Rada
Európskej únie

V Bruseli 5. novembra 2018
(OR. en)

13711/18
ADD 1

Medziinštitucionálny spis:
2018/0339(NLE)

TRANS 488

POZNÁMKA

Od:	Generálny sekretariát Rady
Komu:	Delegácie
Č. predch. dok.:	ST 13711/18 TRANS 448
Č. dok. Kom.:	ST 12727/18 TRANS 426 + ADD 1
Predmet:	Rozhodnutie Rady o pozícii, ktorá sa má zaujať v mene Európskej únie v skupine expertov pre Európsku dohodu Európskej hospodárskej komisie Organizácie Spojených národov o práci osádok vozidiel v medzinárodnej cestnej doprave

Príloha k uvedenému rozhodnutiu Rady

PRÍLOHA

Nový dodatok k dohode AETR

Dodatok 4

Špecifikácie systému TACHOnet

1. Rozsah pôsobnosti a účel

1.1. V tomto dodatku sa stanovujú podmienky týkajúce sa pripojenia zmluvných strán AETR k systému TACHOnet prostredníctvom služby eDelivery.

1.2. Zmluvné strany, ktoré sa pripoja k systému TACHOnet prostredníctvom eDelivery, musia dodržiavať ustanovenia uvedené v tomto dodatku.

2. Vymedzenie pojmov

a) „zmluvná strana“ alebo „strana“ je ktorákoľvek zmluvná strana AETR;

b) „eDelivery“ je služba, ktorú vyvinula Európska komisia a ktorá umožňuje posielanie údajov elektronickými prostriedkami medzi tretími stranami a poskytuje dôkazy o nakladaní s odoslanými údajmi vrátane potvrdenia o odoslaní a doručení údajov a ktorá chráni odosielané údaje pred rizikom straty, krádeže, poškodenia alebo akýchkoľvek neoprávnených úprav;

c) „TACHOnet“ je systém elektronickej výmeny informácií o kartách vodičov medzi zmluvnými stranami podľa článku 31 ods. 2 nariadenia (EÚ) č. 165/2014;

d) „centrálny uzol“ je informačný systém, ktorý umožňuje odovzdávanie správ systému TACHOnet medzi žiadajúcimi a odpovedajúcimi stranami;

e) „žiadajúca strana“ je zmluvná strana emitujúca požiadavku alebo notifikáciu v systéme TACHOnet, ktorú centrálny uzol následne zašle príslušnej odpovedajúcej strane;

f) „odpovedajúca strana“ je zmluvná strana, ktorej je adresovaná požiadavka alebo notifikácia v systéme TACHOnet;

g) „orgán vydávajúci karty“ alebo „CIA“ (Card Issuing Authority) je subjekt poverený zmluvnou stranou na vydávanie a spravovanie tachografových kariet.

3. Všeobecné povinnosti

3.1. Žiadna zo zmluvných strán nemôže uzatvárať dohody o prístupe k systému TACHOnet v mene inej strany, ani žiadnym iným spôsobom zastupovať druhú zmluvnú stranu na základe tohto dodatku. Pri činnostiach uvedených v tomto dodatku žiadna zo zmluvných strán nekoná ako subdodávateľ druhej zmluvnej strany.

3.2. Zmluvné strany sprístupnia svoj vnútroštátny register kariet vodiča cez systém TACHOnet, a to spôsobom a s úrovňou služby podľa poddodatku 4.6.

3.3. Zmluvné strany sa navzájom bezodkladne informujú, ak v rámci vlastnej oblasti zodpovednosti spozorujú poruchy alebo chyby, ktoré môžu ohroziť bežnú prevádzku systému TACHOnet.

3.4. Každá zmluvná strana oznámi sekretariátu AETR kontaktné osoby pre systém TACHOnet. Akákoľvek zmena v kontaktných bodoch sa musí sekretariátu AETR predložiť písomne.

4. Skúšky pripojenia k systému TACHOnet

4.1. Pripojenie zmluvnej strany k systému TACHOnet sa považuje za nadviazané po dokončení testov spojenia, integrácie a výkonnosti, v súlade s pokynmi a pod dozorom Európskej komisie.

4.2. Ak sú prípravné testy neúspešné, Európska komisia môže testovaciu fázu dočasne pozastaviť. Testovanie sa obnoví po tom, ako zmluvná strana Európskej komisii oznámi prijatie potrebných technických zlepšení na vnútroštátnej úrovni, ktoré umožnia úspešné absolvovanie predbežných testov.

4.3. Maximálne trvanie prípravných testov je šesť mesiacov.

5. Architektúra dôveryhodnosti

5.1. Dôvernosť, integrita a nespochybniteľnosť správ v systéme TACHOnet sa zabezpečí architektúrou dôveryhodnosti systému TACHOnet.

5.2. Architektúra dôveryhodnosti systému TACHOnet sa zakladá na službe infraštruktúry verejných kľúčov (PKI) vytvorenej Európskou komisiou, ktorej požiadavky sú stanovené v poddodatkoch 4.8 a 4.9.

5.3. Do architektúry dôveryhodnosti TACHOnet zasahujú tieto subjekty:

a) certifikačný orgán zodpovedný za generovanie digitálnych certifikátov, ktoré má registračný orgán doručiť vnútroštátnym orgánom zmluvných strán (prostredníctvom dôveryhodných kuriérov, ktorých samy vymenujú), ako aj za zriadenie technickej infraštruktúry týkajúcej sa vydávania, rušenia a obnovovania digitálnych certifikátov;

b) vlastník domény zodpovedný za prevádzku centrálneho uzla uvedeného v poddodatku 4.1 a za validáciu a koordináciu architektúry dôveryhodnosti systému TACHOnet;

c) registračný orgán zodpovedný za registráciu a schvaľovanie žiadostí o vydanie, zrušenie a obnovenie digitálnych certifikátov a za overovanie totožnosti dôveryhodných kuriérov;

d) dôveryhodný kuriér, teda osoba vymenovaná vnútroštátnymi orgánmi zodpovedná za odovzdanie verejného kľúča registračnému orgánu a za získanie príslušného certifikátu vygenerovaného certifikačným orgánom;

e) vnútroštátny orgán zmluvnej strany, ktorý:

i) generuje súkromné kľúče a zodpovedajúce verejné kľúče, ktoré sa majú zahrnúť do certifikátov, ktoré má generovať certifikačný orgán;

ii) žiada o digitálne certifikáty od certifikačného orgánu;

iii) vymenúva dôveryhodných kuriérov.

5.4. Certifikačný orgán a registračný orgán vymenúva Európska komisia.

5.5. Každá zmluvná strana, ktorá je pripojená k systému TACHOnet, musí požiadať o vydanie digitálneho certifikátu v súlade s poddodatkom 4.9, aby mohla podpisovať a šifrovať správy v systéme TACHOnet.

5.6. Certifikát sa môže zrušiť v súlade s poddodatkom 4.9.

6. Ochrana údajov a dôvernosť

6.1. Zmluvné strany v súlade so zákonmi o ochrane údajov na medzinárodnej a vnútroštátnej úrovni, a najmä s Dohovorom o ochrane jednotlivcov pri automatizovanom spracovaní osobných údajov, musia prijať všetky potrebné technické a organizačné opatrenia na zaručenie bezpečnosti údajov v systéme TACHOnet a na zabránenie zmene alebo strate, prípadne neoprávnenému spracovaniu takýchto údajov alebo prístupu k nim (ide najmä o pravosť, dátovú dôvernosť, vysledovateľnosť, integritu, prístupnosť a nespochybniteľnosť a bezpečnosť správ).

6.2. Každá zmluvná strana musí chrániť vlastné vnútroštátne systémy pred nezákonným používaním, škodlivými kódmi, vírusmi, vniknutiami do počítačov, porušovaním a nelegálnou manipuláciou údajov a inými porovnateľnými činnosťami tretích strán. Zmluvné strany súhlasia s využitím komerčne primeraného úsilia na zabránenie prenosu akýchkoľvek vírusov, časových bômb, počítačových červov alebo podobných prvkov alebo akéhokoľvek počítačového programovacieho postupu, ktorý by mohol zasahovať do počítačových systémov druhej zmluvnej strany.

7. Náklady

7.1. Zmluvné strany znášajú svoje vlastné náklady na vývoj a prevádzku v spojení so svojimi vlastnými dátovými systémami a postupmi, ktoré sa vyžadujú na plnenie záväzkov podľa tohto dodatku.

7.2. Služby uvedené v poddodatku 4.1, ktoré poskytuje centrálny uzol, sú bezplatné.

8. Využívanie subdodávateľov

8.1. Strany môžu zadávať zákazky na ktorúkoľvek zo služieb, za ktoré sú zodpovedné podľa tohto dodatku.

8.2. Takéto zadanie zákazky subdodávateľovi neoslobodzuje stranu od zodpovednosti podľa tohto dodatku vrátane zodpovednosti za príslušnú úroveň služieb v súlade so poddodatkom 4.6.

Poddodatok 4.1.

Všeobecné aspekty systému TACHOnet

1. Všeobecný opis

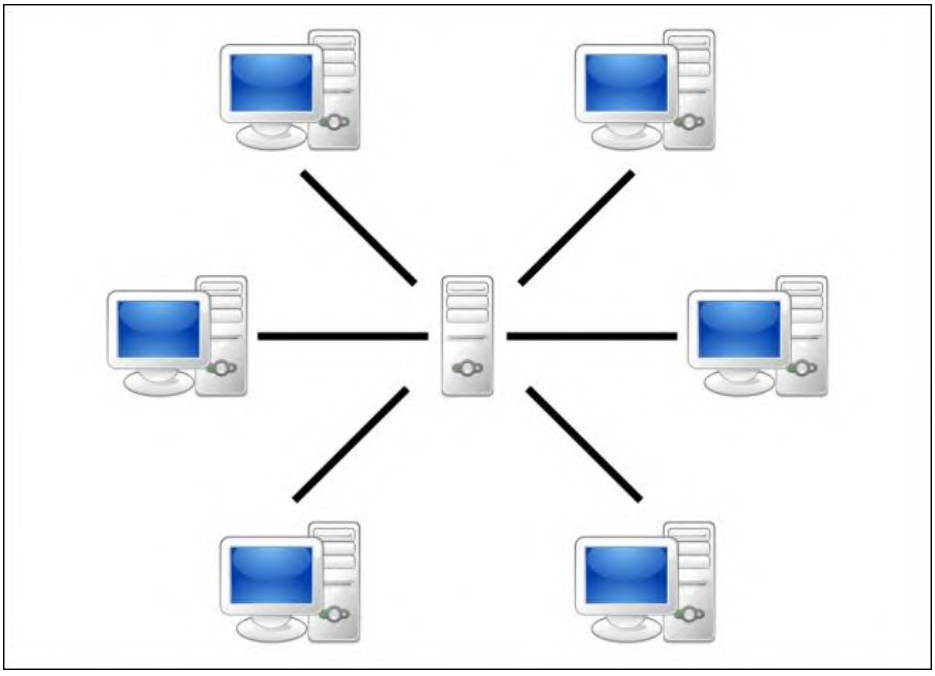
TACHOnet je elektronický systém na výmenu informácií o kartách vodičov medzi zmluvnými stranami AETR. Systém TACHOnet odosiela žiadosti o informácie od žiadajúcich strán odpovedajúcim stranám, ako aj odpovede na ne od odpovedajúcich strán žiadajúcim stranám. Zmluvné strany, ktoré sú súčasťou systému TACHOnet, doň musia pripojiť svoje vnútroštátne registre kariet vodiča.

