Vijeće
Europske unije

Bruxelles, 5. studenoga 2018.
(OR. en)

13711/18
ADD 1

Međuinstitucijski predmet:
2018/0339(NLE)

TRANS 488

NAPOMENA

Od:	Glavno tajništvo Vijeća
Za:	Delegacije
Br. preth. dok.:	ST 13711/18 TRANS 448
Br. dok. Kom.:	ST 12727/18 TRANS 426 + ADD 1
Predmet:	Odluka Vijeća o stajalištu koje treba zauzeti u ime Europske unije u Skupini stručnjaka Gospodarske komisije Ujedinjenih naroda za Europu o Europskom sporazumu o radu posada vozila u međunarodnom cestovnom prijevozu

Privitak uz navedenu Odluku Vijeća.

PRIVITAK

Novi dodatak Europskom sporazumu o radu posada vozila u međunarodnom cestovnom prijevozu (AETR)

Dodatak 4.

Specifikacije sustava TACHOnet

1. Područje primjene i svrha

1.1. Ovim se Dodatkom utvrđuju uvjeti povezivanja ugovornih stranaka AETR-a na sustav TACHOnet putem platforme e-dostava.

1.2. Ugovorne stranke koje se na sustav TACHOnet povezuju putem platforme e-dostava postupaju u skladu s odredbama utvrđenima u ovom Dodatku.

2. Definicije

(a) „ugovorna stranka” ili „stranka” znači svaka ugovorna stranka AETR-a;

(b) „e-dostava” znači usluga koju je razvila Europska komisija koja omogućuje prijenos podataka među trećim stranama elektroničkim putem i pruža dokaze o postupanju s prenesenim podacima, uključujući dokaz o slanju i primanju podataka, čime se preneseni podaci štite od opasnosti neovlaštenih preinaka;

(c) „TACHOnet” znači sustav za elektroničku razmjenu informacija o karticama vozača među ugovornim strankama iz članka 31. stavka 2. Uredbe (EU) br. 165/2014;

(d) „centralno čvorište” znači informacijski sustav koji omogućuje usmjeravanje poruka sustava TACHOnet među strankama koje upućuju zahtjev i strankama koje odgovaraju na zahtjev;

(e) „stranka koja upućuje zahtjev” znači ugovorna stranka koja upućuje zahtjev ili obavijest putem sustava TACHOnet, koje zatim centralno čvorište prosljeđuje odgovarajućoj stranki koja odgovara na zahtjev;

(f) „stranka koja odgovara na zahtjev” znači ugovorna stranka kojoj se upućuje zahtjev ili obavijest iz sustava TACHOnet;

(g) „tijelo koje izdaje karticu” znači tijelo koje je ugovorna stranka ovlastila za izdavanje tahografskih kartica i upravljanje njima.

3. Opće obveze

3.1. Ugovorne stranke ne mogu sklapati sporazume za pristup sustavu TACHOnet u ime druge stranke i ni na koji drugi način zastupati drugu ugovornu stranku na temelju ovog Dodatka. Ugovorne stranke u aktivnostima iz ovog Dodatka ne djeluju u svojstvu podizvođača druge ugovorne stranke.

3.2. Ugovorne stranke omogućuju pristup svojoj nacionalnoj evidenciji kartica vozača putem sustava TACHOnet na način naveden u Poddodatku 4.6. i na razini usluge navedenoj u njemu.

3.3. Ugovorne stranke bez odgode obavještavaju jedna drugu ako u svojem području odgovornosti primijete smetnje ili pogreške koje mogu dovesti u opasnost normalan rad sustava TACHOnet.

3.4. Sve stranke imenuju osobe za kontakt za sustav TACHOnet i o njima obavještavaju Tajništvo AETR-a. Sve promjene podataka o osobama za kontakt moraju se proslijediti Tajništvu AETR-a pisanim putem.

4. Ispitivanje radi povezivanja na sustav TACHOnet

4.1. Ugovorne stranke povezuju se na sustav TACHOnet nakon uspješnog završetka ispitivanja povezivanja, integracije i radnog učinka u skladu s uputama i pod nadzorom Europske komisije.

4.2. U slučaju neuspjeha prethodnih ispitivanja Europska komisija može privremeno obustaviti ispitnu fazu. Ispitivanja se nastavljaju nakon što ugovorna stranka obavijesti Europsku komisiju o uvođenju potrebnih tehničkih poboljšanja na nacionalnoj razini kojima se omogućuje uspješno provođenje prethodnih ispitivanja.

4.3. Najdulje trajanje prethodnih ispitivanja je šest mjeseci.

5. Arhitektura povjerenja

5.1. Povjerljivost, cjelovitost i neosporivost poruka sustava TACHOnet osigurava arhitektura povjerenja sustava TACHOnet.

5.2. Arhitektura povjerenja sustava TACHOnet temelji se na usluzi infrastrukture javnog ključa (PKI) Europske komisije, a povezani zahtjevi navedeni su u poddodacima 4.8. i 4.9.

5.3. U arhitekturi povjerenja sustava TACHOnet mogu intervenirati sljedeće osobe:

(a) certifikacijsko tijelo, koje je odgovorno za generiranje digitalnih certifikata koje tijelo za registraciju dostavlja nacionalnim tijelima ugovornih stranaka (preko pouzdanih kurira koje imenuju) i za uspostavljanje tehničke infrastrukture za izdavanje, opoziv i obnovu digitalnih certifikata;

(b) vlasnik domene, koji je odgovoran za rad centralnog čvorišta iz Poddodatka 4.1. te za validaciju i koordinaciju arhitekture povjerenja sustava TACHOnet;

(c) tijelo za registraciju, koje je odgovorno za registraciju i odobravanje zahtjeva za izdavanje, opoziv i obnovu digitalnih certifikata te za provjeravanje identiteta pouzdanih kurira;

(d) pouzdani kurir, odnosno osoba koju je imenovalo nacionalno tijelo, odgovorna za predavanje javnog ključa tijelu za registraciju i za ishođenje odgovarajućeg certifikata koji generira certifikacijsko tijelo;

(e) nacionalno tijelo ugovorne stranke, koje:

(i) generira privatne ključeve i odgovarajuće javne ključeve koji se uključuju u certifikate koje treba generirati certifikacijsko tijelo;

ii. podnosi zahtjeve za izdavanje digitalnih certifikata certifikacijskom tijelu;

iii. imenuje pouzdanog kurira.

5.4. Certifikacijsko tijelo i tijelo za registraciju imenuje Europska komisija.

5.5. Sve ugovorne stranke koje se povezuju na sustav TACHOnet moraju zatražiti izdavanje digitalnog certifikata u skladu s Poddodatkom 4.9. kako bi poruka poslana putem sustava TACHOnet bila potpisana i šifrirana.

5.6. Certifikat može biti opozvan u skladu s Poddodatkom 4.9.

6. Zaštita podataka i povjerljivost

6.1. U skladu s međunarodnim i nacionalnim zakonima o zaštiti podataka i posebice s Konvencijom za zaštitu pojedinaca u vezi s automatskom obradom osobnih podataka, stranke poduzimaju sve potrebne tehničke i organizacijske mjere kako bi zajamčile sigurnost podataka u sustavu TACHOnet i spriječile mijenjanje ili gubitak tih podataka te neovlašteno pristupanje tim podacima ili njihovu neovlaštenu obradu (posebice autentičnost, povjerljivost podataka, sljedivost, cjelovitost, dostupnost i neosporivost te sigurnost poruka).

6.2. Svaka stranka dužna je štititi svoje nacionalne sustave od nedopuštene uporabe, zlonamjernog koda, virusa, prodora u računalo, povreda i nezakonitog mijenjanja podataka te od drugih sličnih aktivnosti trećih strana. Stranke su suglasne da će uložiti tržišno opravdan napor u izbjegavanje prijenosa virusa, tempiranih bombi, crva i sličnih programskih rutina koje mogu ometati rad računalnih sustava druge stranke.

7. Troškovi

7.1. Ugovorne stranke snose vlastite troškove razvoja i operativne troškove povezane s vlastitim podatkovnim sustavima i postupcima, u skladu sa zahtjevima za ispunjavanje obveza iz ovog Dodatka.

7.2. Za usluge iz Poddodatka 4.1. koje pruža centralno čvorište ne naplaćuje se naknada.

8. Podugovaranje

8.1. Stranke mogu podugovarati sve usluge za koje su odgovorne prema ovom Dodatku.

8.2. Podugovaranje stranku ne oslobađa odgovornosti prema ovom Dodatku, što uključuje odgovornost za odgovarajuću razinu usluge u skladu s Poddodatkom 4.6.

Poddodatak 4.1.

Opći aspekti sustava TACHOnet

1. Opći opis

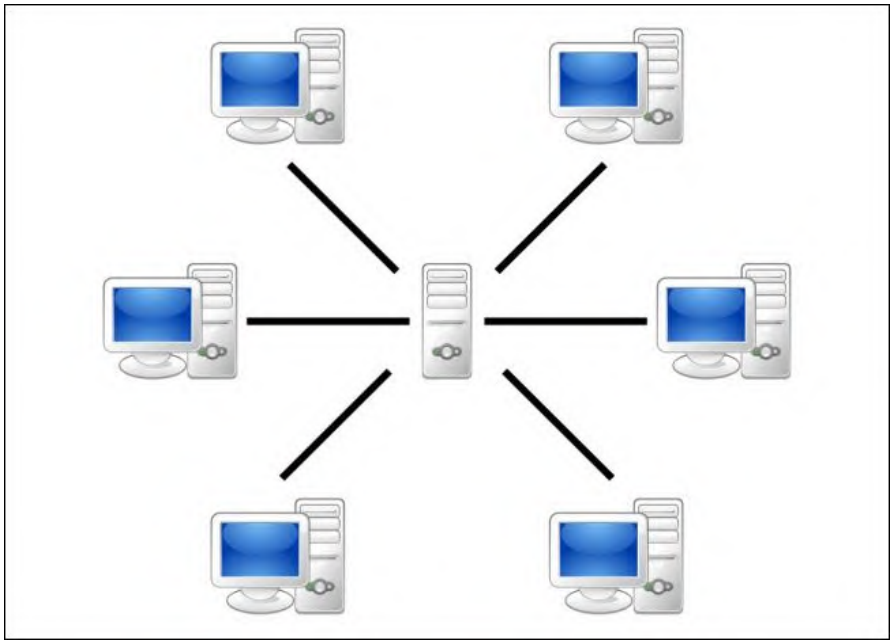
TACHOnet je elektronički sustav za razmjenu informacija o karticama vozača među ugovornim strankama AETR-a. TACHOnet prosljeđuje zahtjeve za informacijama od stranke koja upućuje zahtjev stranki koja odgovara na zahtjev te prosljeđuje odgovore u obrnutom smjeru. Ugovorne stranke koje su dio sustava TACHOnet svoje nacionalne evidencije kartica vozača moraju povezati sa sustavom.

