išdavusi KII gavo pranešimą, kad tos kortelės pakeitimo kitos šalies KII išduota vairuotojo kortele procedūra užbaigta.

4.3 papildomas priedėlis

„TACHOnet“ funkcijos

1. Bendrieji techniniai reikalavimai

1.1. Duomenų centras užtikrina ir sinchroninę, ir asinchroninę sąsajas pranešimų mainams vykdyti. Šalys gali pasirinkti sąsajai su savo taikomosiomis programomis tinkamiausią technologiją.

1.2. Visiems pranešimams, kuriais keičiasi nacionalinės sistemos ir duomenų centras, turi būti naudojama UTF-8 koduotė.

1.3. Nacionalinės sistemos turi gebėti priimti ir apdoroti pranešimus, kuriuose yra graikų abėcėlės arba kirilicos ženklų.

2. XML pranešimų struktūra ir schemos apibrėžtis (XSD)

2.1. Bendroji XML pranešimų struktūra turi atitikti formatą, nustatytą pagal duomenų centre įdiegtas XSD schemas.

2.2. Duomenų centras ir nacionalinės sistemos siunčia ir priima pranešimus, atitinkančius pranešimų XSD schemos reikalavimus.

2.3. Nacionalinės sistemos turi gebėti siųsti, priimti ir apdoroti visus pranešimus, atitinkančius bet kurią iš 4.2 papildomame priedėlyje nustatytų funkcijų.

2.4. XML pranešimai turi atitikti bent 2 lentelėje nurodytus būtinuosius reikalavimus.

2 lentelė

Būtinieji XML pranešimų turinio reikalavimai

Bendra antraštė		**Privaloma**
Version (versija)	Oficialioji XML specifikacijos versija nurodoma pranešimų XSD nustatytoje vardų erdvėje ir kiekvieno XML pranešimo antraštės elemento atributu *version*. Versijos numeris („n.m“) kiekvienos laidos XML schemos apibrėžties faile (xsd) bus nustatomas fiksuota verte.	Taip
Test Identifier (bandymo identifikatorius)	Pasirenkamasis bandymo identifikatorius. Bandymo iniciatorius užpildo identifikatoriaus laukelį, o visi proceso dalyviai perduoda arba nurodo tą patį identifikatorių. Veiklos etape į jį nekreipiama dėmesio ir jis nenaudojamas.	Ne
Technical Identifier (techninis identifikatorius)	Visuotinis unikalus pavadinimas (UUID), kuriuo vienareikšmiškai identifikuojamas kiekvienas atskiras pranešimas. Siuntėjas generuoja UUID ir užpildo šį atributą. Veiklos tikslais šie duomenys nenaudojami.	Taip
Workflow Identifier (proceso identifikatorius)	Proceso indikatorius workflowId – tai UUID, kurį turi generuoti užklausą teikianti šalis. Šis identifikatorius toliau naudojamas visuose pranešimuose procesui koordinuoti.	Taip
Sent At (išsiuntimo laikas)	Pranešimo išsiuntimo data ir laikas (UTC).	Taip
Timeout (skirtasis laikas)	Tai neprivalomas datos ir laiko (UTC formatu) atributas. Persiunčiamoms užklausoms šią reikšmę nustatys tik duomenų centras. Atsakanti šalis iš jos sužino, kada baigiasi užklausai skirtas laikas. Šios reikšmės nereikalaujama MS2TCN_<x>_Req ir visuose atsakomuosiuose pranešimuose. Ji neprivaloma, todėl tą pačią antraštės apibrėžtį galima naudoti visų tipų pranešimams, nepriklausomai nuo to, ar timeoutValue atributas yra privalomas.	Ne
From (siuntėjas)	Pranešimą siunčiančios šalies ISO 3166–1 dviraidis kodas arba „ES“.	Taip
To (adresatas)	Šalies, kuriai skirtas pranešimas, ISO 3166–1 dviraidis kodas arba „ES“.	Taip

4.4 papildomas priedėlis

TRANSLITERACIJOS IR NYSIIS (NIUJORKO VALSTIJOS IDENTIFIKAVIMO IR INFORMACIJOS SISTEMOS) PASLAUGOS

1. Visų vairuotojų pavardės ir vardai nacionaliniame registre koduojami pagal duomenų centre įdiegtą NYSIIS algoritmą.

2. Kortelių paieškai naudojantis CIC funkcija NYSIIS raktai naudojami kaip pagrindinis paieškos mechanizmas.

3. Be to, šalys gali naudoti individualizuotą algoritmą papildomiems rezultatams pateikti.

4. Paieškos rezultatuose nurodoma, kokiu paieškos mechanizmu naudojantis buvo surastas įrašas (NYSIIS ar individualizuotu).

5. Jei šalis nusprendžia registruoti ICDL pranešimus, pranešime nurodyti NYSIIS raktai registruojami kaip ICDL duomenų sudedamoji dalis. Ieškodama ICDL duomenų šalis naudoja pareiškėjo pavardės ir vardo (pavadinimo) NYSIIS raktus.

4.5 papildomas priedėlis

Saugumo reikalavimai

1. Duomenų centro ir nacionalinių sistemų pranešimų mainams naudojamas HTTPS protokolas.

2. Nacionalinėse sistemose naudojami 4.8 ir 4.9 papildomuose priedėliuose nurodyti skaitmeniniai sertifikatai duomenų centro ir nacionalinių sistemų pranešimų mainų saugumui užtikrinti.

3. Nacionalinėse sistemose įdiegiami bent sertifikatai, kuriuose naudojamas SHA-2 (SHA-256) parašo maišos algoritmas ir 2048 bitų ilgio viešasis raktas.

4.6 papildomas priedėlis

Paslaugų lygis

1. Nacionalinės sistemos turi atitikti šiuos būtinuosius paslaugų lygio reikalavimus:

1.1. Jos turi būti prieinamos 24 valandas per parą, 7 dienas per savaitę.

1.2. Jų prieinamumo stebėsena vykdoma iš duomenų centro periodiškai siunčiant takto pranešimus.

1.3. Turi būti užtikrinamas 98 proc. jų prieinamumo lygis pagal šią lentelę (skaičiai suapvalinti iki artimiausio patogaus vieneto):

Prieinamumas	reiškia, kad sistema neprieinama		
	per dieną	per mėnesį	per metus
98 %	0,5 valandos	15 valandų	7,5 dienos

Šalys raginamos užtikrinti dienos prieinamumo lygį, tačiau pripažįstama, kad dėl tam tikros būtinos veiklos, kaip antai techninės priežiūros, gali reikėti sistemą išjungti ilgesniam kaip 30 minučių laikotarpiui. Tačiau mėnesio ir metų prieinamumo rodikliai yra privalomi.

1.4. Jos turi atsakyti ne mažiau kaip į 98 proc. per kalendorinį mėnesį joms persiųstų užklausų.

1.5. Į užklausas jos turi atsakyti per 10 sekundžių.

1.6. Bendrasis užklausai skirtasis laikas (laikas, kurį užklausos teikėjas gali laukti atsakymo) turi neviršyti 20 sekundžių.

1.7. Jos turi užtikrinti 6 užklausų pranešimų per sekundę apdorojimo spartą.

1.8. Nacionalinės sistemos į „TACHOnet“ duomenų centrą turi siųsti ne daugiau kaip 2 užklausas per sekundę.

1.9. Kiekviena nacionalinė sistema turi būti atspari galimoms duomenų centro ar kitų šalių nacionalinių sistemų techninėms problemoms. Be kitų, tokios problemos gali būti:

a) ryšio su duomenų centru praradimas;

b) neatsakymas į užklausą;

c) atsakymų gavimas pasibaigus pranešimo skirtajam laikui;

d) neužsakytų pranešimų gavimas;

e) negaliojančių pranešimų gavimas.

2. Duomenų centras:

2.1. užtikrina 98 proc. prieinamumo lygį;

2.2. teikia pranešimus apie visas klaidas nacionalinėms sistemoms (jie teikiami kaip atsakomasis pranešimas arba kaip specialus klaidos pranešimas). Nacionalinėse sistemose taikomas reagavimo į gautus klaidų pranešimus procesas, kad būtų imtasi tinkamų taisomųjų veiksmų.

3. Techninė priežiūra

Šalys, naudodamosi internetine taikomąja programa, kitoms šalims ir Europos Komisijai praneša apie visus įprastos techninės priežiūros veiksmus bent prieš savaitę iki tų veiksmų pradžios, jei techniškai įmanoma.

4.7 papildomas priedėlis

Duomenų centre renkamų duomenų registravimas ir statistiniai duomenys

1. Siekiant užtikrinti privatumą, statistinėms reikmėms renkami duomenys yra anoniminiai. Konkrečios kortelės, vairuotojo ar vairuotojo pažymėjimo identifikavimo duomenys statistikos tikslais neprieinami.

