



Svet
Evropske unije

Bruselj, 5. november 2018
(OR. en)

13711/18
ADD 1

Medinstitucionalna zadeva:
2018/0339(NLE)

TRANS 488

DOPIS

Pošiljatelj:	generalni sekretariat Sveta
Prejemnik:	delegacije
Št. predh. dok.:	ST 13711/18 TRANS 448
Št. dok. Kom.:	ST 12727/18 TRANS 426 + ADD 1
Zadeva:	Sklep Sveta o stališču, ki se zavzame v imenu Evropske unije v skupini strokovnjakov za Evropski sporazum o delu posadk vozil, ki opravljajo mednarodne cestne prevoze, v okviru Ekonomske komisije Združenih narodov za Evropo

Priloga k navedenemu sklepu Sveta.

Novi dodatek k AETR

Dodatek 4

Specifikacije za sistem TACHOnet

1. Področje uporabe in namen
 - 1.1. V tem dodatku so določeni pogoji v zvezi s povezavo pogodbenic AETR s sistemom TACHOnet prek omrežja eDelivery.
 - 1.2. Pogodbenice, ki se s sistemom TACHOnet povezujejo prek omrežja eDelivery, upoštevajo določbe iz tega dodatka.
2. Opredelitev pojmov
 - (a) „pogodbenica“ pomeni katero koli pogodbenico AETR;
 - (b) „eDelivery (e-dostava)“ pomeni storitev, ki jo je razvila Evropska komisija in ki omogoča prenos podatkov med tretjimi stranmi z elektronskimi sredstvi, zagotavlja dokaze o ravnanju s prenesenimi podatki, vključno z dokazilom o oddaji in prejemu podatkov, ter prenesene podatke varuje pred tveganjem kakršne koli nepooblaščne spremembe;
 - (c) „TACHOnet“ pomeni sistem za elektronsko izmenjavo informacij o vozniških karticah med pogodbenicami, kot je določeno v členu 31(2) Uredbe (EU) št. 165/2014;
 - (d) „osrednje vozlišče“ pomeni informacijski sistem, ki omogoča usmerjanje sporočil TACHOnet med pogodbenicami vložnicami in pogodbenicami prejemnicami;
 - (e) „pogodbenica vložnica“ pomeni pogodbenico, ki odda zahtevek ali obvestilo TACHOnet, ki se nato v osrednjem vozlišču preusmeri na ustrezno pogodbenico prejemnico;

- (f) „pogodbenica prejemnica“ pomeni pogodbenico, na katero je naslovljen zahtevek ali obvestilo TACHOnet;
- (g) „organ izdajatelj kartice“ pomeni subjekt, ki ga pogodbenica pooblasti za izdajo in upravljanje tahografskih kartic.

3. Splošne obveznosti

- 3.1. Nobena pogodbenica ne sme skleniti sporazumov o dostopu do sistema TACHOnet v imenu druge pogodbenice ali na kakršen koli drug način zastopati drugo pogodbenico na podlagi tega dodatka. Nobena pogodbenica pri operacijah iz tega dodatka ne deluje kot podizvajalka druge pogodbenice.
- 3.2. Pogodbenice zagotovijo dostop do svojega nacionalnega registra vozniških kartic prek sistema TACHOnet na način in na ravni storitev, kot sta določena v poddodatku 4.6.
- 3.3. Pogodbenice se medsebojno nemudoma obvestijo, če opazijo motnje ali napake na svojem področju pristojnosti, ki bi lahko ogrozile običajno delovanje sistema TACHOnet.
- 3.4. Vsaka pogodbenica sekretariatu AETR sporoči kontaktne osebe za sistem TACHOnet. Vsaka sprememba kontaktnih oseb mora biti sekretariatu AETR predložena v pisni obliki.

4. Preizkusi za povezavo s sistemom TACHOnet

- 4.1. Povezava pogodbenice s sistemom TACHOnet je vzpostavljena po tem, ko so v skladu z navodili in pod nadzorom Evropske komisije uspešno opravljeni preizkusi povezovanja, integracije in delovanja.
- 4.2. Če predhodni preizkusi niso opravljeni uspešno, lahko Evropska komisija začasno odloži fazo preizkušanja. Preizkusi se nadaljujejo, ko pogodbenica Evropski komisiji sporoči, da so bile uvedene potrebne tehnične izboljšave na nacionalni ravni, ki naj bi omogočile, da bodo predhodni preizkusi opravljeni uspešno.

4.3. Predhodni preizkusi trajajo največ šest mesecev.

5. Arhitektura zaupanja

5.1. Arhitektura zaupanja sistema TACHOnet zagotavlja zaupnost, celovitost in nezatajljivost sporočil TACHOnet.

5.2. Temelji na storitvi infrastrukture javnih ključev (PKI), ki jo je vzpostavila Evropska komisija in katere zahteve so določene v poddodatkih 4.8 in 4.9.

5.3. V arhitekturo zaupanja sistema TACHOnet lahko posegajo naslednji subjekti:

- (a) certifikacijski organ, odgovoren za generiranje digitalnih potrdil, ki jih mora organ za registracijo predložiti nacionalnim organom pogodbenic (prek zaupanja vrednih kurirjev, ki jih ti imenujejo), ter za vzpostavitev tehnične infrastrukture za izdajo, preklic in obnovitev digitalnih potrdil;
- (b) lastnik domene, odgovoren za delovanje osrednjega vozlišča iz poddodatka 4.1 ter za potrjevanje in usklajevanje arhitekture zaupanja sistema TACHOnet;
- (c) organ za registracijo, odgovoren za registracijo in odobritev zahtevkov za izdajo, preklic in obnovitev digitalnih potrdil ter za preverjanje identitete zaupanja vrednih kurirjev;
- (d) zaupanja vredni kurir, tj. oseba, ki jo imenujejo nacionalni organi in je odgovorna za izročitev javnega ključa organu za registracijo in za prevzem pripadajočega potrdila, ki ga generira certifikacijski organ;
- (e) nacionalni organ pogodbenice, ki:
 - (i) generira zasebne ključe in pripadajoče javne ključe, ki bodo vključeni v potrdila, ki jih bo generiral certifikacijski organ;

- (ii) predloži zahteve za digitalna potrdila certifikacijskemu organu;
- (iii) imenuje zaupanja vrednega kurirja.

5.4. Certifikacijski organ in organ za registracijo imenuje Evropska komisija.

5.5. Vsaka pogodbenica, ki se poveže s sistemom TACHOnet, mora v skladu s poddodatkom 4.9 zahtevati izdajo digitalnega potrdila, da podpiše in šifrira sporočilo sistema TACHOnet.

5.6. Potrdilo se lahko prekliče v skladu s poddodatkom 4.9.

6. Varstvo podatkov in zaupnost

6.1. Pogodbenice v skladu z mednarodno in nacionalno zakonodajo o varstvu podatkov, zlasti pa v skladu s Konvencijo o varstvu posameznikov glede na avtomatsko obdelavo osebnih podatkov, sprejmejo vse potrebne tehnične in organizacijske ukrepe, s katerimi zagotovijo varnost podatkov sistema TACHOnet ter preprečijo spremembo, izgubo ali nedovoljeno obdelavo takih podatkov ali nedovoljen dostop do njih (zlasti v zvezi z avtentičnostjo, zaupnostjo, sledljivostjo, celovitostjo, razpoložljivostjo ter nezatajljivostjo in varnostjo sporočil).

6.2. Vsaka pogodbenica zaščiti svoje nacionalne sisteme pred nedovoljeno uporabo, zlonamernimi kodami, virusi, računalniškimi vdori, kršitvami in nedovoljenim poseganjem v podatke ter drugimi primerljivimi dejanji tretjih strani. Pogodbenice se strinjajo, da bodo uporabile razumna tržna sredstva, da bi se izognile prenosom kakršnih koli virusov, časovnih bomb, črvov ali podobnih programov ali kakršnim koli običajnim postopkom računalniškega programiranja, ki bi lahko vplivali na računalniške sisteme druge pogodbenice.

7. Stroški

7.1. Pogodbenice krijejo lastne razvojne in operativne stroške v povezavi s svojimi podatkovnimi sistemi in postopki, ki so potrebni za izpolnjevanje obveznosti iz tega dodatka.

7.2. Storitve iz poddodatka 4.1, ki jih zagotavlja osrednje vozlišče, so brezplačne.

8. Sklepanje pogodb s podizvajalci

8.1. Pogodbenice lahko za katero koli od storitev, za katere so odgovorne v skladu s tem dodatkom, sklenejo pogodbo s podizvajalci.

8.2. Takšno sklepanje pogodb s podizvajalci pogodbenice ne razrešuje odgovornosti v skladu s tem dodatkom, vključno z odgovornostjo za ustrezno raven storitev v skladu s poddodatkom 4.6.

