Rada
Evropské unie

Brusel 5. listopadu 2018
(OR. en)

13711/18
ADD 1

Interinstitucionální spis:
2018/0339(NLE)

TRANS 488

POZNÁMKA

Odesílatel:	Generální sekretariát Rady
Příjemce:	Delegace
Č. předchozího dokumentu:	ST 13711/18 TRANS 448
Č. dok. Komise:	ST 12727/18 TRANS 426 + ADD 1
Předmět:	Rozhodnutí Rady o postoji, který má být přijat jménem Evropské Unie ve skupině odborníků pro Evropskou dohodu o práci osádek vozidel v mezinárodní silniční dopravě Evropské hospodářské komise OSN

Doplněk výše uvedeného rozhodnutí Rady.

Nový dodatek k dohodě AETR

Doplněk 4

Specifikace systému TACHOnet

1. Oblast působnosti a účel

1.1. Tento dodatek stanoví pojmy a podmínky týkající se připojení smluvních stran dohody AETR k systému TACHOnet prostřednictvím služby eDelivery.

1.2. Smluvní strany, které se připojují k systému TACHOnet prostřednictvím služby eDelivery, se řídí ustanoveními stanovenými v tomto dodatku.

2. Definice

a) „Smluvní stranou“ nebo „stranou“ se rozumí jakákoli smluvní strana dohody AETR;

b) pojmem „eDelivery“ se rozumí služba vyvinutá Evropskou komisí, která umožňuje přenášet data mezi třetími osobami elektronickými prostředky a poskytuje důkazy týkající se nakládání s přenášenými daty, včetně dokladu o odeslání a přijetí dat, a která chrání přenášená data před rizikem jakékoli neoprávněné změny;

c) „systémem TACHOnet“ se rozumí systém elektronické výměny informací o kartách řidiče mezi smluvními stranami uvedený v čl. 31 odst. 2 nařízení (EU) č. 165/2014;

d) „centrálním uzlem“ se rozumí informační systém umožňující směrování zpráv systému TACHOnet mezi žádajícími a odpovídajícími stranami;

e) „žádající stranou“ se rozumí smluvní strana vysílající žádost nebo oznámení do systému TACHOnet, které jsou poté směrovány příslušné odpovídající straně prostřednictvím centrálního uzlu;

f) „odpovídající stranou“ se rozumí smluvní strana, které je adresována žádost nebo oznámení ze systému TACHOnet;

g) „orgánem vydávajícím karty“ se rozumí subjekt pověřený smluvní stranou k vydávání a správě karet tachografu.

3. Obecné povinnosti

3.1. Žádná ze smluvních stran nemůže uzavírat dohody o přístupu do systému TACHOnet jménem druhé strany nebo jakýmkoli jiným způsobem zastupovat druhou smluvní stranu na základě tohoto dodatku. Žádná ze smluvních stran v rámci úkonů uvedených v tomto dodatku nejedná jako subdodavatel druhé smluvní strany.

3.2. Smluvní strany poskytují přístup do svých vnitrostátních rejstříků karet řidiče prostřednictvím systému TACHOnet, a to způsobem a na úrovni služeb dle poddodatku 4.6.

3.3. Smluvní strany si navzájem neprodleně oznamují případy, kdy zaznamenají narušení nebo chyby ve své oblasti odpovědnosti, jež mohou ohrozit normální provoz systému TACHOnet.

3.4. Každá strana uvede sekretariátu AETR kontaktní osoby pro systém TACHOnet. Jakákoliv změna v jakémkoliv kontaktním bodě musí být poskytnuta písemně sekretariátu AETR.

4. Testy pro připojení k systému TACHOnet

4.1. Propojení smluvní strany se systémem TACHOnet je zřízeno poté, co jsou v souladu s pokyny Evropské komise a pod jejím dohledem úspěšně dokončeny testy propojení, integrace a výkonnosti.

4.2. Pokud přípravné zkoušky selžou, může Evropská komise zkušební fázi dočasně pozastavit. Zkoušky budou pokračovat poté, co smluvní strana vyrozumí Evropskou komisi o přijetí nezbytných technických zlepšení na vnitrostátní úrovni, jež umožní přípravné zkoušky úspěšně provést.

4.3. Maximální délka trvání přípravných zkoušek je šest měsíců.

5. Důvěryhodná architektura

5.1. Důvěrnost, integrita a nepopíratelnost zpráv systému TACHOnet musí být zajištěna důvěryhodnou architekturou systému TACHOnet.

5.2. Důvěryhodná architektura systému TACHOnet je založena na infrastruktuře veřejných klíčů (PKI) zřízené Evropskou komisí, jejíž požadavky jsou uvedeny v poddodatcích 4.8 a 4.9.

5.3. Do důvěryhodné architektury systému TACHOnet vstupují následující subjekty:

a) certifikační orgán odpovědný za generování digitálních certifikátů, které mají být registračním orgánem doručeny vnitrostátním orgánům smluvních stran (prostřednictvím jimi jmenovaných důvěryhodných kurýrů) a za vytvoření technické infrastruktury v oblasti vydávání, rušení platnosti a obnovy digitálních certifikátů;

b) vlastník domény odpovědný za provoz centrálního uzlu uvedeného v poddodatku 4.1 a za ověření a koordinaci důvěryhodné architektury systému TACHOnet;

c) registrační orgán odpovědný za registrování a schvalování žádostí o vydání, zrušení platnosti a obnovení digitálních certifikátů a za ověření identity důvěryhodného kurýra;

d) důvěryhodný kurýr je osoba jmenovaná vnitrostátními orgány a odpovídá za předání veřejného klíče registračnímu orgánu a za získání odpovídajícího certifikátu, který je generován certifikačním orgánem;

e) vnitrostátní orgán ze smluvní strany, který:

i) vytváří soukromé klíče a odpovídající veřejné klíče, jež mají být zahrnuty v certifikátech, které generuje certifikační orgán;

(ii) žádá o digitální certifikáty certifikační orgán;

iii) jmenuje důvěryhodného kurýra.

5.4. Certifikační orgán a registrační orgán jsou jmenovány Evropskou komisí.

5.5. Jakákoliv smluvní strana propojená se systémem TACHOnet musí zažádat o vydání digitálního certifikátu v souladu s poddodatkem 4.9 za účelem podepsání a šifrování zprávy systému TACHOnet.

5.6. Platnost certifikátu může být zrušena v souladu s poddodatkem 4.9.

6. Ochrana údajů a důvěrnost

6.1. Strany v souladu s právními předpisy o ochraně údajů na mezinárodní a vnitrostátní úrovni a zejména s Úmluvou o ochraně osob se zřetelem na automatizované zpracování osobních dat přijímají všechna nezbytná technická a organizační opatření pro zaručení zabezpečení údajů v systému TACHOnet a předcházení jejich změně nebo ztrátě nebo nepovolenému zpracování těchto údajů nebo přístupu k nim (zejména pravost, důvěrnost údajů, sledovatelnost, integrita, dostupnost, nepopíratelnost a zabezpečení zpráv).

6.2. Každá strana musí chránit své vnitrostátní systémy proti nedovolenému používání, škodlivým kódům, virům, proniknutí do počítače, narušení dat a nelegální manipulaci s nimi a jinému srovnatelnému jednání třetích stran. Strany souhlasí s vynaložením ekonomicky přiměřeného úsilí k zamezení výskytu veškerých virů, časovaných bomb, červů nebo podobných nástrojů či počítačových programů, které mohou narušit počítačové systémy druhé strany.

7. Náklady

7.1. Smluvní strany ponesou vlastní náklady na vývoj a provoz ve spojení s vlastními datovými systémy a postupy dle požadavků tak, aby splnily povinnosti dle tohoto dodatku.

7.2. Služby specifikované v poddodatku 4.1 poskytované centrálním uzlem jsou bez poplatku.

8. Subdodavatelé

8.1. Strany mohou zadat subdodavateli jakoukoliv službu, za kterou zodpovídají v rámci tohoto dodatku.

8.2. Subdodavatelský vztah neosvobozuje stranu od odpovědnosti podle tohoto dodatku, včetně odpovědnosti za přiměřenou úroveň služeb v souladu s poddodatkem 4.6.

Poddodatek 4.1

Obecné aspekty systému TACHOnet

1. Obecný popis

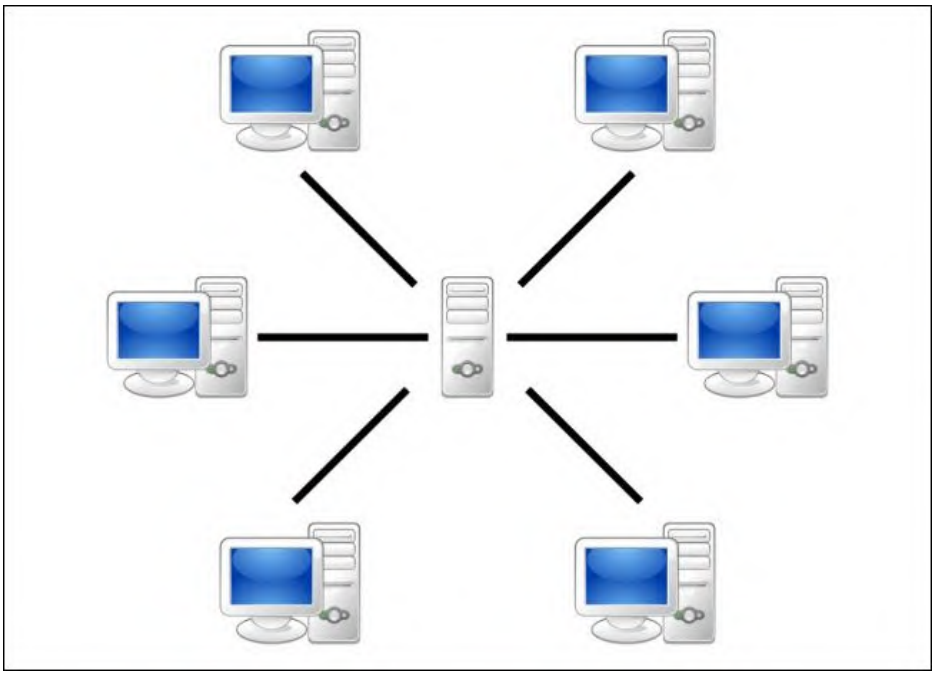
TACHOnet je elektronický systém pro výměnu informací o kartách řidiče mezi smluvními stranami dohody AETR. TACHOnet směruje žádosti o informace od žádajících stran k odpovídajícím stranám a rovněž odpovědi odpovídající strany straně žádající. Smluvní strany, jež jsou součástí systému TACHOnet, musí připojit své vnitrostátní rejstříky karet řidiče k systému.

