Consiliul
Uniunii Europene

Bruxelles, 5 noiembrie 2018
(OR. en)

13711/18
ADD 1

Dosar interinstituțional:
2018/0339(NLE)

TRANS 488

NOTĂ

Sursă:	Secretariatul General al Consiliului
Destinatar:	Delegațiile
Nr. doc. ant.:	ST 13711/18 TRANS 448
Nr. doc. Csie:	ST 12727/18 TRANS 426 + ADD 1
Subiect:	Decizie a Consiliului privind poziția care trebuie adoptată, în numele Uniunii Europene, în cadrul Grupului de experți pentru Acordul european privind activitatea echipajelor vehiculelor care efectuează transporturi rutiere internaționale al Comisiei Economice pentru Europa a Organizației Națiunilor Unite

Anexă la decizia sus-menționată a Consiliului.

ANEXĂ

Apendice nou la AETR

Apendicele 4

Specificațiile TACHOnet

1. Domeniu de aplicare și scop

1.1. Prezentul apendice stabilește termenele și condițiile privind conectarea la TACHOnet a părților contractante la AETR prin intermediul eDelivery.

1.2. Părțile contractante care se conectează la TACHOnet prin eDelivery trebuie să respecte dispozițiile prevăzute în prezentul apendice.

2. Definiții

(a) „parte contractantă” sau „parte” înseamnă orice parte contractantă la AETR;

(b) „eDelivery” înseamnă serviciul creat de Comisia Europeană care permite transmiterea de date între părți terțe prin mijloace electronice și furnizează dovezi referitoare la manipularea datelor transmise, inclusiv dovezi privind trimiterea și primirea datelor, și care protejează datele transmise împotriva riscului oricărei modificări neautorizate;

(c) „TACHOnet” înseamnă sistemul de schimb electronic de informații privind cardurile de conducător auto între părțile contractante, menționat la articolul 31 alineatul (2) din Regulamentul (UE) nr. 165/2014;

(d) „nod central” înseamnă sistemul informatic care permite direcționarea mesajelor TACHOnet între părțile solicitante și părțile respondente;

(e) „parte solicitantă” înseamnă partea contractantă care emite o cerere sau o notificare TACHOnet ce este apoi direcționată de nodul central către partea respondentă corespunzătoare;

(f) „parte respondentă” înseamnă partea contractantă căreia i se adresează cererea sau notificarea TACHOnet;

(g) „autoritate emitentă a cardului” sau „AEC” înseamnă entitatea împuternicită de o parte contractantă să emită și să gestioneze cardurile de tahograf.

3. Responsabilități generale

3.1. Niciuna dintre părțile contractante nu poate încheia acorduri pentru accesul la TACHOnet în numele unei alte părți și nu poate reprezenta în niciun alt mod cealaltă parte contractantă în baza prezentului apendice. Niciuna dintre părțile contractante nu acționează ca subcontractant al celeilalte părți contractante în cadrul operațiunilor menționate în prezentul apendice.

3.2. Părțile contractante asigură accesul la propriul registru național al cardurilor de conducător auto prin intermediul TACHOnet, în modul și la nivelul serviciului stabilite în subapendicele 4.6.

3.3. Părțile contractante se notifică reciproc, fără întârziere, dacă observă perturbări sau erori care țin de domeniul lor de responsabilitate și care ar putea pune în pericol funcționarea normală a TACHOnet.

3.4. Fiecare parte desemnează persoane de contact pentru TACHOnet și le comunică secretariatului AETR. Orice modificare a punctelor de contact trebuie notificată în scris secretariatului AETR.

4. Teste pentru conectarea la TACHOnet

4.1. Conectarea unei părți contractante la TACHOnet este realizată după finalizarea cu succes a testelor de conectare, de integrare și de performanță, în conformitate cu instrucțiunile Comisiei Europene și sub supravegherea acesteia.

4.2. În caz de eșec al testelor preliminare, Comisia Europeană poate suspenda temporar faza de testare. Testele sunt reluate după ce partea contractantă a comunicat Comisiei Europene adoptarea, la nivel național, a îmbunătățirilor tehnice necesare pentru desfășurarea cu succes a testelor preliminare.

4.3. Durata maximă a testelor preliminare este de șase luni.

5. Arhitectura de încredere

5.1. Confidențialitatea, integritatea și nerepudierea mesajelor TACHOnet sunt asigurate de arhitectura de încredere a TACHOnet.

5.2. Arhitectura de încredere a TACHOnet se bazează pe un serviciu de infrastructură de chei publice (PKI) instituit de Comisia Europeană, ale cărui cerințe sunt prevăzute în subapendicele 4.8 și 4.9.

5.3. Următoarele entități intervin în arhitectura de încredere a TACHOnet:

(a) autoritatea de certificare, responsabilă pentru generarea certificatelor digitale care urmează să fie eliberate de autoritatea de înregistrare autorităților naționale ale părților contractante (prin intermediul unor curieri de încredere desemnați de acestea), precum și pentru crearea infrastructurii tehnice în ceea ce privește eliberarea, revocarea și reînnoirea certificatelor digitale;

(b) proprietarul domeniului, responsabil cu funcționarea nodului central menționat în subapendicele 4.1 și cu validarea și coordonarea arhitecturii de încredere a TACHOnet;

(c) autoritatea de înregistrare, responsabilă cu înregistrarea și aprobarea cererilor de eliberare, de revocare și de reînnoire a certificatelor digitale, precum și cu verificarea identității curierilor de încredere;

(d) curierul de încredere, și anume persoana desemnată de autoritățile naționale care este responsabilă cu predarea cheii publice către autoritatea de înregistrare și cu preluarea certificatului corespunzător generat de autoritatea de certificare;

(e) autoritatea națională a părții contractante, care:

(i) generează cheile private și cheile publice corespunzătoare ce trebuie incluse în certificatele care urmează să fie generate de autoritatea de certificare;

(ii) solicită certificatele digitale de la autoritatea de certificare;

(iii) desemnează curierul de încredere.

5.4. Autoritatea de certificare și autoritatea de înregistrare sunt desemnate de Comisia Europeană.

5.5. Orice parte contractantă care se conectează la TACHOnet trebuie să solicite eliberarea unui certificat digital în conformitate cu subapendicele 4.9, pentru semnarea și criptarea unui mesaj TACHOnet.