2. Arhitektura

Sustav za razmjenu poruka TACHOnet sastoji se od sljedećih dijelova:

2.1. centralnog čvorišta, koje mora biti u mogućnosti primiti zahtjev stranke koja upućuje zahtjev te ga provjeriti i obraditi tako da ga proslijedi strankama koje odgovaraju na zahtjev. Centralno čvorište čeka na odgovor svih stranaka koje odgovaraju na zahtjev, konsolidira sve odgovore i konsolidirani odgovor prosljeđuje stranki koja upućuje zahtjev;

2.2. nacionalnih sustava stranaka, koji moraju biti opremljeni sučeljem koje je u mogućnosti slati zahtjeve centralnom čvorištu i primati odgovarajuće odgovore. Nacionalni sustavi za prijenos poruka centralnom čvorištu i primanje poruka iz njega mogu upotrebljavati softver koji je vlasništvo proizvođača ili komercijalni softver.



3. Upravljanje

3.1. Centralnim čvorištem upravlja Europska komisija koja je odgovorna za tehnički rad i održavanje centralnog čvorišta.

3.2. U centralnom se čvorištu podaci pohranjuju najdulje šest mjeseci, osim evidencijskih i statističkih podataka navedenih u Poddodatku 4.7.

3.3. Centralno čvorište ne dopušta pristup osobnim podacima, osim u slučaju ovlaštenog osoblja Europske komisije ako su ti podaci potrebni u svrhu praćenja, održavanja i otklanjanja poteškoća.

3.4. Svaka ugovorna stranka odgovorna je za:

3.4.1. uspostavu nacionalnih sustava i upravljanje njima, uključujući sučelje s centralnim čvorištem;

3.4.2. instaliranje i održavanje hardvera i softvera svojih nacionalnih sustava koji su vlasništvo proizvođača ili komercijalni;

3.4.3. ispravnu interoperabilnost svojih nacionalnih sustava s centralnim čvorištem, uključujući upravljanje porukama o pogrešci primljenima od centralnog čvorišta;

3.4.4. poduzimanje svih mjera za osiguravanje povjerljivosti, cjelovitosti i dostupnosti informacija;

3.4.5. djelovanje nacionalnih sustava u skladu s razinama usluga navedenima u Poddodatku 4.6.

Poddodatak 4.2.

Funkcije sustava TACHOnet

1. Sustav za razmjenu poruka TACHOnet mora omogućivati sljedeće funkcije:

1.1. Provjera izdanih kartica (Check Issued Cards – CIC): omogućuje stranki koja upućuje zahtjev da pošalje zahtjev za provjeru kartica jednoj stranki koja odgovara na zahtjev ili svima njima radi utvrđivanja posjeduje li već podnositelj zahtjeva karticu vozača koju su izdale stranke koje odgovaraju na zahtjev. Stranke koje odgovaraju na zahtjev šalju odgovor o provjeri izdanih kartica.

1.2. Provjera statusa kartice (Check Card Status – CCS): omogućuje stranki koja upućuje zahtjev da slanjem zahtjeva za provjeru statusa kartice zatraži od stranke koja odgovara na zahtjev pojedinosti o kartici koju je potonja izdala. Stranka koja odgovara na zahtjev odgovara slanjem odgovora o provjeri statusa kartice.

1.3. Promjena statusa kartice (Modify Card Status – MCS): omogućuje stranki koja upućuje zahtjev da slanjem zahtjeva za promjenu statusa kartice obavijesti stranku koja odgovara na zahtjev da se promijenio status kartice koju je potonja izdala. Stranka koja odgovara na zahtjev odgovara slanjem potvrde promjene statusa kartice.

1.4. Kartica izdana na temelju vozačke dozvole (Issued Card Driving License – ICDL): omogućuje stranki koja upućuje zahtjev da, putem zahtjeva za karticu izdanu na temelju vozačke dozvole, obavijesti stranku koja odgovara na zahtjev da je prvospomenuta stranka izdala karticu na temelju vozačke dozvole koju je izdala potonja. Stranka koja odgovara na zahtjev odgovara slanjem odgovora na karticu izdanu na temelju vozačke dozvole.

2. Uključit će se i druge vrste poruka koje se smatraju prikladnima za učinkovito funkcioniranje sustava TACHOnet, primjerice obavijesti o pogreškama.

3. Nacionalni sustavi moraju prepoznavati statuse kartica navedene u tablici 1. kada se koriste bilo kojom od funkcija opisanih u točki 1. Međutim, stranke ne moraju primjenjivati administrativni postupak koji se koristi svim navedenim statusima.

4. Kada stranka primi odgovor ili obavijest sa statusom koji se ne upotrebljava u njezinim administrativnim postupcima, nacionalni sustav mora pretvoriti status iz primljene poruke u odgovarajuću vrijednost u tom postupku. Stranka koja odgovara na zahtjev ne smije odbiti tu poruku ako je status u poruci naveden u tablici 1.

5. Status kartice naveden u tablici 1. ne smije se upotrebljavati kako bi se odredilo je li kartica valjana za vožnju. Kada stranka pretražuje evidenciju nacionalnog tijela koje je izdalo karticu s pomoću funkcije CCS, odgovor sadržava posebno polje „valjana za vožnju”. Nacionalni administrativni postupci moraju biti takvi da odgovori funkcije CCS uvijek sadržavaju odgovarajuću vrijednost „valjana za vožnju”.

Tablica 1.

Statusi kartica

Status kartice	**Definicije**
Podnesen zahtjev	Tijelo koje izdaje karticu primilo je zahtjev za izdavanje kartice vozača. Ta je informacija zabilježena i pohranjena u bazu podataka s generiranim ključevima za pretraživanje.
Odobrena	Tijelo koje izdaje karticu odobrilo je zahtjev za izdavanje tahografske kartice.
Odbijena	Tijelo koje izdaje karticu nije odobrilo zahtjev.
Personalizirana	Tahografska kartica personalizirana je.
Poslana	Nacionalno tijelo poslalo je karticu vozača dotičnom vozaču ili agenciji za dostavu.
Uručena	Nacionalno tijelo predalo je karticu vozača dotičnom vozaču.
Oduzeta	Nadležno tijelo oduzelo je vozaču karticu vozača.
Suspendirana	Kartica vozača privremeno je oduzeta vozaču.
Poništena	Tijelo koje izdaje karticu odlučilo je poništiti karticu vozača. Kartica je trajno poništena.
Vraćena	Tahografska kartica vraćena je tijelu koje izdaje karticu i prijavljeno je da više nije potrebna.
Izgubljena	Tijelu koje izdaje karticu prijavljen je gubitak tahografske kartice.
Ukradena	Tijelu koje izdaje karticu prijavljena je krađa tahografske kartice. Ukradena kartica smatra se izgubljenom.
Neispravna	Tijelu koje izdaje karticu tahografska kartica prijavljena je kao neispravna.
Istekla	Isteklo je razdoblje valjanosti tahografske kartice.
Nadomještena	Tahografska kartica koja je prijavljena kao izgubljena, ukradena ili neispravna nadomještena je novom karticom. Podaci na novoj kartici jednaki su onima na staroj, osim broja indeksa zamjene kartice, koji je uvećan za jedan.

Obnovljena	Tahografska kartica obnovljena je zbog promjene administrativnih podataka ili isteka razdoblja valjanosti. Broj nove kartice jednak je broju stare kartice, osim broja indeksa obnove kartice, koji je uvećan za jedan.
U postupku zamjene	Tijelo koje je izdalo karticu vozača primilo je obavijest da je pokrenut postupak za zamjenu te kartice karticom vozača koju izdaje tijelo druge države članice.
Zamijenjena	Tijelo koje je izdalo karticu vozača primilo je obavijest da je završen postupak za zamjenu te kartice karticom vozača koju izdaje tijelo druge države članice.

Poddodatak 4.3.

Odredbe u pogledu poruka sustava TACHOnet

1. Opći tehnički zahtjevi

1.1. Centralno čvorište osigurava sinkrono i asinkrono sučelje za razmjenu poruka. Stranke mogu izabrati najprikladniju tehnologiju sučelja za vlastite aplikacije.

1.2. Sve poruke razmijenjene između centralnog čvorišta i nacionalnih sustava moraju biti kodirane prema standardu UTF-8.

1.3. Nacionalni sustavi moraju omogućivati primanje i obradu poruka koje sadržavaju grčka ili ćirilična slova.

2. Struktura XML poruka i definicija sustava (XSD)

2.1. Opća struktura XML poruka mora biti u skladu s formatom definiranim XSD shemama ugrađenima u centralno čvorište.

2.2. Centralno čvorište i nacionalni sustavi šalju i primaju poruke koje su u skladu s XSD shemom poruke.

2.3. Nacionalni sustavi moraju omogućivati slanje, primanje i obradu svih poruka koje odgovaraju bilo kojoj od funkcija navedenih u Poddodatku 4.2.

2.4. XML poruke obuhvaćaju barem minimalne zahtjeve utvrđene u tablici 2.

Tablica 2.

Minimalni zahtjevi za sadržaj XML poruka

Standardno zaglavlje		**Obvezno**
Verzija	Službena verzija XML specifikacija navest će se u nazivnom prostoru (namespace) definiranom u XSD shemi poruke i u atributu „verzija” u elementu zaglavlja svake XML poruke. Broj verzije („n.m”) definirat će se kao fiksna vrijednost pri svakom generiranju datoteke s XML definicijom sustava (xsd).	Da
Ispitni identifikator	Neobvezna identifikacijska oznaka za ispitivanje. Inicijator ispitivanja popunit će identifikacijsku oznaku i svi će sudionici u radnom tijeku proslijediti odnosno vratiti istu identifikacijsku oznaku. U produkciji je treba ignorirati i ne upotrebljava se ako je navedena.	Ne
Tehnički identifikator	Univerzalni jedinstveni identifikator (UUID) kojim se na jedinstven način identificira svaka pojedinačna poruka. Pošiljatelj generira UUID i popunjava ovaj atribut. Ti se podaci ne upotrebljavaju ni u kakvom poslovnom svojstvu.	Da
Identifikator radnog tijeka	Identifikator radnog tijeka je univerzalni jedinstveni identifikator (UUID) i trebala bi ga generirati stranka koja upućuje zahtjev. Ta se identifikacijska oznaka zatim upotrebljava u svim porukama za povezivanje radnog tijeka.	Da
Poslano	Datum i vrijeme (po sustavu UTC) kada je poruka poslana.	Da
Prekoračenje vremena	Neobavezni atribut datuma i vremena (u UTC formatu). Tu će vrijednost odrediti čvorište za proslijeđene zahtjeve. Time će se stranku koja odgovara na zahtjev obavijestiti o trenutku prekoračenja vremena za zahtjev. Ta vrijednost nije potrebna u MS2TCN_<x>_Req kao ni u porukama odgovora. Vrijednost nije obavezna, tako da se ista definicija zaglavlja može upotrebljavati za sve vrste poruka bez obzira je li atribut vrijednosti prekoračenja vremena potreban ili ne.	Ne
Pošiljatelj	Oznaka ISO 3166-1 alpha-2 stranke koja šalje poruku ili „EU”.	Da
Primatelj	Oznaka ISO 3166-1 alpha-2 stranke kojoj se šalje poruka ili „EU”.	Da

Poddodatak 4.4.