2. Architektura

Systém předávání zpráv TACHOnet se skládá z následujících částí:

2.1. Centrální uzel, který je schopen přijmout žádost od žádající strany, potvrdit ji a zpracovat ji přeposláním odpovídajícím stranám. Centrální uzel vyčká, než každá odpovídající strana odpoví, shromáždí všechny odpovědi a zašle souhrnnou odpověď žádající straně.

2.2. Vnitrostátní systémy stran vybavené rozhraním schopným posílat žádosti do centrálního uzlu a přijímat příslušné odpovědi. Vnitrostátní systémy mohou k předávání a přijímání zpráv do/z centrálního uzlu využívat proprietární nebo komerční software.



3. Řízení

3.1. Centrální uzel spravuje Evropská komise, která je odpovědná za jeho technický provoz a údržbu.

3.2. Centrální uzel neuchovává údaje po dobu delší než šest měsíců, kromě protokolů a statistických údajů uvedených v poddodatku 4.7.

3.3. Centrální uzel neposkytuje přístup k osobním údajům, s výjimkou oprávněných zaměstnanců Evropské komise, je-li to nezbytné pro účely sledování, údržby a odstraňování problémů.

3.4. Každá smluvní strana je odpovědná za:

3.4.1. Zřízení a správu svých vnitrostátních systémů, včetně rozhraní s centrálním uzlem.

3.4.2. Instalaci a údržbu svých vnitrostátních systémů, a to jak hardwaru, tak softwaru, ať již proprietárních nebo komerčních.

3.4.3. Zajištění správné interoperability svého vnitrostátního systému s centrálním uzlem, včetně zpracovávání chybových hlášení obdržených z centrálního uzlu.

3.4.4. Přijetí veškerých opatření pro zajištění důvěrnosti, integrity a dostupnosti informací.

3.4.5. Provoz vnitrostátních systémů v souladu s úrovněmi služeb stanovenými v poddodatku 4.6.

Poddodatek 4.2

Funkce systému TACHOnet

1. Prostřednictvím systému předávání zpráv TACHOnet jsou poskytovány tyto funkce:

1.1. „Check Issued Cards (CIC)“ (kontrola vydaných karet): umožňuje žádající straně poslat žádost o kontrolu vydaných karet jedné nebo všem odpovídajícím stranám s cílem zjistit, zda je žadatel o kartu již držitelem karty řidiče vydané odpovídajícími stranami. Odpovídající strany na žádost odpoví zasláním odpovědi o kontrole vydaných karet.

1.2. „Check Card Status (CCS)“ (kontrola stavu karty): umožňuje žádající straně požádat odpovídající stranu o podrobnosti karty jí vydané prostřednictvím zaslání žádosti o kontrolu stavu karty. Odpovídající strana na žádost odpoví zasláním odpovědi o kontrole stavu karty.

1.3. „Modify Card Status (MCS)“ (změna stavu karty): umožňuje žádající straně prostřednictvím žádosti o změnu stavu karty odpovídající straně oznámit, že došlo ke změně stavu karty, kterou odpovídající strana vydala. Odpovídající strana odpoví zasláním potvrzení změny stavu karty.

1.4. „Issued Card Driving License (ICDL)“ (karta vydaná na základě řidičského průkazu): umožňuje žádající straně prostřednictvím žádosti týkající se karty vydané na základě řidičského průkazu odpovídající straně oznámit, že tato strana vydala kartu na základě řidičského průkazu vydaného odpovídající stranou. Odpovídající strana odpoví zasláním odpovědi týkající se karty vydané na základě řidičského průkazu.

2. Budou zahrnuty další typy zpráv, jež se pro efektivní fungování systému TACHOnet považují za vhodné, například oznámení o chybě.

3. Vnitrostátní systémy při používání jakékoliv z funkcí popsaných v bodě 1 uznávají stavy karty uvedené v tabulce 1. Strany však nejsou povinny zavést správní postup, který využívá všechny uvedené stavy.

4. Obdrží-li strana odpověď nebo oznámení o udělení stavu, jenž se v jejích správních postupech nepoužívá, převede vnitrostátní systém stav použitý v obdržené zprávě na odpovídající hodnotu používanou v uvedených postupech. Je-li stav použitý ve zprávě uveden v tabulce 1, nesmí odpovídající strana tuto zprávu odmítnout.

5. Stav karty uvedený v tabulce 1 nesmí být použit k určení toho, zda je karta řidiče platná pro řízení. Vznese-li strana dotaz na rejstřík strany, která kartu vydala, prostřednictvím funkce kontrola stavu karty (CCS), musí odpověď obsahovat zvláštní pole „valid for driving“ (platná pro řízení). Vnitrostátní správní postupy musí být takové, aby odpovědi týkající se kontroly stavu karty (CCS) vždy obsahovaly příslušnou hodnotu „valid for driving“ (platná pro řízení).

Tabulka 1

Stavy karty

Stav karty	**Definice**
„Application“ (žádost)	Orgán vydávající karty obdržel žádost o vydání karty řidiče. Tato informace byla zaregistrována a uložena v databázi s vygenerovanými vyhledávacími klíči.
„Approved“ (schválená)	Orgán vydávající karty schválil žádost o kartu tachografu.
„Rejected“ (zamítnutá)	Orgán vydávající karty žádost neschválil.
„Personalised“ (individualizovaná)	Karta tachografu byla individualizována.
„Dispatched“ (odeslaná)	Vnitrostátní orgán odeslal kartu řidiče příslušnému řidiči nebo doručující agentuře.
„Handed Over“ (předaná)	Vnitrostátní orgán předal kartu řidiče příslušnému řidiči.
„Confiscated“ (zabavená)	Karta řidiče byla řidiči příslušným orgánem zabavena.
„Suspended“ (pozastavená)	Karta řidiče byla řidiči přechodně odebrána.
„Withdrawn“ (odebraná)	Orgán vydávající karty rozhodl kartu řidiče odebrat. Karta byla trvale znehodnocena.
„Surrendered“ (odevzdaná)	Karta tachografu byla orgánu vydávajícímu karty vrácena a byla prohlášena za dále nepotřebnou.
„Lost“ (ztracená)	Karta tachografu byla orgánu vydávajícímu karty nahlášena jako ztracená.
„Stolen“ (odcizená)	Karta tachografu byla orgánu vydávajícímu karty nahlášena jako odcizená. Odcizená karta se považuje za kartu ztracenou.
„Malfunctioning“ (nesprávně fungující)	Karta tachografu byla orgánu vydávajícímu karty nahlášena jako nesprávně fungující.
„Expired“ (s ukončenou platností)	„Expired“ (s ukončenou platností) Doba platnosti karty tachografu skončila.
„Replaced“ (nahrazená)	Karta tachografu, která byla nahlášena jako ztracená, odcizená nebo nesprávně fungující, byla nahrazena novou kartou. Údaje na nové kartě zůstávají stejné, s výjimkou indexu náhrady čísla karty, který se zvýší o jednu jednotku.

„Renewed“ (obnovená)	Karta tachografu byla obnovena z důvodu změny správních údajů nebo končící doby platnosti. Číslo nové karty zůstává stejné, s výjimkou indexu obnovy čísla karty, který se zvýší o jednu jednotku. „In Exchange“ (probíhá výměna)
„In Exchange“ (probíhá výměna)	Orgán vydávající karty, který vydal kartu řidiče, obdržel oznámení, že byl ukončen postup výměny uvedené karty za kartu řidiče vydanou orgánem vydávajícím karty druhé strany.
„Exchanged“ (vyměněná)	Orgán vydávající karty, který vydal kartu řidiče, obdržel oznámení, že byl ukončen postup výměny uvedené karty za kartu řidiče vydanou orgánem vydávajícím karty druhé strany.

Poddodatek 4.3

Funkce systému TACHOnet

1. Obecné technické požadavky

1.1. Centrální uzel poskytuje pro výměnu zpráv synchronní i asynchronní rozhraní. Strany si mohou k propojení se svými vlastními aplikacemi zvolit tu nejvhodnější technologii.

1.2. Všechny zprávy vyměňované mezi centrálním uzlem a vnitrostátními systémy musí být v kódování UTF-8.

1.3. Vnitrostátní systémy musí být schopny přijímat a zpracovávat zprávy obsahující znaky v řečtině nebo cyrilici.

2. Struktura zpráv XML a definice schématu (XSD)

2.1. Obecná struktura zpráv XML se řídí formátem definovaným schématy XSD instalovanými v centrálním uzlu.

2.2. Centrální uzel a vnitrostátní systémy odesílají a přijímají zprávy, které jsou v souladu se schématem XSD dané zprávy.

2.3. Vnitrostátní systémy musí být schopny zasílat, přijímat a zpracovávat všechny zprávy odpovídající veškerým funkcím uvedeným v poddodatku 4.2.