2. Registravimo informacija stebėsenos ir derinimo tikslais apima informaciją apie visas atliktas operacijas; remiantis tokia registravimo informacija, galima pateikti šių operacijų statistinius duomenis.

3. Asmens duomenys registravimo žurnale nesaugomi ilgiau kaip 6 mėnesius. Statistiniai duomenys saugomi neribotą laiką.

4. Ataskaitoms teikti naudojami statistiniai duomenys:

   a) užklausą teikianti šalis;

   b) atsakanti šalis;

   c) pranešimo tipas;

   d) atsakymo statuso kodas;

   e) pranešimų data ir laikas;

   f) atsakymo laikas.

4.8 papildomas priedėlis

Bendrosios nuostatos dėl „TACHOnet“ skaitmeninių raktų ir sertifikatų

1. Europos Komisijos Informatikos generalinis direktoratas (DIGIT) užtikrina galimybę naudotis PKI paslauga[1] (toliau – CEF PKI paslauga) AETR susitariančiosioms šalims, kurios jungiasi prie „TACHOnet“ (toliau – nacionalinės institucijos) naudodamosi e. pristatymo paslauga.

2. Skaitmeninių sertifikatų užsakymo ir panaikinimo procedūra, taip pat išsamios jų naudojimo sąlygos nustatytos priedėlyje.

3. Sertifikatų naudojimas

3.1. Išduotą sertifikatą nacionalinė institucija[2] naudoja tik naudojimosi „TACHOnet“ tikslais. Sertifikatą galima naudoti:

a) duomenų šaltinio tapatumui nustatyti;

b) duomenims šifruoti;

c) užtikrinti, kad būtų aptinkami duomenų vientisumo pažeidimai.

3.2. Bet koks sertifikato naudojimas kitais nei aiškiai nurodytais leidžiamais tikslais draudžiamas.

4. Susitariančiosios šalys:

a) užtikrina, kad jų privačiaisiais raktais nebūtų naudojamasi be leidimo;

b) neperduoda ir neatskleidžia savo privačiųjų raktų trečiosioms šalims, net kaip atstovėms;

---

1 PKI (viešojo rakto infrastruktūra) – funkcijų, taisyklių, procedūrų ir sistemų, būtinų skaitmeniniams sertifikatams kurti, tvarkyti, platinti ir panaikinti, rinkinys.

2 Identifikuojama pagal išduoto sertifikato lauke *Subject Distinguished Name* nurodytą atributo vertę „O=“.

c) užtikrina sugeneruotų, saugomų ir sistemai „TACHOnet“ naudojamų privačiųjų raktų konfidencialumą, vientisumą ir prieinamumą;

d) sertifikato galiojimo laikotarpiui pasibaigus arba sertifikatą panaikinus privačiojo rakto nebenaudoja, išskyrus šifruotiems duomenims peržiūrėti (pvz., e. laiškams iššifruoti). Nebegaliojantys raktai sunaikinami arba laikomi taip, kad jų nebūtų galima naudoti;

e) registravimo institucijai pateikia įgaliotų atstovų, kuriems leidžiama prašyti panaikinti organizacijai išduotus sertifikatus (panaikinimo prašymuose nurodomas panaikinimo prašymo slaptažodis ir išsami informacija apie įvykius, dėl kurių sertifikatas panaikinamas), identifikavimo duomenis;

f) jei privatusis raktas arba jo aktyvinimo duomenys buvo neteisėtai atskleisti, pareikalauja panaikinti susijusį viešojo rakto sertifikatą ir taip užtikrina, kad privačiaisiais raktais nebūtų galima pasinaudoti be leidimo;

g) elgiasi atsakingai ir laikosi įsipareigojimo prašyti panaikinti sertifikatą sertifikavimo institucijos sertifikavimo taisyklėse (CP) ir sertifikavimo praktikos pareiškime (CPS) nurodytomis aplinkybėmis;

h) nedelsdamos praneša registravimo institucijai apie visų AETR raktų, skirtų naudotis „TACHOnet“, praradimą, vagystę ar galimą atskleidimą.

5. Atsakomybė

Nedarant poveikio Europos Komisijos atsakomybei pagal taikomuose nacionalinės teisės aktuose nustatytus reikalavimus ar atsakomybei, kurios pagal tuos teisės aktus atsižadėti negalima, Europos Komisija nėra atsakinga ar įpareigota dėl:

a) sertifikato turinio, kuris priklauso išimtinai sertifikato savininkui. Sertifikato turinio tikslumo patikrinimas yra sertifikato savininko pareiga;

b) to, kaip sertifikatu naudojasi jo savininkas.

4.9 papildomas priedėlis

„TACHOnet“ skirtos PKI paslaugos aprašas

1. Įvadas

PKI (viešojo rakto infrastruktūra) – funkcijų, taisyklių, procedūrų ir sistemų, būtinų skaitmeniniams sertifikatams kurti, tvarkyti, platinti ir panaikinti, rinkinys[3]. E. pristatymo CEF PKI paslauga užtikrina galimybę išduoti ir tvarkyti skaitmeninius sertifikatus ir taip užtikrinti informacijos, kuria tarpusavyje keičiasi prieigos taškai, konfidencialumą, vientisumą ir nepaneigiamumą.

E. pristatymo PKI paslauga grindžiama sertifikavimo institucija „Trust Center Services TeleSec Shared Business CA“, kuriai taikomi bendrovės „T-Systems International GmbH“[4] sertifikavimo institucijos „TeleSec Shared-Business-CA“ sertifikavimo politika (CP) ir sertifikavimo praktikos pareiškimas (CPS).

PKI tarnyba išduoda sertifikatus, tinkamus įvairiems verslo procesams apsaugoti įmonėse, organizacijose, valdžios institucijose, institucijose, kuriose būtina užtikrinti vidutinio lygio saugumą galutinio subjekto tapatumui, vientisumui ir patikimumui įrodyti, ir už jų ribų.

2. Sertifikato užsakymo procesas

2.1. Funkcijos ir pareigos

2.1.1. Sertifikatą užsakanti organizacija arba nacionalinė institucija

2.1.1.1. Nacionalinė institucija užsako sertifikatus, susijusius su projektu „TACHOnet“.

2.1.1.2 Nacionalinė institucija:

a) CEF PKI tarnybai pateikia sertifikatų užsakymą;

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

[4] Naujausią CP ir CPS versiją galima atsisiųsti iš https://www.telesec.de/en/sbca-en/support/download-area/

b) generuoja privačiuosius raktus ir atitinkamus viešuosius raktus, įtrauktinus į sertifikavimo institucijos išduodamus sertifikatus;

c) atsisiunčia sertifikatą, kai užsakymas patvirtinamas;

d) pasirašo ir registravimo institucijai grąžina:

i) kontaktinių asmenų ir patikimų kurjerių tapatybės nustatymo formą,

ii) pasirašytą atskirą įgaliojimą[5].

2.1.2. Patikimas kurjeris

2.1.2.1. Nacionalinė institucija paskiria patikimą kurjerį.

2.1.2.2. Patikimas kurjeris:

a) tapatybės nustatymo akistatos būdu ir registracijos proceso metu perduoda registravimo institucijai viešąjį raktą;

b) gauna iš registravimo institucijos atitinkamą sertifikatą.

2.1.3. Domeno savininkas

2.1.3.1. Domeno savininkas yra Mobilumo ir transporto generalinis direktoratas.

2.1.3.2. Domeno savininkas:

a) tvirtina ir koordinuoja „TACHOnet“ tinklą ir „TACHOnet“ pasitikėjimo architektūrą ir tvirtina sertifikatų išdavimo tvarką;

b) valdo „TACHOnet“ duomenų centrą ir koordinuoja šalių veiklą, susijusią su „TACHOnet“ veikimu;

c) vykdo, kartu su nacionalinėmis institucijomis, prisijungimo prie „TACHOnet“ bandymus.

---

5 Įgaliojimas yra teisinis dokumentas, kuriuo organizacija įgalioja Europos Komisiją, atstovaujamą nurodyto už CEF PKI paslaugą atsakingo pareigūno, organizacijos vardu pateikti užsakymą bendrovės „T-Systems International GmbH“ sertifikavimo institucijai „TeleSec Shared Business CA“ sukurti sertifikatą. Taip pat žr. 6 punktą. Taup pat žr. 6 punktą.

2.1.4. Registravimo institucija

2.1.4.1. Registravimo institucija yra Jungtinis tyrimų centras (JRC).

2.1.4.2. Registravimo institucija atsakinga už patikimo kurjerio tapatybės patikrinimą ir skaitmeninių sertifikatų išdavimo, panaikinimo ir atnaujinimo prašymų registravimą ir patvirtinimą.