Splošni vidiki sistema TACHOnet

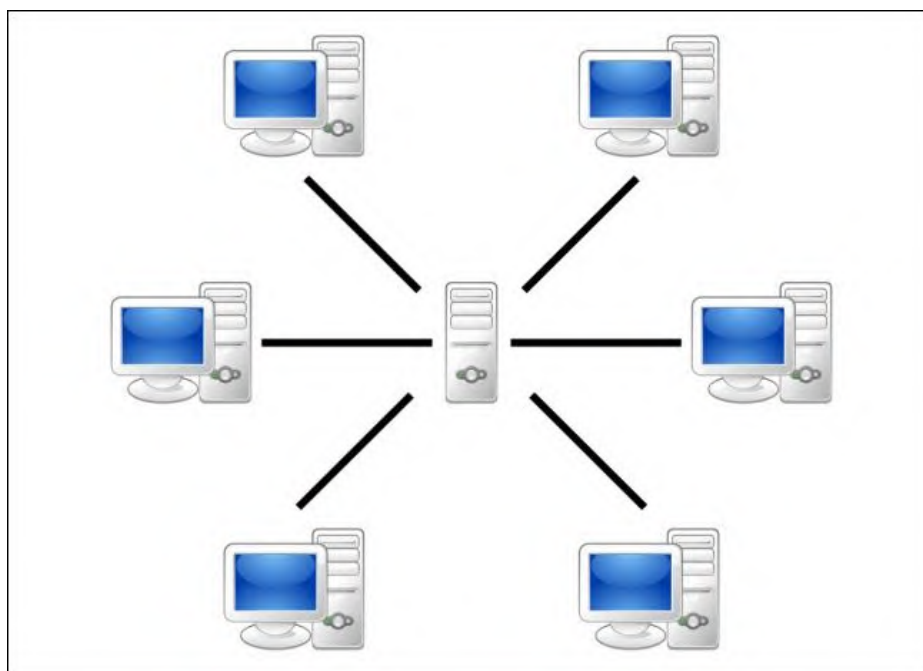
1. Splošni opis

Sistem TACHOnet je elektronski sistem za izmenjavo informacij o vozniških karticah med pogodbenicami AETR. TACHOnet pošilja zahteve po informacijah od pogodbenic vložnic k pogodbenicam prejemnicam, odzive pa v nasprotni smeri. Pogodbenice, ki so del sistema TACHOnet, morajo svoje nacionalne registre vozniških kartic povezati s sistemom.

2. Arhitektura

Sporočilni sistem TACHOnet sestavljajo naslednji deli:

- 2.1. osrednje vozlišče, ki je sposobno sprejeti zahtevek od pogodbenice vložnice, ga potrditi in obdelati s posredovanjem pogodbenicam prejemnicam. Osrednje vozlišče počaka na odzive vseh pogodbenic prejemnic, zbere vse odzive in posreduje konsolidiran odziv pogodbenici vložnici;
- 2.2. nacionalni sistemi pogodbenic, ki so opremljeni z vmesnikom, ki je sposoben pošiljati zahtevke v osrednje vozlišče in prejemati ustrezne odzive. Nacionalni sistemi lahko za posredovanje, prenos in prejem sporočil iz osrednjega vozlišča uporabljajo lastniško ali komercialno programsko opremo.



3. Upravljanje

- 3.1. Osrednje vozlišče upravlja Evropska komisija, ki je odgovorna za njegovo tehnično delovanje in vzdrževanje.
- 3.2. V osrednjem vozlišču se podatki ne hranijo dlje kot šest mesecev, razen dnevnikov in statističnih podatkov iz poddodatka 4.7.
- 3.3. Osrednje vozlišče ne omogoča dostopa do osebnih podatkov, razen pooblaščenim uslužbencem Evropske komisije, kadar je to potrebno za namene spremljanja, vzdrževanja in odpravljanja napak.
- 3.4. Vsaka pogodbenica je odgovorna za:
 - 3.4.1. vzpostavitev in upravljanje svojih nacionalnih sistemov, vključno z njihovo povezavo z osrednjim vozliščem;
 - 3.4.2. namestitev in vzdrževanje svojega nacionalnega sistema, tako strojne kot tudi programske opreme, lastniške ali komercialne;
 - 3.4.3. pravilno interoperabilnost svojega nacionalnega sistema z osrednjim vozliščem, vključno z upravljanjem sporočil o napakah, prejetih iz osrednjega vozlišča;
 - 3.4.4. sprejetje vseh ukrepov za zagotavljanje zaupnosti, celovitosti in razpoložljivosti informacij;
 - 3.4.5. delovanje nacionalnih sistemov v skladu z ravnmi storitev iz poddodatka 4.6.

Funkcije sistema TACHOnet

1. Prek sporočilnega sistema TACHOnet so zagotovljene naslednje funkcije:
 - 1.1. Preverjanje izdanih kartic (CIC): omogoča pogodbenici vložnici, da pošlje zahtevek za preverjanje izdanih kartic eni ali več pogodbenicam prejemnicam, da bi ugotovila, ali vložnik vloge za kartico že ima vozniško kartico, ki jo je izdala pogodbenica prejemnica. Pogodbenice prejemnice odgovorijo na zahtevek tako, da pošljejo odziv na preverjanje izdanih kartic.
 - 1.2. Preverjanje statusa kartice (CCS): omogoča pogodbenici vložnici, da vpraša pogodbenico prejemnico o podatkih kartice, ki jo je izdala slednja, tako da pošlje zahtevek za preverjanje statusa kartice. Pogodbenica prejemnica odgovori na zahtevek tako, da pošlje odziv na preverjanje statusa kartice.
 - 1.3. Sprememba statusa kartice (MCS): omogoča pogodbenici vložnici, da z zahtevkom za spremembo statusa kartice obvesti pogodbenico prejemnico, da se je status kartice, ki jo je izdala slednja, spremenil. Pogodbenica prejemnica odgovori s potrditvijo spremembe statusa kartice.
 - 1.4. Vozniško dovoljenje izdane kartice (ICDL): omogoča pogodbenici vložnici, da z zahtevkom za vozniško dovoljenje izdane kartice obvesti pogodbenico prejemnico, da je izdala kartico na podlagi vozniškega dovoljenja, ki ga je izdala slednja. Pogodbenica prejemnica odgovori z odzivom na vozniško dovoljenje izdane kartice.
2. Vključijo se tudi druge vrste sporočil, ki se štejejo za primerne za učinkovito delovanje sistema TACHOnet, na primer obvestila o napakah.
3. Nacionalni sistemi prepoznajo statute kartic, navedene v preglednici 1, kadar se uporabljajo funkcije iz točke 1. Vendar pa pogodbenice niso dolžne izvajati upravnega postopka, ki bi vključeval vse navedene statute.

4. Kadar pogodbenica prejme odziv ali obvestilo z navedbo statusa, ki ga ne uporablja v svojih upravnih postopkih, nacionalni sistem pretvori status iz prejetega sporočila v ustrezno vrednost v navedenem postopku. Pogodbenica prejemnica ne sme zavrniti sporočila, če je status v sporočilu naveden v preglednici 1.
5. Status kartice, ki je naveden v preglednici 1, se ne uporablja za ugotavljanje, ali je vozniška kartica veljavna za vožnjo. Kadar pogodbenica prek funkcije CCS poizveduje v registru nacionalnega organa, ki je izdal kartico, odziv vsebuje posebno polje „velja za vožnjo“. Nacionalni upravni postopki so taki, da odzivi na CCS vedno vsebujejo ustrezno vrednost „velja za vožnjo“.

Preglednica 1

Statusi kartic

Status kartice	Opredelitev
Vloga	Organ izdajatelj kartice je prejel vlogo za izdajo vozniške kartice. Te informacije so bile evidentirane in shranjene v podatkovno zbirko s pripravljenimi iskalnimi ključi.
Odobreno	Organ izdajatelj kartice je odobril vlogo za tahografsko kartico.
Zavrnjeno	Organ izdajatelj kartice ni odobril vloge.
Prilagojeno	Tahografska kartica je bila prilagojena.
Odpremljeno	Nacionalni organ je vozniško kartico odpremil ustreznemu vozniku ali dostavni agenciji.
Vročeno	Nacionalni organ je vozniško kartico vročil zadevnemu vozniku.
Odvzeto	Pristojni organ je vozniku odvzel vozniško kartico.
Razveljavljeno	Vozniška kartica je bila vozniku začasno odvzeta.
Preklicano	Organ izdajatelj kartice je sklenil preklicati vozniško kartico. Kartica je bila trajno razveljavljena.
Vrnjeno	Tahografska kartica je bila vrnjena organu izdajatelju kartice z izjavo, da ni več potrebna.
Izgubljeno	Organu izdajatelju kartice je bila prijavljena izguba tahografske kartice.
Ukradeno	Organu izdajatelju kartice je bila prijavljena kraja tahografske kartice. Šteje se, da je ukradena kartica izgubljena.
Nepravilno delovanje	Organu izdajatelju kartice je bilo prijavljeno nepravilno delovanje tahografske kartice.
Poteklo	Obdobje veljavnosti tahografske kartice je poteklo.
Nadomeščeno	Tahografska kartica, ki je bila prijavljena kot izgubljena, ukradena ali nepravilno delujoča, je bila nadomeščena z novo kartico. Podatki na novi kartici so enaki z izjemo indeksa zamenjave številke kartice, ki se poveča za eno.

Podaljšano	Tahografski kartici je bila podaljšana veljavnost zaradi spremembe upravnih podatkov ali skorajšnjega poteka obdobja veljavnosti. Številka nove kartice je enaka z izjemo indeksa podaljšanja številke kartice, ki se poveča za eno.
V zamenjavi	Organ izdajatelj kartice, ki je izdal vozniško kartico, je prejel obvestilo, da se je začel postopek zamenjave te kartice z vozniško kartico, ki jo bo izdal organ izdajatelj kartice druge pogodbenice.
Zamenjano	Organ izdajatelj kartice, ki je izdal vozniško kartico, je prejel obvestilo, da se je končal postopek zamenjave te kartice z vozniško kartico, ki jo bo izdal organ izdajatelj kartice druge pogodbenice.

Poddodatek 4.3

Določbe glede sporočil sistema TACHOnet

1. Splošne tehnične zahteve
 - 1.1. Osrednje vozlišče zagotovi tako sinhroni kot asinhroni vmesnik za izmenjavo sporočil. Pogodbenice lahko izberejo najprimernejšo tehnologijo za povezavo s svojimi aplikacijami.
 - 1.2. Vsa sporočila, izmenjana med osrednjim vozliščem in nacionalnimi sistemi, so kodirana po UTF-8.
 - 1.3. Nacionalni sistemi so sposobni prejemati in obdelovati sporočila, ki vsebujejo grške ali cirilične znake.
2. Struktura in definicijske sheme (XSD) sporočil XML
 - 2.1. Splošna struktura sporočil XML ima obliko, ki je opredeljena s shemami XSD, nameščenimi v osrednjem vozlišču.
 - 2.2. Osrednje vozlišče in nacionalni sistemi prenašajo in prejemajo sporočila, ki so skladna s shemo sporočil XSD.
 - 2.3. Nacionalni sistemi omogočajo pošiljanje, prejemanje in obdelavo vseh sporočil, ki ustrezajo kateri od funkcij iz poddodatka 4.2.
 - 2.4. Sporočila XML vključujejo vsaj minimalne zahteve iz preglednice 2.