2.4. Zprávy XML musí splňovat alespoň minimální požadavky stanovené v tabulce 2.

Tabulka 2

Minimální požadavky na obsah zpráv XML

Společné záhlaví		**Povinný údaj**
„Version“ (verze)	Oficiální verze specifikací XML bude specifikována prostřednictvím jmenného prostoru definovaného ve schématu XSD zprávy a v atributu *„version“* prvku „Header“ (záhlaví) všech zpráv XML. Číslo verze („n.m“) je definováno jako pevně stanovená hodnota v každém vydání souboru s definicí schématu XML (XSD).	Ano
„Test Identifier“ (testovací identifikátor)	Nepovinný identifikátor pro testování. Původce testu identifikátor vyplní a všichni účastníci pracovního postupu stejný identifikátor přepošlou/vrátí. V produkčním prostředí by na něj neměl být brán zřetel a bude-li uveden, nepoužije se.	Ne
„Technical Identifier“ (technický identifikátor)	Univerzální jednoznačný identifikátor (UUID), který jednoznačně identifikuje každou jednotlivou zprávu. Odesílatel generuje UUID a vyplňuje tento atribut. Tyto údaje nemají žádné provozní využití.	Ano
„Workflow Identifier“ (identifikátor pracovního postupu)	Identifikátor workflowId je UUID a měl by být generován žádající stranou. Tento identifikátor se poté používá ve všech zprávách ke korelaci v rámci pracovního postupu.	Ano
„Sent At“ (odesláno)	Datum a čas (UTC) odeslání zprávy.	Ano
„Timeout“ (čekací doba)	Toto je nepovinný atribut data a času (ve formátu UTC). Tuto hodnotu stanoví pouze centrální uzel pro přeposlané žádosti. Slouží k informování odpovídající strany o době platnosti žádosti. Tato hodnota se nevyžaduje ve zprávách MS2TCN_<x>_Req a ve zprávách s odpověďmi. Je nepovinná, aby bylo možné použít stejnou definici záhlaví pro všechny typy zpráv bez ohledu na to, zda je atribut „timeoutValue“ vyžadován, či nikoli.	Ne
„From“ (od)	Dvoupísmenný kód strany, která zprávu odeslala, podle normy ISO 3166-1 Alpha 2, nebo „EU“.	Ano
„To“ (pro)	Dvoupísmenný kód strany, které je zpráva odesílána, podle normy ISO 3166-1 Alpha 2, nebo „EU“.	Ano

Poddodatek 4.4

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

1. Pro zakódování jmen všech řidičů do vnitrostátního rejstříku se používá algoritmus NYSIIS implementovaný v centrálním uzlu.

2. Při vyhledávání karty pomocí funkce kontrola vydaných karet (CIC) se jako primární vyhledávací mechanismus použijí klíče NYSIIS.

3. Strany mohou navíc pro získání dalších výsledků použít vlastní algoritmus.

4. Výsledky vyhledávání uvádějí vyhledávací mechanismus, který byl pro nalezení záznamu použit, tj. NYSIIS nebo vlastní.

5. V případě, že se strana rozhodne zaznamenávat oznámení o kartě vydané na základě řidičského průkazu (ICDL), zaznamenávají se klíče NYSIIS obsažené v oznámení jako součást údajů ICDL. Při vyhledávání údajů ICDL strana použije klíče NYSIIS jména žadatele.

Poddodatek 4.5

Bezpečnostní požadavky

1. Pro výměnu zpráv mezi centrálním uzlem a vnitrostátními systémy se použije protokol HTTPS.

2. Vnitrostátní systémy používají pro účely zabezpečení předávání zpráv mezi vnitrostátními systémy a centrálním uzlem digitální certifikáty uvedené v poddodatcích 4.8 a 4.9.

3. Ve vnitrostátních systémech jsou implementovány minimálně certifikáty používající hašovací algoritmus podpisu SHA-2 (SHA-256) a délku veřejného klíče 2048 bitů.

Poddodatek 4.6

Úrovně služeb

1. Vnitrostátní systémy musí splňovat tyto minimální úrovně služeb:

1.1. Musí být dostupné 24 hodin denně, 7 dní v týdnu.

1.2. Jejich dostupnost se sleduje prostřednictvím zpráv HEARTBEAT, které vysílá centrální uzel.

1.3. Jejich míra dostupnosti musí být 98 % podle následující tabulky (údaje jsou zaokrouhleny na nejbližší vhodnou jednotku):

Dostupnost	znamená následující nedostupnost		
	denně	měsíčně	ročně
98%	0,5 h	15 h	7,5 dne

Po stranách se požaduje, aby dodržovaly denní míru dostupnosti, uznává se však, že některé nezbytné činnosti, jako je údržba systému, vyžadují dobu odstávky delší než 30 minut. Měsíční a roční míry dostupnosti nicméně zůstávají povinné.

1.4. Během jednoho kalendářního měsíce musí odpovědět minimálně na 98 % žádostí, které jim byly přeposlány.

1.5. Na žádosti musí reagovat do 10 sekund.

1.6. Celková čekací doba u žádostí (prodleva, během níž může žadatel čekat na odpověď) nesmí překročit 20 sekund.

1.7. Musí být schopny vyřizovat žádosti rychlostí 6 zpráv za sekundu.

1.8. Vnitrostátní systémy nesmí zasílat žádosti centrálnímu systému TACHOnet rychlostí přesahující 2 požadavky za sekundu.

1.9. Každý vnitrostátní systém musí být schopen čelit potenciálním technickým problémům centrálního uzlu nebo vnitrostátních systémů v jiných stranách. Patří sem mimo jiné:

a) ztráta spojení s centrálním uzlem;

b) nezodpovězení žádosti;

c) obdržení odpovědí po uplynutí čekací doby zprávy;

d) obdržení nevyžádaných zpráv;

e) obdržení neplatných zpráv.

2. Centrální uzel musí:

2.1. vykazovat míru dostupnosti 98 %;

2.2. oznamovat vnitrostátním systémům případné chyby, a to buď prostřednictvím odpovědi, nebo prostřednictvím zvláštního chybového hlášení. Vnitrostátní systémy pak musí tato zvláštní chybová hlášení přijímat a mít zaveden postup eskalace za účelem přijetí vhodných opatření k nápravě oznámené chyby.

3. Údržba

Strany musí ostatní strany a Evropskou komisi informovat o veškeré běžné údržbě prostřednictvím webové aplikace, a to nejméně jeden týden před zahájením takové činnosti, pokud je to technicky možné.

Poddodatek 4.7

Protokolování a statistika údajů shromážděných v centrálním uzlu

1. V zájmu zajištění soukromí jsou údaje pro statistické účely anonymní. Údaje identifikující určitou kartu, řidiče nebo řidičský průkaz nejsou pro statistické účely k dispozici.

2. Protokolování zachycuje všechny transakce za účelem monitorování a odstraňování chyb a umožňuje generování statistických údajů o těchto transakcích.

3. Osobní údaje se v protokolech neuchovávají déle než 6 měsíců. Statistické údaje se uchovávají po dobu neurčitou.

4. Statistické údaje používané pro hlášení musí obsahovat následující údaje:

   a) žádající strana;

   b) odpovídající strana;

   c) typ zprávy;

   d) kód stavu odpovědi;

   e) datum a čas zpráv;

   f) dobu odezvy.

Poddodatek 4.8

Obecná ustanovení ohledně digitálních klíčů a certifikátů pro systém TACHOnet

1. Generální ředitelství pro informatiku Evropské komise (GŘ pro informatiku) zpřístupní službu PKI[1] (dále jen „služba PKI v rámci Nástroje pro propojení Evropy) smluvním stranám dohody AETR připojeným k systému TACHOnet (dále jen „vnitrostátní orgány“) prostřednictvím služby eDelivery.

2. Postup žádosti o digitální certifikáty a zrušení jejich platnosti, jakož i podrobné podmínky pro jejich použití jsou definovány v dodatku.

3. Použití certifikátů:

3.1. Jakmile je certifikát vydán, vnitrostátní orgán[2] používá certifikát pouze v souvislosti se systémem TACHOnet. Certifikát použít za účelem:

a) autentizace původu dat;

b) šifrování dat;

c) zajištění odhalení narušení integrity dat.

3.2. Jakékoliv použití, které není výslovně autorizováno jako součást povoleného použití certifikátu, je zakázáno.

4. Smluvní strany:

a) chrání své soukromé klíče proti neautorizovanému použití;

b) se zdrží přenosu nebo odhalení svého soukromého klíče třetím stranám, a to i pokud by měly jednat v roli zástupců;

---

1 PKI („Public Key Infrastructure“, infrastruktura veřejných klíčů) je souhrnem rolí, politik, postupů a systémů potřebných pro tvorbu, správu, distribuci a zrušení platnosti digitálních certifikátů.

2 Identifikovaný pomocí hodnoty atributu „O=“ v předmětu „rozlišující název“ vydaného certifikátu.

c) zajistí důvěrnost, integritu a dostupnost vygenerovaných soukromých klíčů, které jsou ukládány a používány v systému TACHOnet;

d) se zdrží dalšího používání soukromých klíčů po uplynutí doby platnosti nebo po zrušení platnosti certifikátu kromě zobrazení zašifrovaných dat (např. dešifrování e-mailů). Klíče, u nichž uplynula doba platnosti, musí být buď zničeny, nebo uchovány ve stavu, který zabraňuje jejich používání;

e) poskytují registračnímu orgánu identifikaci těch autorizovaných zástupců, kteří jsou pověřeni žádat o zrušení platnosti certifikátů vydaných organizaci (žádosti o zrušení platnosti zahrnují heslo pro žádost o zrušení a podrobnosti o událostech, které vedou ke zrušení platnosti);

f) předchází zneužití soukromého klíče pomocí žádosti o zrušení platnosti souvisejícího veřejného klíče v případě ohrožení bezpečnosti soukromého klíče nebo aktivačních údajů soukromého klíče;

g) mají povinnost vyžadovat zrušení platnosti certifikátu za okolností uvedených v certifikačních politikách a certifikačních prováděcích směrnicích certifikačního orgánu a nesou za tento úkon odpovědnost;

h) neprodleně oznamují registračnímu orgánu ztrátu, odcizení nebo potenciální ohrožení bezpečnosti jakéhokoliv klíče AETR, jež je používán v souvislosti se systémem TACHOnet.

5. Odpovědnost

Aniž je dotčena odpovědnost Evropské komise v případě porušení požadavků stanovených platnými vnitrostátními právními předpisy nebo s ohledem na odpovědnost za záležitosti, kterou nelze podle těchto právních předpisů vyloučit, Evropská komise nenese odpovědnost ani jí nevznikají žádné závazky, pokud jde o:

a) obsah certifikátu, který patří výlučně vlastníkovi certifikátu. Za kontrolování správnost obsahu certifikátu odpovídá vlastník certifikátu;

b) používání certifikátu jeho vlastníkem.

Poddodatek 4.9

Popis služby PKI pro systém TACHOnet

1. Úvod

PKI („Public Key Infrastructure“, infrastruktura veřejných klíčů) je souhrnem rolí, politik, postupů a systémů potřebných pro tvorbu, správu, distribuci a rušení platnosti digitálních certifikátů[3]. Služba PKI v rámci Nástroje pro propojení Evropy služby eDelivery umožňuje vydávání a správu digitálních certifikátů, které jsou používány pro zajištění důvěrnosti, integrity a nepopíratelnosti informací vyměňovaných mezi přístupovými body.