5.6. Un certificat poate fi revocat în conformitate cu subapendicele 4.9.

6. Protecția datelor și confidențialitate

6.1. În conformitate cu legislația privind protecția datelor la nivel internațional și național, în special cu Convenția pentru protejarea persoanelor față de prelucrarea automatizată a datelor cu caracter personal, părțile adoptă toate măsurile tehnice și organizatorice necesare pentru a garanta securitatea datelor TACHOnet și pentru a preveni modificarea sau pierderea acestor date ori accesarea sau prelucrarea lor neautorizată (în special autenticitatea, confidențialitatea datelor, trasabilitatea, integritatea, disponibilitatea și nerepudierea și securitatea mesajelor).

6.2. Fiecare parte își protejează propriile sisteme naționale împotriva utilizării ilicite, a codurilor dăunătoare, a virușilor, a intruziunilor informatice, a infracțiunilor, a modificării ilegale a datelor și a altor acțiuni comparabile ale unor părți terțe. Părțile convin să depună eforturi rezonabile din punct de vedere comercial pentru a evita transmiterea de viruși, de programe cu declanșare programată (time bombs), de programe cu auto-replicare (worms) sau altele asemenea ori de orice rutină de programare informatică ce ar putea afecta sistemele informatice ale altei părți.

7. Costuri

7.1. Părțile contractante își suportă propriile costuri de dezvoltare și de exploatare în legătură cu propriile proceduri și sisteme de date necesare pentru îndeplinirea obligațiilor care le revin în temeiul prezentului apendice.

7.2. Serviciile specificate în subapendicele 4.1, furnizate de nodul central, sunt gratuite.

8. Subcontractarea

8.1. Părţile pot subcontracta oricare dintre serviciile pentru care sunt responsabile în temeiul prezentului apendice.

8.2. Această subcontractare nu exonerează partea de responsabilitatea care îi revine în temeiul prezentului apendice, inclusiv de responsabilitatea pentru nivelul corespunzător al serviciului în conformitate cu subapendicele 4.6.

Subapendicele 4.1

Aspecte generale ale TACHOnet

1. Descriere generală

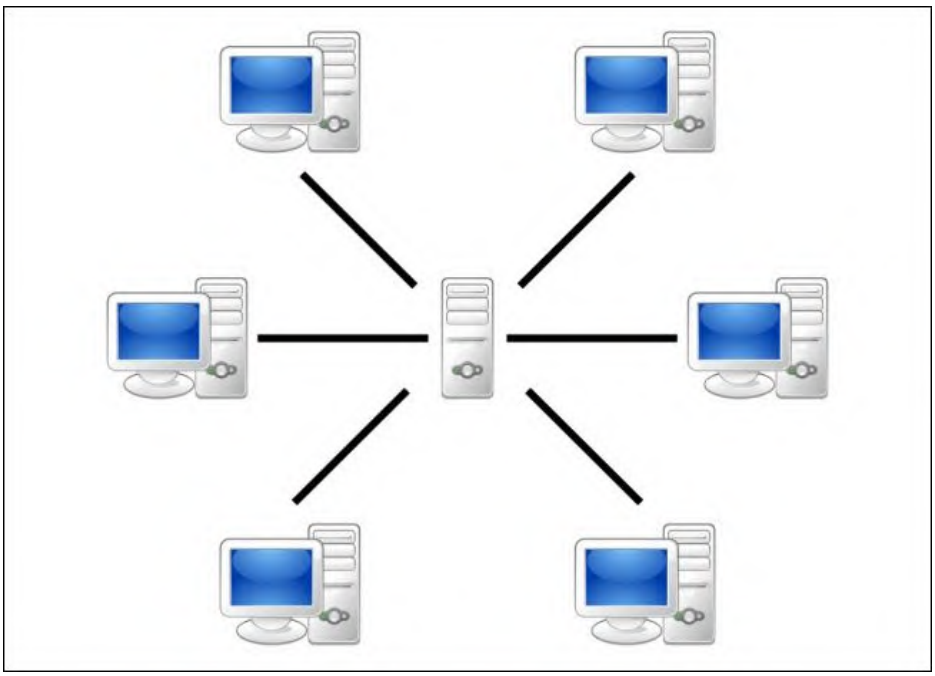
TACHOnet este un sistem electronic de schimb de informații privind cardurile de conducător auto între părțile contractante la AETR. TACHOnet direcționează cererile de informații de la părțile solicitante către părțile respondente, precum și răspunsurile acestora din urmă către primele. Părțile contractante care fac parte din TACHOnet trebuie să își conecteze la sistem registrele naționale ale cardurilor de conducător auto.

2. Arhitectură

Sistemul de mesagerie TACHOnet este compus din următoarele părți:

2.1. Un nod central, care trebuie să fie capabil să primească o cerere de la partea solicitantă, să o valideze și să o prelucreze prin transmiterea ei către părțile respondente. Nodul central așteaptă ca fiecare parte respondentă să răspundă, consolidează toate răspunsurile și transmite răspunsul consolidat părții solicitante.

2.2. Sistemele naționale ale părților, care trebuie să fie echipate cu o interfață capabilă să transmită cereri către nodul central, dar și să primească răspunsurile corespunzătoare. Pentru a transmite și a recepționa mesaje de la nodul central, sistemele naționale pot utiliza software brevetat sau comercial.



3. Gestionare

3.1. Nodul central este administrat de Comisia Europeană, care este responsabilă cu funcționarea tehnică și cu întreținerea nodului central.

3.2. Nodul central nu stochează date pe perioade de peste șase luni, cu excepția datelor înregistrate în jurnal și a datelor statistice stabilite în subapendicele 4.7.

3.3. Nodul central nu oferă acces la datele cu caracter personal decât personalului autorizat al Comisiei Europene, atunci când acest lucru este necesar în scopul monitorizării, al întreținerii și al depanării.

3.4. Fiecare parte contractantă este responsabilă cu:

3.4.1. Crearea și administrarea propriilor sisteme naționale, inclusiv a interfeței cu nodul central.

3.4.2. Instalarea și întreținerea propriilor sisteme naționale, atât în materie de hardware, cât și de software, indiferent dacă acestea sunt brevetate sau comerciale.

3.4.3. Interoperabilitatea corectă a propriului sistem național cu nodul central, inclusiv gestionarea mesajelor de eroare primite de la nodul central.