2.1.4.3. Registravimo institucija:

a) nacionalinei institucijai priskiria unikalųjį žymenį;

b) nustato nacionalinės institucijos, jos kontaktinių asmenų ir patikimų kurjerių tapatumą;

c) palaiko ryšius su CEF pagalbos tarnyba nacionalinės institucijos, jos kontaktinių asmenų ir patikimų kurjerių tapatumo klausimais;

d) informuoja nacionalinę instituciją apie sertifikato patvirtinimą arba atmetimą.

2.1.5. Sertifikavimo institucija

2.1.5.1. Sertifikavimo institucija atsakinga už skaitmeninių sertifikatų užsakymo, išdavimo ir panaikinimo techninės infrastruktūros teikimą.

2.1.5.2. Sertifikavimo institucija:

a) teikia nacionalinių institucijų sertifikatų užsakymams būtiną techninę infrastruktūrą;

b) tvirtina arba atmeta sertifikatų užsakymus;

c) prireikus palaiko ryšius su registravimo institucija dėl prašančiosios organizacijos tapatumo patikrinimo.

2.2. Sertifikatų išdavimas

2.2.1. Sertifikatai išduodami nuosekliai atliekant šiuos etapus, kaip pavaizduota 1 pav.:

a) **1 etapas:** patikimo kurjerio tapatybės nustatymas;

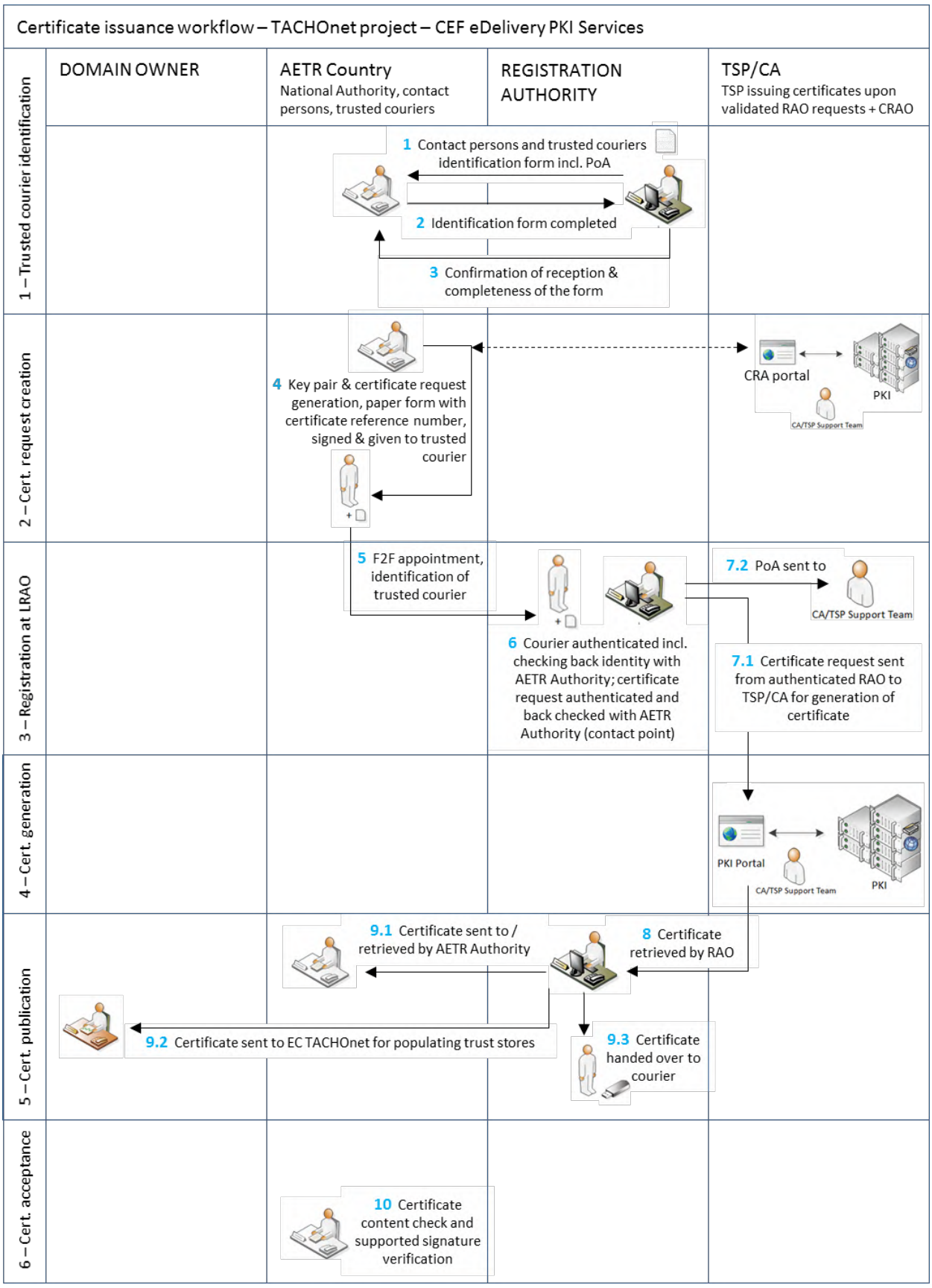
b) **2 etapas:** sertifikato užsakymo sukūrimas;

c) **3 etapas:** registravimas registravimo institucijoje;

d) **4 etapas:** sertifikato sukūrimas;

e) **5 etapas:** sertifikato paskelbimas;

f) **6 etapas:** sertifikato patvirtinimas.



1 pav. Sertifikato išdavimo procesas

2.2.2. 1 etapas: patikimo kurjerio tapatybės nustatymas;

Patikimo kurjerio tapatybės nustatymo procesas:

a) Registravimo institucija nusiunčia nacionalinei institucijai kontaktinių asmenų ir patikimų kurjerių tapatybės nustatymo formą[6]. Šioje formoje yra ir įgaliojimas, kurį organizacija (AETR institucija) pasirašo.

b) Nacionalinė institucija grąžina registravimo institucijai užpildytą formą ir pasirašytą įgaliojimą.

c) Registravimo institucija patvirtina, kad gavo tinkamai užpildytą formą.

d) Registravimo institucija domeno savininkui pateikia atnaujinto kontaktinių asmenų ir patikimų kurjerių sąrašo kopiją.

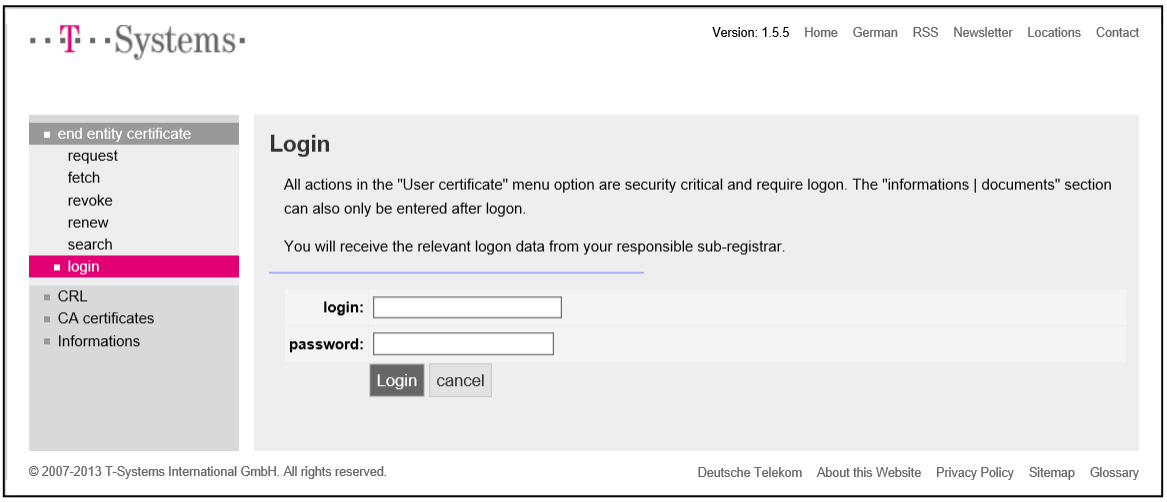
2.2.3. 2 etapas: sertifikato užsakymo sukūrimas;

2.2.3.1. Sertifikatas užsakomas ir atsiimamas tuo pačiu kompiuteriu ir naudojant tą pačią naršyklę.

2.2.3.2. Sertifikato užsakymo sukūrimo procesas:

a) Organizacija naršyklėje atsidaro internetinės vartotojo sąsajos puslapį, kurio URL https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: ir įrašo vartotojo vardą „**sbca/CEF_eDelivery.europa.eu**“ ir slaptažodį „**digit.333**“;

6 Žr. 5 punktą.