2. Architektúra

Systém zasielania správ TACHOnet sa skladá z týchto častí:

2.1. Centrálny uzol, ktorý je schopný prijať požiadavku na vyhľadávanie od žiadajúcej strany, potvrdiť ju a odoslať ju odpovedajúcim stranám. Centrálny uzol počká na odpoveď každej odpovedajúcej strany, skonsoliduje všetky odpovede a postúpi konsolidovanú odpoveď žiadajúcej strane.

2.2. Vnútroštátne systémy zmluvných strán vybavené rozhraním, ktoré je schopné odosielať požiadavky na vyhľadávanie do centrálneho uzla a prijímať príslušné odpovede. Vnútroštátne systémy môžu na odosielanie a prijímanie správ z centrálneho uzla používať vlastný alebo komerčný softvér.



3. Riadenie

3.1. Centrálny uzol spravuje Európska komisia, ktorá je zodpovedná za technickú prevádzku a údržbu centrálneho uzla.

3.2. Centrálny uzol neuchováva údaje za obdobie presahujúce šesť mesiacov okrem protokolových a štatistických údajov uvedených v poddodatku 4.7.

3.3. Centrálny uzol neumožňuje prístup k osobným údajom, a to okrem povolených zamestnancov Európskej komisie v prípade potreby na účely monitorovania, údržby a odstraňovania porúch.

3.4. Každá zmluvná strana je zodpovedná za:

3.4.1. Zriadenie a správu svojich vnútroštátnych systémov vrátane rozhrania s centrálnym uzlom.

3.4.2. Inštaláciu a údržbu svojich vnútroštátnych systémov, hardvéru aj softvéru, či už vlastných alebo komerčných.

3.4.3. Správnu interoperabilitu svojich vnútroštátnych systémov s centrálnym uzlom vrátane riadenia chybových správ prijatých z centrálneho uzla.

3.4.4. Prijatie všetkých opatrení na zabezpečenie dôvernosti, integrity a dostupnosti informácií.

3.4.5. Fungovanie vnútroštátnych systémov v súlade s úrovňami služieb uvedenými v poddodatku 4.6.

Poddodatok 4.2.

Funkcie systému TACHOnet

1. Prostredníctvom systému zasielania správ TACHOnet sú zabezpečené tieto funkcie:

1.1. Kontrola vydaných kariet (CIC – Check Issued Cards): pomocou tejto funkcie môže žiadajúca strana odoslať jednej alebo všetkým odpovedajúcim stranám požiadavku na kontrolu vydaných kariet s cieľom určiť, či osoba žiadajúca o kartu už vlastní kartu vodiča vydanú odpovedajúcimi stranami. Odpovedajúce strany odpovedajú na požiadavku odoslaním odpovede týkajúcej sa kontroly vydaných kariet.

1.2. Kontrola stavu karty (CCS – Check Card Status): pomocou tejto funkcie môže žiadajúca strana požiadať odpovedajúcu stranu o podrobnosti týkajúce sa ňou vydanej karty odoslaním požiadavky na kontrolu stavu karty. Odpovedajúca strana odpovedá na požiadavku odoslaním odpovede týkajúcej sa kontroly stavu karty.

1.3. Zmena stavu karty (MCS – Modify Card Status): pomocou tejto funkcie môže žiadajúca strana prostredníctvom požiadavky na zmenu stavu karty oznámiť odpovedajúcej strane, že stav ňou vydanej karty sa zmenil. Odpovedajúca strana odpovedá prostredníctvom uznania zmeny stavu karty.

1.4. Karta vydaná na základe vodičského preukazu (ICDL – Issued Card Driving License): pomocou tejto funkcie môže žiadajúca strana prostredníctvom požiadavky na kartu vydanú na základe vodičského preukazu oznámiť odpovedajúcej strane, že vydala kartu na základe vodičského preukazu, ktorý vydala odpovedajúca strana. Odpovedajúca strana odpovedá prostredníctvom odpovede týkajúcej sa karty vydanej na základe vodičského preukazu.

2. Sú tu zahrnuté aj iné typy správ, ktoré sa považujú za vhodné z hľadiska efektívneho fungovania systému TACHOnet, napríklad chybové hlásenia.

3. Pri použití akýchkoľvek funkcií opísaných v bode 1 vnútroštátne systémy uznávajú stavy kariet uvedené v tabuľke 1. Strany však nie sú povinné zaviesť administratívny postup využívajúci všetky z uvedených stavov.

4. Keď strana dostane odpoveď alebo oznámenie opisujúce stav, ktoré nie sú využité v rámci administratívnych postupov, vnútroštátny systém premieňa stav prijatej správy na príslušnú hodnotu v rámci daného postupu. Odpovedajúca strana nesmie zamietnuť správu, pokiaľ sa stav uvedený v správe nachádza v tabuľke 1.

5. Stav karty uvedený v tabuľke 1 sa nevyužíva na stanovenie toho, či je karta vodiča platná na riadenie vozidla. Ak strana zadá otázku do registra vnútroštátneho orgánu vydávajúceho kartu prostredníctvom funkcie CCS, odpoveď musí obsahovať špeciálne políčko „valid for driving“ (oprávňuje na riadenie vozidla). Vnútroštátne administratívne postupy musia fungovať tak, aby odpovede CCS vždy obsahovali príslušnú hodnotu „valid for driving“.

Tabuľka 1

Stavy karty

Card Status (Stav karty)	**Definícia**
Application (Žiadosť)	CIA dostal žiadosť o vydanie karty vodiča. Táto informácia bola zaregistrovaná a uložená do databázy s vygenerovanými vyhľadávacími kľúčmi.
Approved (Schválená)	CIA schválil žiadosť týkajúcu sa tachografovej karty.
Rejected (Zamietnutá)	CIA neschválil žiadosť.
Personalised (Personalizovaná)	Tachografová karta bola personalizovaná.
Dispatched (Odoslaná)	Vnútroštátny orgán odoslal kartu vodiča príslušnému vodičovi alebo príslušnej doručovacej agentúre.
Handed Over (Odovzdaná)	Vnútroštátny orgán odovzdal kartu vodiča príslušnému vodičovi.
Confiscated (Skonfiškovaná)	Príslušný orgán vodičovi odobral kartu vodiča.
Suspended (Pozastavená)	Karta vodiča bola vodičovi dočasne odobraná.
Withdrawn (Stiahnutá)	CIA rozhodol stiahnuť kartu vodiča. Platnosť karty bola natrvalo zrušená.
Surrendered (Vrátená)	Tachografová karta bola vrátená CIA a vyhlásená za nepotrebnú.
Lost (Stratená)	Tachografová karta bola orgánu CIA nahlásená ako stratená.
Stolen (Odcudzená)	Tachografová karta bola orgánu CIA nahlásená ako odcudzená. Odcudzená karta sa považuje za stratenú.
Malfunctioning (Nefungujúca)	Tachografová karta bola orgánu CIA nahlásená ako nefungujúca.
Expired (So skončenou platnosťou)	Obdobie platnosti tachografovej karty sa skončilo.
Replaced (Nahradená)	Tachografová karta, ktorá bola nahlásená ako stratená, odcudzená alebo nefungujúca, bola nahradená novou kartou. Údaje na novej karte sú rovnaké s výnimkou indexu nahradenia čísla karty, ktorý sa zvýšil o jednu jednotku.

Renewed (Obnovená)	Tachografová karta bola obnovená z dôvodu zmeny administratívnych údajov alebo skončenia obdobia platnosti. Číslo novej karty je rovnaké s výnimkou indexu obnovenia čísla karty, ktorý sa zvýšil o jednu jednotku.
In Exchange (V procese výmeny)	CIA, ktorý vydal kartu vodiča, dostane oznámenie, že sa začal proces výmeny danej karty za kartu vodiča vydanú orgánom CIA inej strany.
Exchanged (Vymenená)	CIA, ktorý vydal kartu vodiča, dostane oznámenie, že sa skončil proces výmeny danej karty za kartu vodiča vydanú orgánom CIA inej strany.

Poddodatok 4.3.

Ustanovenia o správach v systéme TACHOnet

1. Všeobecné technické požiadavky

1.1. Centrálny uzol poskytuje synchrónne aj asynchrónne rozhranie na výmenu správ. Strany si môžu vybrať najvhodnejšiu technológiu na prepojenie so svojimi vlastnými aplikáciami.

1.2. Všetky správy vymieňané medzi centrálnym uzlom a vnútroštátnymi systémami musia byť zakódované v UTF-8.

1.3. Vnútroštátne systémy musia byť schopné prijímať a spracovávať správy obsahujúce grécku abecedu alebo znaky cyriliky.

2. Štruktúra správ XML a schéma XSD

2.1. Všeobecná štruktúra správ XML využíva formát vymedzený schémami XSD nainštalovanými v centrálnom uzle.

2.2. Centrálny uzol a vnútroštátne systémy odosielajú a prijímajú správy, ktoré zodpovedajú schéme XSD danej správy.

2.3. Vnútroštátne systémy musia byť schopné posielať, prijímať a spracovávať všetky správy zodpovedajúce akejkoľvek z funkcií uvedených v poddodatku 4.2.