3.4.4. Luarea tuturor măsurilor pentru a asigura confidențialitatea, integritatea și disponibilitatea informațiilor.

3.4.5. Exploatarea sistemelor naționale în conformitate cu nivelurile serviciului prevăzute în subapendicele 4.6.

Subapendicele 4.2

Funcționalitățile TACHOnet

1. Sistemul de mesagerie TACHOnet trebuie să asigure următoarele funcții:

1.1. verificarea cardurilor eliberate (Check Issued Cards - CIC): permite părții solicitante să trimită o cerere de verificare a cardurilor eliberate (Check Issued Cards Request) către o parte respondentă sau către toate părțile respondente, pentru a stabili dacă un solicitant de card deține deja un card de conducător auto eliberat de părțile respondente. Părțile respondente răspund cererii prin transmiterea unui răspuns de verificare a cardurilor eliberate (Check Issued Cards Response);

1.2. verificarea stării cardului (Check Card Status - CCS): permite părții solicitante să ceară părții respondente detalii cu privire la un card eliberat de aceasta din urmă, prin transmiterea unei cereri de verificare a stării cardului (Check Card Status Request). Partea respondentă răspunde cererii prin transmiterea unui răspuns de verificare a stării cardului (Check Card Status Response);

1.3. modificarea stării cardului (Modify Card Status - MCS): permite părții solicitante să notifice părții respondente, printr-o cerere de modificare a stării cardului (Modify Card Status Request), că starea unui card eliberat de aceasta din urmă s-a schimbat. Partea respondentă răspunde printr-un mesaj de luare la cunoștință a modificării stării cardului (Modify Card Status Acknowledgement);

1.4. permisul de conducere pe baza căruia a fost eliberat cardul (Issued Card Driving Licence - ICDL): permite părții solicitante să notifice părții respondente, prin intermediul unei cereri de tipul Issued Card Driving Licence Request, că partea solicitantă a eliberat un card pe baza unui permis de conducere eliberat de partea respondentă. Partea respondentă răspunde printr-un mesaj de tipul Issued Card Driving Licence Response.

2. Trebuie incluse și alte tipuri de mesaje considerate adecvate pentru funcționarea eficientă a TACHOnet, de exemplu notificările de eroare.

3. Sistemele naționale trebuie să recunoască stările cardului enumerate în tabelul 1 atunci când utilizează oricare dintre funcțiile descrise la punctul 1. Cu toate acestea, părțile nu sunt obligate să implementeze o procedură administrativă care să utilizeze toate stările enumerate.

4. Atunci când o parte primește un răspuns sau o notificare indicând o stare care nu este folosită în cadrul procedurilor sale administrative, sistemul național transpune starea din mesajul primit în valoarea corespunzătoare din cadrul procedurii respective. Mesajul nu trebuie să fie respins de partea respondentă, atât timp cât starea din mesaj figurează în tabelul 1.

5. Starea cardului care figurează în tabelul 1 nu trebuie utilizată pentru a stabili dacă un card de conducător auto este valabil pentru conducerea unui autovehicul. Atunci când o parte interoghează registrul autorității naționale emitente a cardului prin intermediul funcției CCS, răspunsul trebuie să conțină câmpul dedicat „valabil pentru conducerea unui autovehicul”. Procedurile administrative naționale trebuie să fie de așa natură încât răspunsurile CCS să conțină întotdeauna valoarea adecvată în câmpul „valabil pentru conducerea unui autovehicul”.

Tabelul 1

Stări ale cardului

Starea cardului	**(Card Status)**
Definiție	Application (cerere) AEC a primit o cerere de eliberare a unui card de conducător auto. Aceste informații au fost înregistrate și stocate în baza de date cu cheile de căutare generate.
Approved (aprobat)	AEC a aprobat cererea de eliberare a unui card de tahograf.
Rejected (respins)	AEC nu a aprobat cererea.
Personalised (personalizat)	Cardul de tahograf a fost personalizat.
Dispatched (expediat)	Autoritatea națională a expediat cardul de conducător auto către conducătorul auto relevant sau către agenția de eliberare relevantă.
Handed Over (înmânat)	Autoritatea națională a înmânat cardul de conducător auto conducătorului auto relevant.
Confiscated (confiscat)	Cardul de conducător auto a fost luat de la conducătorul auto de către autoritatea competentă.
Suspended (suspendat)	Cardul de conducător auto a fost luat temporar de la conducătorul auto.
Withdrawn (retras)	AEC a decis să retragă cardul de conducător auto. Cardul a fost anulat definitiv.
Surrendered (predat)	Cardul de tahograf a fost returnat AEC și a fost declarat inutil.
Lost (pierdut)	Cardul de tahograf a fost declarat pierdut la AEC.
Stolen (furat)	Cardul de tahograf a fost declarat furat la AEC. Un card furat este considerat pierdut.
Malfunctioning (defect)	Cardul de tahograf a fost declarat defect la AEC.
Expired (expirat)	Perioada de valabilitate a cardului de tahograf a expirat.
Replaced (înlocuit)	Cardul de tahograf care a fost declarat pierdut, furat sau defect a fost înlocuit cu un nou card. Datele de pe noul card sunt aceleași, cu excepția indicelui de înlocuire din numărul cardului, care a fost mărit cu o unitate.

Renewed (reînnoit)	Cardul de tahograf a fost reînnoit în urma modificării unor date administrative sau a expirării perioadei de valabilitate. Datele de pe noul card sunt aceleași, cu excepția indicelui de reînnoire din numărul cardului, care a fost mărit cu o unitate.
In Exchange (în curs de schimbare)	AEC care a emis un card de conducător auto a primit o notificare prin care este anunțată că a fost demarată procedura de schimbare a cardului respectiv cu un card de conducător auto emis de AEC a altei părți.
Exchanged (preschimbat)	AEC care a emis un card de conducător auto a primit o notificare prin care este anunțată că a fost finalizată procedura de preschimbare a cardului respectiv cu un card de conducător auto emis de AEC a altei părți.

Subapendicele 4.3

Dispoziții privind mesajele TACHOnet

1. Cerințe tehnice generale

1.1. Nodul central trebuie să asigure atât interfețe sincrone, cât și asincrone pentru schimbul de mesaje. Părțile pot alege tehnologia cea mai adecvată pentru interfața cu propriile aplicații.

1.2. Toate mesajele transmise între nodul central și sistemele naționale trebuie să fie codificate UTF-8.

1.3. Sistemele naționale trebuie să aibă capacitatea de a primi și de a prelucra mesaje care conțin caractere grecești sau chirilice.