Preglednica 2

Minimalne zahteve za vsebino sporočil XML

Skupna glava		Obvezno
Različica	Uradna različica specifikacij XML je določena z imenskim prostorom, opredeljenim v XSD sporočila in v atributu različica elementa glave v posameznem sporočilu XML. Številka različice („n.m“) se določi kot fiksna vrednost pri vsaki objavi datoteke z definicijsko shemo protokola XML (XSD).	Da
Testni identifikator	Neobvezen identifikator za preizkušanje. Originator preizkusa vnese identifikator, ki ga vsi udeleženci v delovnem postopku posredujejo/vrnejo. V običajnem delovanju se zanemari in se ne uporablja, če je bil poslan.	Ne
Tehnični identifikator	Univerzalni edinstveni identifikator (UUID), ki enolično označuje vsako posamezno sporočilo. Pošiljatelj generira UUID in vnese ta atribut. Ta podatek se ne uporablja v nobeni poslovni funkciji.	Da
Identifikator delovnega postopka	Identifikator delovnega postopka (workflowID) je UUID in bi ga morala generirati pogodbenica vložnica. Ta identifikator se nato uporabi v vseh sporočilih za primerjanje delovnega postopka.	Da
Poslano ob	Datum in čas (UTC), ko je bilo sporočilo poslano.	Da
Potek časa	To je neobvezen atribut datuma in časa (v formatu UTC). Navedeno vrednost nastavi le osrednje vozlišče v primeru posredovanih zahtevkov. S tem je pogodbenica prejemnica obveščena o tem, kdaj bo čas za zahtevek potekel. Ta vrednost ni potrebna v MS2TCN_<x>_Req in vseh odzivnih sporočilih. Vrednost je neobvezna, tako da se lahko za vse vrste sporočil uporablja enaka definicija glave, ne glede na to, ali se atribut timeoutValue zahteva ali ne.	Ne
Pošiljatelj	Oznaka pogodbenice, ki pošilja sporočilo, po ISO 3166-1 Alpha 2 ali „EU“.	Da
Prejemnik	Oznaka pogodbenice, v katero se sporočilo pošilja, po ISO 3166-1 Alpha 2 ali „EU“.	Da

Poddodatek 4.4

Prečkovanje in storitve NYSIIS (identifikacijski in obveščevalni sistem zvezne države New York)

1. Algoritem NYSIIS v osrednjem vozlišču se uporablja za kodiranje imen vseh voznikov v nacionalnem registru.
2. Za iskanje kartice s funkcijo CIC se kot glavni iskalni mehanizem uporabljajo ključi NYSIIS.
3. Poleg tega lahko pogodbenice uporabljajo prilagojen algoritem za pridobivanje dodatnih rezultatov.
4. V rezultatih iskanja mora biti naveden iskalni mehanizem, ki je bil uporabljen pri iskanju zapisa, bodisi NYSIIS ali prilagojeni.
5. Če se pogodbenica odloči za zapisovanje obvestil ICDL, morajo biti ključi NYSIIS, ki jih vsebuje obvestilo, zabeleženi kot del podatkov ICDL. Pri iskanju podatkov ICDL pogodbenica uporablja ključe NYSIIS za ime vložnika.

Poddodatek 4.5

Varnostne zahteve

1. Za izmenjavo sporočil med osrednjim vozliščem in nacionalnimi sistemi se uporablja HTTPS.
2. Za zaščito prenosa sporočil med nacionalnim sistemom in osrednjim vozliščem nacionalni sistemi uporabljajo digitalna potrdila iz poddodatkov 4.8 in 4.9.
3. Nacionalni sistemi uporabljajo vsaj potrdila, pri katerih se uporabljata zgoščevalni algoritem podpisa SHA-2 (SHA-256) in javni ključ z dolžino 2048 bitov.

Poddodatek 4.6

Ravni storitev

1. Nacionalni sistemi izpolnjujejo naslednje minimalne ravni storitev:
 - 1.1. Na voljo so 24 ur na dan in 7 dni v tednu.
 - 1.2. Njihova razpoložljivost se spremlja s sporočili srčnega utripa (heartbeat), ki se pošiljajo iz osrednjega vozlišča.
 - 1.3. Stopnja njihove razpoložljivosti je 98 % v skladu z naslednjo preglednico (številke so zaokrožene na najbližjo primerno enoto):

Razpoložljivost	pomeni naslednjo nerazpoložljivost		
	tedensko	mesečno	letno
98 %	0,5 ure	15 ur	7,5 dneva

Pogodbenice so pozvane, naj upoštevajo dnevno stopnjo razpoložljivosti, vendar je treba upoštevati, da nekatere dejavnosti, kot je na primer vzdrževanje sistema, zahtevajo čas izpada, daljši od 30 minut. Mesečna in letna stopnja razpoložljivosti pa sta zavezujoči.

- 1.4. Odzovejo se na vsaj 98 % zahtevkov, ki so jim bili posredovani v enem koledarskem mesecu.
- 1.5. Na zahteve se odzovejo v največ 10 sekundah.
- 1.6. Skupni čas do izteka zahtevka (čas, v katerem lahko vložnik zahtevka čaka na odziv) ne presega 20 sekund.
- 1.7. Sposobni so se odzivati na zahteve s hitrostjo 6 sporočil na sekundo.
- 1.8. Nacionalni sistemi ne smejo pošiljati zahtevkov vozlišču TACHOnet s hitrostjo, ki presega 2 zahtevka na sekundo.

1.9. Vsak nacionalni sistem je sposoben delovati v primeru morebitnih tehničnih težav v osrednjem vozlišču ali nacionalnih sistemih v drugih pogodbenicah. Te med drugim vključujejo:

- (a) izpad povezave z osrednjim vozliščem;
- (b) ni odziva na zahtevek;
- (c) prejem odzivov po izteku časa za sporočilo;
- (d) prejem nenaročenih sporočil;
- (e) prejem neveljavnih sporočil.

2. Osrednje vozlišče:

2.1. vzdržuje stopnjo razpoložljivosti 98 %;

2.2. obvešča nacionalne sisteme o morebitnih napakah, bodisi prek odzivnega sporočila bodisi prek namenskega sporočila o napaki. Nacionalni sistemi prejemajo navedena namenska sporočila o napaki in imajo delovni postopek stopnjevanja za sprejem vseh ustreznih ukrepov za odpravo sporočene napake.

3. Vzdrževanje

Pogodbenice obvestijo druge pogodbenice in Evropsko komisijo o vseh običajnih dejavnostih vzdrževanja prek spletne aplikacije vsaj en teden pred začetkom navedenih dejavnosti, če je to tehnično mogoče.

Poddodatek 4.7

Vodenje dnevnikov in statistična obdelava podatkov, zbranih v osrednjem vozlišču

1. Za zaščito zasebnosti se podatki za statistične namene obravnavajo anonimno. Podatki o določeni kartici, vozniku ali voznikem dovoljenju niso na voljo za statistične namene.
2. Informacije iz dnevnikov dokumentirajo vse transakcije za namene spremljanja in odpravljanja napak ter omogočajo pripravo statističnih podatkov o teh transakcijah.
3. Osebni podatki se v dnevnikih ne hranijo več kot 6 mesecev. Statistične informacije se hranijo nedoločen čas.
4. Statistični podatki, ki se uporabljajo za poročanje, vključujejo:
 - (a) pogodbenico vložnico;
 - (b) pogodbenico prejemnico;
 - (c) vrsto sporočila;
 - (d) statusno kodo odziva;
 - (e) datum in čas sporočil;
 - (f) odzivni čas.

Poddodatek 4.8

Splošne določbe v zvezi z digitalnimi ključi in potrdili za sistem TACHOnet

1. Generalni direktorat Evropske komisije za informatiko (DIGIT) pogodbenicam AETR, ki se povezujejo s sistemom TACHOnet (v nadaljnjem besedilu: nacionalni organi), omogoči dostop do storitve PKI¹ („storitev PKI IPE“) prek omrežja eDelivery.
2. Postopek za zahtevo in preklic digitalnih potrdil ter podrobni pogoji za njegovo uporabo so opredeljeni v Dodatku.
3. Uporaba potrdil:
 - 3.1. po izdaji potrdila ga nacionalni organ² uporablja samo v okviru sistema TACHOnet. Potrdilo se lahko uporablja za:
 - (a) ugotavljanje pristnosti izvora podatkov;
 - (b) šifriranje podatkov;
 - (c) odkrivanje kršitev celovitosti podatkov.
 - 3.2. Kakršna koli uporaba, ki ni izrecno odobrena v okviru dovoljenih uporab potrdila, je prepovedana.
4. Pogodbenice:
 - (a) zaščitijo svoj zasebni ključ pred nepooblaščno uporabo;
 - (b) ne prenašajo ali razkrivajo svojega zasebnega ključa tretjim stranem, niti kot zastopnice;

¹ PKI (infrastruktura javnih ključev) je niz vlog, politik, postopkov in sistemov, ki so potrebni za generiranje, upravljanje, razširjanje in preklic digitalnih potrdil.

² Označen z vrednostjo atributa „O=“ v razločevalnem imenu izdanega potrdila.