Usluge transliteracije i sustava NYSIIS (New York State Identification and Intelligence System)

1. Algoritam NYSIIS koji se primjenjuje u centralnom čvorištu upotrebljava se za kodiranje imena svih vozača u nacionalnoj evidenciji.

2. Pri traženju kartice putem funkcije CIC (provjera izdanih kartica) kao primarni mehanizam pretraživanja upotrebljavaju se ključevi NYSIIS.

3. Osim toga, stranke mogu upotrebljavati prilagođeni algoritam za dobivanje dodatnih rezultata.

4. Uz rezultate pretraživanja navodi se mehanizam pretraživanja koji je upotrijebljen za pronalaženje podatka, to jest pretraživanje s pomoću NYSIIS-a ili prilagođeno pretraživanje.

5. Ako stranka odluči zabilježiti obavijesti o karticama izdanima na temelju vozačke dozvole (ICDL), tada se ključevi NYSIIS koji se nalaze u obavijesti bilježe kao dio podataka o karticama izdanima na temelju vozačke dozvole. Pri pretraživanju podataka o karticama izdanima na temelju vozačke dozvole stranka upotrebljava ključeve NYSIIS za ime podnositelja zahtjeva.

Poddodatak 4.5.

Sigurnosni zahtjevi

1. Za razmjenu poruka između centralnog čvorišta i nacionalnih sustava upotrebljava se protokol HTTPS.

2. U nacionalnim sustavima upotrebljavaju se digitalni certifikati iz poddodataka 4.8. i 4.9. za potrebe zaštite prijenosa poruka između nacionalnih sustava i centralnog čvorišta.

3. Nacionalni sustavi primjenjuju, kao minimum, certifikate s hash algoritmom potpisa SHA-2 (SHA-256) i dužinom javnog ključa od 2048 bita.

Poddodatak 4.6.

Razine usluga

1. Nacionalni sustavi moraju pružati sljedeće minimalne razine usluga:

1.1. moraju biti dostupni 24 sata dnevno, sedam dana u tjednu;

1.2. njihova se dostupnost prati porukama koje centralno čvorište šalje u redovitim vremenskim razmacima (heartbeat messages);

1.3. njihova stopa dostupnosti mora iznositi 98 %, u skladu sa sljedećom tablicom (iznosi su zaokruženi na najbližu prikladnu jedinicu):

Dostupnost od	značI nedostupnost od		
	Dnevno	Mjesečno	Godišnje
98 %	0,5 sati	15 sati	7,5 dana

Stranke se potiču da poštuju dnevnu stopu dostupnosti. No poznato je da je prilikom određenih nužnih aktivnosti, primjerice tijekom održavanja sustava, sustav nedostupan više od 30 minuta. Međutim, mjesečne i godišnje stope dostupnosti obvezne su;

1.4. moraju odgovoriti na najmanje 98 % zahtjeva koji su im proslijeđeni u jednom kalendarskom mjesecu;

1.5. na zahtjeve moraju odgovoriti u roku od 10 sekundi;

1.6. ukupno vrijeme za pružanje odgovora na zahtjev (vrijeme u kojem podnositelj zahtjeva smije čekati odgovor) ne smije biti dulje od 20 sekundi;

1.7. moraju biti u mogućnosti obraditi šest zahtjeva u sekundi;

1.8. nacionalni sustavi ne smiju čvorištu TACHOneta slati više od dva zahtjeva u sekundi;

1.9. svaki nacionalni sustav mora biti u stanju prevladati potencijalne tehničke probleme centralnog čvorišta ili nacionalnih sustava u drugim strankama. Ti problemi obuhvaćaju, među ostalim:

(a) gubitak veze s centralnim čvorištem;

(b) slučajeve kada nema odgovora na zahtjev;

(c) primanje odgovora nakon prekoračenja vremena poruke;

(d) primanje nezatraženih poruka;

(e) primanje nevaljanih poruka.

2. Centralno čvorište mora:

2.1. omogućiti stopu dostupnosti od 98 %;

2.2. obavještavati nacionalne sustave o svim pogreškama, bilo porukom odgovora ili namjenskom porukom o pogrešci. Nacionalni sustavi moraju primiti te namjenske poruke o pogrešci i imati eskalacijski postupak za poduzimanje odgovarajućih mjera za ispravljanje prijavljene pogreške.

3. Održavanje

Stranke putem mrežne aplikacije obavještavaju ostale stranke i Europsku komisiju o svim uobičajenim postupcima održavanja najmanje tjedan dana prije početka tih postupaka, ako je to tehnički moguće.

Poddodatak 4.7.

Evidentiranje i statistička obrada prikupljenih podataka u centralnom čvorištu

1. Kako bi se osigurala privatnost, podaci za statističke svrhe anonimni su. Identifikacijski podaci koji se odnose na određenu karticu, vozača ili vozačku dozvolu ne smiju biti dostupni za statističke svrhe.

2. Evidencijske informacije moraju sadržavati podatke o svim transakcijama za potrebe nadzora i otklanjanja pogrešaka te omogućiti pripremu statistika o tim transakcijama.

3. Osobni se podaci ne zadržavaju u datotekama dulje od šest mjeseci. Statistički se podaci čuvaju neograničeno.

4. Statistički podaci koji se upotrebljavaju za izvješćivanje uključuju:

   (a) stranku koja upućuje zahtjev;

   (b) stranku koja odgovara na zahtjev;

   (c) vrstu poruke;

   (d) oznaku statusa odgovora;

   (e) datum i vrijeme slanja poruka;

   (f) vrijeme odgovora.

Poddodatak 4.8.

Opće odredbe u pogledu digitalnih ključeva i certifikata za sustav TACHOnet

1. Glavna uprava za informatiku Europske komisije (DIGIT) ugovornim strankama AETR-a koje se povezuju na sustav TACHOnet („nacionalna tijela”) pruža uslugu infrastrukture javnog ključa[1] („usluga CEF PKI”) putem platforme e-dostava.

2. Postupak podnošenja zahtjeva za izdavanje i opoziv digitalnih certifikata te detaljni uvjeti za služenje njime definirani su u Dodatku.

3. Uporaba certifikata:

3.1. Nakon izdavanja certifikata nacionalno tijelo[2] certifikatom se koristi samo u okviru sustava TACHOnet. Certifikat se može upotrebljavati za:

(a) potvrđivanje izvora podataka;

(b) šifriranje podataka;

(c) osiguranje otkrivanja povrede cjelovitosti podataka.

3.2. Uporaba certifikata na način koji nije izričito naveden kao dopušten zabranjena je.

4. Ugovorne stranke dužne su:

(a) štititi svoj privatni ključ od neovlaštene uporabe;

(b) ne prenositi ili otkrivati svoje privatne ključeve trećim stranama, čak ni u svojstvu zastupnika;

---

1 PKI (infrastruktura javnog ključa) skup je uloga, politika, postupaka i sustava potrebnih za kreiranje, dodjelu i opoziv digitalnih certifikata te upravljanje njima.

2 Označeno kao „O=” vrijednost atributa u polju „Razlikovno ime subjekta” izdanog certifikata

(c) osigurati povjerljivost, cjelovitost i dostupnost privatnih ključeva generiranih, pohranjenih i upotrebljavanih za sustav TACHOnet;

(d) ne upotrebljavati privatni ključ nakon isteka razdoblja valjanosti ili opoziva certifikata, osim radi čitanja šifriranih podataka (primjerice dešifriranja elektroničke pošte). Ključevi kojima je isteklo razdoblje valjanosti uništavaju se ili zadržavaju tako da se spriječi njihova uporaba;

(e) tijelu za registraciju dostaviti identifikaciju zastupnika ovlaštenih zatražiti opoziv certifikata izdanih organizaciji (zahtjevi za opoziv uključuju lozinku za zahtjev za opoziv i pojedinosti o događajima koji su doveli do opoziva);

(f) spriječiti zlouporabu privatnog ključa tako da zatraže opoziv odgovarajućeg certifikata za javni ključ u slučaju da su ugroženi privatni ključ ili podaci za aktivaciju privatnog ključa;

(g) biti odgovorne i obvezne zatražiti opoziv certifikata u slučajevima navedenima u politikama certifikacije (CP) i izjavi o certifikacijskim praksama (CPS) certifikacijskog tijela;

(h) bez odgode obavijestiti tijelo za registraciju o gubitku, krađi ili mogućem ugrožavanju bilo kojih ključeva AETR-a koji se upotrebljavaju u kontekstu sustava TACHOnet.

5. Odgovornost

Ne dovodeći u pitanje odgovornost Europske komisije u slučaju kršenja zahtjeva propisanih mjerodavnim nacionalnim pravom ili u pogledu slučajeva koje u skladu s nacionalnim pravom nije moguće isključiti, Europska komisija nije odgovorna za:

(a) sadržaj certifikata, za koji je odgovoran isključivo vlasnik certifikata. Odgovornost je vlasnika certifikata provjeriti točnost njegova sadržaja;

(b) način na koji vlasnik certifikata upotrebljava certifikat.

Poddodatak 4.9.

Opis usluge PKI za sustav TACHOnet

1. Uvod

PKI (infrastruktura javnog ključa) skup je uloga, politika, postupaka i sustava potrebnih za generiranje, dodjelu i opoziv digitalnih certifikata te upravljanje njima[3]. Usluga CEF PKI platforme e-dostava omogućuje izdavanje digitalnih certifikata kojima se osigurava povjerljivost, cjelovitost i neosporivost informacija koje se razmjenjuju među pristupnim točkama (AP) i upravljanje tim certifikatima.

Usluga PKI platforme e-dostava temelji se na usluzi centra povjerenja Trust Centre TeleSec Shared Business CA (certifikacijsko tijelo) za koju se primjenjuje politika certifikacije (CP)/izjava o certifikacijskim praksama (CPS) TeleSec Shared-Business CA društva T-Systems International GmbH[4].