2. Structura mesajelor XML și definiția schemei (XSD)

2.1. Structura generală a mesajelor XML trebuie să respecte formatul definit de schemele XSD instalate în nodul central.

2.2. Nodul central și sistemele naționale trebuie să transmită și să recepționeze mesaje care sunt conforme cu schema XSD a mesajelor.

2.3. Sistemele naționale trebuie să aibă capacitatea de a transmite, de a recepționa și de a prelucra toate mesajele care corespund oricăreia dintre funcțiile stabilite în subapendicele 4.2.

2.4. Mesajele XML trebuie să includă cel puțin cerințele minime stabilite în tabelul 2.

Tabelul 2

Cerințe minime privind conținutul mesajelor XML

Antet comun		**Obligatorie**
Version (versiune)	Versiunea oficială a specificațiilor XML va fi specificată prin spațiul de nume (namespace) definit în XSD a mesajului și în atributul „versiune” (version) din elementul antet al oricărui mesaj XML. Numărul versiunii („n.m”) va fi definit ca valoare fixă la fiecare lansare a fișierului de definiție a schemei XML (xsd).	Da
Test Identifier (identificator de testare)	ID opțional pentru testare. Inițiatorul testului va completa ID-ul, iar toți ceilalți participanți la fluxul de lucru vor redirecționa/returna același ID. În producție, el trebuie ignorat și nu va fi folosit dacă este furnizat.	Nu
Technical Identifier (identificator tehnic)	Un UUID care identifică în mod unic fiecare mesaj în parte. Expeditorul generează un UUID și completează acest atribut. Aceste date nu se folosesc în niciun scop legat de activități economice.	Da
Workflow Identifier (identificator al fluxului de lucru)	Identificatorul fluxului de lucru este un UUID și trebuie să fie generat de partea solicitantă. Acest ID este apoi utilizat în toate mesajele pentru a corela fluxul de lucru.	Da
Sent At (trimis la)	Data și ora (UTC) la care a fost trimis mesajul.	Da
Timeout (timpul a expirat)	Acesta este un atribut opțional privind data și ora (în format UTC). Această valoare va fi stabilită doar de nodul central pentru cererile redirecționate. Ea va informa partea respondentă cu privire la ora la care expiră cererea. Această valoare nu este necesară în MS2TCN_<x>_Req și în niciun mesaj de răspuns. Ea este opțională, pentru a permite utilizarea aceleiași definiții de antet pentru toate tipurile de mesaje, indiferent dacă atributul „timeoutValue” este necesar sau nu.	Nu
De la	Codul ISO 3166-1 alfa 2 al părții care transmite mesajul sau „UE”.	Da
Către	Codul ISO 3166-1 alfa 2 al părții căreia i se transmite mesajul sau „UE”.	Da

Subapendicele 4.4

Servicii de transliterare și NYSIIS (New York State Identification and Intelligence System)

1. Algoritmul NYSIIS implementat în nodul central este folosit pentru a codifica numele tuturor conducătorilor auto în registrul național.

2. La căutarea unui card prin intermediul funcției CIC se utilizează cheile NYSIIS ca mecanism principal de căutare.

3. În plus, părțile pot utiliza un algoritm personalizat, pentru a obține rezultate suplimentare.

4. Rezultatele căutării trebuie să indice mecanismul de căutare care a fost utilizat pentru a găsi o înregistrare, fie NYSIIS, fie un algoritm personalizat.

5. Dacă o parte alege să înregistreze notificările ICDL, atunci cheile NYSIIS conținute în notificare se înregistrează ca parte a datelor ICDL. La căutarea datelor ICDL, partea respectivă utilizează cheile NYSIIS ale numelui solicitantului.

Subapendicele 4.5

Cerințe de securitate

1. Pentru schimbul de mesaje între nodul central și sistemele naționale se utilizează protocolul HTTPS.

2. Sistemele naționale trebuie să utilizeze certificatele digitale menționate în subapendicele 4.8 și 4.9 pentru a securiza transmiterea mesajelor între sistemul național și nodul central.

3. Sistemele naționale trebuie să implementeze cel puțin certificate care folosesc algoritmul hash semnătură SHA-2 (SHA-256) și o lungime a cheilor publice de 2048 de biți.

Subapendicele 4.6

Nivelurile serviciului

1. Sistemele naționale asigură următorul nivel minim al serviciului:

1.1. Sunt disponibile 24 de ore pe zi, 7 zile pe săptămână.

1.2. Disponibilitatea lor este monitorizată prin intermediul unui mesaj heartbeat emis de nodul central.

1.3. Rata lor de disponibilitate este de 98 %, în conformitate cu tabelul următor (cifrele au fost rotunjite la cea mai apropiată unitate):

O disponibilitate de	înseamnă o indisponibilitate de		
	Zilnică	Lunară	Anuală
98 %	0,5 ore	15 ore	7,5 zile

Părțile sunt încurajate să respecte rata de disponibilitate zilnică, însă se recunoaște faptul că anumite activități necesare, cum ar fi întreținerea sistemului, necesită o perioadă de indisponibilitate de peste 30 de minute. Cu toate acestea, ratele de disponibilitate lunare și anuale rămân obligatorii.

1.4. Sistemele naționale trebuie să răspundă la minimum 98 % din cererile redirecționate către ele într-o lună calendaristică.

1.5. Ele trebuie să răspundă cererilor în cel mult 10 secunde.

1.6. Timpul total până la expirarea cererii (timpul în care solicitantul poate să aștepte un răspuns) nu trebuie să depășească 20 de secunde.

1.7. Ele trebuie să fie capabile să prelucreze cereri la o rată de șase mesaje pe secundă.

1.8. Sistemele naționale nu pot transmite cereri către nodul TACHOnet la o rată care depășește două solicitări pe secundă.

1.9. Fiecare sistem național trebuie să fie capabil să facă față eventualelor probleme tehnice ale nodului central sau ale sistemelor naționale ale altor părți. Acestea includ, dar nu se limitează la:

(a) pierderea legăturii cu nodul central;

(b) neprimirea unui răspuns la o cerere;

(c) primirea răspunsurilor după ce mesajul a expirat;

(d) primirea de mesaje nesolicitate;

(e) primirea de mesaje incorecte.

2. Nodul central trebuie:

2.1. să aibă o rată de disponibilitate de 98 %;

2.2. să transmită către sistemele naționale notificări ale oricăror erori, fie prin intermediul mesajului de răspuns, fie prin intermediul unui mesaj de eroare specific. La rândul lor, sistemele naționale trebuie să primească aceste mesaje de eroare specifice și să dispună de un flux de lucru progresiv (escalation workflow) pentru a lua toate măsurile adecvate în vederea remedierii erorii notificate.