- (c) zagotovijo zaupnost, celovitost in razpoložljivost zasebnih ključev, ki se generirajo, hranijo in uporabljajo za sistem TACHOnet;
- (d) ne nadaljujejo z uporabo zasebnega ključa po poteku veljavnosti ali preklicu potrdila, razen za ogled šifriranih podatkov (npr. dešifriranje elektronske pošte). Potekli ključi se uničijo ali zadržijo na način, ki preprečuje njihovo uporabo;
- (e) organu za registracijo predložijo identifikacijo zastopnikov, pooblaščenih za zahtevanje preklica potrdil, izdanih organizaciji (zahtevek za preklic vključuje geslo za zahtevek za preklic in podrobnosti o dogodkih, ki vodijo do preklica);
- (f) preprečijo zlorabo zasebnega ključa, tako da zahtevajo preklic pripadajočega javnega ključa v primeru ogroženosti zasebnega ključa ali podatkov o aktivaciji zasebnega ključa;
- (g) imajo odgovornost in obveznost, da zahtevajo preklic potrdil v okoliščinah, opredeljenih v politiki certificiranja (CP) in izjavi o postopkih certificiranja (CPS) certifikacijskega organa;
- (h) organ za registracijo nemudoma uradno obvestijo o izgubi, kraji ali morebitni ogroženosti kakršnih koli ključev AETR, ki se uporabljajo v okviru sistema TACHOnet.

5. Odgovornost

Brez omejevanja odgovornosti Evropske komisije za delovanje v nasprotju s kakršnimi koli zahtevami iz veljavne nacionalne zakonodaje ali za dejanja, za katera izključitev odgovornosti ni zakonsko dovoljena, Evropska Komisija ni odgovorna za:

- (a) vsebino potrdila, za katero je odgovoren izključno lastnik potrdila. Lastnik potrdila je odgovoren za preverjanje točnosti njegove vsebine;
- (b) uporabo potrdila s strani lastnika.

Opis storitve PKI za sistem TACHOnet

1. Uvod

PKI (infrastruktura javnih ključev) je niz vlog, politik, postopkov in sistemov, ki so potrebni za generiranje, upravljanje, razširjanje in preklic digitalnih potrdil³. Storitve PKI IPE omrežja eDelivery omogoča izdajanje in upravljanje digitalnih potrdil, ki se uporabljajo za zagotavljanje zaupnosti, celovitosti in nezatajljivosti informacij, izmenjanih med dostopovnimi točkami (AP).

Storitve PKI omrežja eDelivery temelji na storitvi TeleSec Shared Business CA (certifikacijski organ) središča zaupanja Trust Center Services, za katero se uporablja politika certificiranja (CP)/izjava o postopkih certificiranja (CPS) storitve TeleSec Shared-Business CA podjetja T-Systems International GmbH⁴.

Storitve PKI omogoča izdajo potrdil, primernih za zagotavljanje različnih poslovnih procesov znotraj in zunaj podjetij, organizacij, javnih organov in institucij, za katere je potrebna srednja stopnja varnosti, da se dokaže avtentičnost, celovitost in zanesljivost končnega subjekta.

2. Postopek zahtevka za potrdilo

2.1. Vloge in odgovornosti

2.1.1. „Organizacija“ ali „nacionalni organ“, ki zahteva potrdilo

2.1.1.1. Nacionalni organ zahteva potrdila v okviru projekta TACHOnet.

2.1.1.2 Nacionalni organ:

- (a) zahteva potrdila od storitve PK IPE;

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

⁴ Najnovejšo različico CP in CPS lahko prenesete s spletne strani <https://www.telesec.de/en/sbca-en/support/download-area/>

- (b) generira zasebne ključe in pripadajoče javne ključe, ki bodo vključeni v potrdila, ki jih bo izdal certifikacijski organ;
- (c) po odobritvi prenese potrdilo;
- (d) podpiše in organu za registracijo vrne:
 - (i) identifikacijski obrazec kontaktnih oseb in zaupanja vrednih kurirjev,
 - (ii) podpisano individualno pisno pooblastilo⁵.

2.1.2. Zaupanja vredni kurir

2.1.2.1. Nacionalni organ imenuje zaupanja vrednega kurirja.

2.1.2.2. Zaupanja vredni kurir:

- (a) izroči javni ključ organu za registracijo med postopkom osebne identifikacije in registracije;
- (b) od organa za registracijo prejme pripadajoče potrdilo.

2.1.3. Lastnik domene

2.1.3.1. Lastnik domene je GD MOVE.

2.1.3.2. Lastnik domene:

- (a) potrdi in usklajuje omrežje in arhitekturo zaupanja sistema TACHOnet, vključno s potrditvijo postopkov za izdajo potrdil;
- (b) upravlja osrednje vozlišče sistema TACHOnet in usklajuje dejavnosti pogodbenic v zvezi z delovanjem sistema TACHOnet;
- (c) skupaj z nacionalnimi organi izvede preizkuse povezave s sistemom TACHOnet.

⁵ Pisno pooblastilo je pravni dokument, s katerim organizacija pooblašča Evropsko komisijo, ki jo zastopa določeni pooblaščen uradnik, odgovoren za storitev PKI IPE, da v njenem imenu storitev TeleSec Shared Business CA podjetja T-Systems International GmbH zaprosi za potrdilo. Glej tudi točko 6.

2.1.4. Organ za registracijo

2.1.4.1. Organ za registracijo je Skupno raziskovalno središče (JRC).

2.1.4.2. Organ za registracijo je odgovoren za preverjanje identitete zaupanja vrednega kurirja ter za registracijo in odobritev zahtevkov za izdajo, preklic in obnovitev digitalnih potrdil.

2.1.4.3. Organ za registracijo:

- (a) dodeli enolični identifikator nacionalnemu organu;
- (b) ugotovi istovetnost nacionalnega organa, njegovih kontaktnih oseb in zaupanja vrednih kurirjev;
- (c) komunicira s službo za podporo IPE v zvezi z istovetnostjo nacionalnega organa, njegovih kontaktnih oseb in zaupanja vrednih kurirjev;
- (d) obvesti nacionalni organ o odobritvi ali zavrnitvi potrdila.

2.1.5. Certifikacijski organ

2.1.5.1. Certifikacijski organ je odgovoren za zagotavljanje tehnične infrastrukture za zahtevo, izdajo in preklic digitalnih potrdil.

2.1.5.2. Certifikacijski organ:

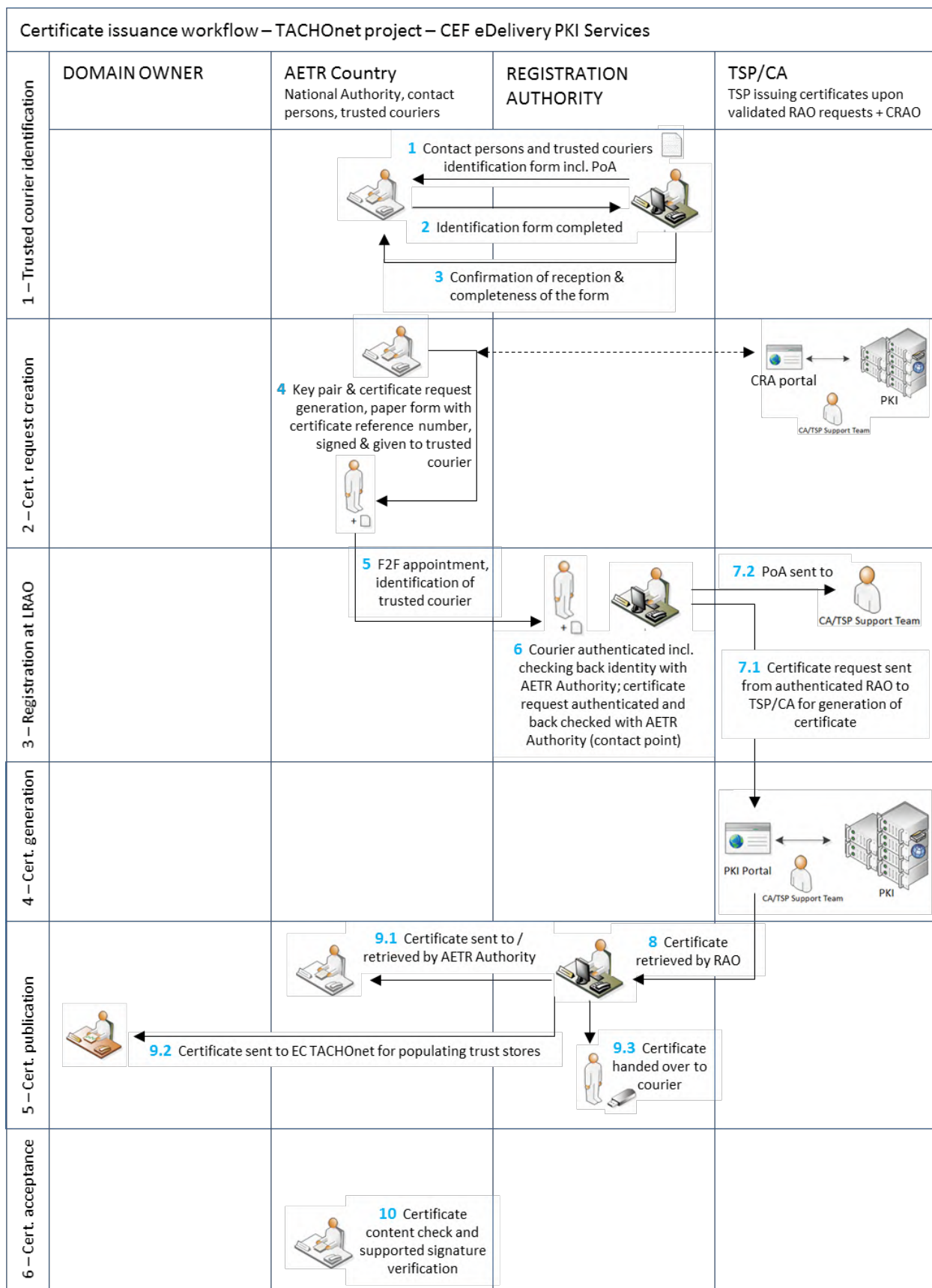
- (a) zagotovi tehnično infrastrukturo za zahteve nacionalnih organov za potrdila;
- (b) potrdi ali zavrne zahteve za potrdila;
- (c) po potrebi komunicira z organom za registracijo pri preverjanju identitete organizacije, ki vloži zahtevek.