Služba PKI služby eDelivery je založena na službách centra zabezpečení Trust Center Services TeleSec Shared Business CA (certifikační orgán), pro niž platí certifikační politika/certifikační prováděcí směrnice TeleSec Shared-Business-CA společnosti T-Systems International GmbH[4].

Služba PKI vydává certifikáty, které jsou vhodné pro zabezpečení různých podnikových procesů ve společnostech, organizacích, veřejných orgánech a institucích i mimo ně, které vyžadují střední úroveň zabezpečení pro ověření pravosti, integrity a důvěryhodnosti konečného subjektu.

2. Postup při rušení platnosti certifikátu

2.1. Úlohy a povinnosti

2.1.1. „Organizace“ nebo „vnitrostátní orgán“ žádající o certifikát

2.1.1.1. Vnitrostátní orgán žádá o certifikáty v souvislosti s projektem TACHOnet.

2.1.1.2 Vnitrostátní orgán:

a) žádá certifikáty od služby PKI v rámci Nástroje pro propojení Evropy;

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

[4] Poslední verzi certifikační politiky a certifikační prováděcí směrnice lze stáhnout na adrese https://www.telesec.de/en/sbca-en/support/download-area/

b) generuje soukromé klíče a příslušné veřejné klíče, které jsou zahrnuty v certifikátech vydaných certifikačním orgánem;

c) po schválení stahuje certifikát;

d) podepisuje a zasílá nazpět registračnímu orgánu:

i) identifikační formulář pro kontaktní osoby a důvěryhodné kurýry;

ii) podepsanou individuální plnou moc[5].

2.1.2. Důvěryhodný kurýr

2.1.2.1. Vnitrostátní orgán jmenuje důvěryhodného kurýra.

2.1.2.2. Důvěryhodný kurýr:

a) předává veřejný klíč registračnímu orgánu během procesu osobní identifikace a registrace;

b) obdrží příslušný certifikát od registračního orgánu.

2.1.3. Vlastník domény

2.1.3.1. Vlastníkem domény je GŘ pro mobilitu a dopravu.

2.1.3.2. Vlastník domény:

a) potvrzuje a koordinuje síť systému TACHOnet a důvěryhodnou architekturu systému TACHOnet, včetně potvrzení postupů při vydávání certifikátů;

b) provozuje centrální uzel systému TACHOnet a koordinuje činnost stran s ohledem na fungování systému TACHOnet;

c) provádí ve spolupráci s vnitrostátními orgány testy připojení k systému TACHOnet.

---

5 Plná moc je právní dokument, kterým organizace zmocňuje Evropskou komisi zastoupenou vybraným úředníkem, který je odpovědný za službu PKI v rámci Nástroje pro propojení Evropy, požádat jejím jménem o generování certifikátu certifikačním orgánem TeleSec Shared Business CA společnosti T-Systems International GmbH a dává jí k tomu pravomoc, viz také bod 6. Viz též bod 6.

2.1.4. Registrační orgán

2.1.4.1. Registračním orgánem je Společné výzkumné středisko (JRC).

2.1.4.2. Registrační orgán je odpovědný za ověřování identity důvěryhodného kurýra, za registrování a schvalování žádostí o vydání, zrušení platnosti a obnovení digitálních certifikátů.

2.1.4.3. Registrační orgán:

a) přiděluje unikátní identifikátor vnitrostátnímu orgánu;

b) autentizuje identitu vnitrostátního orgánu, jeho kontaktních bodů a důvěryhodných kurýrů;

c) komunikuje s týmem podpory Nástroje pro propojení Evropy v oblasti autenticity vnitrostátního orgánu, jeho kontaktních bodů a důvěryhodných kurýrů;

d) informuje vnitrostátní orgán o schválení nebo zamítnutí certifikátu.

2.1.5. Certifikační orgán

2.1.5.1. Certifikační orgán je odpovědný za poskytování technické infrastruktury pro žádosti, vydávání a zrušení platnosti digitálních certifikátů.

2.1.5.2. Certifikační orgán:

a) zajišťuje technickou infrastrukturu pro žádosti o certifikát vnitrostátními úřady;

b) potvrzuje nebo zamítá žádosti o certifikát;

c) v případě potřeby komunikuje s registračním orgánem za účelem ověření identity žádající organizace.

2.2. Vydávání certifikátu

2.2.1. Vydávání certifikátu je prováděno v souladu s následujícími postupnými kroky, které jsou znázorněny v obr. 1.:

a) **Krok 1:** identifikace důvěryhodného kurýra;

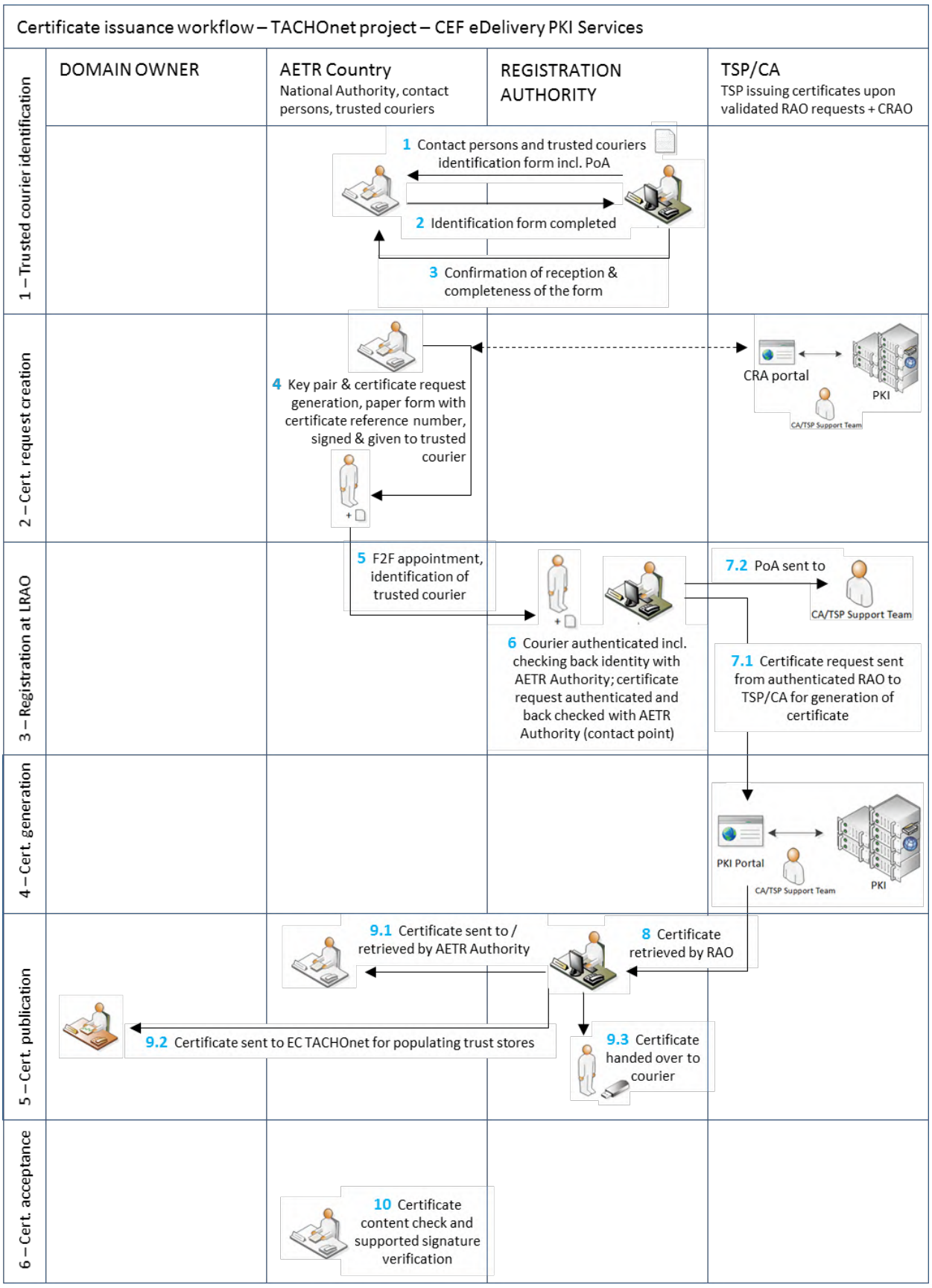
b) **Krok 2:** vytvoření žádosti o certifikát;

c) **Krok 3:** registrace u registračního orgánu;

d) **Krok 4:** generování certifikátu;

e) **Krok 5:** zveřejnění certifikátu;

f) **Krok 6:** přijetí certifikátu.



Obr. 1 – pracovní postup při vydávání certifikátu

2.2.2. Krok 1: Identifikace důvěryhodného kurýra

Za účelem identifikace důvěryhodného kurýra se provádí následující proces:

a) Registrační orgán zašle vnitrostátním orgánům identifikační formulář pro kontaktní osoby a důvěryhodné kurýry[6]. Tento formulář zahrnuje také plnou moc, kterou organizace (orgán AETR) podepíše.

b) Vnitrostátní orgán zašle vyplněný formulář a podepsanou plnou moc nazpět registračnímu orgánu.

c) Registrační orgán potvrdí příjem a úplnost formuláře.

d) Registrační orgán poskytne vlastníkovi domény aktualizovanou kopii seznamu kontaktních osob a důvěryhodných kurýrů.