2.4. Správy XML musia zodpovedať aspoň minimálnym požiadavkám stanoveným v tabuľke 2.

Tabuľka 2

Minimálne požiadavky na obsah správ XML

Common Header (Spoločné záhlavie)		**Povinný údaj**
Verzia	Oficiálna verzia špecifikácie XML bude špecifikovaná prostredníctvom menného priestoru (namespace) definovaného v správe XSD a v atribúte verzia (version) prvku záhlavia každej správy XML. Číslo verzie (n.m) sa pri každom zverejnení novej verzie špecifikácie pre definíciu schémy XML (xsd) bude definovať ako fixná hodnota.	Áno
Test Identifier (Identifikátor testovania)	Nepovinné ID na testovanie. Iniciátor testu zadá ID údaj a všetci účastníci procesu postúpia/vrátia ten istý ID údaj. Pri produkcii ho treba ignorovať, a pokiaľ je uvedený, nepoužije sa.	Nie
Technical Identifier (Technický identifikátor)	UUID (Universally Unique Identifier) jednoznačne identifikujúci každú jednotlivú správu. Odosielateľ vygeneruje UUID a doplní tento atribút. Tento údaj sa nevyužíva na komerčné účely.	Áno
Workflow Identifier (Identifikátor procesu)	WorkflowId je UUID a mala by ho vygenerovať žiadajúca strana. Tento ID údaj sa potom použije vo všetkých správach, ktoré s týmto procesom súvisia.	Áno
Sent At (Čas odoslania)	Dátum a čas (UTC) odoslania správy.	Áno
Timeout (Prekročenie lehoty)	Ide o voliteľný atribút dátumu a času (vo formáte UTC). Túto hodnotu stanoví iba centrálny uzol v prípade postúpených požiadaviek. Odpovedajúca strana sa týmto informuje o čase, keď nastane prekročenie lehoty požiadavky. Táto hodnota sa nevyžaduje v prípade MS2TCN_<x>_Req, ani vo všetkých odpovediach. Je nepovinná, aby sa mohlo rovnaké záhlavie použiť pre všetky typy správ bez ohľadu na to, či sa vyžaduje atribút timeoutValue.	Nie
From (Odosielateľ)	2-miestny alfabetický kód ISO 3166-1 strany, ktorá správu odosiela, alebo „EÚ“.	Áno
To (Adresát)	2-miestny alfabetický kód ISO 3166-1 strany, ktorej je správa určená, alebo „EÚ“.	Áno

Poddodatok 4.4.

Transliterácia a služby NYSIIS (New York State Identification and Intelligence System)

1. Algoritmus NYSIIS zavedený do centrálneho uzla sa využíva na zakódovanie mien všetkých vodičov vo vnútroštátnom registri.

2. Pri vyhľadávaní karty pomocou funkcie CIC sa ako hlavné vyhľadávacie mechanizmy musia použiť kľúče NYSIIS.

3. Na získanie ďalších výsledkov môžu okrem toho strany použiť vlastný algoritmus.

4. Vo výsledkoch vyhľadávania sa uvedie, či bol na vyhľadanie záznamu použitý vyhľadávací mechanizmus NYSIIS alebo individuálny vyhľadávací mechanizmus.

5. Ak sa strana rozhodne zaregistrovať oznámenia ICDL, kľúče NYSIIS obsiahnuté v oznámení sa zaregistrujú ako súčasť údajov ICDL. Pri vyhľadávaní údajov ICDL použije strana kľúče NYSIIS mena žiadateľa.

Poddodatok 4.5

Bezpečnostné požiadavky

1. Protokoly HTTPS sa používajú na výmenu správ medzi centrálnym uzlom a vnútroštátnymi systémami.

2. Vnútroštátne systémy používajú digitálne certifikáty uvedené v poddodatkoch 4.8 a 4.9 na účely bezpečného prenosu správ medzi vnútroštátnym systémom a centrálnym uzlom.

3. Vo vnútroštátnych systémoch sa ako minimum zavedú certifikáty využívajúce hašovací algoritmus podpisu SHA-2 (SHA-256) a dĺžku verejného kľúča 2048 bitov.

Poddodatok 4.6

Úrovne služieb

4. Vnútroštátne systémy musia spĺňať tieto minimálne úrovne služieb:

1.1. Musia byť k dispozícii 24 hodín denne, 7 dní v týždni.

1.2. Ich dostupnosť je monitorovaná prostredníctvom správy typu HEARTBEAT vyslanej z centrálneho uzla.

1.3. Ich miera dostupnosti musí zodpovedať 98 % v súlade s touto tabuľkou (číselné údaje boli zaokrúhlené na najbližšie vhodné jednotky):

Dostupnosť	znamená nedostupnosť		
	Denne	Mesačne	Ročne
98 %	0,5 hodiny	15 hodín	7,5 dňa

Strany sa vyzývajú, aby dodržiavali dennú mieru dostupnosti, pričom sa však uznáva, že určité činnosti, ako napr. systém údržby, si vyžadujú vypnutie systému na viac ako 30 minút. Miery dostupnosti v rámci mesiaca a v rámci roka zostávajú napriek tomu povinné.

1.4. Musia odpovedať minimálne na 98 % požiadaviek na vyhľadanie, ktoré im boli zaslané v jednom kalendárnom mesiaci.

1.5. Na požiadavky musia odpovedať do 10 sekúnd.

1.6. Globálny čas čakania na odpoveď (čas, v rámci ktorého žiadateľ čaká na odpoveď) nesmie presiahnuť 20 sekúnd.

1.7. Musia byť schopné spracovať 6 správ za sekundu.

1.8. Vnútroštátne systémy môžu do uzla TACHOnetu odoslať maximálne 2 požiadavky na vyhľadanie za sekundu.

1.9. Každý vnútroštátny systém musí byť schopný zvládnuť potenciálne technické problémy centrálneho uzla alebo vnútroštátnych systémov iných strán. Patria medzi ne okrem iného:

a) strata spojenia s centrálnym uzlom;

b) chýbajúca odpoveď na požiadavku;

c) doručenie odpovede po uplynutí času čakania na odpoveď;

d) doručenie nevyžiadaných správ;

e) doručenie neplatných správ.

5. Centrálny uzol musí:

2.1. dosahovať mieru dostupnosti 98 %;

2.2. vnútroštátnym systémom oznámiť akúkoľvek chybu, buď prostredníctvom odpovede, alebo prostredníctvom špeciálneho chybového hlásenia. Vnútroštátne systémy, ktoré zas prijímajú tieto špeciálne chybové hlásenia, musia disponovať urýchlenou reakčnou schopnosťou, aby bolo možné prijať všetky náležité opatrenia na nápravu oznámených chýb.

6. Údržba

Strany oznámia ostatným stranám a Európskej komisii akúkoľvek pravidelnú údržbovú činnosť prostredníctvom webovej aplikácie aspoň jeden týždeň pred začiatkom týchto činností, ak je to technicky možné.

Poddodatok 4.7.

Protokolové a štatistické údaje zozbierané v centrálnom uzle

7. Údaje využívané na štatistické účely sú v záujme ochrany súkromia anonymné. Údaje identifikujúce konkrétnu kartu, vodiča alebo vodičský preukaz nie sú dostupné pre štatistické účely.

8. Protokolové údaje obsahujú záznamy o všetkých operáciách na účely monitorovania a odstraňovania chýb a na umožnenie vygenerovania štatistík o týchto operáciách.

9. Osobné údaje sa v protokoloch nesmú uchovávať dlhšie než 6 mesiacov. Štatistické informácie sa uchovávajú na neobmedzené obdobie.

10. Štatistické údaje použité na podávanie správ zahŕňajú:

    a) žiadajúcu stranu;

    b) odpovedajúcu stranu;

    c) typ správy;

    d) kód stavu odpovede;

    e) dátum a čas správ;

    f) čas odpovede.

Poddodatok 4.8.

Všeobecné ustanovenia týkajúce sa digitálnych kľúčov a certifikátov pre systém TACHOnet

11. Generálne riaditeľstvo Európskej komisie pre informatiku (DIGIT) poskytuje službu PKI[1] (označovanú ako „služba CEF PKI“) zmluvným stranám AETR, ktoré sa pripoja k systému TACHOnet (ďalej len „vnútroštátne orgány“), prostredníctvom služby eDelivery.

12. Postup žiadosti o digitálne certifikáty a ich zrušenie, ako aj podrobné podmienky jeho používania sú vymedzené v dodatku.

13. Používanie certifikátov:

3.1. Po vydaní certifikátu ho smie vnútroštátny orgán[2] používať len v súvislosti so systémom TACHOnet. Certifikát sa môže používať na:

a) autentifikáciu pôvodu údajov;

b) šifrovanie údajov;

c) zabezpečenie zisťovania porušení integrity údajov.

3.2. Akékoľvek použitie, ktoré nie je výslovne povolené ako súčasť povolených použití certifikátu, je zakázané.

14. Zmluvné strany:

a) musia chrániť svoj súkromný kľúč proti neoprávnenému použitiu;

b) nesmú previesť ani odhaliť svoj súkromný kľúč tretím stranám, a to ani ak pôsobia ako ich zástupcovia;

---

[1] Infraštruktúra verejného kľúča (Public Key Infrastructure) je súbor úloh, politík, postupov a systémov, ktoré sú potrebné na vytváranie, riadenie, distribúciu a rušenie digitálnych certifikátov.

[2] Identifikovaný hodnotou atribútu „O=“ v časti Subject Distinguished Name vydaného certifikátu

c) musia zabezpečiť dôvernosť, integritu a dostupnosť súkromných kľúčov vygenerovaných, uložených a používaných v rámci systému TACHOnet;

d) nesmú naďalej používať súkromný kľúč po uplynutí obdobia platnosti alebo zrušení certifikátu za iným účelom, než je nahliadnutie do šifrovaných údajov (napr. dešifrovanie e-mailov). Kľúče, ktorých platnosť sa skončila, sa musia buď zničiť, alebo sa musia uchovávať spôsobom zabraňujúcim ich použitiu;

e) musia poskytnúť registračnému orgánu totožnosť tých splnomocnených zástupcov, ktorí sú oprávnení požiadať o zrušenie certifikátov vydaných organizácii (žiadosť o zrušenie musí obsahovať heslo slúžiace na zrušenie a údaje o udalostiach, ktoré viedli k zrušeniu);

f) musia zabrániť zneužitiu súkromného kľúča tým, že požiadajú o zrušenie príslušného certifikátu verejného kľúča v prípade narušenia súkromného kľúča alebo aktivačných údajov súkromného kľúča;

g) sú zodpovedné za žiadosť o zrušenie certifikátu za okolností stanovených v certifikačných pravidlách (Certification Policies - CP) a vo vyhlásení o certifikačných postupoch (Certification Practices Statement - CPS) certifikačného orgánu a majú povinnosť ju v prípade potreby predložiť;

h) musia bezodkladne informovať registračný orgán o strate, odcudzení alebo potenciálnom narušení akýchkoľvek kľúčov AETR použitých v súvislosti so systémom TACHOnet.