3. Întreținere

Părțile notifică celorlalte părți și Comisiei Europene, prin intermediul aplicației web, orice activități de întreținere de rutină, cu cel puțin o săptămână înainte de începerea respectivelor activități, dacă acest lucru este posibil din punct de vedere tehnic.

Subapendicele 4.7

Înregistrarea în jurnal și statisticile datelor colectate la nivelul nodului central

1. Pentru a se asigura confidențialitatea, datele colectate în scopuri statistice trebuie să fie anonimizate. Datele de identificare a unui anumit card, conducător auto sau permis de conducere trebuie să nu fie disponibile în scopuri statistice.

2. Informațiile înregistrate în jurnal trebuie să țină evidența tuturor tranzacțiilor, în scopul monitorizării și al corectării erorilor de sistem, și trebuie să permită generarea de statistici referitoare la respectivele tranzacții.

3. Datele cu caracter personal nu se păstrează în jurnale mai mult de șase luni. Informațiile statistice se păstrează pe o perioadă nedeterminată.

4. Datele statistice utilizate pentru raportare trebuie să includă:

   (a) partea solicitantă;

   (b) partea respondentă;

   (c) tipul de mesaj;

   (d) codul de stare al răspunsului;

   (e) data și ora mesajelor;

   (f) timpul de răspuns.

Subapendicele 4.8

Dispoziții generale privind cheile și certificatele digitale pentru TACHOnet

1. Direcția Generală Informatică a Comisiei Europene (DIGIT) pune la dispoziția părților contractante la AETR care se conectează la TACHOnet (prin urmare, autorităților naționale) un serviciu PKI[1] (denumit „serviciul PKI MIE”) prin intermediul eDelivery.

2. Procedura de solicitare și de revocare a certificatelor digitale, precum și termenele și condițiile detaliate pentru utilizarea lor sunt definite în apendice.

3. Utilizarea certificatelor:

3.1. Odată eliberat certificatul, autoritatea națională[2] trebuie să îl utilizeze numai în contextul TACHOnet. Certificatul poate fi utilizat pentru:

(a) autentificarea originii datelor;

(b) criptarea datelor;

(c) asigurarea detectării cazurilor de violare a integrității datelor.

3.2. Orice utilizare care nu este autorizată în mod explicit în cadrul utilizărilor permise ale certificatului este interzisă.

4. Părțile contractante trebuie:

(a) să își protejeze cheia privată împotriva utilizării neautorizate;

(b) să evite transferarea sau dezvăluirea cheii lor private către terți, chiar dacă aceștia au calitatea de reprezentanți;

---

1 O PKI (infrastructură de chei publice) este un set de roluri, de politici, de proceduri și de sisteme necesare pentru crearea, gestionarea, distribuirea și revocarea certificatelor digitale.

2 Identificat prin valoarea atributului „O=” din câmpul Subject Distinguished Name al certificatului eliberat.

(c) să asigure confidențialitatea, integritatea și disponibilitatea cheilor private generate, stocate și utilizate pentru TACHOnet;

(d) să evite utilizarea în continuare a cheii private după expirarea perioadei de valabilitate sau după revocarea certificatului, în alte scopuri decât pentru a vizualiza date criptate (de exemplu pentru a decripta e-mailuri). Cheile expirate trebuie distruse sau păstrate în așa fel încât să se împiedice utilizarea lor;

(e) să pună la dispoziția autorității de înregistrare datele de identificare ale reprezentanților autorizați care sunt autorizați să solicite revocarea certificatelor eliberate organizației (cererile de revocare trebuie să includă o parolă aferentă cererii de revocare și detalii privind evenimentele care au condus la revocare);

(f) să prevină utilizarea abuzivă a cheii private prin solicitarea revocării certificatului de cheie publică asociat în cazul compromiterii cheii private sau a datelor de activare a cheii private;

(g) să fie responsabile și să dețină obligația de a solicita revocarea certificatului în circumstanțele identificate în politicile de certificare (PC) și în declarația privind practicile de certificare (DPC) ale autorității de certificare;

(h) să notifice autorității de înregistrare, fără întârziere, pierderea, furtul sau potențiala compromitere a oricăror chei AETR utilizate în contextul TACHOnet.

5. Răspunderi

Fără a aduce atingere răspunderii Comisiei Europene într-un mod care contravine cerințelor stabilite în legislația națională aplicabilă sau cu privire la răspunderea legată de aspecte care nu pot fi excluse în temeiul legislației respective, Comisia Europeană nu deține responsabilitatea sau răspunderea pentru:

(a) conținutul certificatului, care îi revine exclusiv proprietarului certificatului. Este responsabilitatea proprietarului certificatului să verifice exactitatea conținutului certificatului;

(b) utilizarea certificatului de către proprietarul acestuia.

Subapendicele 4.9

Descrierea serviciului PKI pentru TACHOnet

1. Introducere

O PKI (infrastructură de chei publice) este un set de roluri, de politici, de proceduri și de sisteme necesare pentru crearea, gestionarea, distribuirea și revocarea certificatelor digitale[3]. Serviciul PKI MIE al eDelivery permite eliberarea și gestionarea certificatelor digitale utilizate pentru a asigura confidențialitatea, integritatea și nerepudierea informațiilor transmise între punctele de acces (PA).

Serviciul PKI al eDelivery se bazează pe serviciul TeleSec Shared Business CA (autoritate de certificare) care ține de serviciile de centru de încredere (Trust Center Services) și căruia i se aplică politica de certificare (PC) / declarația de practici de certificare (DPC) privind TeleSec Shared-Business-CA a companiei T-Systems International GmbH[4].

Serviciul PKI eliberează certificate adecvate pentru securizarea diverselor procese operaționale din cadrul și din afara companiilor, organizațiilor, autorităților publice și instituțiilor care necesită un nivel de securitate mediu pentru a demonstra autenticitatea, integritatea și credibilitatea entității finale.