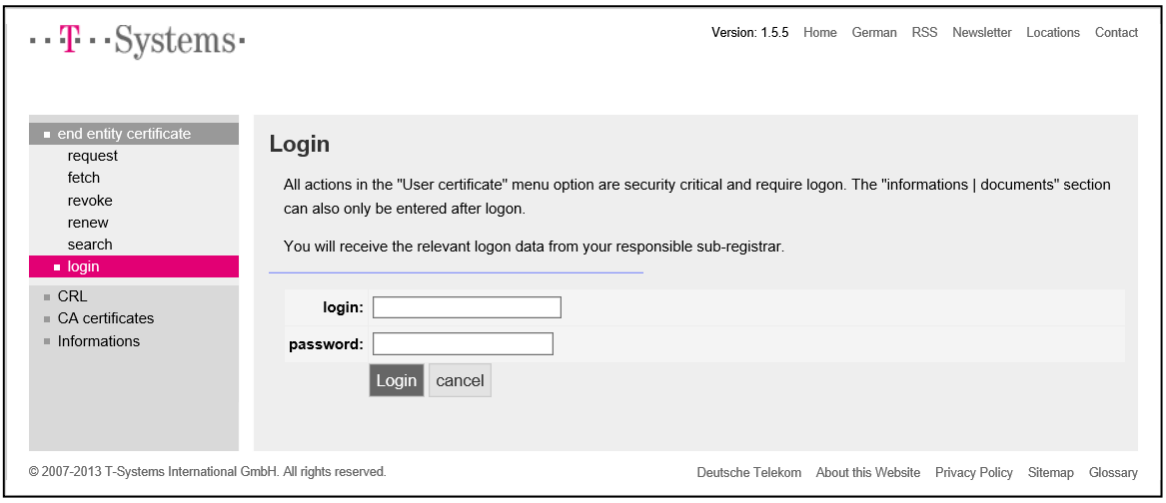
2.2.3. Krok 2: Vytvoření žádosti o certifikát

2.2.3.1. Žádost o certifikát a jeho vyhledání se musí provést na stejném počítači a ve stejném prohlížeči.

2.2.3.2. Za účelem vytvoření žádosti o certifikát musí být proveden následující postup:

a) Organizace přejde na uživatelské webové rozhraní pro žádost o certifikát přes URL https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: a zadá uživatelské jméno „**sbca/CEF_eDelivery.europa.eu**“ a heslo „**digit.333**“

[6] Viz bod 5

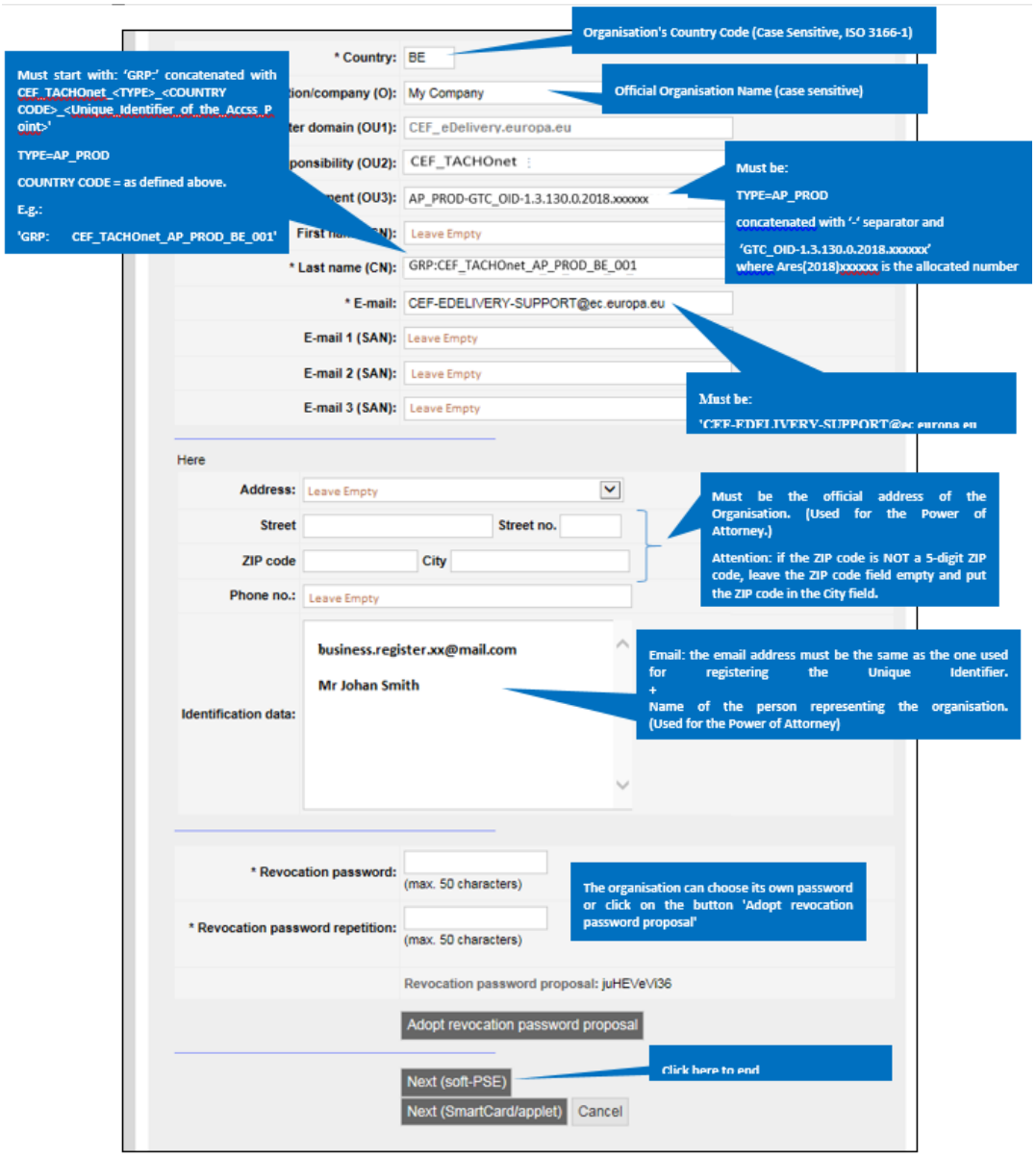


Obrázek 2

b) Organizace klikne na „request“ (žádost) na levé straně okna a vybere z rozbalovací nabídky „CEF_TACHOnet“.

Obrázek 3

c) Organizace vyplní formulář žádosti o certifikát vyobrazený v obrázku 4 s uvedením informací v tabulce 3 a kliknutím na „Next (soft-PSE)“ ukončí proces.


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
* 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
Here
Address: Leave Empty
Street
Street no.
ZIP code
City
Phone no.: Leave Empty
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

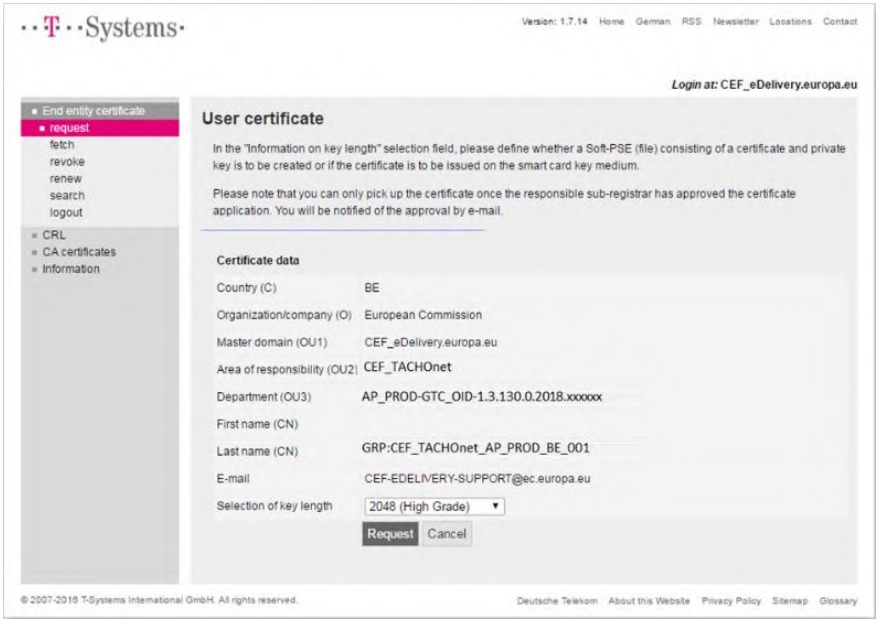
Obrázek 4

Povinná pole	Popis
„Country“ (země)	**C=kód země**, místo vlastníka certifikátu, ověřené veřejným rejstříkem, Omezení: 2 písmena v souladu s dvoupísmenným kódem podle normy ISO 3166-1 Alpha-2, rozlišená velká a malá písmena; Příklady: DE, BE, NL, Zvláštní případy: UK (Spojené království), EL (Řecko)
„Country“ (země)	**O=název organizace vlastníka certifikátu**
„Master domain (OU1)“ (hlavní doména)	**OU=CEF_eDelivery.europa.eu**
„Area of responsibility (OU2)“ (oblast odpovědnosti)	**OU=CEF_TACHOnet**
„Department (OU3)“ (oddělení)	Povinná hodnota podle „OBLASTI ODPOVĚDNOSTI“ Obsah musí být při žádosti o certifikát ověřen pomocí pozitivního seznamu (bílá listina). Pokud informace neodpovídá informaci v listině, je žádosti zabráněno. Formát: **OU=<TYPE>-<GTC_NUMBER>** Přičemž „<TYPE>“ je nahrazen AP_PROD: Přístupový bod v produkčním prostředí. A kde <GTC_NUMBER> je **GTC_OID-1.3.130.0.2018.xxxxxx**, kde Ares(2018)xxxxxx je číslo protokolu GTC pro projekt TACHOnet. např.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
„First name (CN)“ (jméno)	Musí být prázdné
„Last name (CN)“ (příjmení)	Musí začínat na"GRP:“ a po něm následuje obecný název. Formát: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** např.: GRP:CEF_TACHOnet_AP_PROD_BE_001
„E-mail“ (e-mail)	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
„E-mail 1 (SAN)“ (e-mail)	Musí být prázdné
„E-mail 2 (SAN)“ (e-mail)	Musí být prázdné
„E-mail 3 (SAN)“ (e-mail)	Musí být prázdné

„Address“ (adresa)	Musí být prázdné
„Street“ (ulice)	Musí být oficiální adresou organizace vlastníka certifikátu. (Použité v plné moci.)
„Street no.“ (č. ulice)	Musí být oficiální adresou organizace vlastníka certifikátu. (Použité v plné moci.)
„Zip Code“ (PSČ)	Musí být oficiální adresou organizace vlastníka certifikátu. (Použité v plné moci.) **Upozornění:** pokud PSČ NENÍ 5místným číselným kódem, ponechte pole „ZIP code“ prázdné a vložte PSČ do pole „City“ (město).
„City“ (město)	Musí být oficiální adresou organizace vlastníka certifikátu. (Použité v plné moci.) **Upozornění:** pokud PSČ NENÍ 5místným číselným kódem, ponechte pole „ZIP code“ prázdné a vložte PSČ do pole „City“ (město).
„Phone no“ (tel. č.)	Musí být prázdné
„Identification data“ (identifikační údaje)	E-mailová adresa musí být shodná s tou, která byla použita pro registraci unikátního identifikátoru. + Musí být jméno osoby zastupující organizaci. (Použité v plné moci.) + „**Commercial Register No**“ (číslo v obchodním rejstříku) (povinné pouze pro soukromé organizace) „**Entered at the Local Court of**“ (zapsáno u místního soudu v) (povinné pouze pro soukromé organizace v Německu a Rakousku)
Heslo pro zrušení platnosti	Povinné pole zvolené žadatelem
Opakování hesla pro zrušení platnosti	Opakování povinného pole zvoleného žadatelem

Tabulka 3. Vyplnění podrobností každého požadovaného pole

d) Délka zvoleného klíče činí 2048 bitů (High Grade).