Usluga PKI omogućuje izdavanje certifikata koji su prikladni za osiguranje različitih poslovnih procesa u društvima, organizacijama, javnim tijelima i institucijama koji zahtijevaju srednju razinu sigurnosti za dokazivanje autentičnosti, cjelovitosti i pouzdanosti krajnjeg korisnika, kao i izvan njih.

2. Postupak upućivanja zahtjeva za izdavanje certifikata

2.1. Uloge i nadležnosti

2.1.1. „Organizacija” ili „nacionalno tijelo” koje upućuje zahtjev za izdavanje certifikata

2.1.1.1. Nacionalno tijelo upućuje zahtjev za izdavanje certifikata u okviru projekta TACHOnet.

2.1.1.2. Nacionalno tijelo:

(a) upućuje zahtjev za izdavanje certifikata usluzi CEF PKI;

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

[4] Najnoviju verziju CP-a i CPS-a možete preuzeti na https://www.telesec.de/en/sbca-en/support/download-area/.

(b) generira privatne ključeve i odgovarajuće javne ključeve koji se uključuju u certifikate koje treba izdati certifikacijsko tijelo;

(c) preuzima certifikat kada se on odobri;

(d) potpisuje i vraća tijelu za registraciju:

(i) obrazac za identifikaciju osobe za kontakt i pouzdanog kurira;

(ii) potpisanu individualnu punomoć[5].

2.1.2. Pouzdani kurir

2.1.2.1. Nacionalno tijelo imenuje pouzdanog kurira.

2.1.2.2. Pouzdani kurir:

(a) predaje javni ključ tijelu za registraciju tijekom postupka osobne identifikacije i registracije;

(b) preuzima odgovarajući certifikat od tijela za registraciju.

2.1.3. Vlasnik domene

2.1.3.1. Vlasnik domene je DG MOVE.

2.1.3.2. Vlasnik domene:

(a) validira i koordinira mrežu TACHOnet i arhitekturu povjerenja TACHOnet-a, što uključuje validaciju postupaka za izdavanje certifikata;

(b) upravlja centralnim čvorištem sustava TACHOnet i koordinira aktivnost stranaka u pogledu funkcioniranja sustava TACHOnet;

(c) zajedno s nacionalnim tijelima provodi ispitivanja povezivanja na sustav TACHOnet.

[5] Punomoć je pravni dokument kojim organizacija opunomoćuje i ovlašćuje Europsku komisiju, koju zastupa za to određen službenik odgovoran za uslugu CEF PKI, za upućivanje zahtjeva certifikacijskom tijelu TeleSec Shared-Business društva T-Systems International GmbH za generiranje certifikata u svoje ime. Vidjeti i točku 6.

2.1.4. Tijelo za registraciju

2.1.4.1. Tijelo za registraciju je Zajednički istraživački centar (JRC).

2.1.4.2. Tijelo za registraciju odgovorno je za provjeru identiteta pouzdanog kurira, registraciju i odobravanje zahtjeva za izdavanje, opoziv i obnovu digitalnih certifikata.

2.1.4.3. Tijelo za registraciju:

(a) dodjeljuje jedinstvenu identifikacijsku oznaku nacionalnom tijelu;

(b) potvrđuje identitet nacionalnog tijela, njegovih osoba za kontakt i pouzdanih kurira;

(c) komunicira sa službom za podršku CEF-a u pogledu autentičnosti nacionalnog tijela, njegovih osoba za kontakt i pouzdanih kurira;

(d) obavještava nacionalno tijelo o odobravanju ili odbijanju certifikata.

2.1.5. Certifikacijsko tijelo

2.1.5.1. Certifikacijsko tijelo odgovorno je za osiguravanje tehničke infrastrukture za upućivanje zahtjeva te izdavanje i opoziv digitalnih certifikata.

2.1.5.2. Certifikacijsko tijelo:

(a) osigurava tehničku infrastrukturu za zahtjeve nacionalnih tijela za izdavanje certifikata;

(b) potvrđuje ili odbija zahtjev za izdavanje certifikata;

(c) po potrebi komunicira s tijelom za registraciju radi potvrđivanja identiteta organizacije koja upućuje zahtjev.

2.2. Izdavanje certifikata

2.2.1. Za izdavanje certifikata valja slijediti sljedeće uzastopne korake, prikazane na slici 1.:

(a) **korak 1.:** identifikacija pouzdanog kurira;

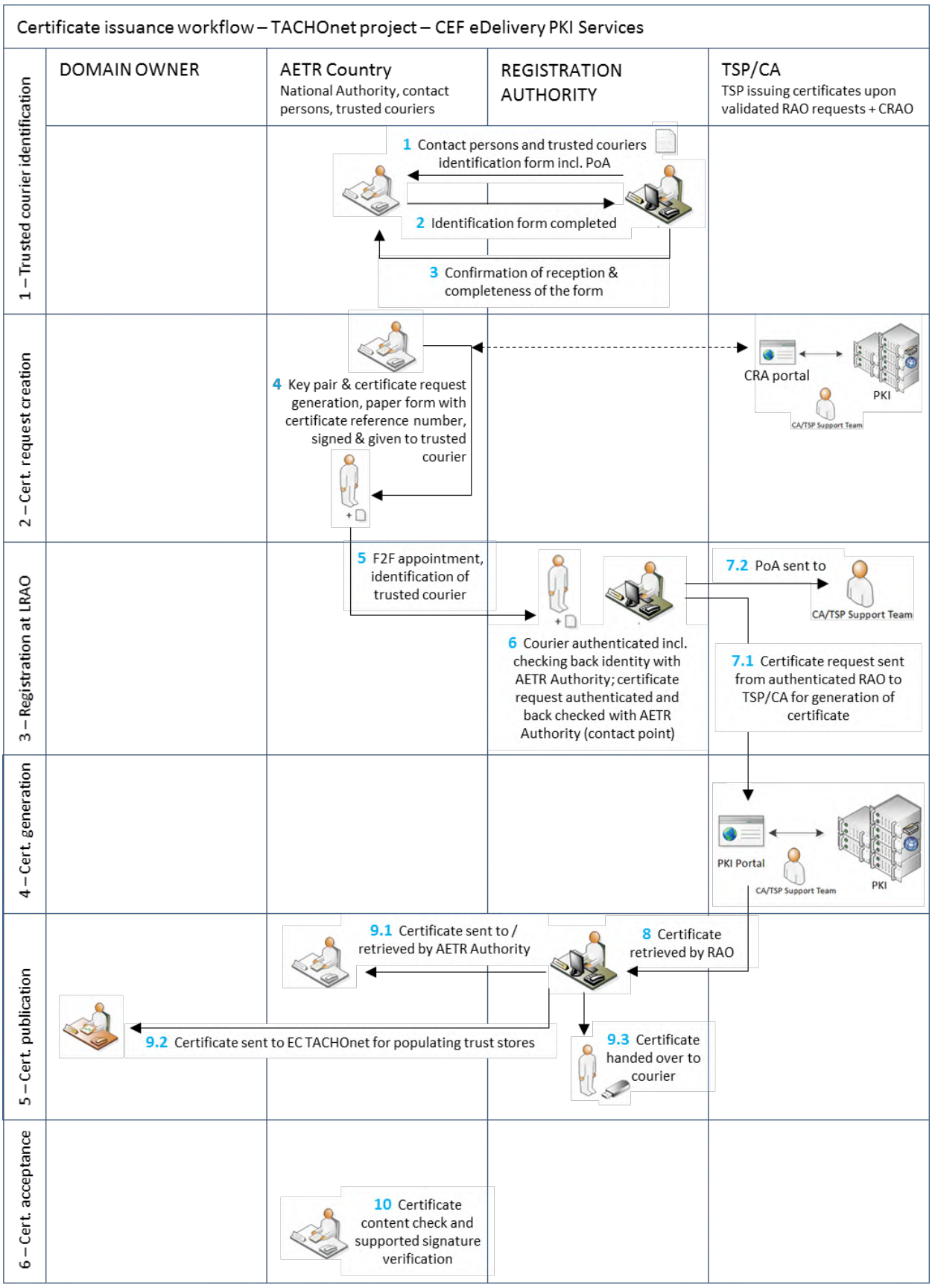
(b) **korak 2.:** kreiranje zahtjeva za izdavanje certifikata;

(c) **korak 3.:** registracija pri tijelu za registraciju;

(d) **korak 4.:** generiranje certifikata;

(e) **korak 5.:** objavljivanje certifikata;

(f) **korak 6.:** prihvaćanje certifikata.



Slika 1. – Tijek izdavanja certifikata

2.2.2. korak 1.: identifikacija pouzdanog kurira;

Postupak identifikacije pouzdanog kurira sljedeći je:

(a) tijelo za registraciju nacionalnom tijelu prosljeđuje obrazac za identifikaciju osobe za kontakt i pouzdanog kurira[6]. U taj je obrazac uključena i punomoć koju je potpisala organizacija (tijelo u okviru AETR-a);

(b) nacionalno tijelo popunjeni obrazac i potpisanu punomoć vraća tijelu za registraciju;

(c) tijelo za registraciju potvrđuje da je primilo obrazac i da je on valjano popunjen;

(d) tijelo za registraciju vlasniku domene prosljeđuje ažuriran primjerak popisa osoba za kontakt i pouzdanih kurira.

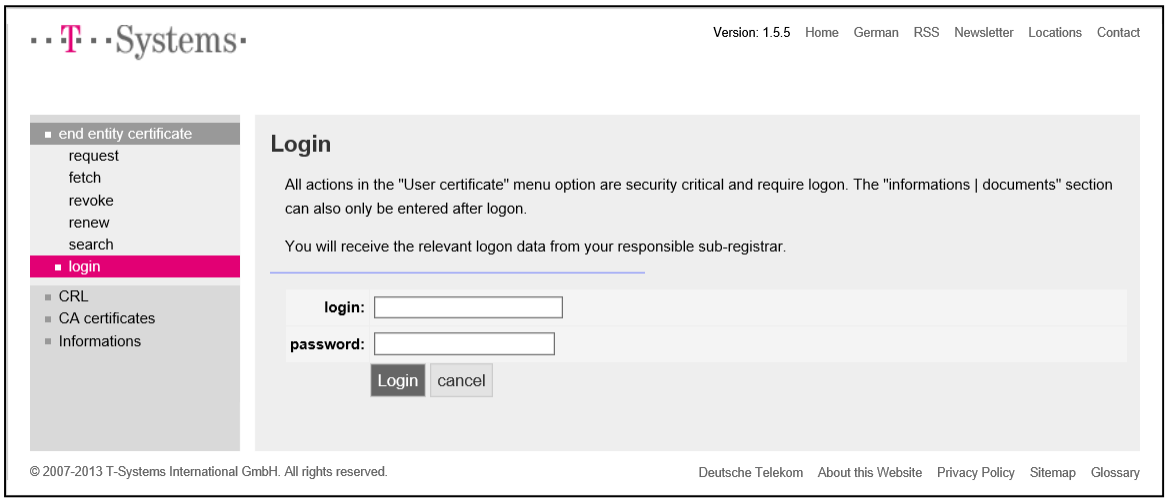
2.2.3. korak 2.: kreiranje zahtjeva za izdavanje certifikata;

2.2.3.1. Zahtjev za izdavanje certifikata upućuje se s istog računala i iz istog preglednika s kojega se certifikat preuzima.