2. Procesul de solicitare a certificatului

2.1. Roluri și responsabilități

2.1.1. „Organizația” sau „autoritatea națională” care solicită certificatul

2.1.1.1. Autoritatea națională trebuie să solicite certificatele în contextul proiectului TACHOnet.

2.1.1.2 Autoritatea națională trebuie:

(a) să solicite certificatele de la serviciul PKI MIE;

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

[4] Cea mai recentă versiune a PC și DPC pot fi descărcate de la adresa https://www.telesec.de/en/sbca-en/support/download-area/

(b) să genereze cheile private și cheile publice corespunzătoare ce trebuie incluse în certificatele eliberate de autoritatea de certificare;

(c) să descarce certificatul, atunci când acesta este aprobat;

(d) să semneze și să trimită înapoi autorității de înregistrare:

(i) formularul de identificare a persoanelor de contact și a curierilor de încredere,

(ii) procura individuală semnată[5].

2.1.2. Curierul de încredere

2.1.2.1. Autoritatea națională desemnează un curier de încredere.

2.1.2.2. Curierul de încredere trebuie:

(a) să predea cheia publică autorității de înregistrare în decursul unui proces de identificare și de înregistrare față în față;

(b) să obțină certificatul corespunzător de la autoritatea de înregistrare.

2.1.3. Proprietarul domeniului

2.1.3.1. DG MOVE este proprietarul domeniului.

2.1.3.2. Proprietarul domeniului trebuie:

(a) să valideze și să coordoneze rețeaua TACHOnet și arhitectura de încredere TACHOnet, inclusiv validarea procedurilor de eliberare a certificatelor;

(b) să exploateze nodul central al TACHOnet și să coordoneze activitatea părților în ceea ce privește funcționarea TACHOnet;

(c) să efectueze, împreună cu autoritățile naționale, testele de conectare la TACHOnet.

5 O procură este un document juridic prin care organizația împuternicește și autorizează Comisia Europeană, reprezentată de funcționarul identificat responsabil pentru serviciul PKI MIE, să solicite generarea unui certificat în numele său de la autoritatea de certificare TeleSec Shared Business CA a T-Systems International GmbH. A se vedea, de asemenea, punctul 6.

2.1.4. Autoritatea de înregistrare

2.1.4.1. Centrul Comun de Cercetare (JRC) este autoritatea de înregistrare.

2.1.4.2. Autoritatea de înregistrare este responsabilă cu verificarea identității curierului de încredere și cu înregistrarea și aprobarea cererilor de eliberare, de revocare și de reînnoire a certificatelor digitale.

2.1.4.3. Autoritatea de înregistrare trebuie:

(a) să atribuie identificatorul unic autorității naționale;

(b) să autentifice identitatea autorității naționale, a punctelor sale de contact și a curierilor săi de încredere;

(c) să comunice cu echipa de asistență a MIE în ceea ce privește autenticitatea autorității naționale, a punctelor sale de contact și a curierilor săi de încredere;

(d) să informeze autoritatea națională cu privire la aprobarea sau la respingerea certificatului.

2.1.5. Autoritatea de certificare

2.1.5.1. Autoritatea de certificare este responsabilă cu punerea la dispoziție a infrastructurii tehnice pentru solicitarea, eliberarea și revocarea certificatelor digitale.

2.1.5.2. Autoritatea de certificare trebuie:

(a) să pună la dispoziție infrastructura tehnică pentru depunerea de cereri de certificate de către autoritățile naționale;

(b) să valideze sau să respingă cererea de certificat;

(c) să comunice cu autoritatea de înregistrare pentru verificarea identității organizației solicitante, atunci când este necesar.

2.2. Eliberarea certificatelor

2.2.1. Eliberarea certificatelor se efectuează conform următoarelor etape succesive, reprezentate în figura 1:

(a) **etapa 1:** identificarea curierului de încredere;

(b) **etapa 2:** crearea cererii de certificat;

(c) **etapa 3:** înregistrarea la autoritatea de înregistrare;

(d) **etapa 4:** generarea certificatului;

(e) **etapa 5:** publicarea certificatului;

(f) **etapa 6:** acceptarea certificatului.