2.2. Izdaja potrdila

2.2.1. Izdaja potrdila se opravi v skladu z naslednjimi zaporednimi koraki, ki so prikazani na sliki 1:

- (a) **Korak 1:** identifikacija zaupanja vrednega kurirja;

- (b) **Korak 2:** generiranje zahtevka za potrdilo;
- (c) **Korak 3:** registracija pri organu za registracijo;
- (d) **Korak 4:** generiranje potrdila;
- (e) **Korak 5:** objava potrdila;
- (f) **Korak 6:** sprejem potrdila.



Slika 1 – Postopek izdaje potrdila

2.2.2. Korak 1: Identifikacija zaupanja vrednega kurirja

Za identifikacijo zaupanja vrednega kurirja se izvede naslednji postopek:

- (a) organ za registracijo nacionalnemu organu pošlje identifikacijski obrazec kontaktnih oseb in zaupanja vrednih kurirjev⁶. Ta obrazec vključuje tudi pisno pooblastilo, ki ga organizacija (organ AETR) podpiše;
- (b) nacionalni organ vrne izpolnjen obrazec in podpisano pisno pooblastilo organu za registracijo;
- (c) organ za registracijo potrdi prejem in popolnost obrazca;
- (d) organ za registracijo lastniku domene predloži posodobljen izvod seznama kontaktnih oseb in zaupanja vrednih kurirjev.

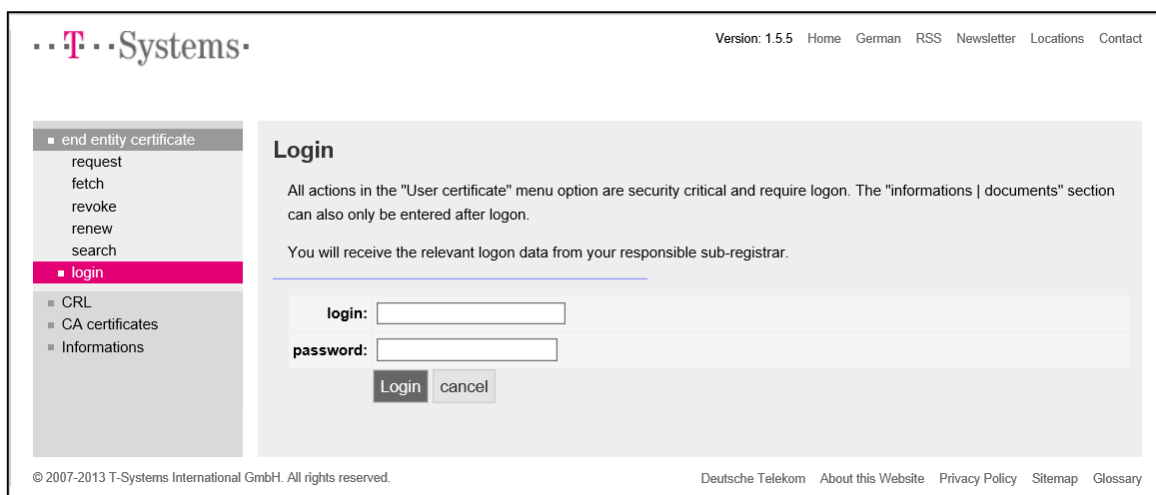
2.2.3. Korak 2: Generiranje zahtevka za potrdilo

2.2.3.1. Zahtevki za potrdilo in njegov prevzem se opravita na istem računalniku in z istim brskalnikom.

2.2.3.2. Za generiranje zahtevka za potrdilo se izvede naslednji postopek:

- (a) organizacija odpre uporabniški spletni vmesnik in zahteva potrdilo prek URL <https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en>: ter vpiše uporabniško ime „sbca/CEF_eDelivery.europa.eu“ in geslo „digit.333“;

⁶ Glej točko 5.



Slika 2

- (b) organizacija klikne „request“ na levi strani okna in na spustnem seznamu izbere „CEF_TACHOnet“;



Slika 3

- (c) organizacija izpolni obrazec za zahtevek za potrdilo iz slike 4 z informacijami iz preglednice 3 ter s klikom na „Next (soft-PSE)“ zaključi postopek;

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

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

Official Organisation Name (case sensitive)

Must be:
TYPE=AP_PROD
concatenated with '-' separator and
'GTC_OID-1.3.130.0.2018.xxxxxx'
where Ares(2018)xxxxxx is the allocated number

Must be:
'CEF-EDelivery-SUPPORT@ec.europa.eu'

Must be the official address of the Organisation. (Used for the Power of Attorney.)
Attention: if the ZIP code is NOT a 5-digit ZIP code, leave the ZIP code field empty and put the ZIP code in the City field.

Email: the email address must be the same as the one used for registering the Unique Identifier, + Name of the person representing the organisation. (Used for the Power of Attorney)

The organisation can choose its own password or click on the button 'Adopt revocation password proposal'

Click here to end

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

Country: BE

Organisation/company (O): My Company

Internet domain (OU1): CEF_eDelivery.europa.eu

Responsibility (OU2): CEF_TACHOnet

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

First name (CN): Leave Empty

Last name (CN): GRP:CEF_TACHOnet_AP_PROD_BE_001

E-mail: CEF-EDelivery-SUPPORT@ec.europa.eu

E-mail 1 (SAN): Leave Empty

E-mail 2 (SAN): Leave Empty

E-mail 3 (SAN): Leave Empty

Address: Leave Empty

Street: Street no.

ZIP code: City

Phone no.: Leave Empty

business.register.xx@mail.com

Mr Johan Smith

Revocation password: (max. 50 characters)

Revocation password repetition: (max. 50 characters)

Revocation password proposal: juHEVeV136

Adopt revocation password proposal

Slika 4

Zahtevana polja	Opis
Država	C = oznaka države, lokacija lastnika potrdila, preverjena z uporabo javnega imenika Omejitve: 2 znaka v skladu s standardom ISO 3166-1, alfa-2, razlikovanje velikih in malih črk Primeri: DE, BE, NL Posebni primeri: UK (za Združeno kraljestvo), EL (za Grčijo)
Organizacija/podjetje (O)	O = ime organizacije lastnika potrdila
Glavna domena (OU1)	OU = CEF_eDelivery.europa.eu
Področje odgovornosti (OU2)	OU = CEF_TACHOnet
Oddelek (OU3)	Obvezna vrednost za vsako „OBMOČJE ODGOVORNOSTI“ Vsebinsko je treba preveriti s pozitivnim seznamom (beli seznam), ko se zahteva potrdilo. Če informacije ne ustrezajo seznamu, se zahteva prepreči. Format: OU = <TYPE>-<GTC_NUMBER> Pri tem se „<TYPE>“ nadomesti z AP_PROD: dostopovna točka v proizvodnem okolju. In pri čemer je <GTC_NUMBER> GTC_OID-1.3.130.0.2018.xxxxxxx, pri čemer je Ares(2018)xxxxxx številka GTC za projekt TACHOnet. Npr.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxxx
Ime (CN)	Mora ostati prazno.
Priimek (CN)	Mora se začeti z „GRP:“, čemur sledi splošno ime. Format: CN = GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER> Npr.: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-pošta	E=CEF-EDELIVERY-SUPPORT@ec.europa.eu
E-naslov 1 (SAN)	Mora ostati prazno.
E-naslov 2 (SAN)	Mora ostati prazno.
E-naslov 3 (SAN)	Mora ostati prazno.

Naslov	Mora ostati prazno.
Ulica	Mora biti uradni naslov organizacije lastnika potrdila (ki se uporablja za pisno pooblastilo).
Ulična št.	Mora biti uradni naslov organizacije lastnika potrdila (ki se uporablja za pisno pooblastilo).
Poštna številka	Mora biti uradni naslov organizacije lastnika potrdila (ki se uporablja za pisno pooblastilo). <u>Opozorilo:</u> če poštna številka NI 5-številčna poštna številka, polje pustite prazno in poštno številko vpišite v polje za mesto.
Mesto	Mora biti uradni naslov organizacije lastnika potrdila (ki se uporablja za pisno pooblastilo). <u>Opozorilo:</u> če poštna številka NI 5-številčna poštna številka, polje pustite prazno in poštno številko vpišite v polje za mesto.
Telefonska številka	Mora ostati prazno.
Identifikacijski podatki	Elektronski naslov mora biti enak tistemu, ki se uporablja za registracijo enoličnega identifikatorja. + Mora biti ime osebe, ki zastopa organizacijo (ki se uporablja za pisno pooblastilo). + Št. poslovnega registra (obvezno samo za zasebne organizacije). Vpisano na lokalnem sodišču (velja le za nemške in avstrijske zasebne organizacije).
Geslo za preklic	Obvezno polje, ki ga je izbral vložnik.
Ponovitev gesla za preklic	Ponovljeno obvezno polje, ki ga je izbral vložnik.

Preglednica 3 Izpolnite podrobne podatke za vsako zahtevano polje.

(d) izbrana dolžina ključa 2048 (visoka stopnja);

The screenshot shows the 'User certificate' request form on the T-Systems website. The left sidebar contains a menu with 'request' highlighted. The main form area has the following fields:

- Country (C): BE
- Organization/company (O): European Commission
- Master domain (OU1): CEF_eDelivery.europa.eu
- Area of responsibility (OU2): CEF_TACHOnet
- Department (OU3): AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
- First name (CN):
- Last name (CN): GRP:CEF_TACHOnet_AP_PROD_BE_001
- E-mail: CEF-EDELIVERY-SUPPORT@ec.europa.eu
- Selection of key length: 2048 (High Grade) (dropdown menu)

Buttons for 'Request' and 'Cancel' are at the bottom of the form. The footer includes copyright information and links to 'Deutsche Telekom', 'About this Website', 'Privacy Policy', 'Sitemap', and 'Glossary'.