15. Zodpovednosť

Bez toho, aby bola dotknutá zodpovednosť Európskej komisie, ak dôjde k porušeniu akýchkoľvek požiadaviek stanovených v príslušných vnútroštátnych právnych predpisoch, alebo pokiaľ ide o zodpovednosť vo veciach, ktoré na základe tohto práva nemožno vylúčiť, Európska komisia nenesie žiadnu zodpovednosť, pokiaľ ide o:

a) obsah certifikátu, za ktorý zodpovedá výlučne vlastník certifikátu. Je povinnosťou vlastníka certifikátu skontrolovať správnosť obsahu certifikátu;

b) používanie certifikátu jeho vlastníkom.

Poddodatok 4.9

Opis služby PKI v rámci systému TACHOnet

1. Úvod

Infraštruktúra verejného kľúča (Public Key Infrastructure) je súbor úloh, politík, postupov a systémov, ktoré sú potrebné na vytváranie, riadenie, distribúciu a rušenie digitálnych certifikátov[3]. Služba CEF PKI v rámci eDelivery umožňuje vydávanie a riadenie digitálnych certifikátov používaných na zabezpečenie dôvernosti, integrity a nespochybniteľnosti informácií vymieňaných medzi prístupovými bodmi (Access Points – AP).

Služba PKI v rámci eDelivery je založená na službách Trust Center Services TeleSec Shared-Business-CA (pričom CA tu znamená certifikačný orgán), na ktoré sa vzťahujú certifikačné pravidlá (Certification Policy – CP)/vyhlásenie o certifikačných postupoch (Certification Practices Statement – CPS) certifikačného orgánu TeleSec Shared-Business-CA, čo je súčasť T-Systems International GmbH[4].

Služba PKI vydáva certifikáty, ktoré sú vhodné na zabezpečenie rôznych obchodných procesov v rámci a mimo spoločností, organizácií, verejných orgánov a inštitúcií, ktoré si vyžadujú strednú úroveň bezpečnostnej ochrany na preukázanie pravosti, integrity a dôveryhodnosti konečného subjektu.

2. Proces žiadosti o certifikát

2.1. Úlohy a zodpovednosti

2.1.1. „Organizácia“ alebo „vnútroštátny orgán“, ktoré žiadajú o certifikát

2.1.1.1. Vnútroštátny orgán žiada o certifikáty v rámci projektu TACHOnet.

2.1.1.2 Vnútroštátny orgán:

a) žiada o certifikáty v rámci služby CEF PKI;

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

[4] Najnovšia verzia CP a CPS sa dá stiahnuť na internetovej stránke https://www.telesec.de/en/sbca-en/support/download-area/

b) generuje súkromné kľúče a zodpovedajúce verejné kľúče, ktoré sa majú zahrnúť do certifikátov vydaných certifikačným orgánom;

c) certifikát po schválení stiahne z elektronického úložiska;

d) podpíše a pošle naspäť príslušnému registračnému orgánu:

i) formulár identifikácie kontaktných osôb a dôveryhodných kuriérov;

ii) podpísané individuálne splnomocnenie[5].

2.1.2. Dôveryhodný kuriér

2.1.2.1. Vnútroštátny orgán vymenuje dôveryhodného kuriéra.

2.1.2.2. Dôveryhodný kuriér:

a) odovzdá verejný kľúč registračnému orgánu v rámci osobného identifikačného a registračného procesu;

b) získa príslušné potvrdenie od registračného orgánu.

2.1.3. Vlastník domény

2.1.3.1. Vlastníkom domény je GR MOVE.

2.1.3.2. Vlastník domény:

a) overuje a koordinuje sieť TACHOnet a architektúru dôveryhodnosti systému TACHOnet vrátane validácie postupov na vydávanie certifikátov;

b) prevádzkuje centrálny uzol TACHOnet a koordinuje činnosť strán, pokiaľ ide o fungovanie systému TACHOnet;

c) spolu s vnútroštátnymi orgánmi realizuje testy pripojenia k systému TACHOnet.

---

[5] Splnomocnenie je právny dokument, ktorým organizácia splnomocňuje a poveruje Európsku komisiu zastúpenú určenou osobou zodpovednou za službu CEF PKI žiadať o generovanie certifikátu v jej mene prostredníctvom služby T-Systems International GmbH TeleSec Shared Business CA. Pozri tiež bod 6.

2.1.4. Registračný orgán

2.1.4.1. Registračný orgán je Spoločné výskumné centrum (JRC).

2.1.4.2. Registračný orgán je zodpovedný za overenie totožnosti dôveryhodného kuriéra, ako aj za registráciu a schvaľovanie žiadostí o vydanie, zrušenie a obnovenie digitálnych certifikátov.

2.1.4.3. Registračný orgán:

a) prideľuje jedinečný identifikátor vnútroštátnemu orgánu;

b) autentifikuje totožnosť vnútroštátneho orgánu, jeho kontaktných bodov a dôveryhodných kuriérov;

c) komunikuje s podporným tímom NPE, pokiaľ ide o autentickosť vnútroštátneho orgánu, jeho kontaktných bodov a dôveryhodných kuriérov;

d) informuje vnútroštátny orgán o schválení alebo zamietnutí certifikátu.

2.1.5. Certifikačný orgán

2.1.5.1. Certifikačný orgán je zodpovedný za poskytovanie technickej infraštruktúry na podávanie žiadostí a vydávanie a rušenie digitálnych certifikátov.

2.1.5.2. Certifikačný orgán:

a) zabezpečuje technickú infraštruktúru pre žiadosti o certifikáty zo strany vnútroštátnych orgánov;

b) potvrdzuje alebo zamieta žiadosti o certifikáty;

c) komunikuje s registračným orgánom na účely overenia totožnosti žiadajúcej organizácie, ak sa to vyžaduje.

2.2. Vydávanie certifikátov

2.2.1. Certifikát sa vydáva v súlade s týmito postupnými krokmi znázornenými na obrázku 1:

a) **krok 1:** určenie dôveryhodného kuriéra;

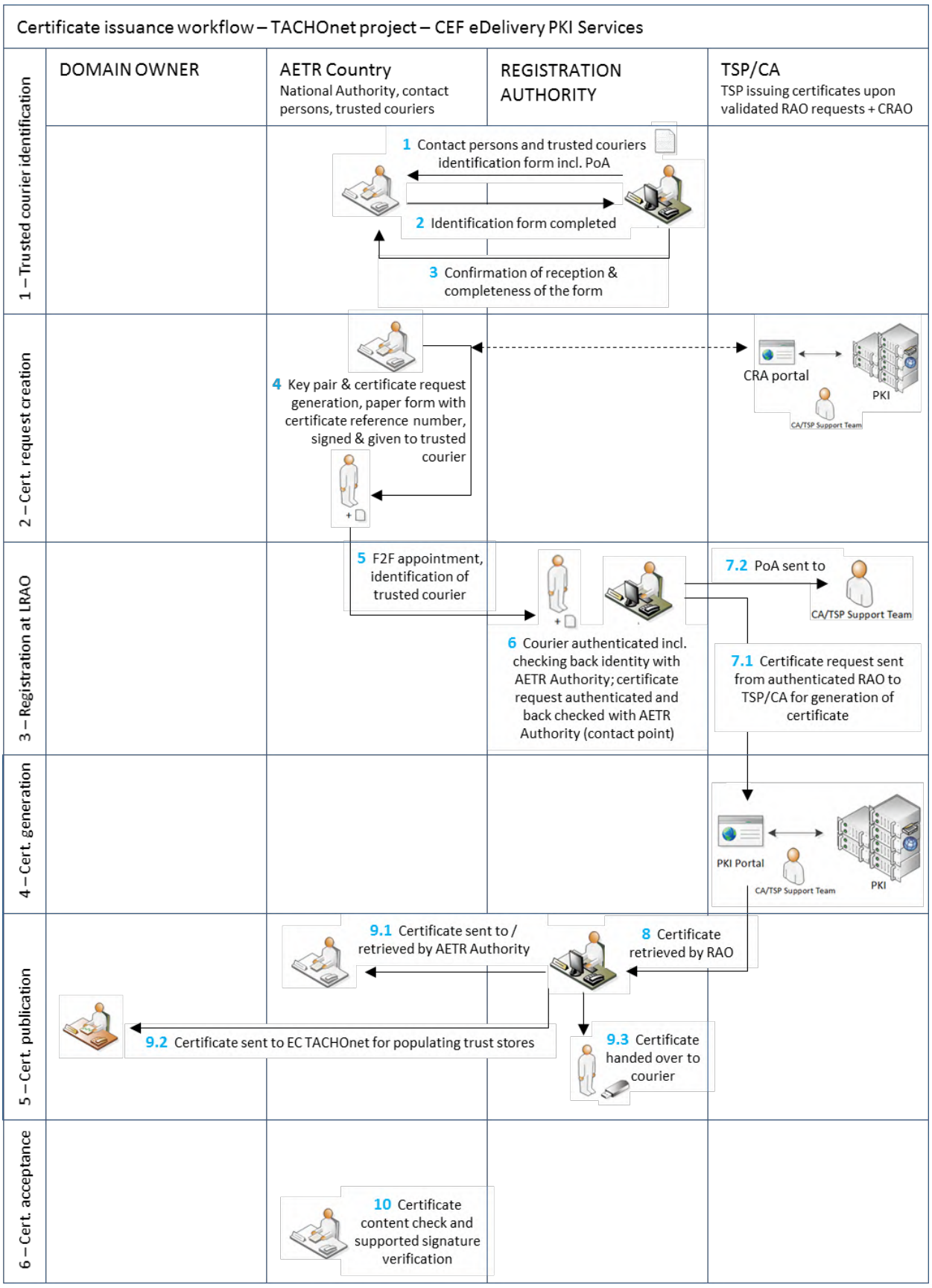
b) **krok 2:** vytvorenie žiadosti o certifikát;

c) **krok 3**: registrácia v registračnom orgáne;

d) **krok 4:** generovanie certifikátu;

e) **krok 5:** uverejnenie certifikátu;

f) **krok 6:** prijatie certifikátu.