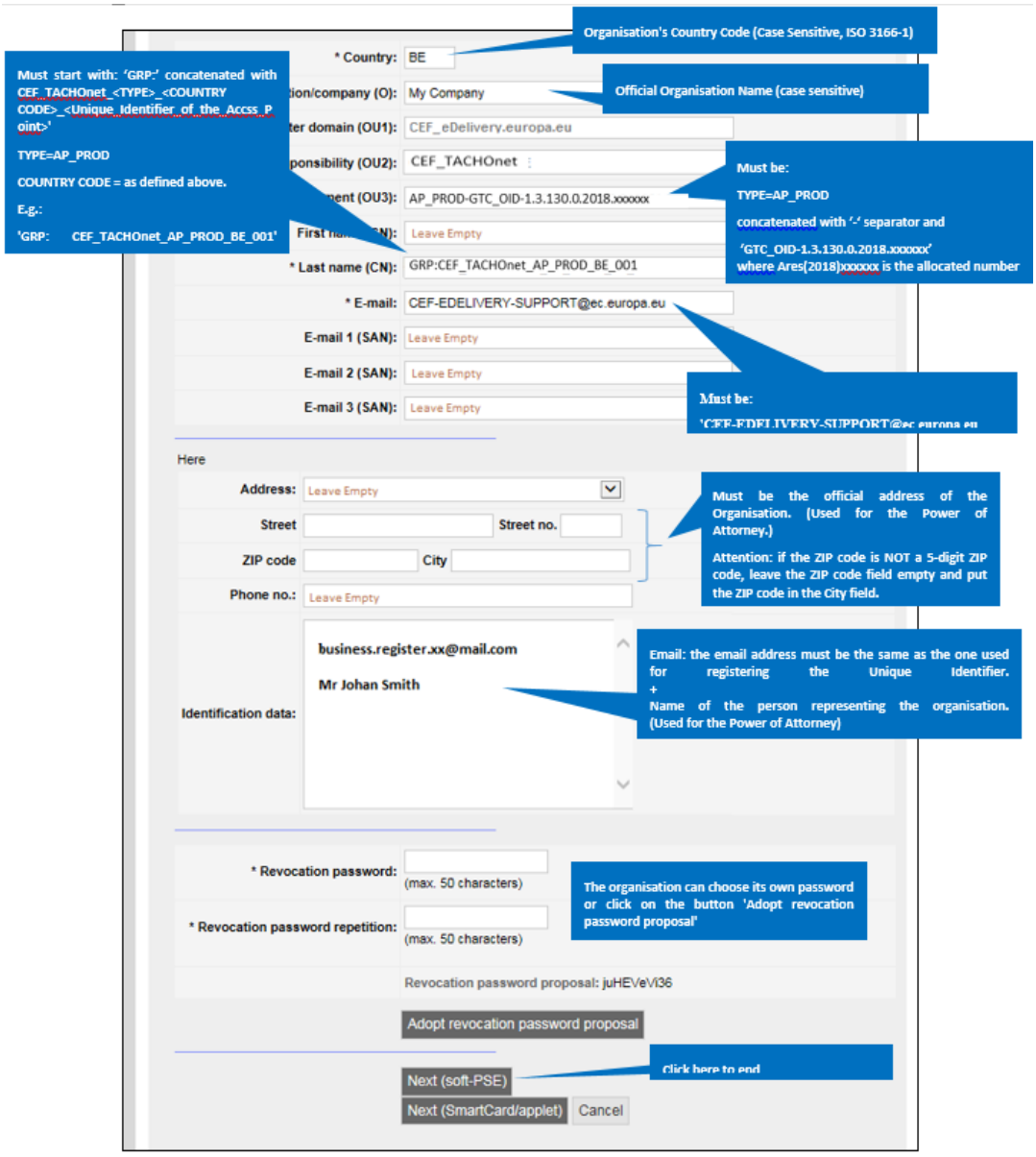


2 pav.

b) Organizacija spusteli mygtuką „request“ (užsakyti) kairėje polangio pusėje ir išskleidžiamajame sąraše pasirenka „CEF_TACHOnet“.

3 pav.

c) Organizacija užpildo 4 pav. pavaizduotą sertifikato užsakymo formą 3 lentelėje nurodyta informacija ir spustelėdama mygtuką „Next (soft-PSE)“ užbaigia procesą.


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

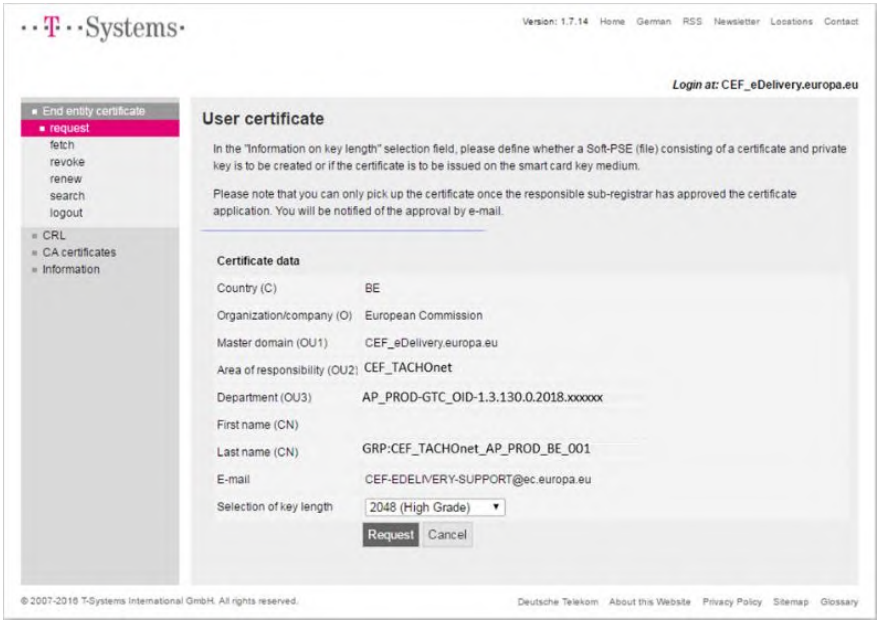
4 pav.

Laukeliai, kuriuos prašoma užpildyti	Aprašymas
Country (šalis)	**C=šalies kodas**, sertifikato savininko vieta, patikrinta pagal viešąjį registrą; Apribojimai: 2 ženklai pagal ISO 3166-1, dviraidis kodas, skirti didžiąsias ir mažąsias raides. Pavyzdžiai: DE, BE, NL. Specifiniai atvejai: UK (Didžioji Britanija), EL (Graikija)
Organisation/Company (O) (organizacija, įmonė)	**O=sertifikato savininko organizacijos pavadinimas**
Master domain (OU1) (pagrindinis domenas)	**OU=CEF_eDelivery.europa.eu**
Area of responsibility (OU2) (atsakomybės sritis)	**OU=CEF_TACHOnet**
Department (OU3) (skyrius)	Privaloma nurodyti kiekvienai „AREA OF RESPONSIBILITY“. Sertifikato užsakymo metu turinį būtina patikrinti pagal leidžiamų reikšmių sąrašą (white list). Jei informacija neatitinka nurodytosios sąraše, užsakymas nepriimamas. Formatas: **OU=<TYPE>-<GTC_NUMBER>** Čia "<TYPE>" pakeičiamas reikšme AP_PROD – prieigos taškas gamybos aplinkoje. Ir kai <GTC_NUMBER> yra **GTC_OID-1.3.130.0.2018.xxxxxx**, čia Ares(2018)xxxxxx yra „TACHOnet“ projekto GTC numeris. Pvz.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN) (vardas)	Turi būti paliktas tuščias
Last name (CN) (pavardė)	Turi prasidėti „GRP:“, toliau bendrinis pavadinimas. Formatas: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** Pvz.: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail (e. paštas)	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
E-mail 1 (SAN)	Turi būti paliktas tuščias
E-mail 2 (SAN)	Turi būti paliktas tuščias
E-mail 3 (SAN)	Turi būti paliktas tuščias