2.2.3.2. Postupak kreiranja zahtjeva za izdavanje certifikata sljedeći je:

(a) organizacija upućuje zahtjev za izdavanje certifikata putem mrežnog sučelja za korisnike na adresi https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: , gdje upisuje korisničko ime „**sbca/CEF_eDelivery.europa.eu**” i lozinku „**digit.333**”;

6 Vidjeti točku 5.

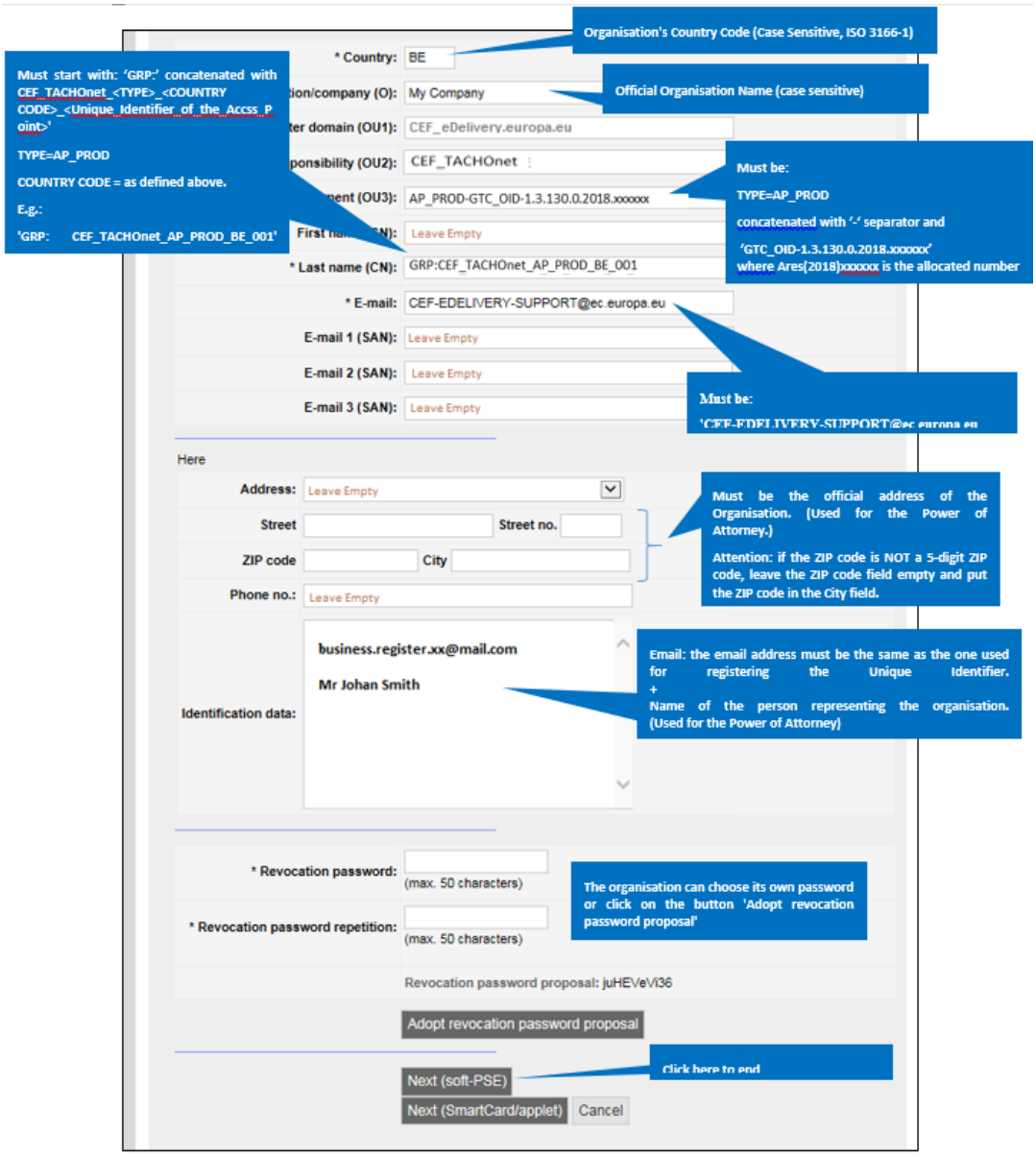


Slika 2.

(b) zatim je potrebno kliknuti na gumb za zahtjev („request”) na lijevoj strani prozora i iz padajućeg popisa odabrati „CEF_TACHOnet”;

Slika 3.

(c) organizacija u obrazac zahtjeva za izdavanje certifikata prikazan na slici 4. unosi podatke iz tablice 3., a za završetak postupka treba kliknuti na gumb „Next (soft-PSE)”.


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

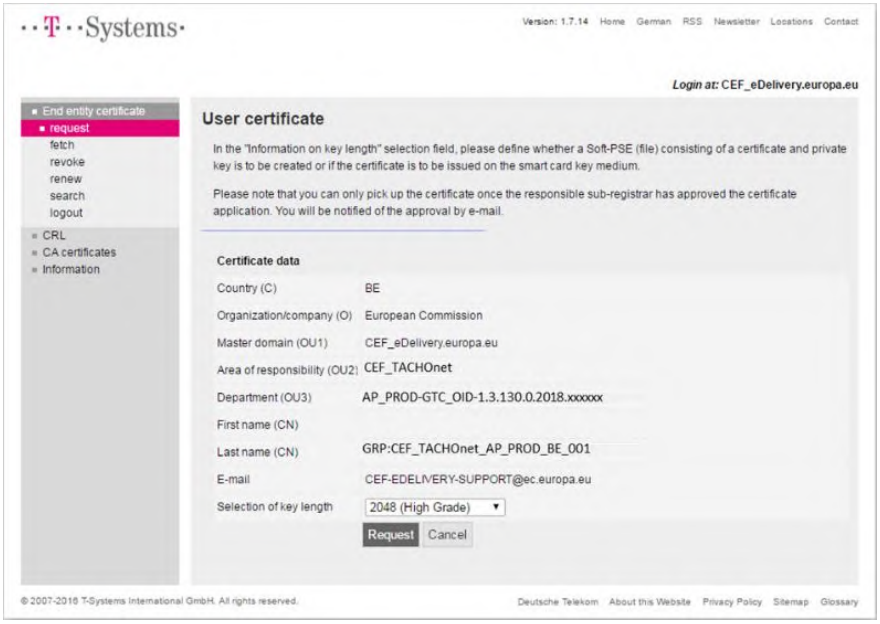
Slika 4.

Obvezna polja	Opis
Zemlja (Country)	**C=oznaka države**, lokacija vlasnika certifikata, provjerena putem javnog direktorija; Ograničenja: 2 znaka, u skladu s oznakama država alpha-2 iz norme ISO 3166-1, uz razlikovanje malih i velikih slova; Primjeri: DE, BE, NL Posebni slučajevi: UK (za Ujedinjenu Kraljevinu), EL (za Grčku)
Organizacija/društvo (O) (Organisation/Company (O))	**O=ime organizacije vlasnika certifikata**
Glavna domena (OU1) (Master domain (OU1))	**OU=CEF_eDelivery.europa.eu**
Područje nadležnosti (OU2) (Area of responsibility (OU2))	**OU=CEF_TACHOnet**
Odjel (OU3) (Department (OU3))	Obavezna vrijednost za svako „PODRUČJE NADLEŽNOSTI” Sadržaj se mora provjeriti uspoređujući ga s popisom dopuštenih vrijednosti pri upućivanju zahtjeva za izdavanje certifikata. Ako informacije ne odgovaraju tom popisu, zahtjev se ne može uputiti. Oblik: **OU=<TYPE>-<GTC_NUMBER>** gdje se „<TYPE>” zamjenjuje s AP_PROD: Access Point in Production environment, a <GTC_NUMBER> jest **GTC_OID-1.3.130.0.2018.xxxxxx**, gdje je Ares(2018)xxxxxx GTC broj za projekt TACHOnet. Primjerice: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
Ime (CN) (First name (CN))	Mora se ostaviti prazno.
Prezime (CN) (Last name (CN))	Mora početi s „GRP:”, nakon čega slijedi opće ime (common name). Oblik: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** Primjerice: GRP:CEF_TACHOnet_AP_PROD_BE_001
Adresa e-pošte (E-mail)	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
Adresa e-pošte 1 (SAN) (E-mail 1 (SAN))	Mora se ostaviti prazno.
Adresa e-pošte 2 (SAN) (E-mail 1 (SAN))	Mora se ostaviti prazno.
Adresa e-pošte 3 (SAN) (E-mail 1 (SAN))	Mora se ostaviti prazno.