Slika 5

(e) organizacija za prevzem potrdila zabeleži referenčno številko;

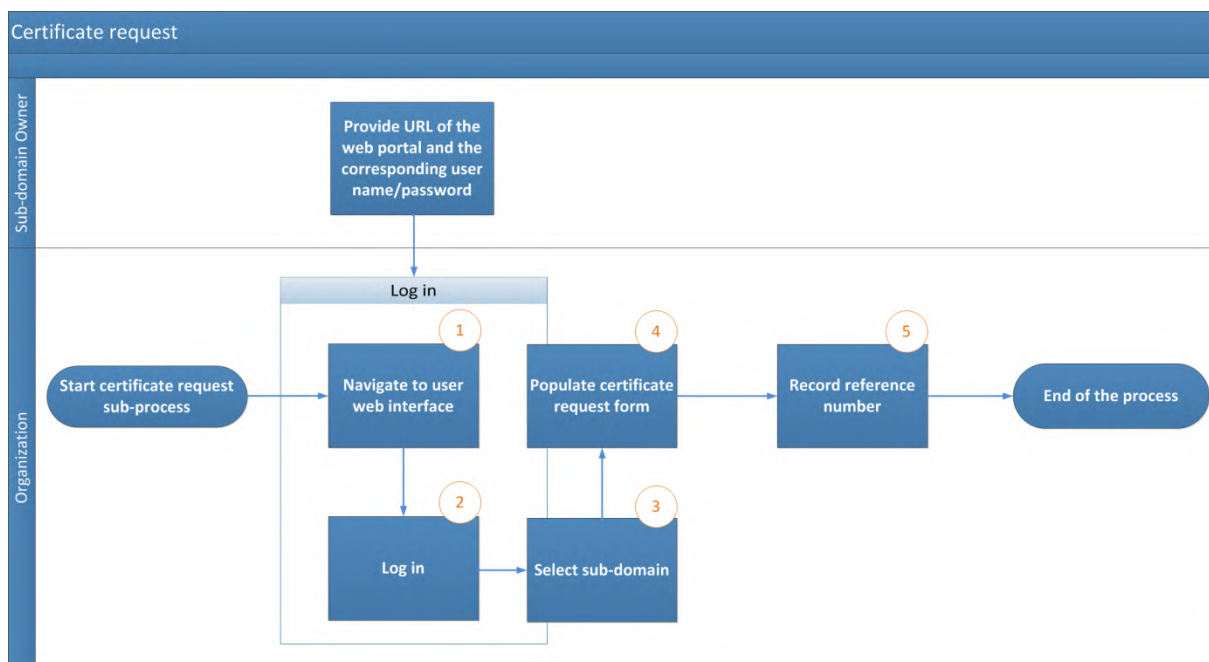
The screenshot shows the confirmation page after a certificate request. A blue callout bubble points to the text 'Your request was stored with reference number 776002.' with the label 'Certificate Reference Number'.

The page content includes:

- Header: T-Systems logo, Version: 1.55, Home, German, RSS, Newsletter, Locations, Contact
- Left sidebar: Menu with 'request' highlighted
- Main content: 'User certificate' section with the message: 'The certificate was requested. Your request was stored with reference number 776002. Please note that you can only pick up the certificate once the responsible sub-registrar has approved the certificate application. You will be notified of the approval by e-mail.'
- Footer: Copyright information and links to 'Deutsche Telekom', 'About this Website', 'Privacy Policy', 'Sitemap', and 'Glossary'

Slika 6

- (f) podporna skupina IPE pregleda nove zahteve za potrdila in preveri, ali so informacije v zahtevku za potrdilo veljavne, tj. da so v skladu z dogovorom glede poimenovanja potrdil iz Dodatka 5.1;
- (g) podporna skupina IPE preveri, ali so informacije, vnesene v zahtevek, v veljavnem formatu;
- (h) če preverjanje iz točk 5 ali 6 zgoraj ni uspešno, podporna skupina IPE pošlje elektronsko sporočilo na elektronski naslov, naveden v „identifikacijskih podatkih“ obrazca za zahtevek z lastnikom domene v kopiji, v katerem organizacijo zaprosi, da ponovno začne postopek. Neuspešen zahtevek za potrdilo se razveljavi;
- (i) podporna skupina IPE organu za registracijo pošlje elektronsko sporočilo o veljavnosti zahtevka. Elektronsko sporočilo vsebuje:
 - (1) ime organizacije iz polja „Organizacija (O)“ zahtevka za potrdilo;
 - (2) podatke o potrdilu, vključno z imenom dostopovne točke, za katero se potrdilo izda, iz polja „priimek (CN)“ zahtevka za potrdilo;
 - (3) referenčno številko potrdila;
 - (4) naslov organizacije, e-naslov organizacije in ime osebe, ki jo zastopa.



Slika 7 – Postopek zahtevka za potrdilo

2.2.4. Korak 3: Registracija pri organu za registracijo (odobritev potrdila)

2.2.4.1. Zaupanja vredni kurir ali kontaktna oseba se po elektronski pošti prijavita pri organu za registracijo ter sporočita identiteto zaupanja vrednega kurirja, ki bo osebno prišel na sestanek.

2.2.4.2. Organizacija pripravi dokumentacijski paket, ki vključuje:

- (a) izpolnjeno in podpisano pisno pooblastilo;
- (b) kopijo veljavnega potnega lista zaupanja vrednega kurirja, ki bo osebno prišel na sestanek. To kopijo mora podpisati ena od kontaktnih oseb organizacije, opredeljenih v koraku 1;
- (c) papirni obrazec zahtevka za potrdilo, ki ga podpiše ena od kontaktnih oseb organizacije.

2.2.4.3. Organ za registracijo po pregledu identitete na recepciji sprejme zaupanja vrednega kurirja. Organ za registracijo opravi osebno registracijo zahtevka za potrdilo, tako da:

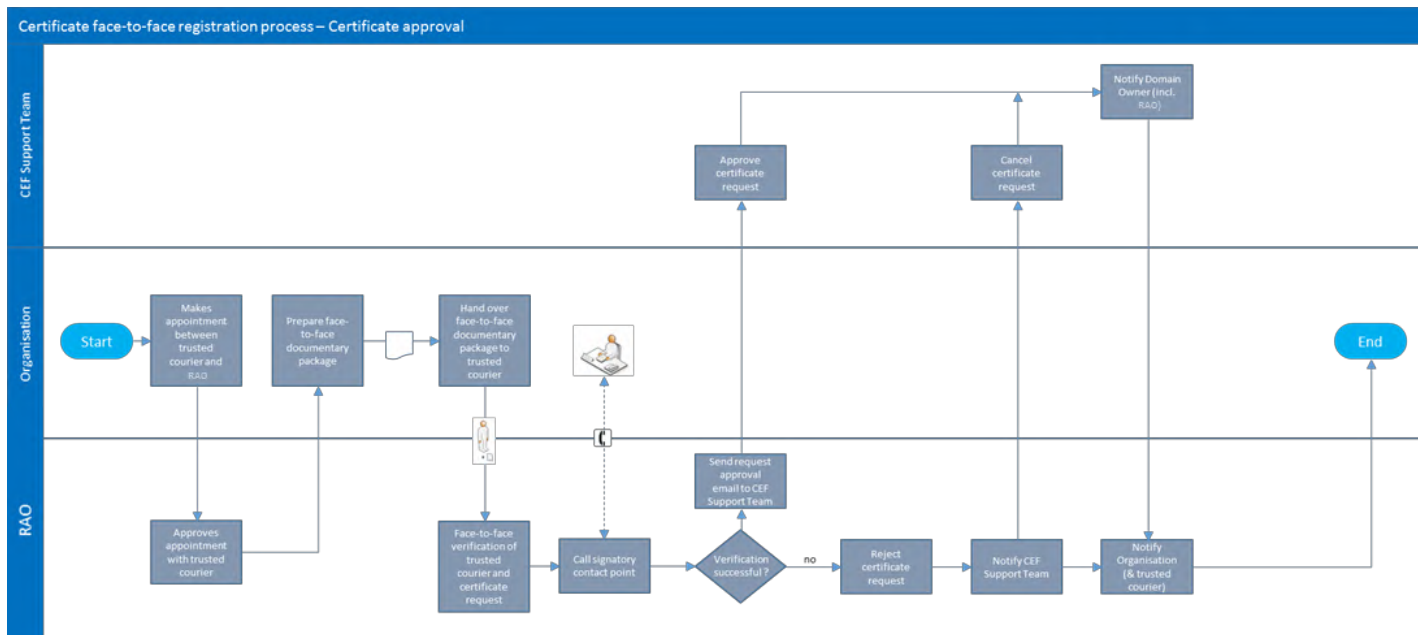
- (a) identificira in preveri istovetnost zaupanja vrednega kurirja;
- (b) preveri videz zaupanja vrednega kurirja glede na sliko v njegovem potnem listu;
- (c) preveri veljavnost potnega lista zaupanja vrednega kurirja;
- (d) veljavni potni list, ki ga predloži zaupanja vredni kurir, primerja s kopijo veljavnega potnega lista zaupanja vrednega kurirja, ki jo je podpisala ena od opredeljenih kontaktnih oseb organizacije. Istovetnost podpisa se preveri s primerjavo z originalnim podpisom iz „identifikacijskega obrazca kontaktnih oseb in zaupanja vrednih kurirjev“;
- (e) preveri izpolnjeno in podpisano pisno pooblastilo;
- (f) preveri papirni obrazec zahtevka za potrdilo in podpis na njem glede na izvirni „identifikacijski obrazec kontaktnih oseb in zaupanja vrednih kurirjev“;
- (g) pokliče kontaktno osebo podpisnika, da ponovno preveri identiteto zaupanja vrednega kurirja in vsebino zahtevka za potrdilo.