Adress (adresas)	Turi būti paliktas tuščias
Street (gatvė)	Turi būti nurodytas oficialus sertifikato savininko organizacijos adresas (naudojamas įgaliojimui).
Street no. (namo numeris)	Turi būti nurodytas oficialus sertifikato savininko organizacijos adresas (naudojamas įgaliojimui).
Zip Code (pašto kodas)	Turi būti nurodytas oficialus sertifikato savininko organizacijos adresas (naudojamas įgaliojimui). **Dėmesio:** jei pašto kodas yra NE 5 skaitmenų pašto kodas, palikite pašto kodo lauką tuščią ir nurodykite pašto kodą lauke „City“ (miestas).
City (miestas)	Turi būti nurodytas oficialus sertifikato savininko organizacijos adresas (naudojamas įgaliojimui). **Dėmesio:** jei pašto kodas yra NE 5 skaitmenų pašto kodas, palikite pašto kodo lauką tuščią ir nurodykite pašto kodą lauke „City“ (miestas).
Phone no (telefono numeris)	Turi būti paliktas tuščias
Identification data (tapatybės duomenys)	E. pašto adresas turi būti tas pats, kuriuo naudotasi unikaliajam žymeniui užregistruoti. + Turi būti nurodytas organizacijai atstovaujančio asmens vardas ir pavardė (naudojamas įgaliojimui). + **Numeris įmonių registre** (privaloma nurodyti tik privačioms organizacijoms). **Įrašyta vietos teismo registre** (reikalaujama nurodyti tik Vokietijos ir Austrijos privačioms organizacijoms)
Revocation password (panaikinimo slaptažodis)	Lauką būtina užpildyti užsakovo pasirinktu slaptažodžiu
Revocation password repetition (pakartoti panaikinimo slaptažodį)	Lauką būtina užpildyti tuo pačiu užsakovo pasirinktu slaptažodžiu

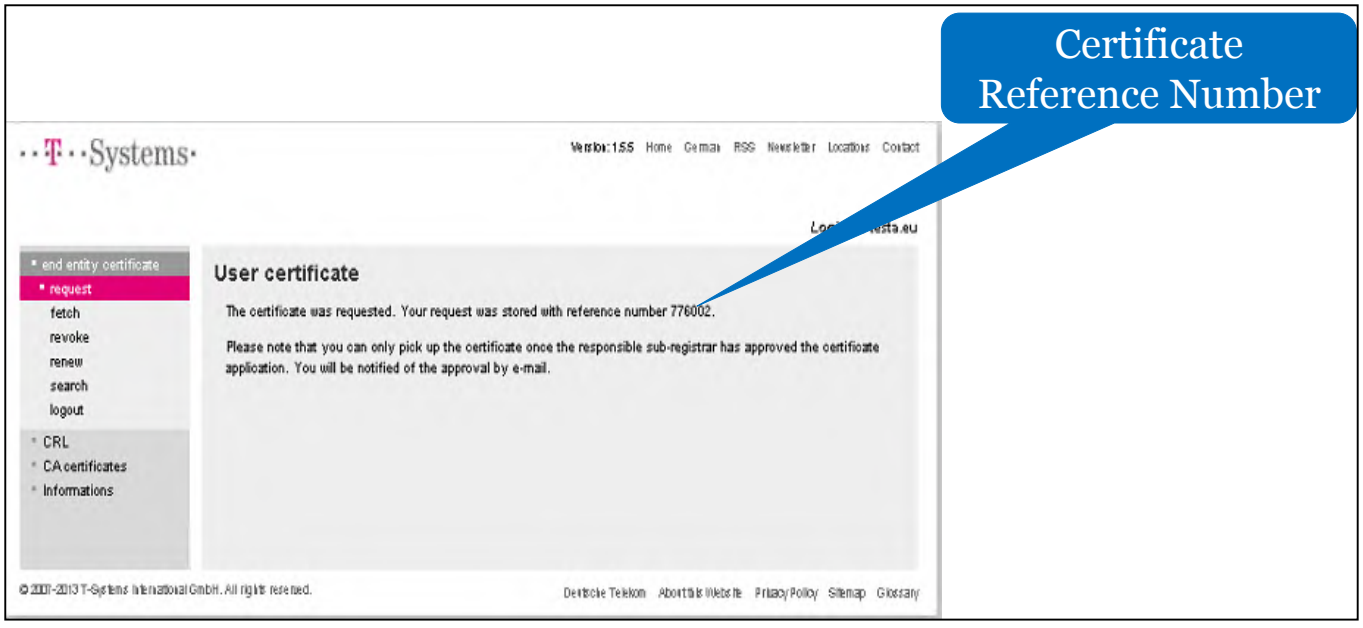
3 lentelė. Išsami informacija apie kiekvieną lauką, kurį prašoma užpildyti.

d) Pasirenkamas rakto ilgis turi būti „2048(High Grade)“.



5 pav.

e) Organizacija užsirašo sertifikato numerį, pagal kurį bus galima atsiimti sertifikatą.



6 pav.

f) CEF pagalbos tarnyba patikrina, ar yra naujų sertifikatų užsakymų ir ar sertifikato užsakyme pateikta informacija yra tinkama, t. y., ar ji nurodyta laikantis pavadinimų darybos nuostatų, pateiktų 5.1 priedėlyje „Sertifikatų pavadinimų darybos nuostatos“.

g) CEF pagalbos tarnyba patikrina, ar užsakyme pateikta informacija yra tinkamo formato.

h) Jei 5 arba 6 punkto patikrinimo rezultatas neigiamas, CEF pagalbos tarnyba nusiunčia e. laišką, kuriame organizacijos prašoma procesą pradėti iš naujo, užsakymo formos skyrelyje „Identification data“ nurodytu e. pašto adresu, o jo kopiją (cc) – domeno savininkui. Nesėkmingas sertifikato užsakymas atmetamas.

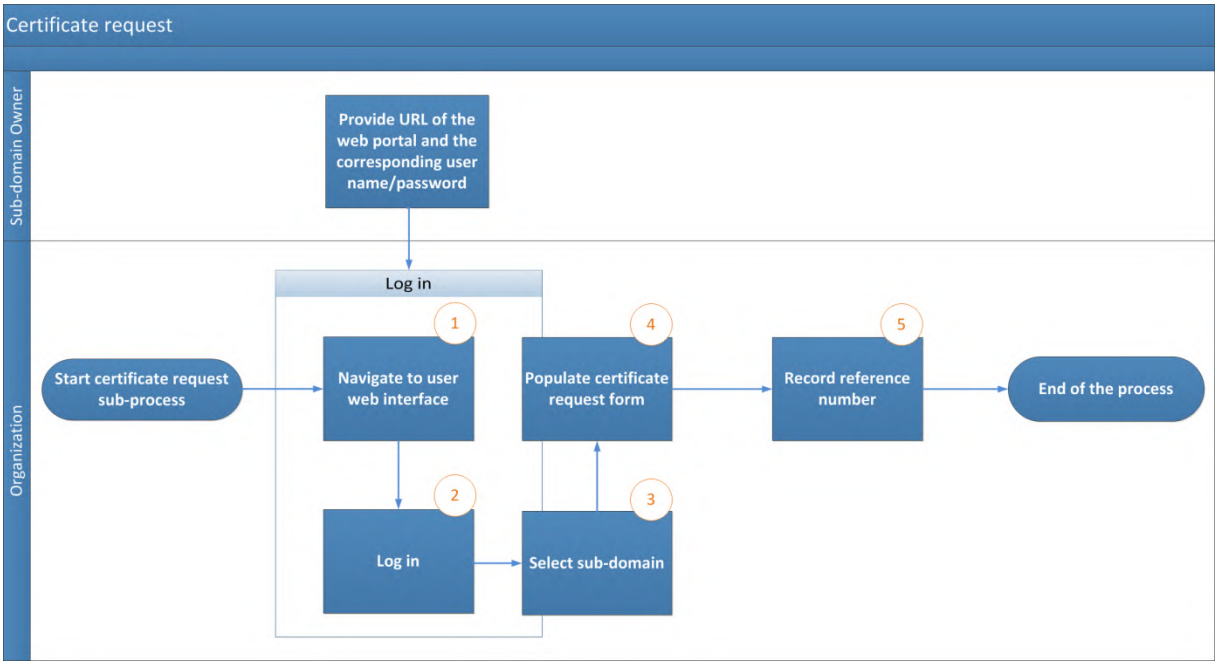
i) CEF pagalbos tarnyba nusiunčia e. laišką registravimo institucijai, jame nurodydama, ar užsakymas galioja. E. laiške nurodoma:

   1) organizacijos pavadinimas, nurodytas sertifikato užsakymo lauke „Organisation (O)“;

   2) sertifikato duomenys, kuriuos sudaro prieigos taško, kuriam turi būti išduotas sertifikatas, pavadinimas, nurodytas sertifikato užsakymo laukelyje „Last Name (CN)“;

   3) sertifikato numeris;

   4) organizacijos adresas, e. pašto adresas ir jai atstovaujančio asmens vardas ir pavardė.