Obrázok 1 – Postup vydávania certifikátov

2.2.2. Krok 1: Určenie dôveryhodného kuriéra

Identifikácia dôveryhodných kuriérov sa riadi týmto postupom:

a) registračný orgán zašle vnútroštátnemu orgánu formulár identifikácie kontaktných osôb a dôveryhodných kuriérov[6]. Tento formulár musí zahŕňať aj splnomocnenie, ktoré musí podpísať organizácia (orgán AETR).

b) Vnútroštátny orgán zašle vyplnený formulár a podpísané splnomocnenie naspäť registračnému orgánu.

c) Registračný orgán potvrdí prijatie a úplnosť formulára.

d) Registračný orgán poskytne aktualizovaný zoznam kontaktných osôb a dôveryhodných kuriérov vlastníkovi domény.

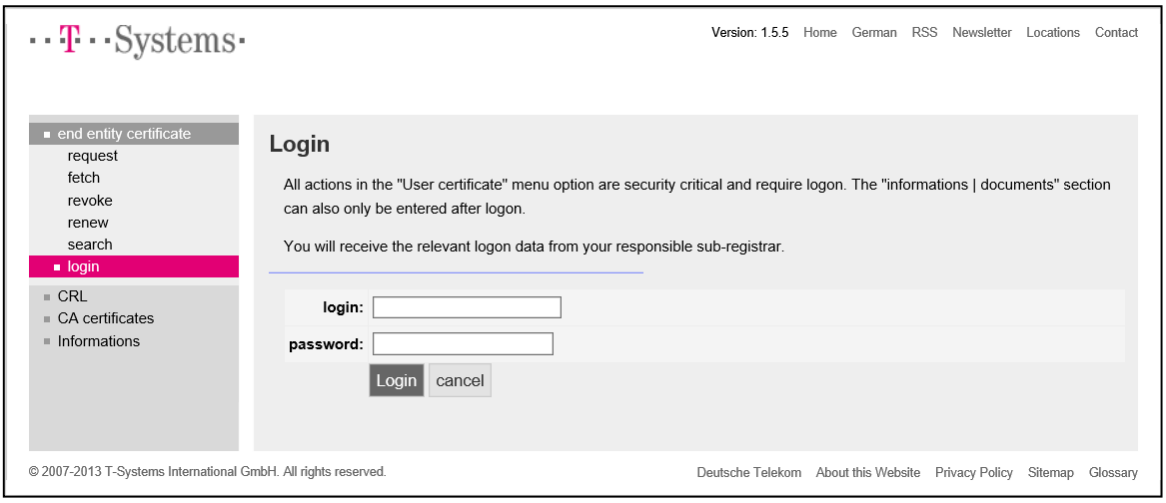
2.2.3. Krok 2: Vytvorenie žiadosti o certifikát

2.2.3.1. Žiadosť o certifikát a získanie certifikátu sa musia uskutočniť na tom istom počítači a v tom istom prehliadači.

2.2.3.2. Vytvorenie žiadosti o certifikát sa riadi týmto postupom:

a) Ak organizácia chce požiadať o certifikát, pripojí sa do používateľského webového rozhrania na adrese https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: a zadá používateľské meno „**sbca/CEF_eDelivery.europa.eu**“ a heslo „**digit.333**“.

[6] Pozri bod 5.

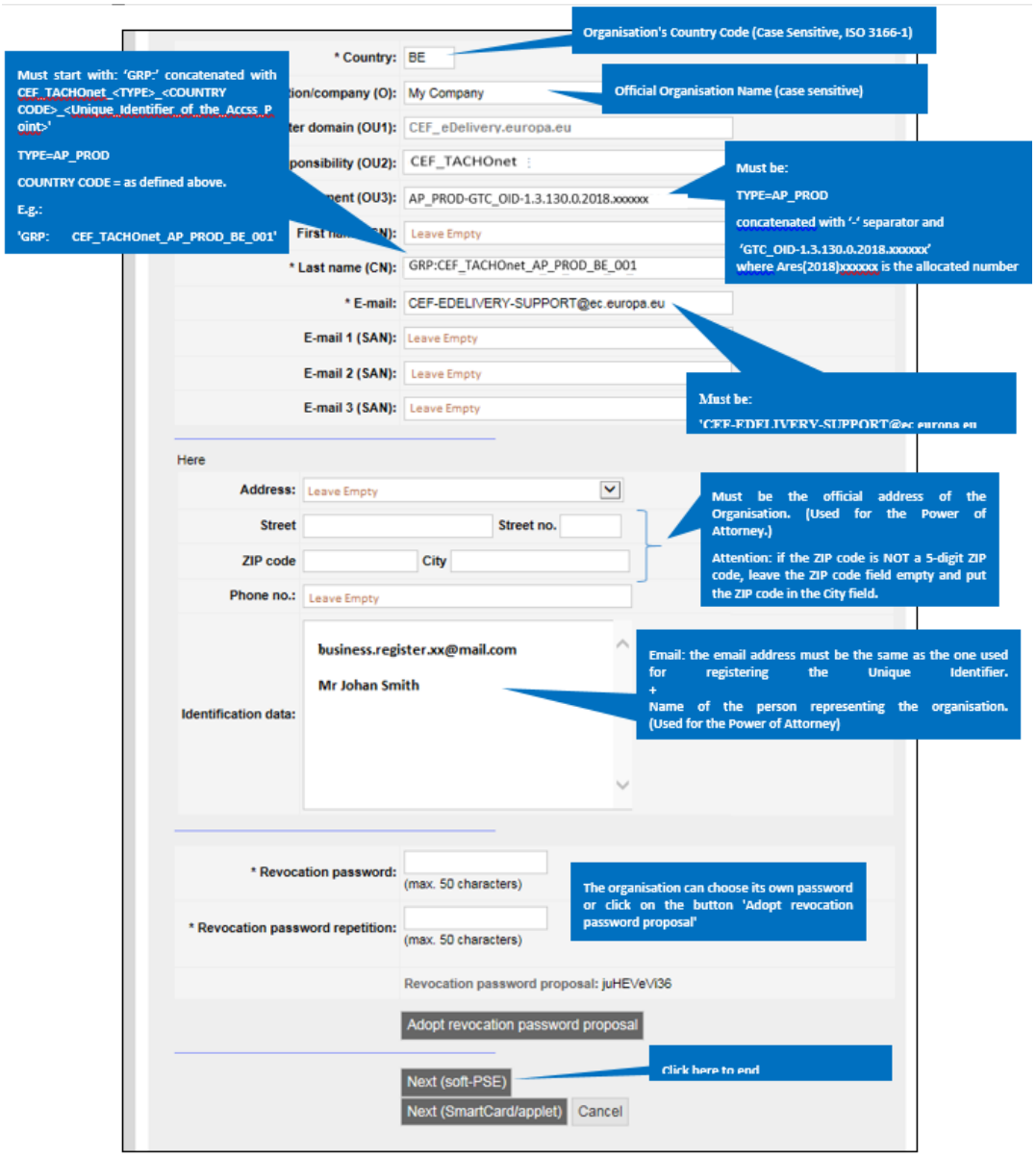


Obrázok 2

b) Organizácia klikne na možnosť „request“ na ľavej strane panelu a z rozbaľovacieho zoznamu vyberie „CEF_TACHOnet“.

Obrázok 3

c) Organizácia vyplní formulár žiadosti o certifikát uvedený na obrázku 4 informáciami podľa tabuľky 3 a proces ukončí kliknutím na tlačidlo „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:
'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
* Country:
BE
My Company
CEF_eDelivery.europa.eu
CEF_TACHOnet
AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
Leave Empty
GRP:CEF_TACHOnet_AP_PROD_BE_001
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

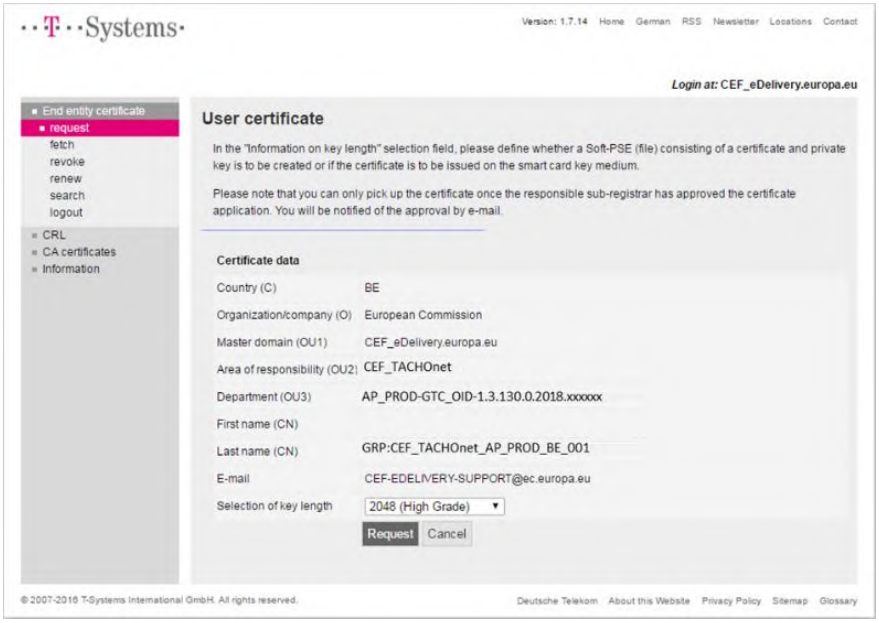
Obrázok 4

Požadované polia	Opis
Krajina	**C = kód krajiny**, umiestnenie vlastníka certifikátu, overené s použitím verejného registra Obmedzenia: 2 znaky, v súlade s ISO 3166-1, 2-miestny alfabetický kód, rozlišujú sa veľké a malé písmená Príklady: DE, BE, NL Osobitné prípady: UK (Spojené kráľovstvo), EL (Grécko)
Organizácia/Spoločnosť (O)	**O = názov organizácie vlastníka certifikátu**
Hlavná doména (OU1)	**OU = CEF_eDelivery.europa.eu**
Oblasť zodpovednosti (OU2)	**OU = CEF_TACHOnet**
Útvar (OU3)	Povinná hodnota pre „OBLASŤ ZODPOVEDNOSTI“ Pri žiadosti o certifikát sa musí obsah skontrolovať na základe pozitívneho zoznamu (bieleho zoznamu). Ak sa informácie nezhodujú so zoznamom, požiadavka sa musí zablokovať. Formát: **OU = <TYPE>-<GTC_NUMBER>** kde sa „<TYPE>“ nahradí výrazom „AP_PROD“: prístupový bod v produkčnom prostredí a kde <GTC_NUMBER> je **GTC_OID-1.3.130.0.2018.xxxxxx**, kde Ares(2018)xxxxxx je číslo GTC pre projekt TACHOnet. Napr.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
Meno (CN)	Nevypĺňa sa
Priezvisko (CN)	Musí sa začínať skratkou „GRP:“, po ktorej nasleduje bežný názov. Formát: **CN = GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** Napr.: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
E-mail 1 (SAN)	Nevypĺňa sa
E-mail 2 (SAN)	Nevypĺňa sa
E-mail 3 (SAN)	Nevypĺňa sa