Adresa (Address)	Mora se ostaviti prazno.
Ulica (Street)	Mora biti službena adresa organizacije vlasnika certifikata (kao u punomoći).
Kućni broj (Street no.)	Mora biti službena adresa organizacije vlasnika certifikata (kao u punomoći).
Poštanski broj	Mora biti službena adresa organizacije vlasnika certifikata (kao u punomoći). **Napomena:** ako poštanski broj nije u obliku peteroznamenkastog poštanskog broja, to polje ostavite prazno, a poštanski broj upišite u polje Grad.
Grad (*City*)	Mora biti službena adresa organizacije vlasnika certifikata (kao u punomoći). **Napomena:** ako poštanski broj nije u obliku peteroznamenkastog poštanskog broja, to polje ostavite prazno, a poštanski broj upišite u polje Grad.
Telefonski broj (*Phone no.*)	Mora se ostaviti prazno.
Identifikacijski podaci (Identification data)	Adresa e-pošte mora biti jednaka onoj koja je upotrijebljena za registraciju jedinstvene registracijske oznake. + Mora biti ime osobe koja zastupa organizaciju (kao u punomoći). + **Matični broj društva** (obavezan samo za privatne organizacije) **Upisano na sudu u** (samo za njemačke i austrijske privatne organizacije)
Lozinka za opoziv (Revocation password)	Obvezno polje, bira je podnositelj zahtjeva
Ponovljena lozinka za opoziv (Revocation password repetition)	Ponovljeno obvezno polje, bira je podnositelj zahtjeva

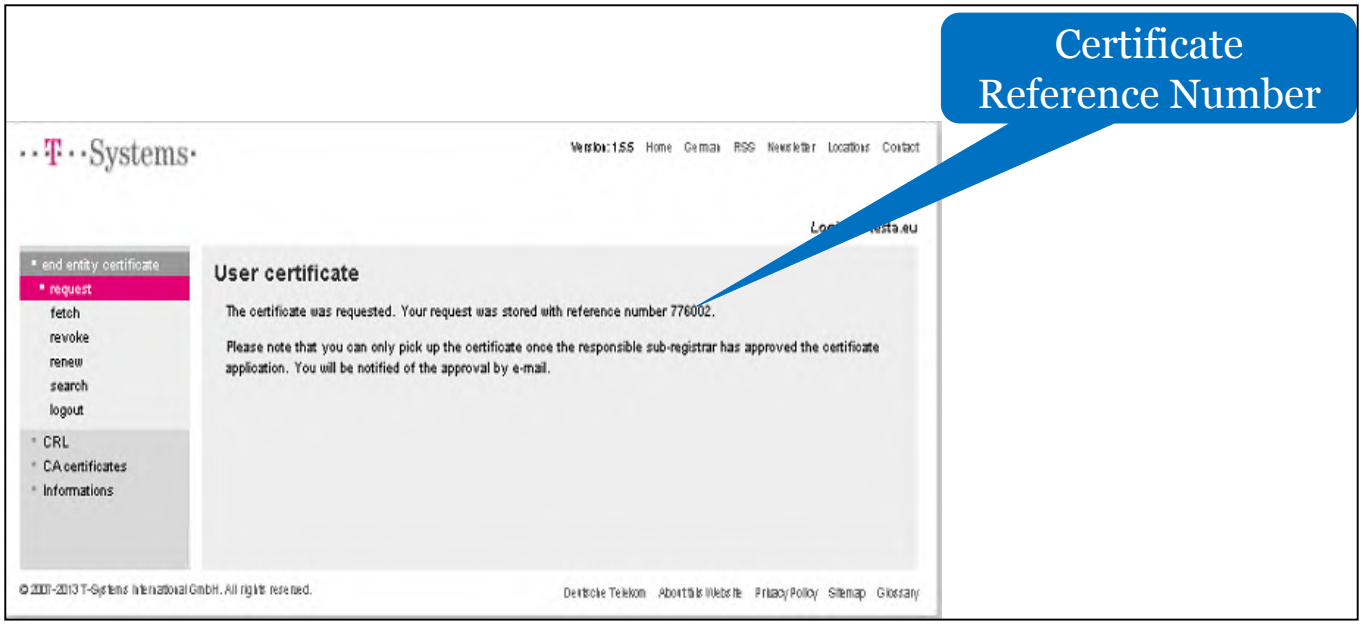
Tablica 3. Pojedinosti za svako obvezno polje

(d) odabire se ključ duljine 2048 bita (visoki stupanj);



Slika 5.

(e) organizacija sprema referentni broj certifikata za njegovo preuzimanje;



Slika 6.

(f) služba za podršku CEF-a provjerava ima li novih zahtjeva za izdavanje certifikata i provjerava jesu li informacije u zahtjevu za izdavanje certifikata valjane, odnosno odgovaraju li pravilima o imenovanju iz Dodatka 5.1. Pravila o imenovanju certifikata;

(g) služba za podršku CEF-a provjerava jesu li informacije upisane u zahtjev u valjanom obliku;

(h) ako provjera informacija iz točke 5. ili 6. ne uspije, služba za podršku CEF-a na adresu e-pošte iz polja „Identifikacijski podaci” u obrascu zahtjeva šalje poruku kojom se organizacija obavještava da mora ponoviti postupak, stavljajući vlasnika domene u kopiju. Neuspjeli zahtjev za izdavanje certifikata otkazuje se;

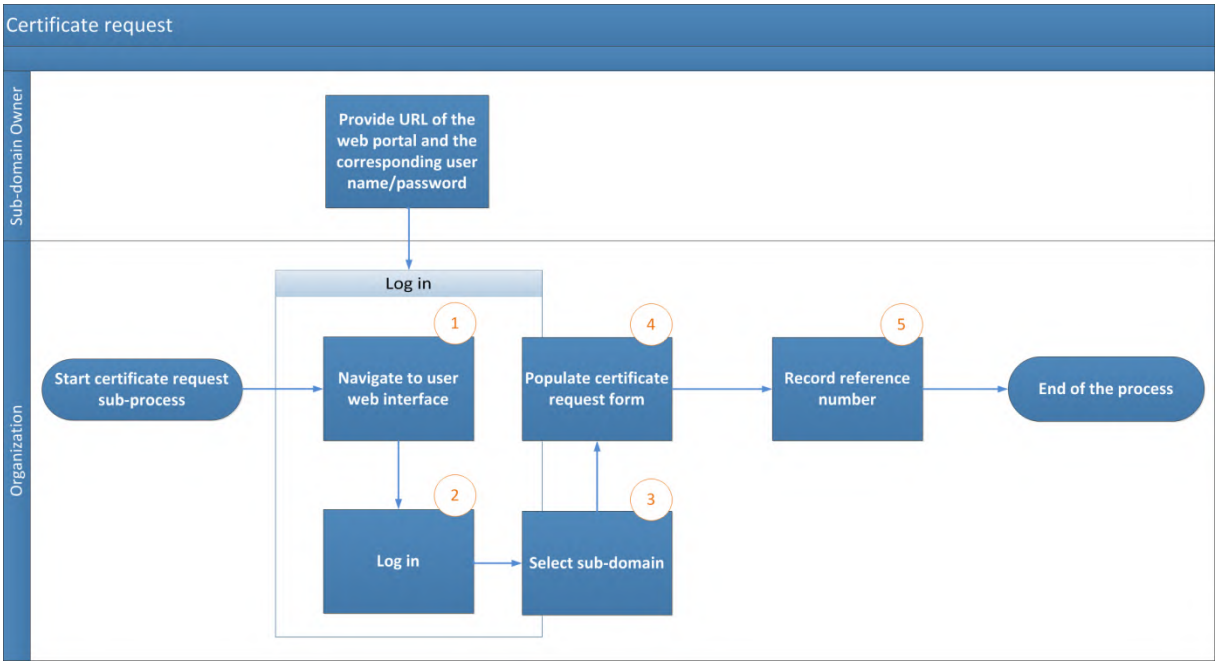
(i) služba za podršku CEF-a tijelu za registraciju e-poštom šalje obavijest o valjanosti zahtjeva. U poruci e-pošte treba se nalaziti:

(1) ime organizacije iz polja „Organizacija (O)” zahtjeva za izdavanje certifikata;

(2) podaci o certifikatu, uključujući naziv pristupne točke za koju se certifikat treba izdati iz polja „Prezime (CN)” zahtjeva za izdavanje certifikata;

(3) referentni broj certifikata;

(4) adresa organizacije, adresa e-pošte i ime osobe koja ju zastupa.



Slika 7. – Postupak upućivanja zahtjeva za izdavanje certifikata

2.2.4. korak 3.: registracija pri tijelu za registraciju (odobravanje certifikata)

2.2.4.1. Pouzdani kurir ili osoba za kontakt e-poštom ugovara sastanak s tijelom za registraciju i javlja identitet pouzdanog kurira koji će osobno doći na sastanak.

2.2.4.2. Organizacija priprema dokumentaciju koja se sastoji od:

(a) popunjene i potpisane punomoći;

(b) preslike valjane putovnice pouzdanog kurira koji će osobno doći na sastanak. Presliku mora potpisati jedna od osoba za kontakt organizacije navedenih u koraku 1.;

(c) papirnog formulara zahtjeva za izdavanje certifikata koji je potpisala jedna od osoba za kontakt organizacije.

2.2.4.3. Tijelo za registraciju prima pouzdanog kurira nakon provjere njegova identiteta na recepciji zgrade. Tijelo za registraciju osobno registrira zahtjev za izdavanje certifikata tako da:

(a) identificira i potvrdi identitet pouzdanog kurira;

(b) provjeri fizički izgled pouzdanog kurira uspoređivanjem sa slikom na putovnici koju predoči;

(c) provjeri valjanost putovnice pouzdanog kurira;

(d) usporedi provjerenu putovnicu koju je predočio pouzdani kurir s preslikom valjane putovnice pouzdanog kurira koju je potpisala jedna od osoba za kontakt organizacije. Istovjetnost potpisa potvrđuje se uspoređivanjem s izvornim „obrascem za identifikaciju osobe za kontakt i pouzdanog kurira”;

(e) provjeri popunjenu i potpisanu punomoć;

(f) provjeri papirni formular zahtjeva za izdavanje certifikata i potpis na njemu uspoređivanjem s izvornim „obrascem za identifikaciju osobe za kontakt i pouzdanog kurira”;