Obrázek 5

e) Organizace zaznamenává referenční číslo pro vyhledání certifikátu.

Obrázek 6

f) Tým podpory Nástroje pro propojení Evropy kontroluje nové žádosti o certifikát a potvrzuje, zda jsou informace v žádosti o certifikát platné, tzn. že vyhovují zásadám vytváření názvů specifikovaným v dodatku 5.1 s názvem Zásady vytváření názvů certifikátů.

g) Tým podpory Nástroje pro propojení Evropy potvrdí, že zadané informace v žádosti jsou v platném formátu.

h) Pokud kontrola bodů 5 nebo 6 uvedených výše selže, zašle Tým podpory Nástroje pro propojení Evropy e-mail na e-mailovou adresu, která byla poskytnuta v poli „identifikační údaje“ formuláře žádosti spolu s kopií vlastníkovi domény, ve které bude organizace požádána, aby proces zahájila znovu. Neúspěšná žádost o certifikát musí být zrušena.

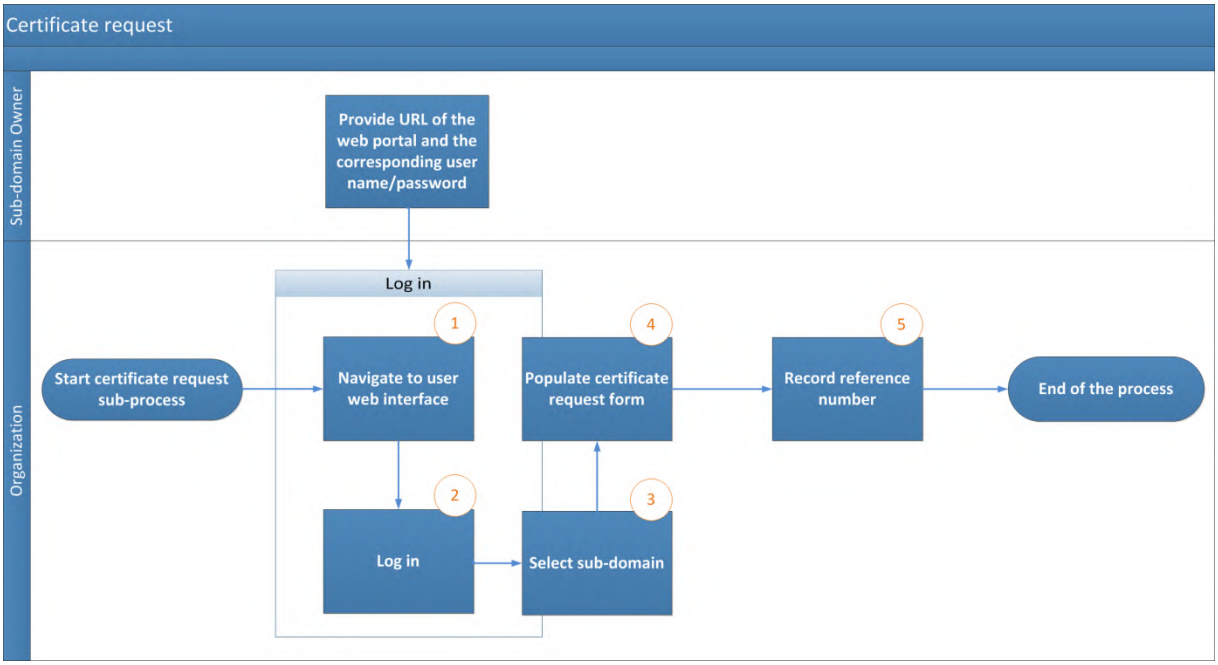
i) Tým podpory Nástroje pro propojení Evropy zašle e-mail registračnímu orgánu ohledně platnosti žádosti. Tento e-mail musí obsahovat:

   1) název organizace, který je k dispozici v poli „Organisation (O)” (organizace) žádosti o certifikát;

   2) údaje certifikátu včetně přístupového bodu, pro který má být certifikát vydán a je k dispozici v poli “Last Name (CN)” (příjmení) žádosti o certifikát;

   3) referenční číslo certifikátu;

   4) adresu organizace, její e-mail a jméno osoby, která ji zastupuje.



Obrázek 7 – Proces žádosti o certifikát

2.2.4. Krok 3: Registrace u registračního orgánu (schválení certifikátu)

2.2.4.1. Důvěryhodný kurýr nebo kontaktní bod sjedná s registračním orgánem schůzku prostřednictvím e-mailové korespondence, přičemž identifikuje důvěryhodného kurýra, který se zúčastní osobního jednání.

2.2.4.2. Organizace připraví balíček dokumentace sestávající z:

a) vyplněné a podepsané plné moci;

b) kopie platného cestovního pasu důvěryhodného kurýra, který se zúčastní osobního jednání. Tato kopie musí být podepsána jedním z kontaktních bodů organizace, která byla identifikována v kroku 1;

c) tištěný formulář žádosti o certifikát podepsaný jedním z kontaktních bodů organizace.

2.2.4.3. Registrační orgán přijme důvěryhodného kurýra po ověření identity na recepci budovy. Registrační orgán provede osobní registraci žádosti o certifikát tak, že:

a) identifikuje a provede autentizaci důvěryhodného kurýra;

b) ověří fyzický vzhled důvěryhodného kurýra vůči cestovnímu pasu, který předložil;

c) ověří platnost cestovního pasu předloženého důvěryhodným kurýrem;

d) ověří ověřený cestovní pas předložený důvěryhodným kurýrem vůči kopii platného pasu důvěryhodného kurýra, která je podepsána jedním z identifikovaných kontaktních bodů organizace. Pravost podpisu je ověřena porovnáním s původním „identifikačním formulářem důvěryhodného kurýra a kontaktních bodů“;

e) ověří vyplněnou a podepsanou plnou moc;

f) ověří tištěný formulář žádosti o certifikát a jeho podpis vůči originálnímu vyhotovení „identifikačního formuláře důvěryhodného kurýra a kontaktních bodů“;

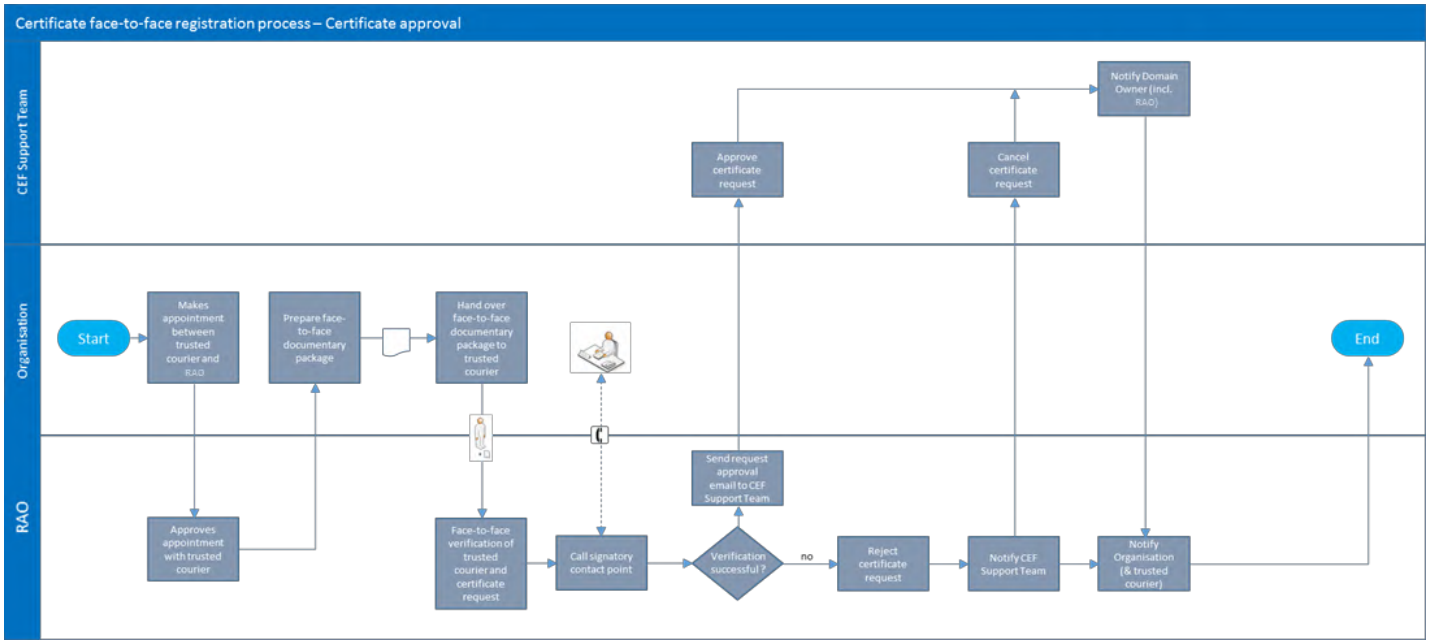
g) uskuteční telefonní hovor s podepsaným kontaktním bodem za účelem dvojí kontroly identity důvěryhodného kurýra a obsahu žádosti o certifikát.