7 pav. Sertifikato užsakymo procesas

2.2.4. 3 etapas: registravimas registravimo institucijoje (sertifikato patvirtinimas)

2.2.4.1. Patikimas kurjeris arba kontaktinis asmuo e. paštu susitaria su registravimo institucija dėl vizito ir nurodo patikimą kurjerį, kuris atvyks akistaton.

2.2.4.2. Organizacija parengia dokumentų rinkinį, kurį sudaro:

a) užpildytas ir pasirašytas įgaliojimas;

b) patikimo kurjerio, kuris atvyks akistaton, galiojančio paso kopija. Ši kopija turi būti pasirašyta vieno iš 1 etape nurodytų organizacijos kontaktinių asmenų;

c) rašytinė sertifikato užsakymo forma, pasirašyta vieno iš organizacijos kontaktinių asmenų.

2.2.4.3. Pastato registratūroje patikrinusi patikimo kurjerio tapatybę, registravimo institucija priima patikimą kurjerį. Registravimo institucija akistatoje užregistruoja sertifikato užsakymą, t. y. atlieka šiuos veiksmus:

a) nustato ir patvirtina patikimo kurjerio tapatybę;

b) patikrina patikimo kurjerio išvaizdą pagal jo pateiktą pasą;

c) patikrina, ar galioja patikimo kurjerio pateiktas pasas;

d) patikrina, ar patikimo kurjerio pateiktas ir patikrintas pasas atitinka vieno iš organizacijos kontaktinių asmenų pasirašytą galiojančio patikimo kurjerio paso kopiją. Parašo autentiškumas patikrinamas pagal patikimų kurjerių ir kontaktinių asmenų tapatybės nustatymo formos originalą;

e) patikrina užpildytą ir pasirašytą įgaliojimą;

f) patikrina rašytinę sertifikato užsakymo formą ir joje esantį parašą pagal patikimų kurjerių ir kontaktinių asmenų tapatybės nustatymo formos originalą;

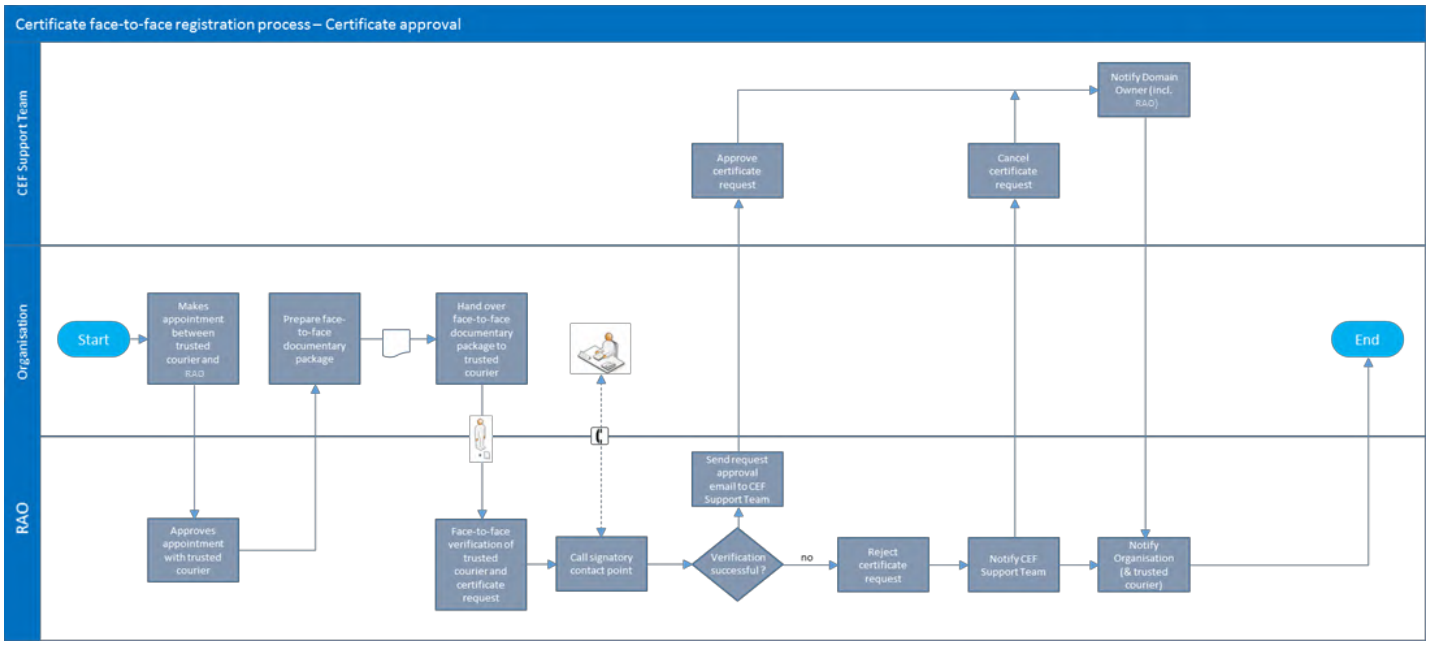
g) paskambina pasirašiusiam kontaktiniam asmeniui ir dar kartą patikrina patikimo kurjerio tapatybę ir sertifikato užsakymo turinį.

2.2.4.4. Registravimo institucija CEF pagalbos tarnybai patvirtina, kad nacionalinė institucija iš tiesų įgaliota naudotis komponentais, kuriems prašo išduoti sertifikatus, ir kad atitinkamas registracijai skirtas akistatos procesas atliktas sėkmingai. Patvirtinimas siunčiamas naudojant „CommiSign“ sertifikatą, saugiu paštu, pridedant skenuotą dokumentų rinkinį, kurio autentiškumas patvirtintas per akistatą, ir pasirašytą proceso metu registravimo institucijos atliktų patikrinimų sąrašą.

2.2.4.5. Jei registravimo institucija patvirtina, kad užsakymas galioja, procesas vykdomas toliau, kaip nustatyta 2.2.4.6 ir 2.2.4.7 punktuose. Priešingu atveju išduoti sertifikatą atsisakoma ir apie tai informuojama organizacija.

2.2.4.6. CEF pagalbos tarnyba patvirtina sertifikato užsakymą ir praneša registravimo institucijai apie sertifikato patvirtinimą.

2.2.4.7. Registravimo institucija praneša organizacijai, kad sertifikatą galima atsiimti vartotojų portale.



8 pav. Sertifikato patvirtinimas

2.2.5. 4 etapas: sertifikato sukūrimas

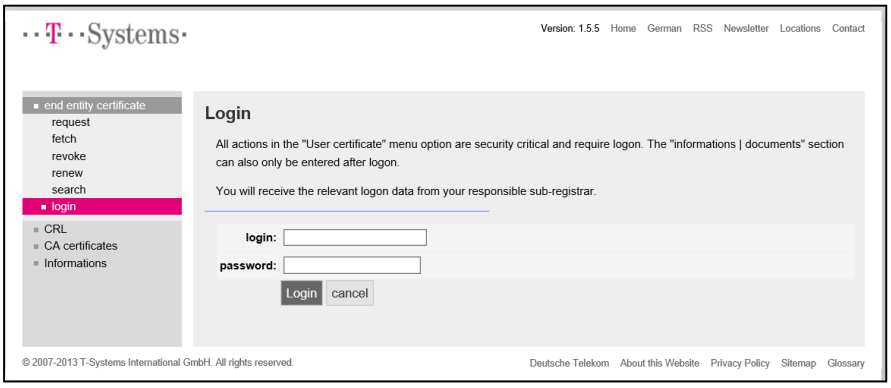
Kai sertifikato užsakymas patvirtinamas, sukuriamas sertifikatas.

2.2.6. 5 etapas: sertifikato paskelbimas ir atsiėmimas

2.2.6.1. Kai patvirtinamas sertifikato užsakymas, registravimo institucija paima sertifikatą ir perduoda kopiją patikimam kurjeriui.

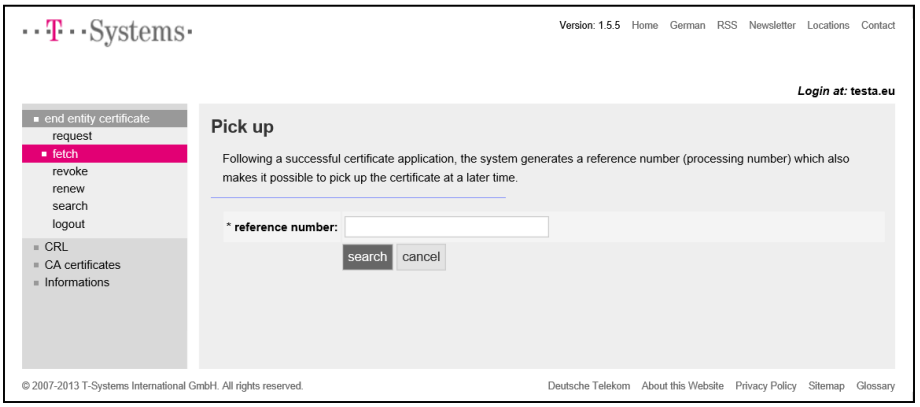
2.2.6.2. Organizacija gauna registravimo institucijos pranešimą, kad sertifikatus galima atsiimti.