Adresa	Nevypĺňa sa
Ulica	Musí ísť o oficiálnu adresu organizácie vlastníka certifikátu (používa sa na splnomocnenie)
Č. ulice	Musí ísť o oficiálnu adresu organizácie vlastníka certifikátu (používa sa na splnomocnenie)
PSČ	Musí ísť o oficiálnu adresu organizácie vlastníka certifikátu (používa sa na splnomocnenie) **Upozornenie**: ak PSČ nie je 5-miestne, políčko PSČ sa nevypĺňa a kód PSČ sa vpíše do poľa pre obec
Obec	Musí ísť o oficiálnu adresu organizácie vlastníka certifikátu (používa sa na splnomocnenie) **Upozornenie**: ak PSČ nie je 5-miestne, políčko PSČ sa nevypĺňa a kód PSČ sa vpíše do poľa pre obec
Telefón	Nevypĺňa sa
Identifikačné údaje	E-mailová adresa sa musí zhodovať s tou, ktorá sa použila na registráciu jednoznačného identifikátora + Musí ísť o meno osoby zastupujúcej organizáciu (používa sa na splnomocnenie) + **č. v obchodnom registri** (údaj povinný len pre súkromné organizácie) **zápis na miestnom súde** (údaj povinný len pre nemecké a rakúske súkromné organizácie)
Heslo na zrušenie	Povinné pole zvolené žiadateľom
Opakované zadanie hesla na zrušenie	Povinné pole zvolené žiadateľom, ktoré sa zhoduje s poľom „heslo na zrušenie“

Tabuľka 3: Podrobný opis každého požadovaného poľa

d) Zvolí sa dĺžka kľúča 2048 (High Grade).



Obrázok 5

e) Aby organizácia mohla certifikát vyhľadať, zaznačí si referenčné číslo.

Obrázok 6

f) Podporný tím NPE kontroluje nové žiadosti o certifikáty a overuje, či sú informácie uvedené v žiadosti o certifikát platné, t. j. či zodpovedajú názvoslovné pravidlá uvedené v dodatku 5.1 Názvoslovné pravidlá v certifikátoch.

g) Podporný tím NPE overí, či sú informácie uvedené v žiadosti v platnom formáte.

h) Ak sa pri kontrole podľa predchádzajúcich bodov 5 alebo 6 príde na nezrovnalosť, podporný tím NPE zašle e-mail na e-mailovú adresu uvedenú v časti „Identifikačné údaje“ formulára žiadosti, v ktorom organizáciu požiada, aby postup začala znova, pričom v kópii uvedie vlastníka domény. Neúspešná žiadosť o certifikát sa zruší.

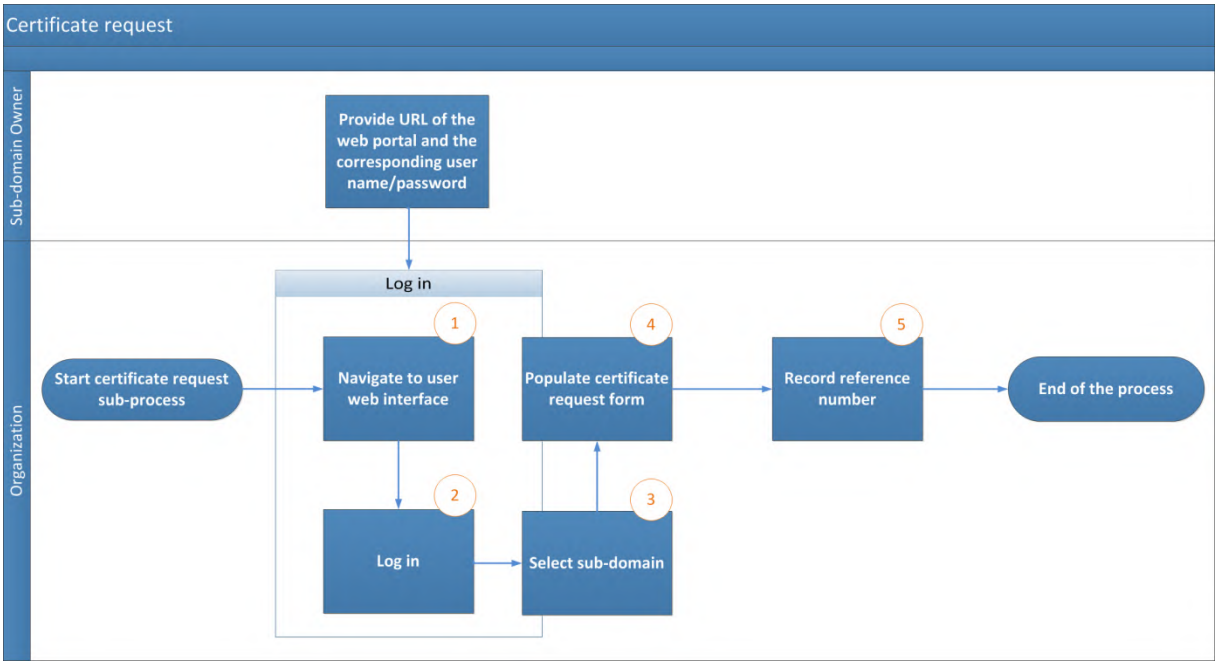
i) Podporný tím NPE zašle registračnému orgánu e-mail o platnosti žiadosti. Tento e-mail musí obsahovať:

   1) názov organizácie z poľa „Organizácia (O)“ žiadosti o certifikát;

   2) údaje z certifikátu vrátane názvu prístupového bodu, pre ktorý sa certifikát vydáva, z poľa „Priezvisko (CN)“ žiadosti o certifikát;

   3) referenčné číslo certifikátu;

   4) adresu organizácie, jej e-mail a meno osoby, ktorá organizáciu zastupuje.



Obrázok 7: Postup podávania žiadosti o certifikát

2.2.4. Krok 3: Registrácia v registračnom orgáne (schválenie certifikátu)

2.2.4.1. Dôveryhodný kuriér alebo kontaktné miesto zorganizuje stretnutie s registračným orgánom zaslaním e-mailu s uvedením dôveryhodného kuriéra, ktorý sa zúčastní na osobnom stretnutí.

2.2.4.2. Organizácia pripraví balík dokumentov, ktorý musí obsahovať:

a) vyplnené a podpísané splnomocnenie;

b) kópiu platného pasu dôveryhodného kuriéra, ktorý sa zúčastní na osobnom stretnutí. Túto kópiu musí podpísať jedno z kontaktných miest organizácie určených v kroku 1;

c) formulár žiadosti o certifikát v papierovej forme podpísaný jedným z kontaktných miest organizácie.

2.2.4.3. Registračný orgán prijme dôveryhodného kuriéra po overení totožnosti pri vstupe do budovy. Registračný orgán vykoná osobnú registráciu žiadosti o certifikát, ktorá pozostáva z týchto krokov:

a) identifikácia a autentifikácia dôveryhodného kuriéra,

b) overenie fyzického vzhľadu dôveryhodného kuriéra v porovnaní s pasom, ktorý predložil dôveryhodný kuriér;

c) overenie platnosti pasu, ktorý predložil dôveryhodný kuriér;

d) overenie platného pasu predloženého dôveryhodným kuriérom v porovnaní s kópiou platného pasu podpísanou jedným z určených kontaktných miest organizácie. Podpis sa overí v porovnaní s originálom „formulára identifikácie kontaktných bodov a dôveryhodných kuriérov“;

e) overenie vyplneného a podpísaného splnomocnenia;

f) overenie žiadosti o certifikát v papierovej forme a jeho podpisu v porovnaní s originálnom „formulára identifikácie kontaktných bodov a dôveryhodných kuriérov“;

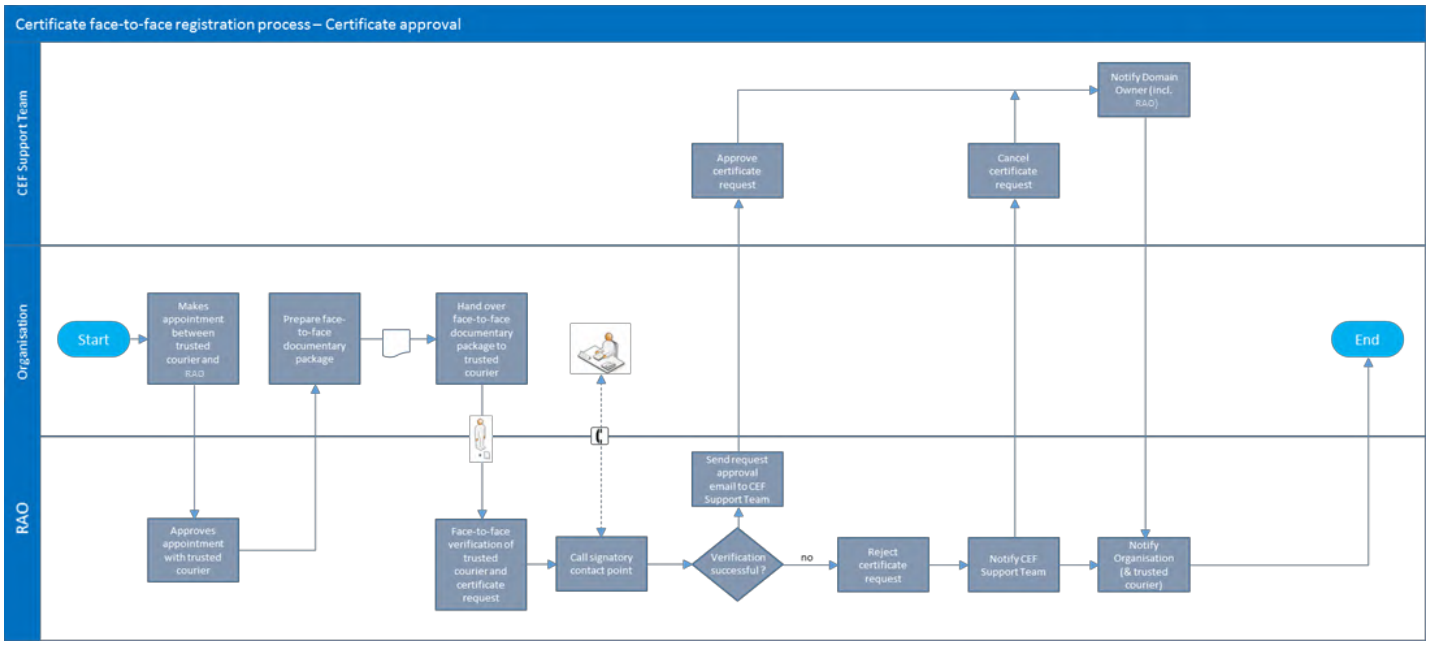
g) telefonát podpisujúcemu kontaktnému bodu s cieľom opätovného overenia totožnosti dôveryhodného kuriéra a obsahu žiadosti o certifikát.