2.2.4.4. Registrační orgán potvrdí týmu podpory Nástroje pro propojení Evropy, že vnitrostátní orgán je skutečně autorizován k provozu složek, pro které žádá certifikáty, a že odpovídající proces osobní registrace byl úspěšný. Potvrzení musí být odesláno prostřednictvím e-mailu zabezpečeného prostřednictvím certifikátu „CommiSign“ s připojenou naskenovanou kopií autentizovaného balíčku dokumentace z osobního setkání a podepsanou kopií kontrolního seznamu provedeného registračním orgánem.

2.2.4.5. Jestliže registrační orgán potvrdí platnost žádosti, bude proveden postup tak, jak je stanoveno v bodech 2.2.4.6 a 2.2.4.7. V opačném případě je vydání certifikátu zamítnuto a organizace je o tom informována.

2.2.4.6. Tým podpory Nástroje pro propojení Evropy schvaluje žádost o certifikát a oznamuje jeho schválení registračnímu orgánu.

2.2.4.7. Registrační orgán informuje organizaci, že certifikát lze získat přes uživatelský portál.



Obr. 8 – schválení certifikátu

2.2.5. Krok 4: Vygenerování certifikátu

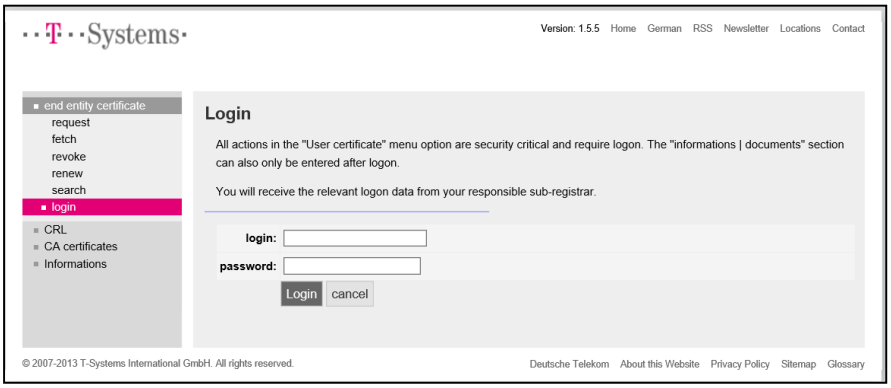
Na základě schválení žádosti o certifikát se certifikát vygeneruje.

2.2.6. Krok 5: Zveřejnění a zpřístupnění certifikátu

2.2.6.1. Po schválení žádosti o certifikát registrační orgán certifikát zpřístupní a předá důvěryhodnému kurýrovi kopii.

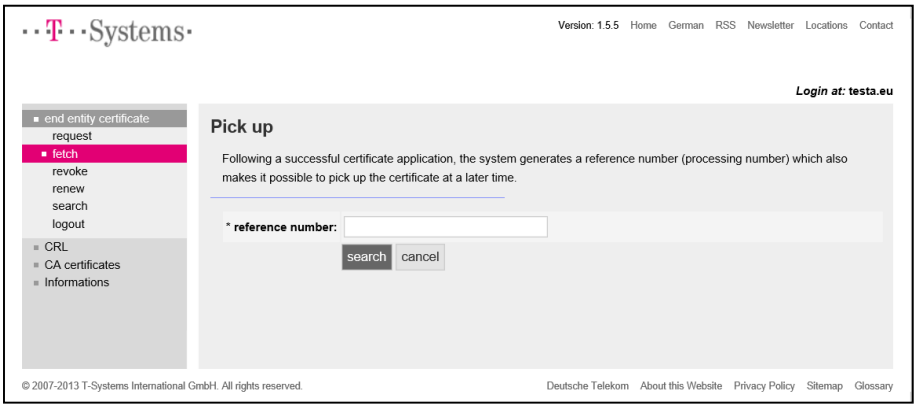
2.2.6.2. Organizace přijme od registračního orgánu oznámení o tom, že certifikáty mohou být získány.

2.2.6.3. Organizace přejde na uživatelském portálu na adresu https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en a přihlásí se uživatelským jménem „**sbca/CEF_eDelivery.europa.eu**“ a heslem „**digit.333**“.



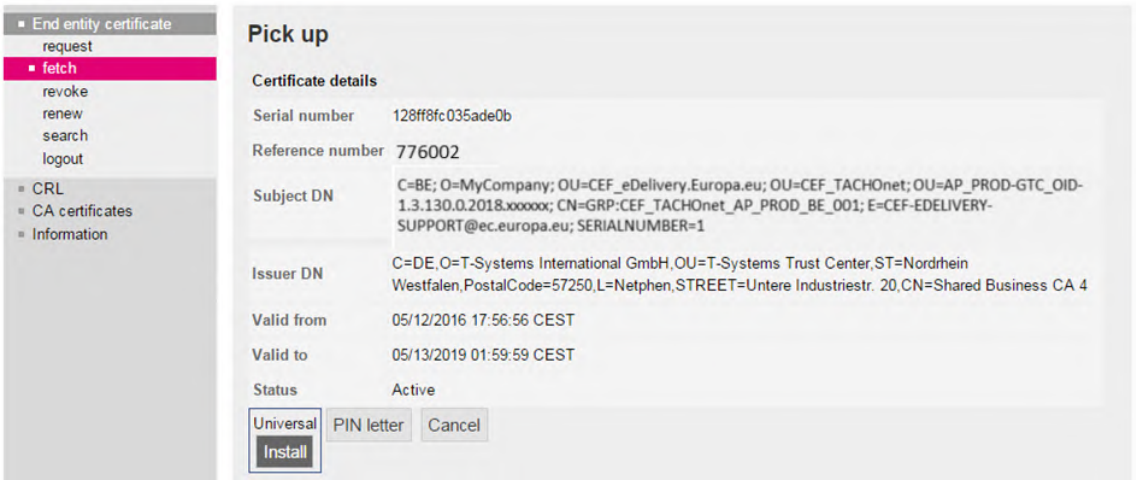
Obrázek 9

2.2.6.4. Organizace klikne na tlačítko „fetch“ na levé straně a poskytne referenční číslo zaznamenané během procesu žádosti o certifikát.



Obrázek 10

2.2.6.5. Organizace nainstaluje certifikáty kliknutím na tlačítko „install“ (instalovat).



Obrázek 11

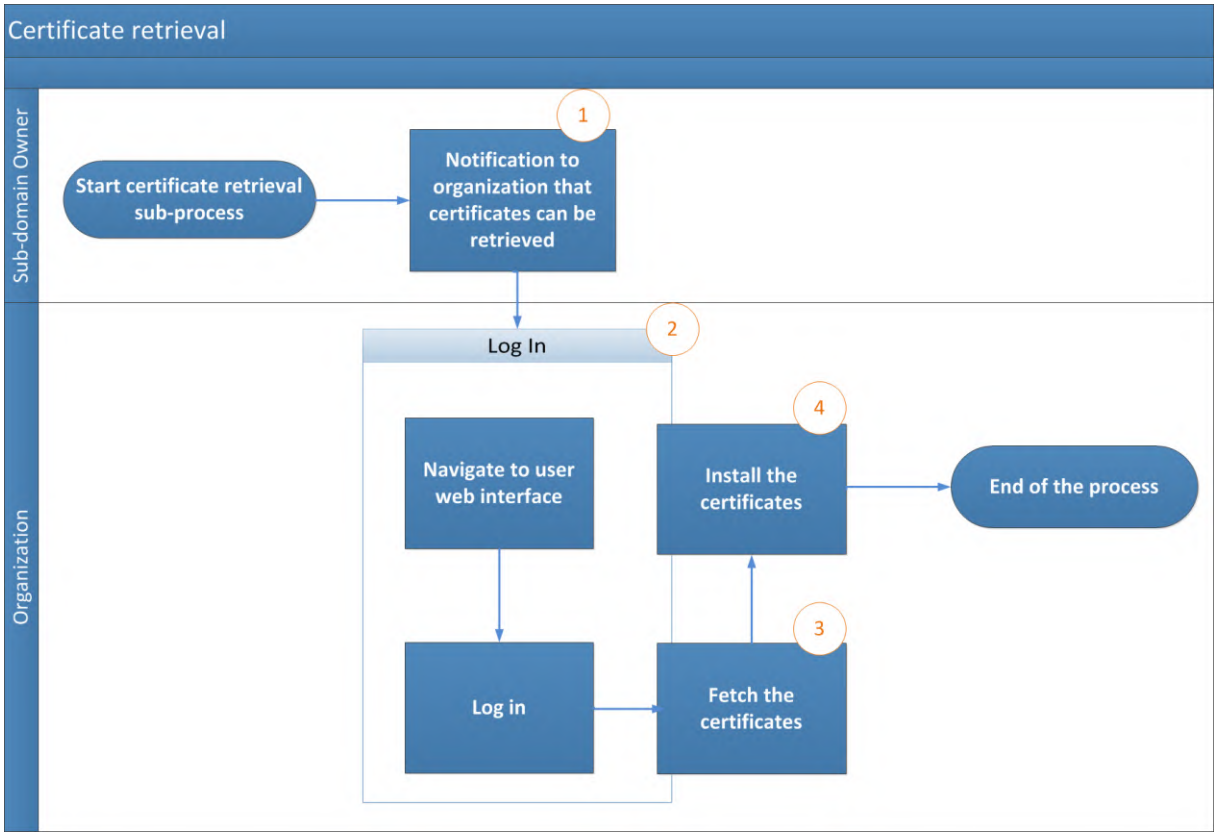
2.2.6.6. Certifikát musí být nainstalován na přístupovém bodu. Jedná se o úkon specifický pro danou implementaci a organizace se musí obrátit na svůj přístupový bod pro získání popisu tohoto procesu.

2.2.6.7. Pro instalaci certifikátu na přístupovém bodě je nutno provést následující kroky:

a) exportovat soukromý klíč a certifikát;

b) vytvořit úložiště klíčů a úložiště důvěryhodných certifikátů;

c) instalovat na tomto přístupovém bodě úložiště klíčů a úložiště důvěryhodných certifikátů.