2.2.6.3. Organizacija atsidaro vartotojų portalo puslapį https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en ir prisijungia vartotojo vardu „**sbca/CEF_eDelivery.europa.eu**“ ir slaptažodžiu „digit.333“.



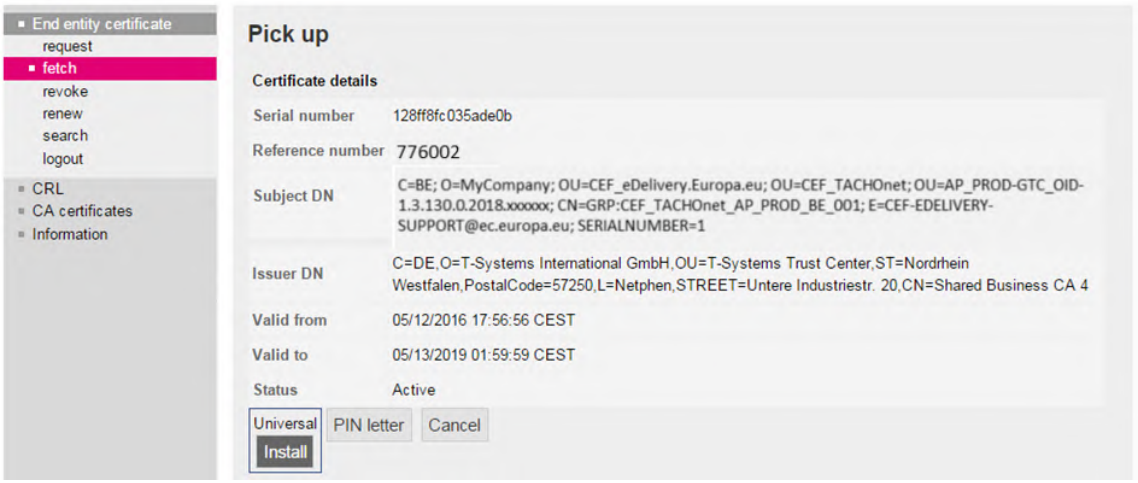
9 pav.

2.2.6.4. Organizacija spusteli mygtuką „fetch“ (pasiimti) kairėje pusėje ir nurodo numerį, kurį užsirašė užsakydama sertifikatą.



10 pav.

2.2.6.5. Organizacija įdiegia sertifikatus, spustelėdama įdiegimo mygtuką.



11 pav.

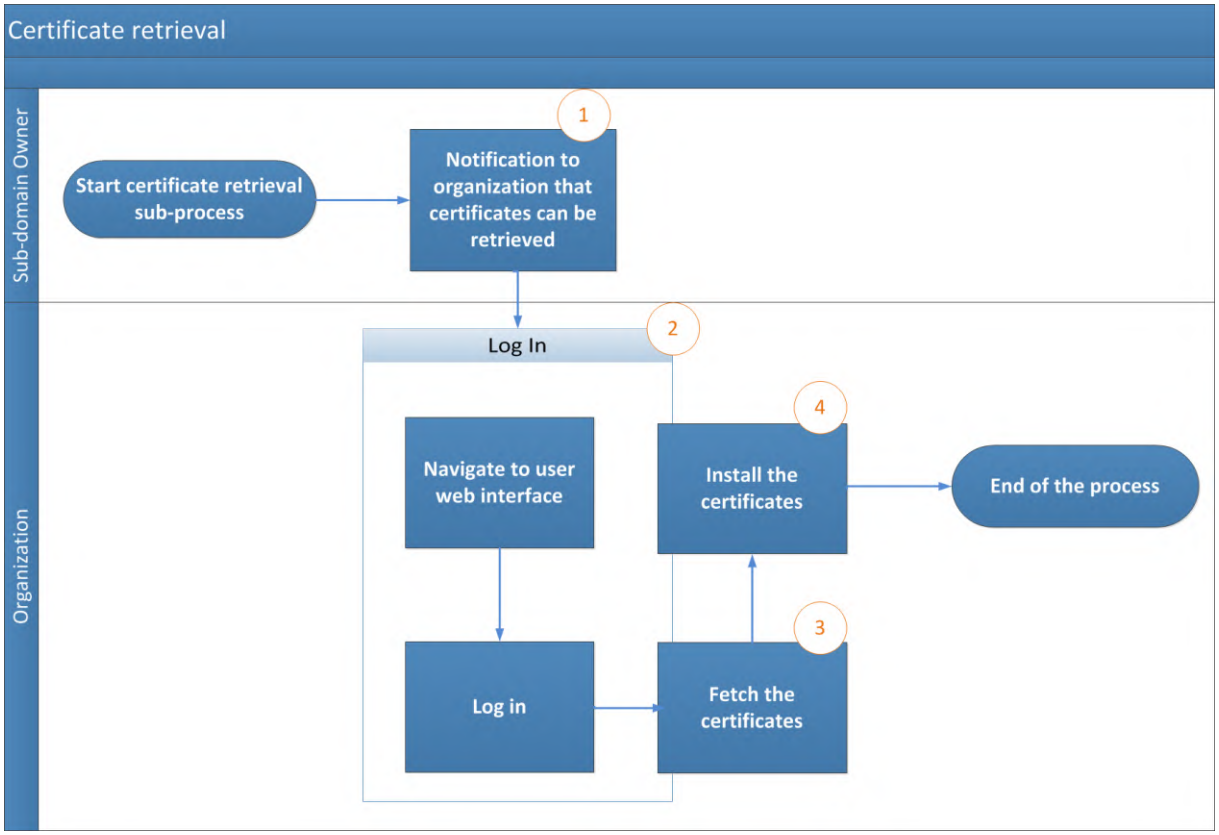
2.2.6.6. Sertifikatas įdiegiamas prieigos taške. Kadangi tai priklauso nuo konkretaus įgyvendinimo, organizacija šio proceso aprašą gauna iš prieigos taško teikėjo.

2.2.6.7. Sertifikatui įdiegti prieigos taške reikia atlikti šiuos veiksmus:

a) eksportuoti privatųjį raktą ir sertifikatą,

b) sukurti raktų saugyklą ir pasitikėjimo sertifikatų saugyklą,

c) įdiegti raktų saugyklą ir pasitikėjimo sertifikatų saugyklą prieigos taške.

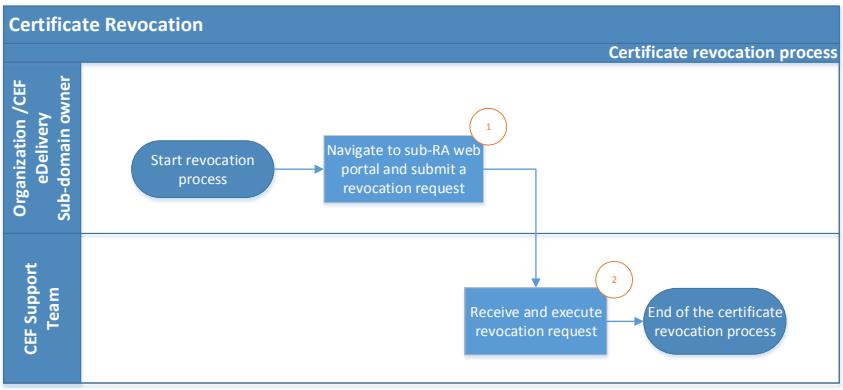


12 pav. Sertifikato atsiėmimas

3. Sertifikato panaikinimo procesas

3.1. Panaikinimo prašymą organizacija pateikia internetiniame vartotojų portale;

3.2. CEF pagalbos tarnyba panaikina sertifikatą.



13 pav. Sertifikato panaikinimas

4. Bendrosios CEF PKI paslaugos sąlygos

4.1. Bendrosios aplinkybės

Vykdydamas Europos infrastruktūros tinklų priemonės e. pristatymo funkcinio bloko sprendimo teikėjo funkciją, Informatikos generalinis direktoratas AETR susitariančiosioms šalims teikia PKI paslaugą[7] (CEF PKI paslauga). CEF PKI paslauga naudojasi nacionalinės institucijos (galutiniai paslaugos gavėjai), dalyvaujančios „TACHOnet“ veikloje.