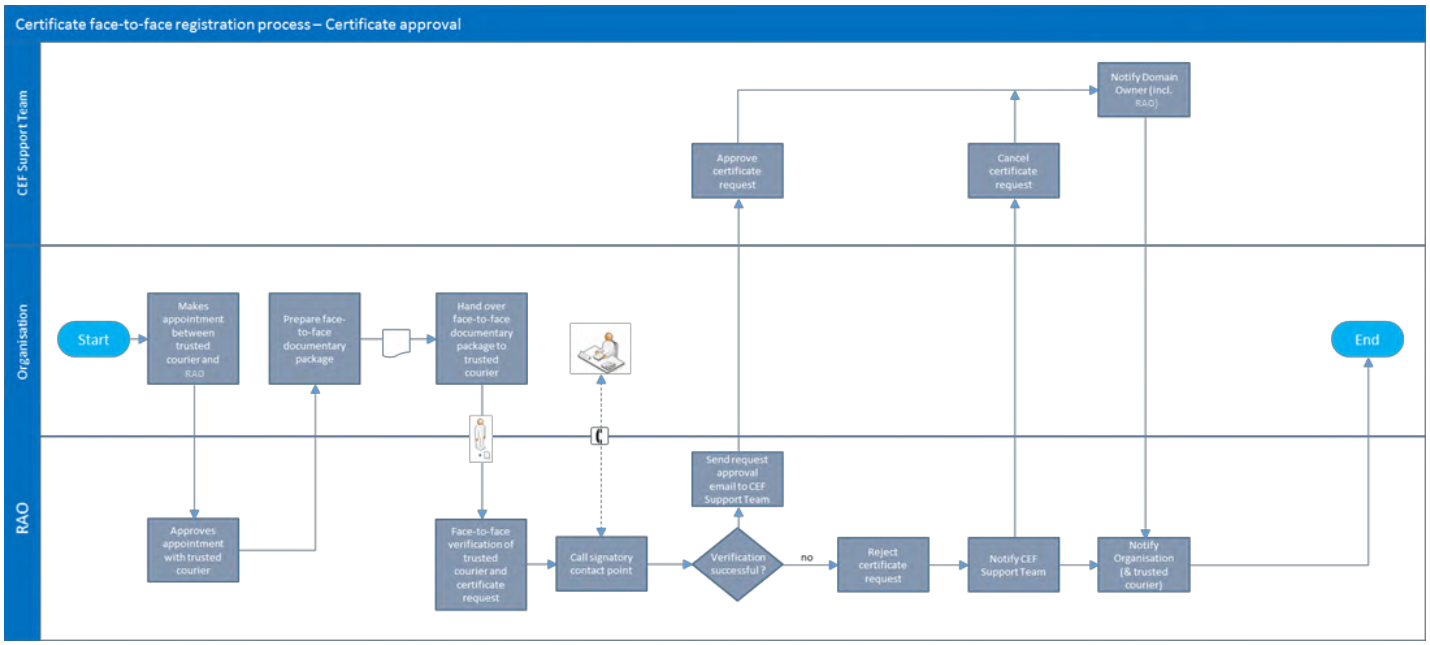
(g) nazove osobu za kontakt potpisnika kako bi dodatno provjerilo identitet pouzdanog kurira i sadržaj zahtjeva za izdavanje certifikata.

2.2.4.4. Tijelo za registraciju službi za podršku CEF-a potvrđuje da je nacionalno tijelo doista ovlašteno upravljati komponentama za koje traži certifikate i da je odgovarajući postupak osobne registracije bio uspješan. Potvrda se šalje šifriranom e-poštom s certifikatom „CommiSign”, pri čemu se prilaže skenirana kopija potvrđene dokumentacije i potpisan kontrolni popis za postupak koji je provelo tijelo za registraciju.

2.2.4.5. Ako tijelo za registraciju potvrdi valjanost zahtjeva, postupak se nastavlja kao što je navedeno u točkama 2.2.4.6. i 2.2.4.7. U suprotnom se izdavanje certifikata odbija, o čemu se obavještava organizacija.

2.2.4.6. Služba za podršku CEF-a odobrava zahtjev za izdavanje certifikata i o tome obavještava tijelo za registraciju.

2.2.4.7. Tijelo za registraciju obavještava organizaciju da se certifikat može preuzeti putem korisničkog portala.



Slika 8. – Odobravanje certifikata

2.2.5. korak 4.: generiranje certifikata

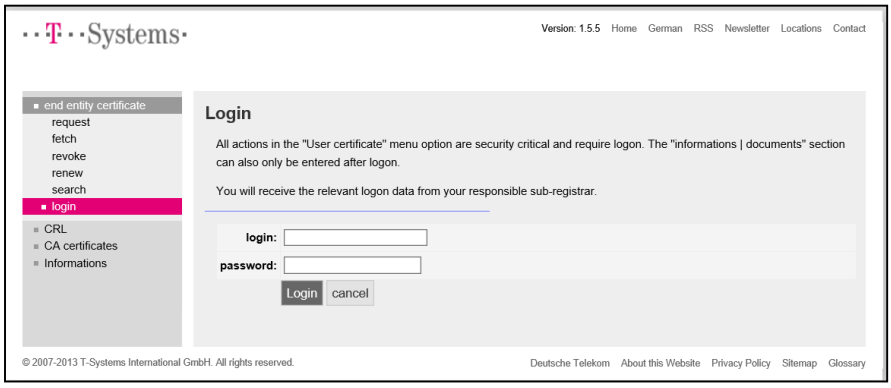
Certifikat se generira nakon odobravanja zahtjeva za izdavanje.

2.2.6. korak 5.: objavljivanje i preuzimanje certifikata

2.2.6.1. Nakon odobravanja zahtjeva za izdavanje certifikata, tijelo za registraciju preuzima certifikat i kopiju predaje pouzdanom kuriru.

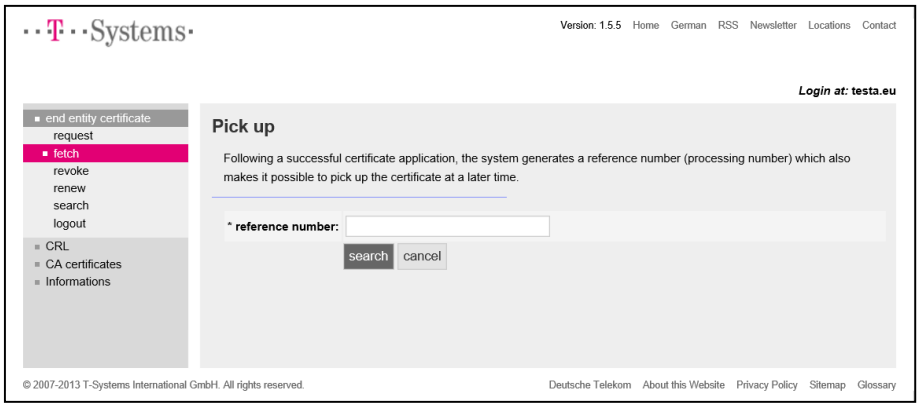
2.2.6.2. Organizacija prima obavijest od tijela za registraciju da se certifikat može preuzeti.

2.2.6.3. Organizacija se na korisničkom portalu https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en prijavljuje s korisničkim imenom „s**bca/CEF_eDelivery.europa.eu**” i lozinkom „**digit.333**”.



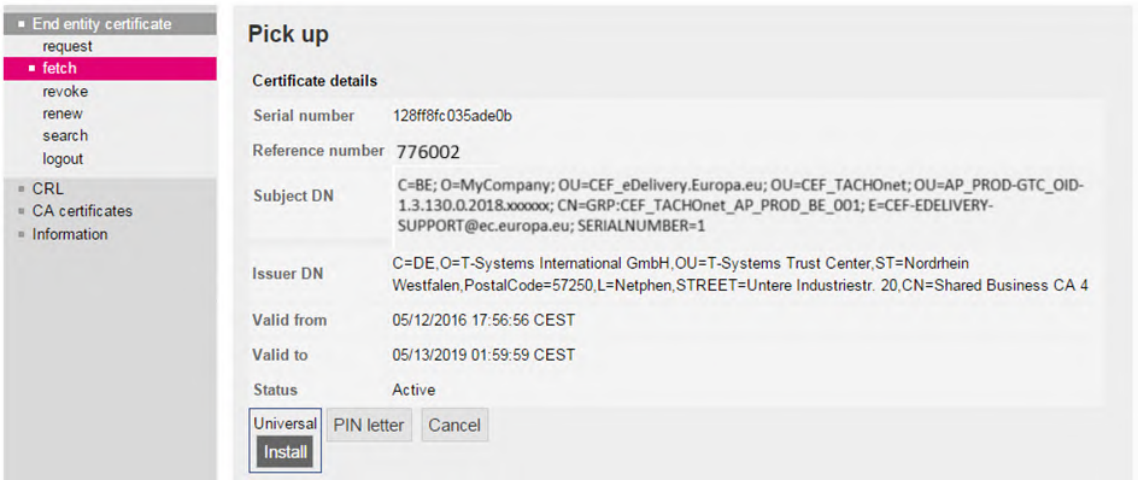
Slika 9.

2.2.6.4. Organizacija treba kliknuti na gumb za preuzimanje (fetch) na lijevoj strani prozora i unijeti referentni broj spremljen pri upućivanju zahtjeva za izdavanje certifikata.



Slika 10.

2.2.6.5. Organizacija instalira certifikate pritiskom na gumb za instalaciju (Install).



Slika 11.

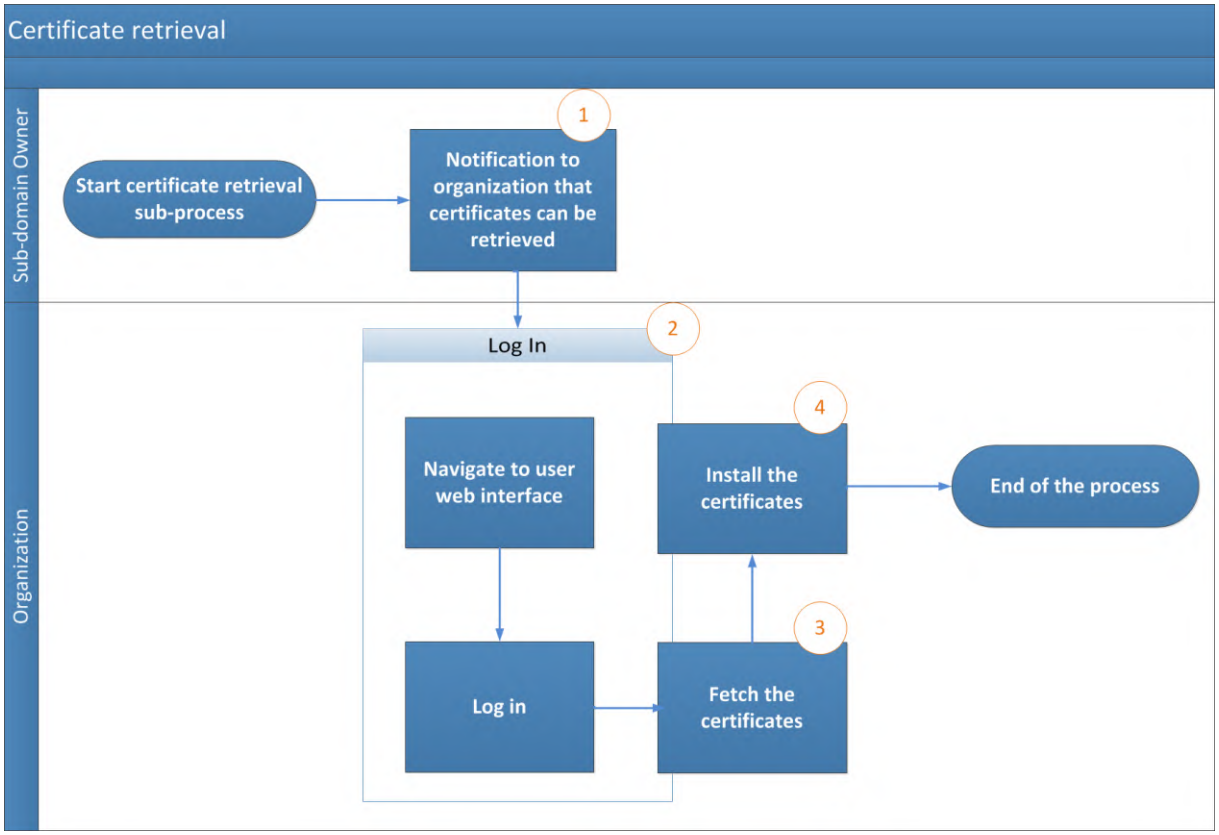
2.2.6.6. Certifikat se instalira na pristupnu točku (AP). Budući da se postupak razlikuje ovisno o provedbi, organizacija se za opis postupka obraća pružatelju pristupne točke.