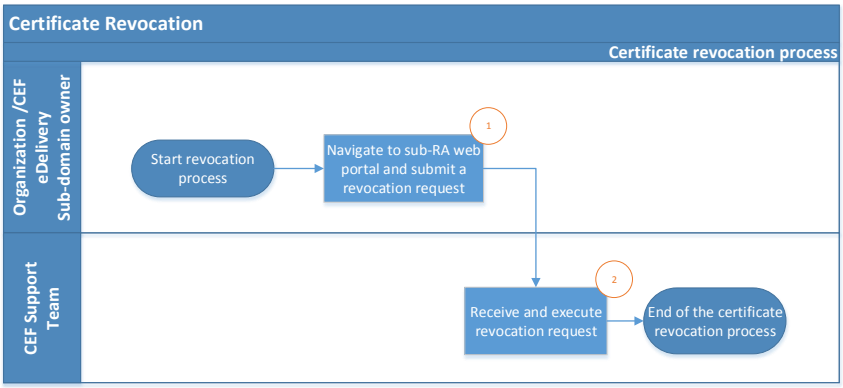


Obrázek 12 – Získání certifikátu

3. Postup při rušení platnosti certifikátu

3.1. Organizace předloží žádost o zrušení platnosti prostřednictvím uživatelského webového portálu.

3.2. Tým podpory Nástroje pro propojení Evropy provede zrušení platnosti certifikátu.



Obrázek 13 – Zrušení platnosti certifikátu

4. Obecné podmínky služby PKI v rámci Nástroje pro propojení Evropy

4.1. Souvislosti

Ve své funkci poskytovatele řešení stavebního bloku služby eDelivery v rámci Nástroje pro propojení Evropy umožní GŘ pro informatiku dostupnost služby PKI[7] (dále jen „služba PKI v rámci Nástroje pro propojení Evropy“) smluvním stranám dohody AETR. Službu PKI v rámci Nástroje pro propojení Evropy musí používat vnitrostátní orgány (dále jen „koncoví uživatelé“), kteří jsou účastníky systému TACHOnet.

GŘ pro informatiku je klientem infrastruktury veřejných klíčů v softwarovém řešení TeleSec Shared-Business-CA (dále jen „SBCA“), jež je provozováno v centru zabezpečení jednotky skupiny T-Systems International GmbH (dále jen „T-Systems“[8]). GŘ pro informatiku zaujímá roli registrátora domény „CEF_eDelivery.europa.eu“ řešení SBCA. V této roli GŘ pro informatiku vytváří poddomény na doméně „CEF_eDelivery.europa.eu“ pro každý projekt, který užívá službu PKI v rámci Nástroje pro propojení Evropy.

Tento dokument poskytuje podrobnosti o zásadách a podmínkách subdomény TACHOnet. GŘ pro informatiku zaujímá roli dílčího registrátora této subdomény. V této funkci vydává, ruší a obnovuje certifikáty v rámci tohoto projektu.

4.2. Prohlášení o odpovědnosti

Evropská komise vylučuje jakoukoli odpovědnost za obsah certifikátu, za nějž nese odpovědnost výlučně vlastník certifikátu. Vlastník certifikátu nese zodpovědnost za kontrolu správnosti obsahu certifikátu.

Evropská komise vylučuje jakoukoli odpovědnost za použití certifikátu jeho vlastníkem, jenž je třetím právním subjektem mimo Evropskou komisi.

---

7 PKI („Public Key Infrastructure“, infrastruktura veřejných klíčů) je souhrnem rolí, politik, postupů a systémů potřebných pro tvorbu, správu, distribuci a zrušení platnosti digitálních certifikátů.

8 Důvěryhodná role operátora centra zabezpečení, který je umístěn v centru zabezpečení T-Systems Trust Center, také vykonává úlohu interního registračního orgánu.

Záměrem tohoto prohlášení není omezit odpovědnost Evropské komise v případě porušení požadavků stanovených platnými vnitrostátními právními předpisy ani vyloučit odpovědnost Komise v záležitostech, ve kterých ji podle takových právních předpisů vyloučit nelze.

4.3. Autorizovaná/zakázaná použití certifikátů

4.3.1. Povolené použití certifikátů

Jakmile je certifikát vydán, vlastník certifikátu[9] používá certifikát pouze v souvislosti se systémem TACHOnet. V tomto kontextu lze certifikát použít za účelem:

- autentizace původu dat;
- šifrování dat;
- zajištění odhalení narušení integrity dat.

4.3.2. Zakázané použití certifikátů

Jakékoliv použití, které není výslovně autorizováno jako součást povoleného použití certifikátu, je zakázáno.

4.4. Další povinnosti vlastníka certifikátu

Podrobné zásady a podmínky SBCA jsou uvedeny subjektem T-Systems v certifikační politice / certifikační prováděcí směrnici služby SBCA[10]. Tento dokument zahrnuje bezpečnostní specifikace a pokyny ohledně technických a organizačních aspektů a popisuje činnost operátora centra zabezpečení v rolích certifikačního orgánu a registračního orgánu a rovněž třetí strany delegované registračním orgánem.

O certifikát mohou požádat pouze subjekty, které jsou autorizované pro účast v systému TACHOnet.

---

9 Identifikovaný pomocí hodnoty atributu „O=“ v předmětu „rozlišující název“ vydaného certifikátu.

10 Nejnovější verze certifikační politiky / certifikační prováděcí směrnice SBCA společnosti T-Systems je dostupná na adrese https://www.telesec.de/en/sbca-en/support/download-area/.

Ohledně přijetí certifikátu platí bod 4.4.1 certifikační politiky a certifikační prováděcí směrnice SBCA, kromě toho jsou podmínky používání a ustanovení popsané v tomto dokumentu považovány za přijaté organizací, které je certifikát vydán („O=“) při prvním použití.

Ohledně zveřejnění certifikátu platí bod 2.2 certifikační politiky / certifikační prováděcí směrnice SBCA.

Všichni vlastníci certifikátu musí splňovat tyto požadavky:

1) chrání své soukromé klíče proti neautorizovanému použití;

2) zdržet se přenosu nebo odhalení svého soukromého klíče třetím stranám, a to i pokud by měly jednat v roli zástupců;

3) se zdrží dalšího používání soukromých klíčů po uplynutí doby platnosti nebo po zrušení platnosti certifikátu kromě zobrazení zašifrovaných dat (např. dešifrování e-mailů).

4) vlastník certifikátu je odpovědný za kopírování nebo přeposlání klíče koncovému subjektu nebo subjektům;

5) vlastník certifikátu musí uložit koncovému subjektu / všem koncovým subjektům povinnost dodržovat stávající zásady a podmínky včetně certifikační politiky / certifikační prováděcí směrnice SBCA, pokud pracují se soukromým klíčem;

6) vlastník certifikátu musí poskytnout identifikaci těch autorizovaných zástupců, kteří jsou pověřeni žádat o zrušení platnosti certifikátů vydaných organizaci, spolu s uvedením podrobností o události, která vedla k zrušení a heslo pro zrušení platnosti;

7) v případě certifikátů spojených se skupinami osob a funkcemi a/nebo právnickými osobami poté, co jedna z osob opustila skupinu koncových subjektů (např. ukončení zaměstnaneckého poměru), vlastník certifikátu musí předcházet zneužití soukromého klíče zrušením certifikátu;

8) vlastník certifikátu je odpovědný za zrušení platnosti certifikátu a žádá o něj za okolností, které jsou uvedeny v bodě 4.9.1 certifikační politiky / certifikační prováděcí směrnice SBCA.

Ohledně obnovení nebo opětovného vytvoření klíčů u certifikátu platí bod 4.6 nebo 4.7 certifikační politiky / certifikační prováděcí směrnice SBCA.

Ohledně změny certifikátu platí bod 4.8 certifikační politiky / certifikační prováděcí směrnice SBCA.

Ohledně zrušení platnosti certifikátu platí bod 4.9 certifikační politiky / certifikační prováděcí směrnice SBCA.

5. Identifikační formulář pro kontaktní osoby a důvěryhodné kurýry (příklad)

Já, *[jméno a adresa zástupce organizace]***, potvrzuji, že následující informace budou použity v souvislosti se žádostí, generováním a zpřístupněním digitálních certifikátů veřejného klíče pro přístupové body systému TACHOnet podporující důvěrnost, integritu a nepopíratelnost zpráv vyměňovaných v systému TACHOnet:**

Údaje o kontaktní osobě**:**

– **Kontaktní osoba #1**	– **Kontaktní osoba #2**
– Jméno:	– Jméno:
– Jména:	– Jména:
– Mobilní telefon:	– Mobilní telefon:
– Telefonní číslo:	– Telefonní číslo:
– E-mail:	– E-mail:
– Vzor vlastnoručního podpisu: –	– Vzor vlastnoručního podpisu: – – –

Údaje o důvěryhodném kurýrovi**:**

– **Důvěryhodný kurýr č. 1**	– **Důvěryhodný kurýr č. 2**
– Jméno:	– Jméno:
– Jména:	– Jména:
– Mobilní telefon:	– Mobilní telefon:
– E-mail:	– E-mail:
– Země vydání cestovního pasu:	– Země vydání cestovního pasu:
– Číslo cestovního pasu:	– Číslo cestovního pasu:
– Datum konce platnosti pasu:	– Datum konce platnosti pasu:

Místo, datum, razítko společnosti nebo pečeť organizace:

Podpis pověřeného zástupce:

6. Dokumenty

6.1. Plná moc (vzor)

Vzor individuální plné moci, která musí být podepsána a předložena důvěryhodným kurýrem při osobní registraci v kanceláři registračního orgánu, lze najít zde:

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. Tištěný formulář žádosti o certifikát (vzor)

Vzor tištěného formuláře žádosti o certifikát, který musí být podepsán a předložen důvěryhodným kurýrem při osobní registraci v kanceláři registračního orgánu, lze najít zde:

7. Glosář

Klíčové pojmy používané v tomto poddodatku jsou definovány v oddělení definic Nástroje pro propojení Evropy na jednotném webovém portálu CEF Digital:

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

Klíčové zkratky používané v tomto popisu nabídky komponentů jsou definovány v glosáři Nástroje pro propojení Evropy na jednotném webovém portálu CEF Digital:

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