Informatikos generalinis direktoratas yra „TeleSec Shared-Business-CA“ (SBCA) sprendimo, teikiamo grupės „T-Systems International GmbH“ („T-Systems“[8]) patikimumo centre, PKI nuomininkas. Informatikos generalinis direktoratas vykdo SBCA srities „CEF_eDelivery.europa.eu“ pagrindinio registro funkciją. Vykdydamas šią funkciją Informatikos generalinis direktoratas kuria srities „CEF_eDelivery.europa.eu“ posričius kiekvienam projektui, kuriam naudojama CEF PKI paslauga.

Šiame dokumente pateikiama išsami informacija apie „TACHOnet“ posričio sąlygas. Informatikos generalinis direktoratas vykdo šio posričio papildomo registro funkciją. Ją vykdydamas, jis išduoda, panaikina ir atnaujina šio projekto sertifikatus.

4.2. Atsakomybės ribojimas

Europos Komisija neprisiima jokios atsakomybės dėl sertifikato turinio – tai išimtinė sertifikato savininko atsakomybė. Sertifikato turinio tikslumo patikrinimas yra sertifikato savininko pareiga.

Europos Komisija neprisiima jokios atsakomybės dėl to, kaip sertifikatu naudojasi jo savininkas, kuris yra Komisijai nepriklausantis trečiasis teisinis subjektas.

---

7 PKI (viešojo rakto infrastruktūra) – funkcijų, taisyklių, procedūrų ir sistemų, būtinų skaitmeniniams sertifikatams kurti, tvarkyti, platinti ir panaikinti, rinkinys.

8 T-Systems“ Patikimumo centro operatoriaus patikimumo funkcija apima ir tarptautinės registravimo institucijos užduočių vykdymą.

Šiuo atsakomybės apribojimo pareiškimu nesiekiama apriboti Europos Komisijos atsakomybės pažeidžiant kokius nors taikytinoje nacionalinėje teisėje nustatytus reikalavimus ar atsižadėti atsakomybės tais klausimais, kuriais atsakomybės pagal tokius teisės aktus atsižadėti negalima.

4.3. Leidžiamas ir draudžiamas sertifikatų naudojimas

4.3.1. Leidžiamas sertifikatų naudojimas

Išduotą sertifikatą jo savininkas[9] naudoja tik naudojimosi „TACHOnet“ tikslais. Tuo tikslu sertifikatą galima naudoti:

- duomenų šaltinio tapatumui nustatyti;
- duomenims šifruoti;
- užtikrinti, kad būtų aptinkami duomenų vientisumo pažeidimai.

4.3.2. Draudžiamas sertifikatų naudojimas

Bet koks sertifikato naudojimas kitais nei aiškiai nurodytais leidžiamais tikslais draudžiamas.

4.4. Papildomos sertifikato savininko pareigos

Išsamios SBCA sąlygos nustatytos bendrovės „T-Systems“ SBCA paslaugos[10] Sertifikavimo politikos (CP) ir sertifikavimo praktikos pareiškimo (CPS) dokumente. Šiame dokumente pateikiamos saugumo specifikacijos ir techninių bei organizacinių aspektų gairės ir aprašoma patikimumo centro operatoriaus veikla vykdant sertifikavimo institucijos ir registravimo institucijos, taip pat registravimo institucijos deleguotos trečiosios šalies funkcijas.

Užsakyti sertifikatą gali tik subjektai, kuriems leidžiama dalyvauti „TACHOnet“ veikloje.

---

9 Identifikuojama pagal išduoto sertifikato lauke *Subject Distinguished Name* nurodytą atributo vertę „O=“.

10 Naujausią bendrovės „T-Systems“ SBCA CP/CPS versiją galima rasti adresu https://www.telesec.de/en/sbca-en/support/download-area/.

Dėl sertifikato priėmimo taikomas SBCA Sertifikavimo politikos ir sertifikavimo praktikos pareiškimo (CP/CPS) 4.4.1 punktas, be to, laikoma, kad organizacija, kuriai išduotas sertifikatas („O=“), sutinka su šiame dokumente aprašytomis naudojimo sąlygomis, kai pirmą kartą panaudoja sertifikatą.

Dėl sertifikato paskelbimo taikomas SBCA CP/CPS 2.2 punktas.

Visi sertifikatų savininkai laikosi šių reikalavimų:

1) užtikrina, kad jų privačiaisiais raktais nebūtų naudojamasi be leidimo;

2) neperduoda ir neatskleidžia savo privačiųjų raktų trečiosioms šalims, net kaip atstovėms;

3) sertifikato galiojimo laikotarpiui pasibaigus arba sertifikatą panaikinus privačiojo rakto nebenaudoja, išskyrus šifruotiems duomenims peržiūrėti (pvz., e. laiškams iššifruoti).

4) sertifikato savininkas atsako už rakto kopijavimą arba persiuntimą galutiniam subjektui ar subjektams;

5) sertifikato savininkas privalo įpareigoti galutinį subjektą (visus galutinius subjektus) naudoti privatųjį raktą laikantis šių sąlygų, įskaitant SBCA CP/CPS;

6) sertifikato savininkas privalo nurodyti identifikavimo duomenis įgaliotųjų atstovų, kurie, nurodydami išsamias įvykių, dėl kurių reikia panaikinti sertifikatą, aplinkybes ir panaikinimo slaptažodį, turi teisę prašyti panaikinti organizacijai išduotus sertifikatus;

7) jei sertifikatas susijęs su asmenų ir pareigų grupe ir (arba) juridiniu asmeniu, kai asmuo palieka galutinių subjektų grupę (pvz., nutraukiami darbo santykiai), sertifikato savininkas privalo panaikinti sertifikatą ir taip užtikrinti, kad privatusis raktas nebūtų panaudotas be leidimo;

8) susidarius SBCA CP/CPS 4.9.1 punkte nurodytoms aplinkybėms, atsakingas yra sertifikato savininkas ir jis paprašo panaikinti sertifikatą.

Dėl sertifikato ar jo raktų atnaujinimo taikomas SBCA CP/CPS 4.6 arba 4.7 punktas.

Dėl sertifikato pakeitimų taikomas SBCA CP/CPS 4.8 punktas.

Dėl sertifikato panaikinimo taikomas SBCA CP/CPS 4.9 punktas.

5. Kontaktinių asmenų ir patikimų kurjerių tapatybės nustatymo forma (pavyzdys)

Aš, *[organizacijos atstovo vardas, pavardė ir adresas]*, **patvirtinu, kad užsakant, kuriant ir atsiimant „TACHOnet“ prieigos taškų viešųjų raktų skaitmeninius sertifikatus, padedančius užtikrinti „TACHOnet“ pranešimų konfidencialumą, vientisumą ir nepaneigiamumą, turi būti naudojama ši informacija:**

Kontaktinių asmenų duomenys:

– **1-as kontaktinis asmuo**	– **2-as kontaktinis asmuo**
– Pavardė:	– Pavardė:
– Vardai:	– Vardai:
– Mobilaus telefono Nr.:	– Mobilaus telefono Nr.:
– Telefonas	– Telefonas
– El. paštas:	– El. paštas:
– Parašo pavyzdys: –	– Parašo pavyzdys: – – –

Patikimų kurjerių duomenys**:**

– **1-as patikimas kurjeris**	– **2-as patikimas kurjeris**
– Pavardė:	– Pavardė:
– Vardai:	– Vardai:
– Mobilaus telefono Nr.:	– Mobilaus telefono Nr.:
– El. paštas:	– El. paštas:
– Pasą išdavusi šalis:	– Pasą išdavusi šalis:
– Paso Nr.:	– Paso Nr.:
– Paso galiojimo pabaigos data:	– Paso galiojimo pabaigos data:

Vieta, data ir įmonės arba organizacijos antspaudas:

Įgaliotojo atstovo parašas:

6. Dokumentai

6.1. Atskiras įgaliojimas (pavyzdys)

Atskiro įgaliojimo, kurį būtina pasirašyti ir kurį patikimas kurjeris turi pateikti akistatoje registravimo institucijos organizacijoje, pavyzdys:

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. Rašytinė sertifikato užsakymo forma (pavyzdys)

Rašytinės sertifikato užsakymo formos, kurią būtina pasirašyti ir kurią patikimas kurjeris turi pateikti akistatoje registravimo institucijos organizacijoje, pavyzdys:

7. Žodynėlis

Pagrindiniai šiame papildomame priedėlyje vartojami terminai apibrėžti Europos infrastruktūros tinklų priemonės bendrojo skaitmeninio portalo Infrastruktūros tinklų priemonės apibrėžčių skirsnyje:

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

Pagrindiniai šiame siūlomų komponentų apraše vartojami akronimai apibrėžti Europos infrastruktūros tinklų priemonės bendrojo skaitmeninio portalo Infrastruktūros tinklų priemonės žodynėlyje:

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