2.2.4.4. Organ za registracijo skupini za podporo IPE potrdi, da ima nacionalni organ dejansko dovoljenje za upravljanje komponent, za katere zahteva potrdila, in da je bil ustrezni postopek osebne registracije uspešen. Potrditev se pošlje z varno elektronsko pošto s pomočjo potrdila „CommiSign“, pri čemer se priloži skenirana kopija overjenega osebno predloženega dokumentacijskega paketa in podpisanega kontrolnega seznama postopka, ki ga je izvedel organ za registracijo.

2.2.4.5. Če organ za registracijo potrdi veljavnost zahtevka, se postopek nadaljuje, kot je določeno v točkah 2.2.4.6 in 2.2.4.7. V nasprotnem primeru se izdaja potrdila zavrne in o tem obvesti organizacija.

2.2.4.6. Podporna skupina IPE odobri zahtevek za potrdilo in o tem obvesti organ za registracijo.

2.2.4.7. Organ za registracijo obvesti organizacijo, da je potrdilo mogoče prevzeti prek uporabniškega portala.



Slika 8 – Odobritev potrdila

2.2.5. Korak 4: Generiranje potrdila

Potrdilo se generira po odobritvi zahtevka za potrdilo.

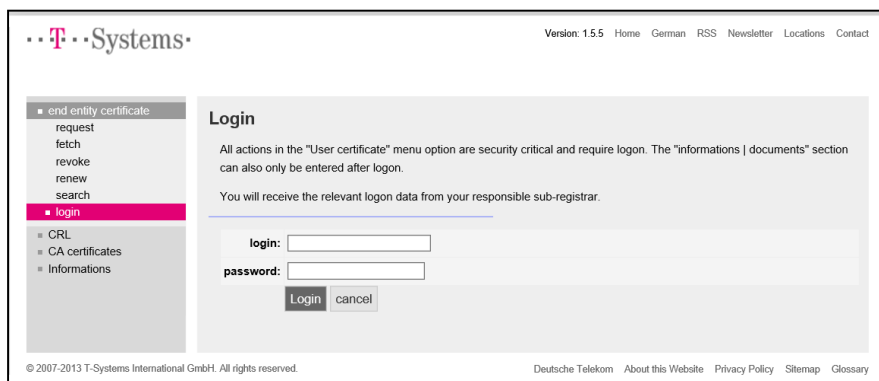
2.2.6. Korak 5: Objava in prevzem potrdila

2.2.6.1. Po odobritvi zahtevka za potrdilo organ za registracijo prevzame potrdilo in kopijo preda zaupanja vrednemu kurirju.

2.2.6.2. Organizacija prejme obvestilo organa za registracijo, da je potrdilo mogoče prevzeti.

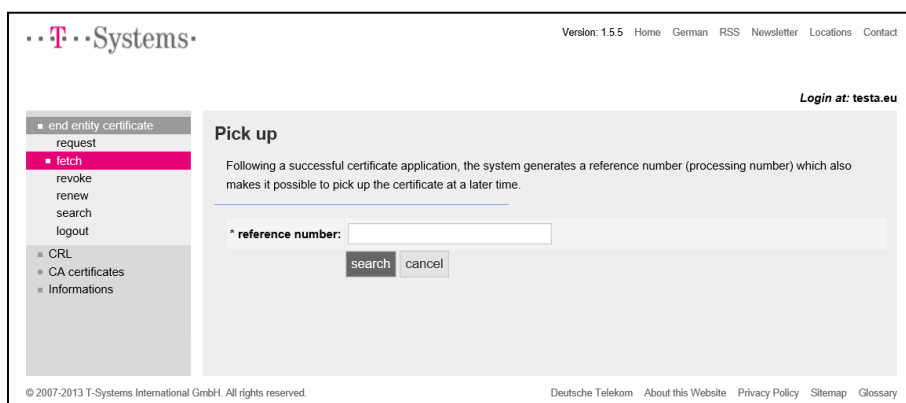
2.2.6.3. Organizacija se na uporabniškem portalu

<https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en> prijavi z uporabniškim imenom „sbca/CEF_eDelivery.europa.eu“ in geslom „digit.333“.



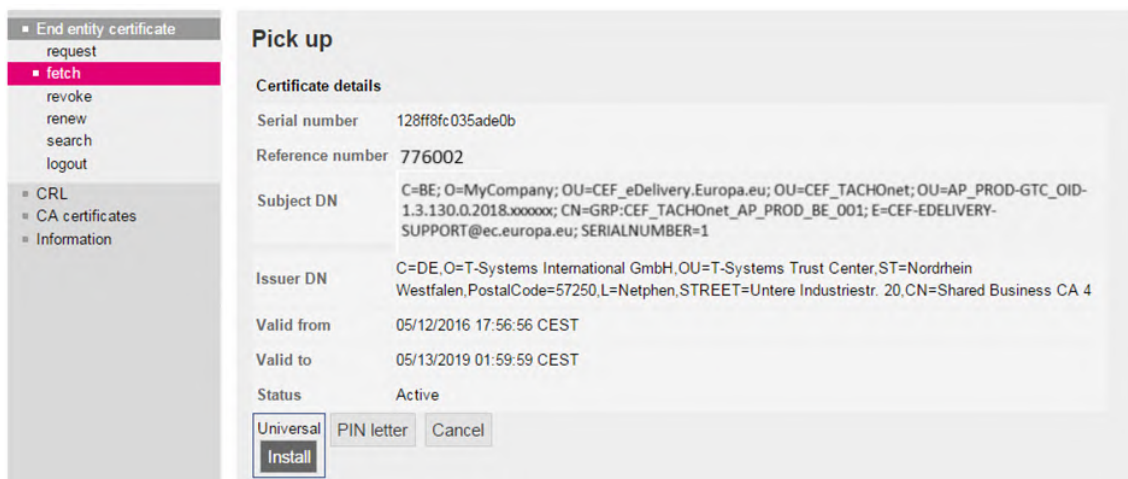
Slika 9

2.2.6.4. Organizacija klikne na gumb „fetch“ na levi strani in navede referenčno številko, ki je bila zabeležena med postopkom zahtevka za potrdilo.



Slika 10

2.2.6.5. Organizacija namesti potrdila s klikom na gumb „install“.

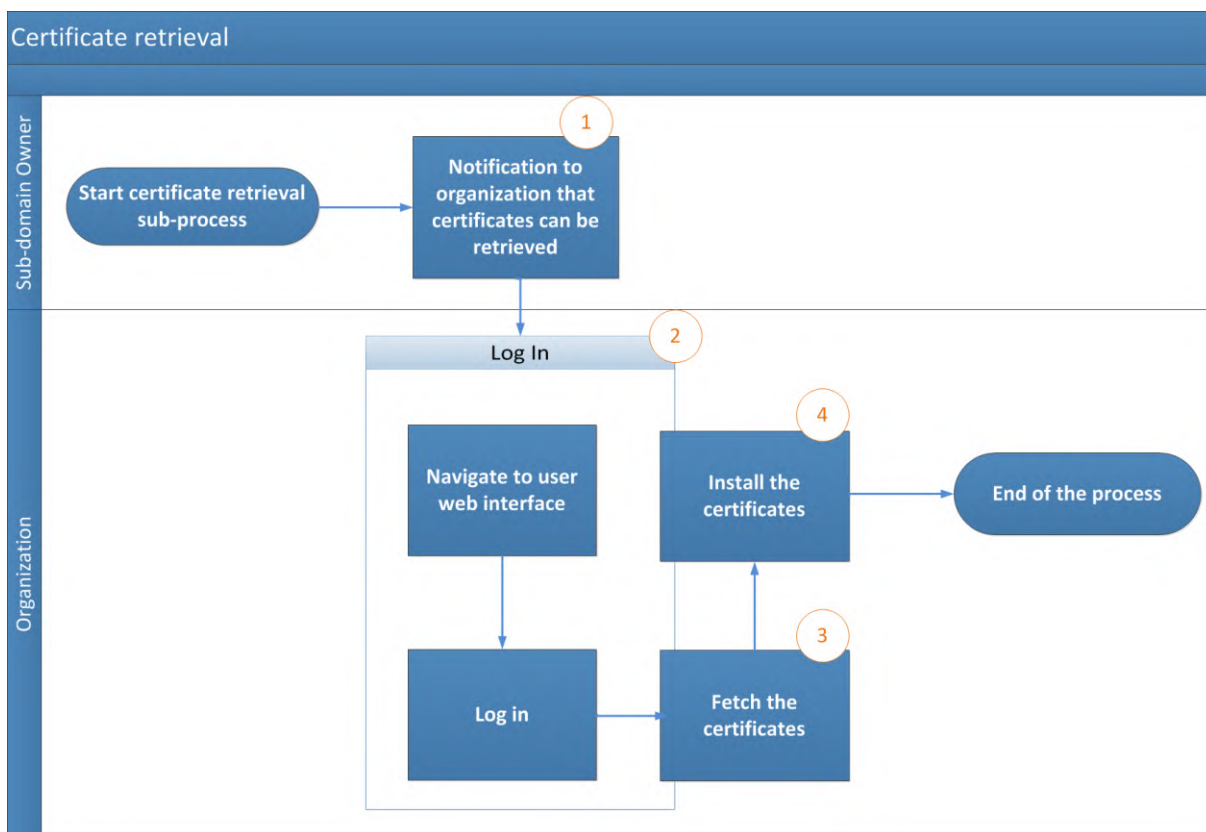


Slika 11

2.2.6.6. Potrdilo se namesti na dostopovno točko. Ker je postopek odvisen od izvedbe, se organizacija za opis tega postopka obrne na svojega ponudnika dostopovne točke.

2.2.6.7. Naslednji koraki so potrebni za namestitev potrdila na dostopovno točko:

- (a) izvoz zasebnega ključa in potrdila;
- (b) oblikovanje shrambe ključev (keystore) in shrambe potrdil (truststore);
- (c) namestitev shrambe ključev in shrambe potrdil na dostopovno točko.