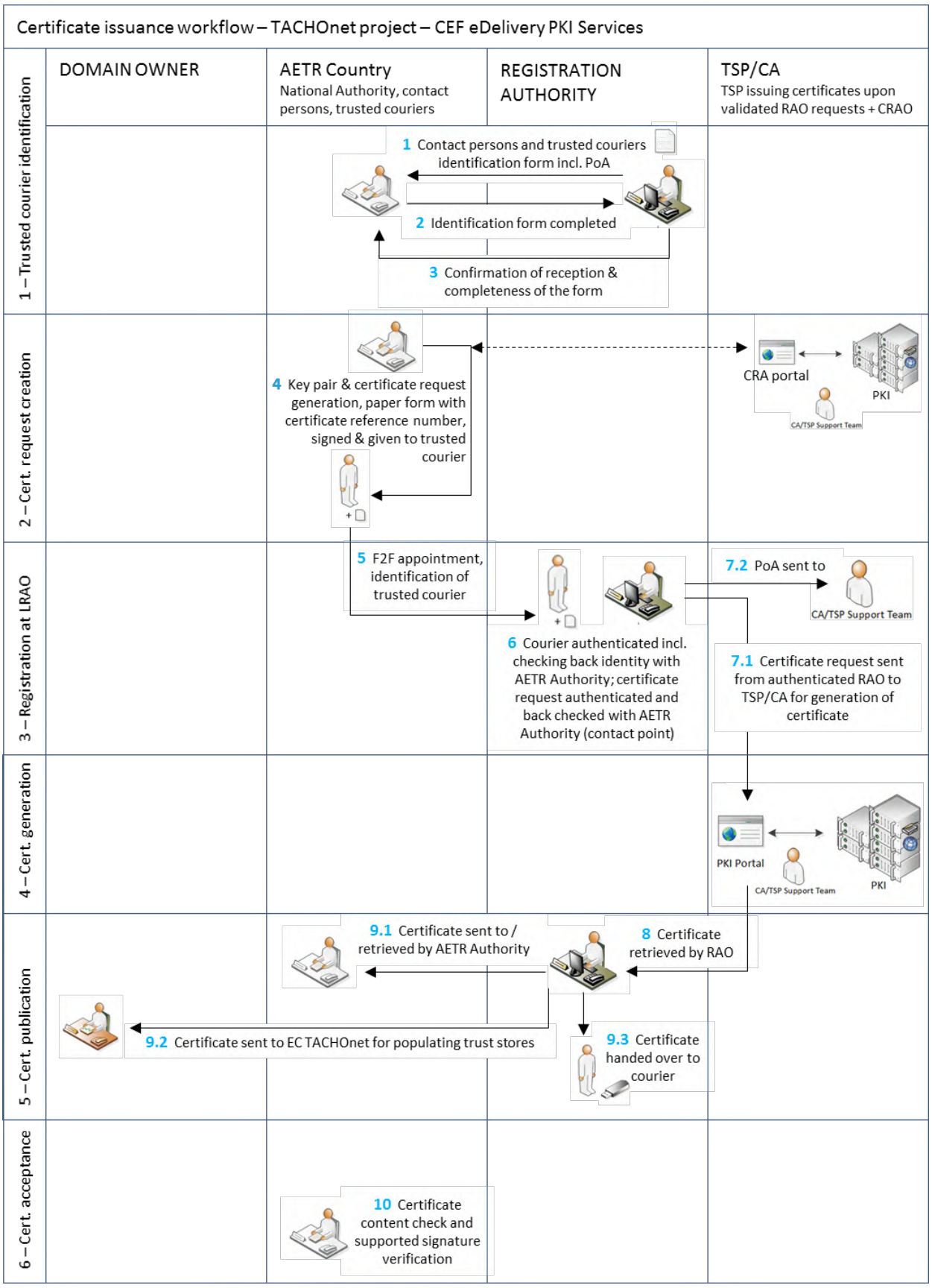


Figura 1 - Fluxul de lucru pentru eliberarea certificatelor

2.2.2. etapa 1: identificarea curierului de încredere

Pentru identificarea curierului de încredere trebuie urmat procesul de mai jos:

(a) autoritatea de înregistrare transmite autorității naționale formularul de identificare a persoanelor de contact și al curierilor de încredere[6]. Acest formular trebuie să includă, de asemenea, o procură pe care organizația (autoritatea AETR) trebuie să o semneze;

(b) autoritatea națională transmite înapoi autorității de înregistrare formularul completat și procura semnată;

(c) autoritatea de înregistrare confirmă primirea corespunzătoare și integralitatea formularului;

(d) autoritatea de înregistrare transmite proprietarului domeniului o copie actualizată a listei persoanelor de contact și a curierilor de încredere.

2.2.3. etapa 2: crearea cererii de certificat

2.2.3.1. Solicitarea și recuperarea certificatului trebuie să se efectueze pe același computer și cu același browser.

2.2.3.2. Pentru crearea cererii de certificat trebuie urmat procesul de mai jos:

(a) organizația navighează către interfața web pentru utilizatori în vederea solicitării certificatului prin intermediul URL https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: și introduce numele de utilizator „**sbca/CEF_eDelivery.europa.eu**” și parola „**digit.333**”;

6 A se vedea punctul 5.

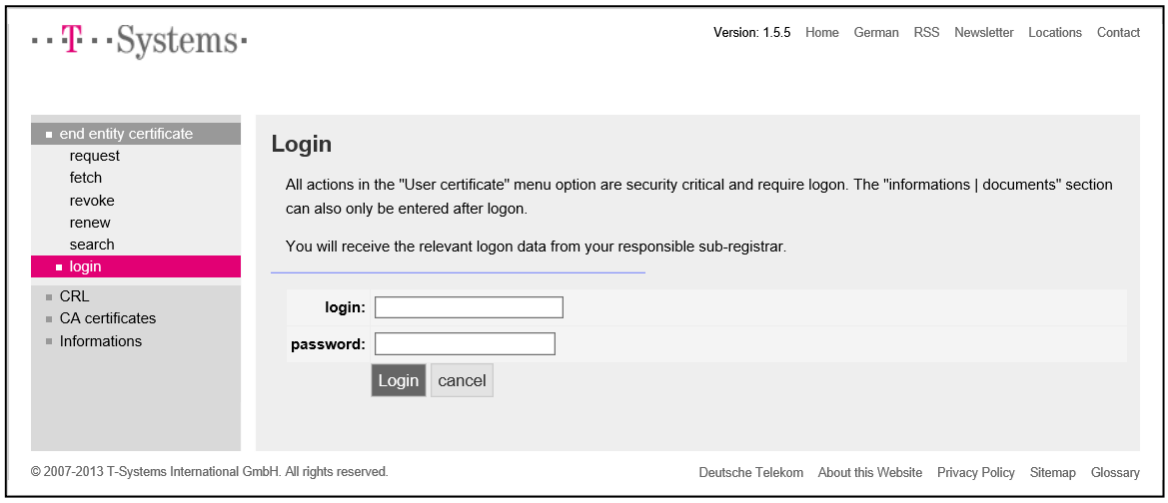


Figura 2

(b) organizația face clic pe „request” în meniul din partea stângă și selectează „CEF_TACHOnet” din lista verticală;

Figura 3

(c) organizația completează formularul de cerere a certificatului prezentat în figura 4 cu informațiile din tabelul 3 și face clic pe „Next (soft-PSE)” pentru a finaliza procesul;