2.2.6.7. Za instalaciju certifikata na pristupnu točku potrebno je provesti sljedeće korake:

(a) izvesti privatni ključ i certifikat;

(b) kreirati spremište ključeva (keystore) i spremište certifikata (truststore);

(c) instalirati spremište ključeva (keystore) i spremište certifikata (truststore) na pristupnu točku.

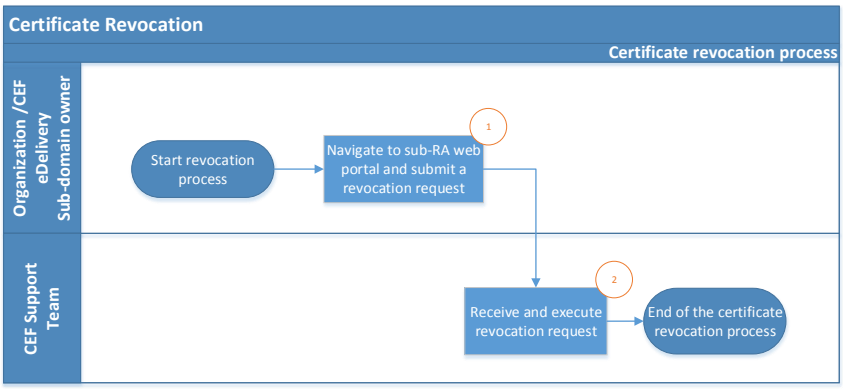


Slika 12. – Preuzimanje certifikata

3. Postupak opoziva certifikata

3.1. Organizacija upućuje zahtjev za opoziv putem korisničkog mrežnog portala.

3.2. Služba za podršku CEF-a opoziva certifikat.



Slika 13. – Opoziv certifikata

4. Opći uvjeti usluge CEF PKI

4.1. Kontekst

U svojstvu pružatelja rješenja elementa e-dostava Instrumenta za povezivanje Europe, DIGIT ugovornim strankama AETR-a stavlja na raspolaganje uslugu PKI[7] („usluga CEF PKI”). Uslugom CEF PKI koriste se nacionalna tijela („krajnji korisnici”) u sklopu sustava TACHOnet.

DIGIT je zakupac PKI-a u okviru TeleSec Shared-Business-CA („SBCA”) u centru povjerenja skupine T-Systems International GmbH („T-Systems”[8]). DIGIT ima ulogu glavnog registra domene „CEF_eDelivery.europa.eu” SBCA. U toj ulozi DIGIT kreira poddomene unutar domene „CEF_eDelivery.europa.eu” za svaki projekt koji se koristi uslugom CEF PKI.

U ovom su dokumentu navedene pojedinosti o uvjetima za uporabu poddomene TACHOnet. DIGIT ima ulogu podregistra te poddomene. U tom svojstvu on izdaje, opoziva i obnavlja certifikate u okviru ovog projekta.

4.2. Izjava o odricanju od odgovornosti

Europska komisija ne prihvaća odgovornost za sadržaj certifikata te svu odgovornost za njega snosi isključivo vlasnik certifikata. Odgovornost je vlasnika certifikata provjeriti točnost njegova sadržaja.

Europska komisija ne prihvaća odgovornost za način na koji se vlasnik certifikata njime koristi te svu odgovornost za njega snosi isključivo vlasnik certifikata koji je treća strana izvan Europske komisije.

---

7 PKI (infrastruktura javnog ključa) skup je uloga, politika, postupaka i sustava potrebnih za kreiranje, dodjelu i opoziv digitalnih certifikata te upravljanje njima.

8 Operator u centru povjerenja u društvu T-Systems ima i ulogu internog tijela za registraciju.

Ovom se izjavom ne ograničava odgovornost Europske komisije u slučaju kršenja zahtjeva propisanih mjerodavnim nacionalnim pravom niti se isključuje njezina odgovornost u slučajevima u kojima to u skladu s nacionalnim pravom nije moguće.

4.3. Dopuštena i zabranjena uporaba certifikata

4.3.1. Dopuštena uporaba certifikata

Nakon izdavanja certifikata vlasnik[9] se certifikatom koristi samo u okviru sustava TACHOnet. U tom okviru certifikat se može upotrebljavati za:

- potvrđivanje izvora podataka;
- šifriranje podataka;
- osiguranje otkrivanja povrede cjelovitosti podataka.

4.3.2. Zabranjena uporaba certifikata

Uporaba certifikata na način koji nije izričito naveden kao dopušten zabranjena je.

4.4. Dodatne obveze vlasnika certifikata

Detaljne uvjete za SBCA definirao je T-Systems u politici certifikacije (CP)/izjavi o certifikacijskim praksama (CPS) usluge SBCA[10]. Taj dokument sadržava sigurnosne specifikacije i smjernice o tehničkim i organizacijskim aspektima i u njemu se opisuju aktivnosti operatera centra povjerenja u ulogama certifikacijskog tijela (CA) i tijela za registraciju (RA) kao i delegirane treće strane tijela za registraciju.

Samo osobe ovlaštene za sudjelovanje u sustavu TACHOnet mogu zatražiti certifikat.

---

9 Označeno kao „O=” vrijednost atributa u polju „Razlikovno ime subjekta” izdanog certifikata

10 Najnoviju verziju CP a/CPS-a SBCA-e za T-Systems možete pronaći na https://www.telesec.de/en/sbca-en/support/download-area/.

U pogledu prihvaćanja certifikata primjenjuje se točka 4.4.1. politike certifikacije/izjave o certifikacijskim praksama („CP/CPS”) SBCA, a smatra se da je organizacija kojoj je certifikat izdan („O=”) pri prvoj uporabi prihvatila uvjete uporabe i odredbe iz ovog dokumenta.

Za objavljivanje certifikata primjenjuje se točka 2.2. CP/CPS SBCA.

Svi vlasnici certifikata moraju ispunjavati sljedeće zahtjeve:

(1) štititi svoj privatni ključ od neovlaštene uporabe;

(2) ne prenositi ili otkrivati svoje privatne ključeve trećim stranama, čak ni u svojstvu zastupnika;

(3) ne upotrebljavati privatni ključ nakon isteka razdoblja valjanosti ili opoziva certifikata, osim radi čitanja šifriranih podataka (primjerice dešifriranja elektroničke pošte).

(4) vlasnik certifikata odgovoran je za kopiranje ili prosljeđivanje ključa krajnjem korisniku odnosno krajnjim korisnicima;

(5) vlasnik certifikata od svih krajnjih korisnika mora zahtijevati poštovanje ovih uvjeta, uključujući CP/CPS SBCA, u postupcima s privatnim ključem;

(6) vlasnik certifikata mora osigurati identifikacijske podatke zastupnika koji su ovlašteni zatražiti opoziv certifikata izdanih organizaciji i pojedinosti o događajima koji su uzrokovali opoziv certifikata te lozinku za opoziv;

(7) za certifikate povezane sa skupinama osoba i funkcijama i/ili pravnim osobama, vlasnik certifikata, nakon što osoba napusti skupinu krajnjih korisnika (primjerice zbog prestanka radnog odnosa), mora opozvati certifikat i tako spriječiti zlouporabu privatnog ključa;

(8) vlasnik certifikata odgovoran je za opoziv certifikata pod uvjetima iz točke 4.9.1. CP/CPS SBCA.

Za obnovu ili ponovno izdavanje certifikata primjenjuje se točka 4.6. ili 4.7. CP/CPS SBCA.

Za objavljivanje certifikata primjenjuje se točka 4.8. CP/CPS SBCA.

Za opoziv certifikata primjenjuje se točka 4.9. CP/CPS SBCA.

5. Obrazac za identifikaciju osobe za kontakt i pouzdanog kurira (primjer)

Ja, *[ime i adresa zastupnika organizacije]*, **potvrđujem da se sljedeće informacije upotrebljavaju za upućivanje zahtjeva za izdavanje, generiranje i dohvaćanje digitalnih certifikata za javni ključ za pristupne točke u sustavu TACHOnet koji osiguravaju povjerljivost, cjelovitost i neosporivost poruka u sustavu TACHOnet:**

Podaci o osobi za kontakt:

– **Osoba za kontakt br. 1**	– **Osoba za kontakt br. 2**
– Prezime:	– Prezime:
– Ime:	– Ime:
– Mobitel:	– Mobitel:
– Telefon:	– Telefon:
– E-pošta:	– E-pošta:
– Uzorak vlastoručnog potpisa: –	– Uzorak vlastoručnog potpisa: – – –

Podaci o pouzdanom kuriru:

– **Pouzdani kurir br. 1**	– **Pouzdani kurir br. 2**
– Prezime:	– Prezime:
– Ime:	– Ime:
– Mobitel:	– Mobitel:
– E-pošta:	– E-pošta:
– Zemlja u kojoj je izdana putovnica:	– Zemlja u kojoj je izdana putovnica:
– Broj putovnice:	– Broj putovnice:
– Datum isteka valjanosti putovnice:	– Datum isteka valjanosti putovnice:

Mjesto, datum, žig društva ili pečat organizacije:

Potpis ovlaštenog zastupnika:

6. Dokumenti

6.1. Pojedinačna punomoć (primjer)

Primjer pojedinačne punomoći koju pouzdani kurir mora potpisati i predočiti pri osobnoj registraciji u tijelu za registraciju:

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. Papirni formular zahtjeva za izdavanje certifikata (primjer):

Primjer papirnog formulara zahtjeva za izdavanje certifikata koji pouzdani kurir mora potpisati i predočiti pri osobnoj registraciji u tijelu za registraciju:

7. Pojmovnik

Ključni izrazi koji su upotrijebljeni u ovom Poddodatku mogu se pronaći u definicijama pojmova CEF-a na jedinstvenom internetskom portalu CEF-a:

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

Ključne pokrate koje su upotrijebljene u ovom Poddodatku mogu se pronaći u glosaru CEF-a na jedinstvenom internetskom portalu CEF-a:

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