2.2.4.4. Registračný orgán potvrdí podpornému tímu NPE, že vnútroštátny orgán je skutočne oprávnený riadiť komponenty, na ktoré žiada certifikáty, a že príslušný osobný registračný proces prebehol úspešne. Potvrdenie sa musí zaslať e-mailom zabezpečeným použitím certifikátu „CommiSign“, pričom sa priloží naskenovaná kópia autentifikovanej dokumentácie potvrdenej pri osobnom stretnutí, ako aj podpísaný kontrolný zoznam k postupu, ktorý vykonal registračný orgán.

2.2.4.5. Ak registračný orgán potvrdí platnosť žiadosti, postup pokračuje v súlade s bodmi 2.2.4.6 a 2.2.4.7. V opačnom prípade sa vydanie certifikátu zamietne a príslušná organizácia o tom bude informovaná.

2.2.4.6. Podporný tím NPE musí žiadosť o certifikát schváliť a o tejto skutočnosti informuje registračný orgán.

2.2.4.7. Registračný orgán informuje organizáciu o tom, že certifikát možno získať cez používateľský portál.



Obrázok 8: Schvaľovanie certifikátu

2.2.5. Krok 4: Generovanie certifikátu

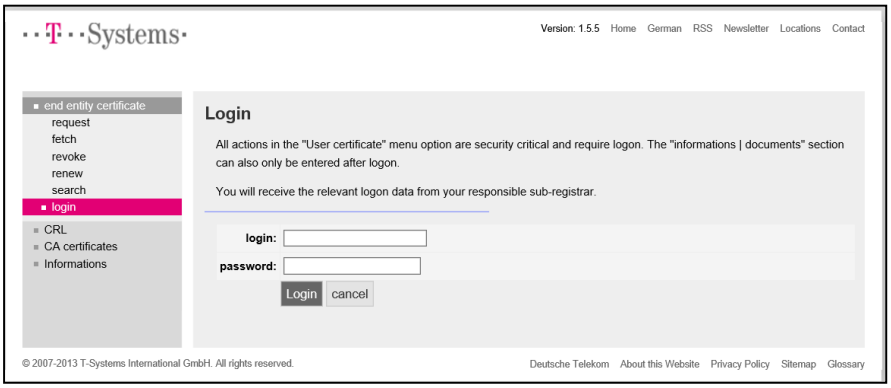
Po schválení žiadosti o certifikát sa certifikát vygeneruje.

2.2.6. Krok 5: Uverejnenie a získanie certifikátu

2.2.6.1. Po schválení žiadosti o certifikát registračný orgán certifikát získa a odovzdá jeho kópiu dôveryhodnému kuriérovi.

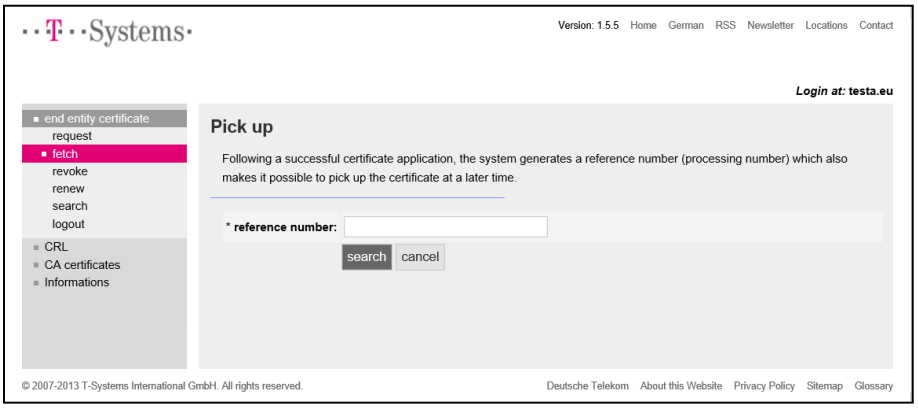
2.2.6.2. Organizácia dostane od registračného orgánu notifikáciu, že certifikát je možné získať.

2.2.6.3. Organizácia sa pripojí k používateľskému portálu na adrese https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en a prihlási sa zadaním používateľského mena „**sbca/CEF_eDelivery.europa.eu**“ a hesla „**digit.333**“.



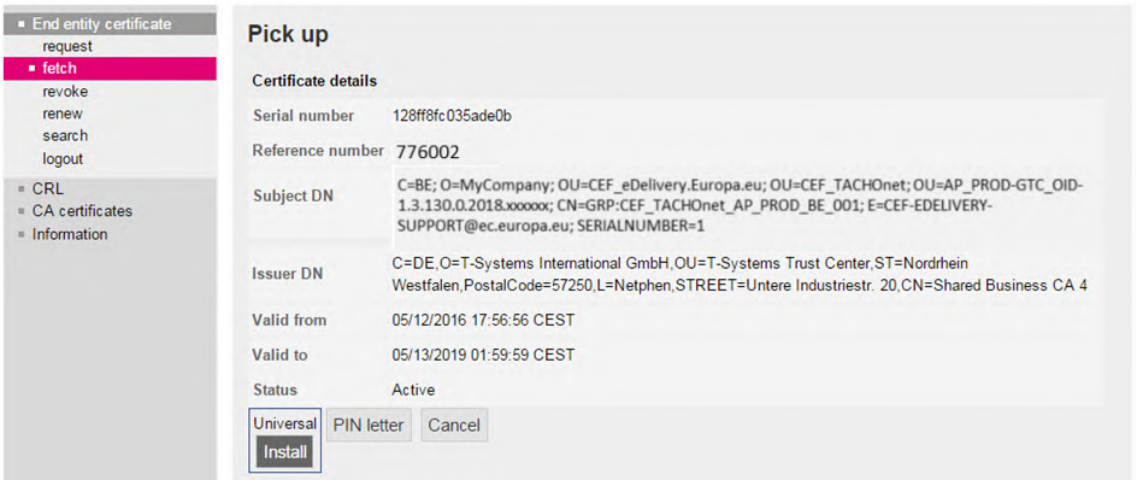
Obrázok 9

2.2.6.4. Organizácia klikne na tlačidlo „fetch“ na ľavej strane a uvedie referenčné číslo zaznamenané počas procesu žiadosti o certifikát.



Obrázok 10

2.2.6.5. Organizácia nainštaluje certifikáty kliknutím na tlačidlo „Install“.



Obrázok 11

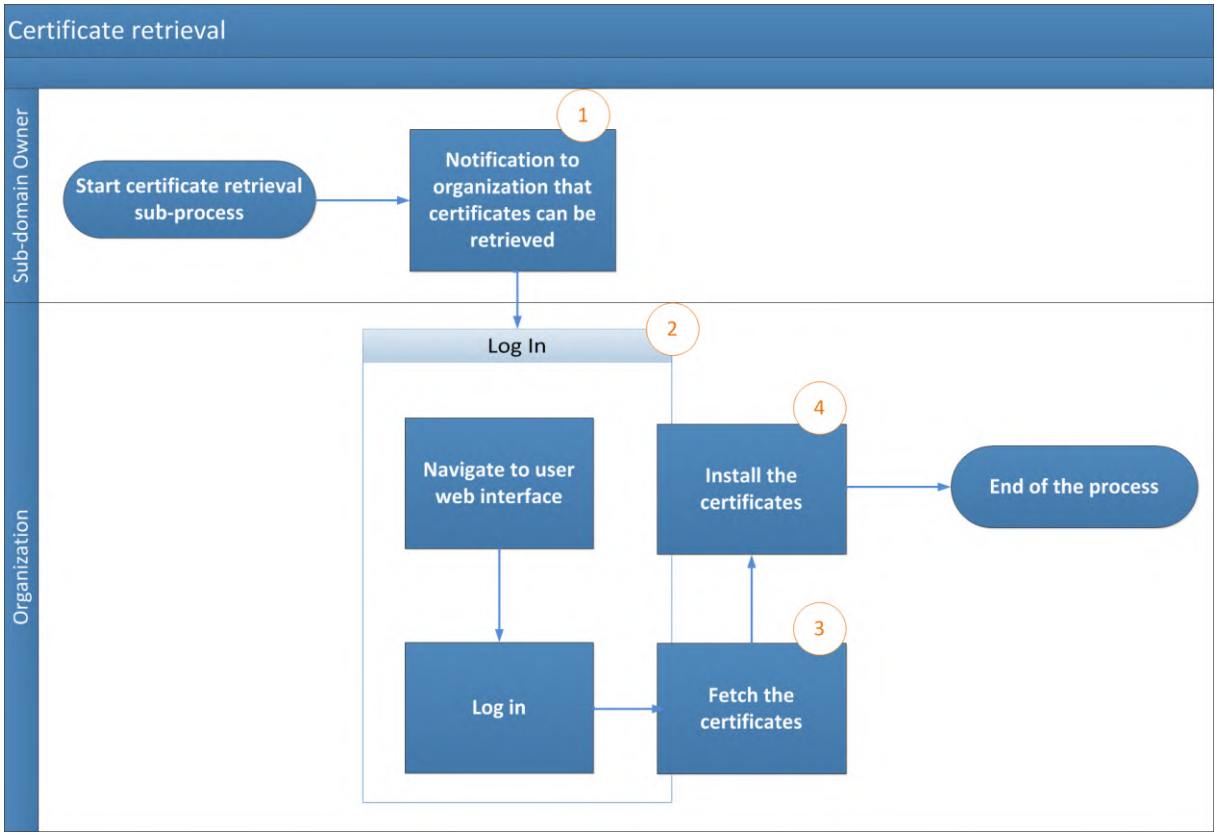
2.2.6.6. Certifikát sa nainštaluje do prístupového bodu. Keďže postup závisí od špecifík daného systému, organizácia sa so žiadosťou o návod obráti na svojho poskytovateľa prístupových bodov.