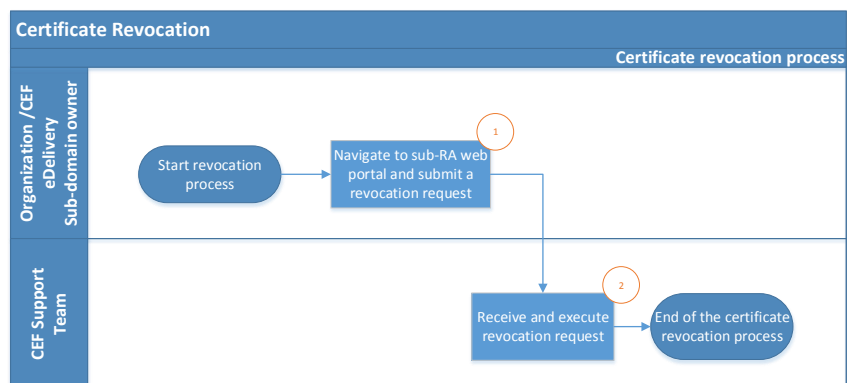


Slika 12 – Prevzem potrdila

3. Postopek preklica potrdila

3.1. Organizacija predloži zahtevek za preklic prek spletnega uporabniškega portala.

3.2. Podporna skupina IPE izvede preklic potrdila.



Slika 13 – Preklic potrdila

4. Splošni pogoji storitve PKI IPE

4.1. Ozadje

Kot ponudnik rešitev gradnika eDelivery Instrumenta za povezovanje Evrope DIGIT pogodbenicam AETR zagotovi dostop do storitve PKI⁷ (v nadaljnjem besedilu: storitev PKI IPE). Storitve PKI IPE uporabljajo nacionalni organi („končni uporabniki“), ki sodelujejo v sistemu TACHOnet.

DIGIT je zakupnik PKI v okviru rešitve TeleSec Shared-Business-CA („SBCA“), ki deluje v središču zaupanja (Trust Center) skupine T-Systems International GmbH („T-Systems“⁸). DIGIT ima vlogo glavnega registrarja domene „CEF_eDelivery.europa.eu“ SBCA. V tej vlogi DIGIT ustvarja poddomene znotraj domene „CEF_eDelivery.europa.eu“ za vsak projekt, ki uporablja storitev PKI IPE.

V tem dokumentu so navedene podrobnosti o pogojih za uporabo poddomene TACHOnet. DIGIT ima vlogo podregistrarja te poddomene. V tej vlogi izdaja, preklicuje in obnavlja potrdila za ta projekt.

4.2. Izjava o omejitvi odgovornosti

Evropska komisija ne prevzema nikakršne odgovornosti v zvezi z vsebino potrdila, za katero je odgovoren izključno lastnik potrdila. Lastnik potrdila je odgovoren za preverjanje točnosti njegove vsebine.

Evropska komisija ne prevzema nikakršne odgovornosti v zvezi z uporabo potrdila s strani njegovega lastnika, ki je tretji pravni subjekt zunaj Evropske komisije.

⁷ PKI (infrastruktura javnih ključev) je niz vlog, politik, postopkov in sistemov, ki so potrebni za generiranje, upravljanje, razširjanje in preklic digitalnih potrdil.

⁸ Operater središča zaupanja v podjetju T-Systems v svoji zaupani vlogi prav tako prevzema naloge internega organa za registracijo.

Ta izjava o omejitvi odgovornosti nikakor ne omejuje odgovornosti Evropske komisije za kakršno koli delovanje v nasprotju z veljavno nacionalno zakonodajo niti ne izključuje odgovornosti Komisije za dejanja, za katera izključitev odgovornosti ni zakonsko dovoljena.

4.3. Dovoljena/prepovedana uporaba potrdil

4.3.1. Dovoljena uporaba potrdil

Po izdaji potrdila ga lastnik⁹ uporablja samo v okviru sistema TACHOnet. V tem okviru se potrdilo lahko uporablja za:

- ugotavljanje pristnosti izvora podatkov;
- šifriranje podatkov;
- odkrivanje kršitev celovitosti podatkov.

4.3.2. Prepovedana uporaba potrdil

Kakršna koli uporaba, ki ni izrecno odobrena v okviru dovoljenih uporab potrdila, je prepovedana.

4.4. Dodatne obveznosti lastnika potrdila

Podrobne pogoje za SBCA je skupina T-Systems opredelila v politiki certificiranja (CP) / izjavi o postopkih certificiranja (CPS) storitve SBCA¹⁰. Ta dokument vsebuje varnostne specifikacije in smernice v zvezi s tehničnimi in organizacijskimi vidiki ter opisuje dejavnosti operaterja središča zaupanja v vlogi certifikacijskega organa (CA) in organa za registracijo (RA) ter pooblašcene tretje strani organa za registracijo.

Potrdilo lahko zahtevajo samo subjekti, pooblašчени za sodelovanje v sistemu TACHOnet.

⁹ Označen z vrednostjo atributa „O=“ v razločevalnem imenu izdanega potrdila.

¹⁰ Najnovejša različica politike certificiranja (CP)/izjave o postopkih certificiranja (CPS) SBCA skupine T-System je na voljo na <https://www.telesec.de/en/sbca-en/support/download-area/>.

Kar zadeva sprejetje potrdil, se uporablja točka 4.4.1 politike certificiranja (CP)/izjave o postopkih certificiranja (CPS) SBCA; poleg tega se šteje, da organizacija, kateri je izdano potrdilo („O =“), ob prvi uporabi sprejema pogoje uporabe in določbe iz tega dokumenta.

V zvezi z objavo potrdila se uporablja točka 2.2 CP/CPS SBCA.

Vsi lastniki potrdil izpolnjujejo naslednje zahteve:

- (1) zaščitijo svoj zasebni ključ pred nepooblaščno uporabo;
- (2) ne prenašajo ali razkrivajo svojega zasebnega ključa tretjim stranem, niti kot zastopniki;
- (3) ne nadaljujejo z uporabo zasebnega ključa po poteku veljavnosti ali preklicu potrdila, razen za ogled šifriranih podatkov (npr. dešifriranje elektronske pošte).
- (4) lastnik potrdila je odgovoren za kopiranje ali posredovanje ključa končnim subjektom;
- (5) od vseh končnih subjektov mora zahtevati, da ob ravnanju z zasebnim ključem upoštevajo veljavne pogoje, vključno s CP/CPS SBCA;
- (6) lastnik potrdila mora zagotoviti identifikacijske podatke zastopnikov, ki so pooblašчени za zahtevo preklica potrdil, izdanih organizaciji, ter podrobnosti o dogodkih, ki so povzročili preklic, in geslo za preklic;
- (7) za potrdila, povezana s skupinami oseb ter funkcijami in/ali pravnimi osebami, mora lastnik potrdila, potem ko oseba zapusti skupino končnih subjektov (npr. prenehanje delovnega razmerja), preprečiti zlorabo zasebnega ključa, tako da potrdilo prekliče;
- (8) lastnik potrdila je odgovoren za preklic potrdila pod pogoji iz točke 4.9.1 CP/CPS SBCA.

V zvezi z obnovitvijo ali ponovno izdajo potrdil se uporablja točka 4.6 ali 4.7 CP/CPS SBCA.

V zvezi s spremembo potrdila se uporablja točka 4.8 CP/CPS SBCA.

V zvezi s preklicem potrdila se uporablja točka 4.9 CP/CPS SBCA.

5. Identifikacijski obrazec kontaktnih oseb in zaupanja vrednih kurirjev (vzorec)

Podpisani, [ime in naslov zastopnika organizacije], potrjujem, da je treba v zvezi z zahtevkom, generiranjem in prevzemom digitalnih potrdil javnega ključa za dostopovne točke TACHOnet, ki podpirajo zaupnost, celovitost in nezatajljivost sporočil TACHOnet, uporabljati naslednje informacije:

Informacije o kontaktni osebi:

– Kontaktna oseba #1	– Kontaktna oseba #2
– Priimek:	– Priimek:
– Ime:	– Ime:
– Mobilni telefon:	– Mobilni telefon:
– Telefon:	– Telefon:
– Elektronski naslov:	– Elektronski naslov:
– Vzorec lastnoročnega podpisa:	– Vzorec lastnoročnega podpisa:
–	–
	–
	–

Informacije o zaupanja vrednem kurirju:

– Zaupanja vredni kurir #1	– Zaupanja vredni kurir #2
– Priimek:	– Priimek:
– Ime:	– Ime:
– Mobilni telefon:	– Mobilni telefon:
– Elektronski naslov:	– Elektronski naslov:
– Država izdaje potnega lista:	– Država izdaje potnega lista:
– Številka potnega lista:	– Številka potnega lista:
– Datum izteka veljavnosti potnega lista:	– Datum izteka veljavnosti potnega lista:

Kraj, datum, žig podjetja ali organizacije:

Podpis pooblaščenega zastopnika:

6. Dokumenti

6.1. Individualno pisno pooblastilo (vzorec)

Vzorec individualnega pisnega pooblastila, ki ga je treba podpisati in predložiti prek zaupanja vrednega kurirja med osebno registracijo pri organu za registracijo, je na voljo tukaj:

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 FERIAI**

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

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

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

☐ server²: e.g. identity of web server, TLS/SSL client server authentication
Please enter additionally the country, organization, locality, state or province name of the server:

☐ eMail-Gateway³: e.g. identity of eMail gateways / eMail-Appliance, virtual mail-administrating centre.

Validity

☒ The power of attorney is valid until further notice, but up to a **maximum of 27 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 obrazec zahtevka za potrdilo (vzorec)

Vzorec papirnega obrazca zahtevka za potrdilo, ki ga je treba podpisati in predložiti prek zaupanja vrednega kurirja med osebno registracijo pri organu za registracijo, je na voljo tukaj:

7. Glosar

Ključni izrazi, uporabljeni v tem poddodatku, so opredeljeni v oddelku z opredelitvami pojmov IPE na enotnem spletnem portalu digitalnega IPE:

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

Ključne okrajšave, uporabljene v tem opisu komponent, so opredeljene v glosarju IPE na enotnem spletnem portalu digitalnega IPE:

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