2.2.6.7. Na inštaláciu certifikátu do prístupového bodu sú potrebné tieto kroky:

a) export súkromného kľúča a certifikátu;

b) vytvorenie úložísk „keystore“ a „truststore“;

c) inštalácia „keystore“ a „truststore“ do prístupového bodu.

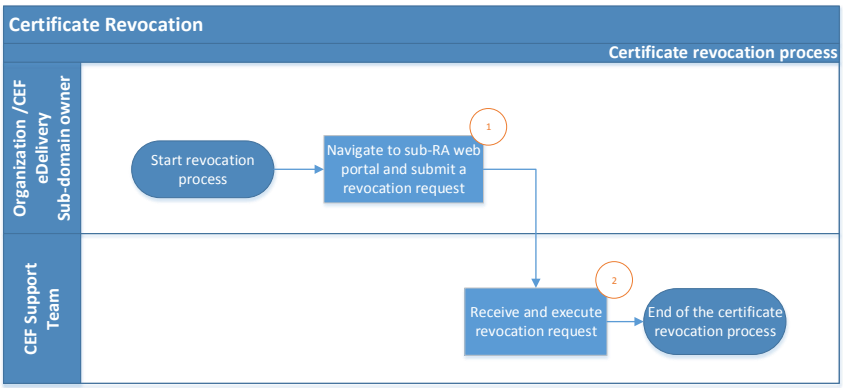


Obrázok 12: Získanie certifikátu

3. Proces zrušenia certifikátu

3.1. Organizácia podá žiadosť o zrušenie cez webový používateľský portál.

3.2. Zrušenie certifikátu vykoná podporný tím NPE.



Obrázok 13: Zrušenie certifikátu

4. Všeobecné podmienky služby CEF PKI

4.1. Kontext

Vo svojej funkcii poskytovateľa riešení týkajúcich sa stavebného prvku eDelivery v správe Nástroja na prepájanie Európy poskytne DIGIT zmluvným stranám AETR službu PKI[7] (ďalej len „služba CEF PKI“). Službu PKI NPE používajú vnútroštátne orgány (ďalej len „koncoví používatelia“) zúčastňujúce sa na systéme TACHOnet.

DIGIT si prenajíma PKI v rámci riešenia TeleSec Shared-Business-CA (SBCA), ktoré prevádzkuje centrum dôveryhodnosti (Trust Center) divízie T-Systems International GmbH (T-Systems[8]). DIGIT zohráva úlohu hlavného registrátora domény „CEF_eDelivery.europa.eu“ v rámci SBCA. V tejto úlohe DIGIT vytvára v rámci domény „CEF_eDelivery.europa.eu“ poddomény za každý projekt využívajúci službu CEF PKI.

V tomto dokumente sa uvádzajú podrobné informácie o podmienkach poddomény systému TACHOnet. DIGIT zohráva úlohu subregistrátora tejto poddomény. V rámci tejto funkcie vydáva, zrušuje a obnovuje certifikáty pre tento projekt.

4.2. Vyhlásenie o odmietnutí zodpovednosti

Európska komisia nenesie žiadnu zodpovednosť za obsah certifikátu, ktorá prináleží výlučne vlastníkovi certifikátu. Je zodpovednosťou vlastníka certifikátu skontrolovať správnosť obsahu certifikátu.

Európska komisia nenesie žiadnu zodpovednosť za to, ako vlastníci nakladajú so svojimi certifikátmi, keďže ide o tretie právnické subjekty mimo Európskej komisie.

---

[7] Infraštruktúra verejného kľúča (Public Key Infrastructure) je súbor úloh, politík, postupov a systémov, ktoré sú potrebné na vytváranie, riadenie, distribúciu a rušenie digitálnych certifikátov.

[8] Dôveryhodná úloha operátora Trust Center, ktorý sa nachádza v T-Systems Trust Center, spočíva aj v plnení úloh interného registračného orgánu.

Cieľom tohto vyhlásenia o odmietnutí zodpovednosti nie je obmedziť zodpovednosť Európskej komisie v rozpore s požiadavkami stanovenými v príslušných vnútroštátnych právnych predpisoch, ani vylúčenie jej zodpovednosti vo veciach, v ktorých ju podľa týchto právnych predpisov nie je možné vylúčiť.

4.3. Povolené/zakázané používanie certifikátov

4.3.1. Povolené používanie certifikátov

Po vydaní certifikátu ho smie vlastník certifikátu[9] používať len v súvislosti so systémom TACHOnet. Certifikát sa v tomto kontexte môže používať na:

- autentifikáciu pôvodu údajov;
- šifrovanie údajov;
- zabezpečenie zisťovania porušení integrity údajov.

4.3.2. Zakázané používanie certifikátov

Akékoľvek použitie, ktoré nie je výslovne povolené ako súčasť povolených použití certifikátu, je zakázané.

4.4. Dodatočné povinnosti vlastníka certifikátu

Podrobné pravidlá a podmienky SBCA definovala spoločnosť T-Systems v certifikačných pravidlách (CP)/certifikačných postupoch (CPS) služby SBCA[10]. Tento dokument obsahuje bezpečnostné špecifikácie a usmernenia týkajúce sa technických a organizačných aspektov a opisuje činnosti prevádzkovateľa Trust Centre v úlohách certifikačného orgánu (CA) a registračného orgánu (RA), ako aj tretej strany delegovanej registračným orgánom (RA).

O certifikát môžu požiadať iba subjekty oprávnené na účasť na systéme TACHOnet.

---

9 Identifikovaný hodnotou atribútu „O=“ v časti Subject Distinguished Name vydaného certifikátu

10 Najnovšia verzia CP/CPS T-Systems SBCA je dostupná na adrese https://www.telesec.de/en/sbca-en/support/download-area/.

Pokiaľ ide o súhlas s certifikátmi, uplatňuje sa klauzula 4.4.1 vyhlásení o certifikačných pravidlách/certifikačných postupoch SBCA (CP/CPS); navyše podmienky používania a ustanovenia opísané v tomto dokumente sa považujú za odsúhlasené organizáciou, ktorej bol vydaný certifikát (O=), pri jeho prvom použití.

Pokiaľ ide o uverejnenie certifikátu, uplatňuje sa klauzula 2.2 SBCA CP/CPS.

Všetci vlastníci certifikátov musia spĺňať tieto požiadavky:

1) musia chrániť svoj súkromný kľúč proti neoprávnenému použitiu;

2) nesmú previesť ani odhaliť svoj súkromný kľúč tretím stranám, a to ani ak pôsobia ako ich zástupcovia;

3) nesmú naďalej používať súkromný kľúč po uplynutí obdobia platnosti alebo zrušení certifikátu za iným účelom, než je nahliadnutie do šifrovaných údajov (napr. dešifrovanie e-mailov).

4) vlastník certifikátu je zodpovedný za kopírovanie alebo postúpenie kľúča konečnému subjektu alebo subjektom;

5) pri nakladaní so súkromným kľúčom musí vlastník certifikátu zaviazať konečný subjekt/všetky konečné subjekty, aby dodržiavali tieto podmienky vrátane SBCA CP/CPS;

6) vlastník certifikátu musí určiť splnomocnených zástupcov, ktorí sú oprávnení žiadať o zrušenie certifikátov vydaných organizácii spolu s údajmi o udalostiach, ktoré vedú k zrušeniu, a s heslom o zrušení;

7) pokiaľ ide o certifikáty týkajúce sa skupín osôb a funkcií a/alebo právnických osôb, po tom, ako daná osoba opustí skupinu konečných subjektov (napr. pri ukončení pracovného pomeru), vlastník certifikátu musí zabrániť zneužitiu súkromného kľúča tak, že certifikát zruší;

8) vlastník certifikátu je zodpovedný za okolností uvedených v klauzule 4.9.1 SBCA CP/CPS a v takejto situácii musí požiadať o zrušenie certifikátu.

Pokiaľ ide o obnovenie certifikátu alebo opätovné pridelenie kľúča, uplatňuje sa klauzula 4.6 alebo 4.7 SBCA CP/CPS.

Pokiaľ ide o zmenu certifikátu, uplatňuje sa klauzula 4.8 SBCA CP/CPS.

Pokiaľ ide o zrušenie certifikátu, uplatňuje sa klauzula 4.9 SBCA CP/CPS.

5. Formulár identifikácie kontaktných osôb a dôveryhodných kuriérov (vzor)

Ja *dolupodpísaný/-á* *[meno a adresa zástupcu organizácie]* **osvedčujem, že v súvislosti so žiadosťou, generovaním a získavaním digitálnych certifikátov s verejnými kľúčmi pre prístupové body TACHOnet sa majú použiť tieto informácie, ktoré zaručujú dôvernosť, integritu a nespochybniteľnosť správ systému TACHOnet**:

Údaje o kontaktnej osobe:

– **Kontaktná osoba č. 1**	– **Kontaktná osoba č. 2**
– Priezvisko:	– Priezvisko:
– Meno/-á:	– Meno/-á:
– Mobilný telefón:	– Mobilný telefón:
– Telefón:	– Telefón:
– Email:	– Email:
– Vzorový vlastnoručný podpis: –	– Vzorový vlastnoručný podpis: – – –

Údaje o dôveryhodnom kuriérovi:

– **Dôveryhodný kuriér č. 1**	– **Dôveryhodný kuriér č. 2**
– Priezvisko:	– Priezvisko:
– Meno/-á:	– Meno/-á:
– Mobilný telefón:	– Mobilný telefón:
– Email:	– Email:
– Krajina vydania pasu:	– Krajina vydania pasu:
– Číslo pasu:	– Číslo pasu:
– Dátum skončenia platnosti pasu:	– Dátum skončenia platnosti pasu:

Miesto, dátum, pečiatka organizácie alebo pečať organizácie:

Podpis oprávneného zástupcu:

6. Dokumenty

6.1. Individuálne splnomocnenie (vzor)

Vzorka individuálneho splnomocnenia, ktoré musí podpísať a predložiť dôveryhodný kuriér počas osobnej registrácie v priestoroch registračného orgánu, je k dispozícii tu:

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. Papierový formulár žiadosti o certifikát (vzor)

Vzorka papierového formulára žiadosti o certifikát, ktorý musí podpísať a predložiť dôveryhodný kuriér počas osobnej registrácie v priestoroch registračného orgánu, je k dispozícii tu:

7. Glosár

Kľúčové pojmy použité v tomto poddodatku sú vymedzené v oddiele Vymedzenie pojmov NPE na internetovom portáli CEF Digital Single Web Portal:

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

Kľúčové skratky použité v tomto katalógu prvkov sú vymedzené v oddiele Glosár NPE na internetovom portáli CEF Digital Single Web Portal:

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