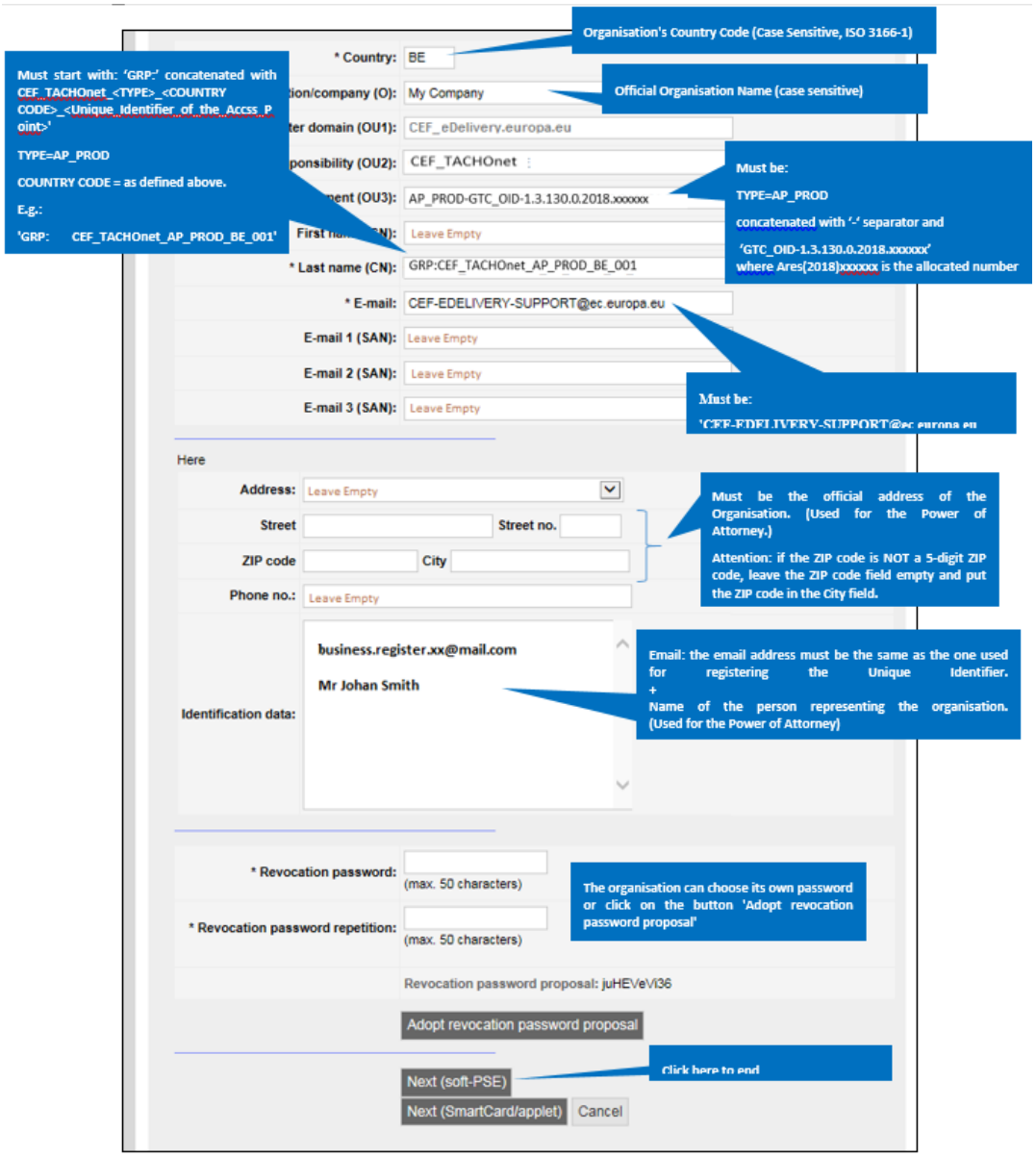

Organisation's Country Code (Case Sensitive, ISO 3166-1)
Official Organisation Name (case sensitive)
Must start with: 'GRP:' concatenated with CEF_TACHOnet_<TYPE>_<COUNTRY CODE>_<Unique_Identifier_of_the_Accss_Point>'
TYPE=AP_PROD
COUNTRY CODE = as defined above.
E.g.:
'GRP: CEF_TACHOnet_AP_PROD_BE_001'
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
Leave Empty
Leave Empty
Leave Empty
Here
Address:
Leave Empty
Street
Street no.
ZIP code
City
Phone no.:
Leave Empty
business.register.xx@mail.com
Mr Johan Smith
Identification data:
* 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

Figura 4

Câmpuri solicitate	Descriere
Country (țară)	**C=codul țării**, locul unde se află proprietarul certificatului, verificat cu ajutorul unui registru public; Restricții: două caractere, în conformitate cu ISO 3166-1, alpha-2, sensibil la scrierea cu literă majusculă sau cu literă minusculă; Exemple: DE, BE, NL, Cazuri specifice: UK (pentru Marea Britanie), EL (pentru Grecia)
Organisation/Company (O) (organizație/companie)	**O=denumirea organizației proprietarului certificatului**
Master domain (OU1) (domeniu principal)	**OU=CEF_eDelivery.europa.eu**
Area of responsibility (OU2) (domeniul de responsabilitate)	**OU=CEF_TACHOnet**
Department (OU3) (departament)	Valoare obligatorie per „AREA OF RESPONSIBILITY” Conținutul trebuie verificat cu ajutorul unei liste pozitive (listă albă) în momentul solicitării certificatului. Dacă informațiile nu corespund listei, cererea nu se transmite. Format: **OU=<TYPE>-<GTC_NUMBER>** Unde „<TYPE >” se înlocuiește cu AP_PROD: Access Point in Production environment (punct de acces în mediul de producție). Și unde <GTC_NUMBER> este **GTC_OID-1.3.130.0.2018.xxxxxx**, unde Ares(2018)xxxxxx este numărul GTC pentru proiectul TACHOnet. De exemplu: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN) (prenume)	Trebuie să rămână necompletat
Last name (CN) (nume)	Trebuie să înceapă cu „GRP:”, urmat de un nume comun. Format: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** De exemplu: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
E-mail 1 (SAN)	Trebuie să rămână necompletat
E-mail 2 (SAN)	Trebuie să rămână necompletat
E-mail 3 (SAN)	Trebuie să rămână necompletat

Address (adresa)	Trebuie să rămână necompletat
Street (strada)	Trebuie să fie adresa oficială a organizației proprietarului certificatului. (Utilizată pentru procură).
Street no. (numărul străzii)	Trebuie să fie adresa oficială a organizației proprietarului certificatului. (Utilizată pentru procură).
Zip Code (codul poștal)	Trebuie să fie adresa oficială a organizației proprietarului certificatului. (Utilizată pentru procură). **Atenție**: în cazul în care codul poștal NU este un cod din cinci cifre, lăsați necompletat câmpul „ZIP Code” și înscrieți codul poștal în câmpul „City”.
City (localitatea)	Trebuie să fie adresa oficială a organizației proprietarului certificatului. (Utilizată pentru procură). **Atenție**: în cazul în care codul poștal NU este un cod din cinci cifre, lăsați necompletat câmpul „ZIP Code” și înscrieți codul poștal în câmpul „City”.
Phone no (numărul de telefon)	Trebuie să rămână necompletat
Identification data (date de identificare)	Adresa de e-mail trebuie să fie aceeași ca cea utilizată pentru înregistrarea identificatorului unic. + Trebuie să fie numele persoanei care reprezintă organizația. (Utilizată pentru procură) + **Numărul din Registrul Comerțului** (obligatoriu numai pentru organizațiile private) **Înscrisă la tribunalul local din** (obligatoriu numai pentru organizațiile private din Germania și din Austria)
Revocation password (parola de revocare)	Câmp obligatoriu ales de solicitant
Revocation password repetition (repetarea parolei de revocare)	Câmp obligatoriu ales de solicitant, repetat

Tabelul 3. Detalii complete privind fiecare câmp solicitat

(d) lungimea cheii selectate este de 2048 (categorie superioară);

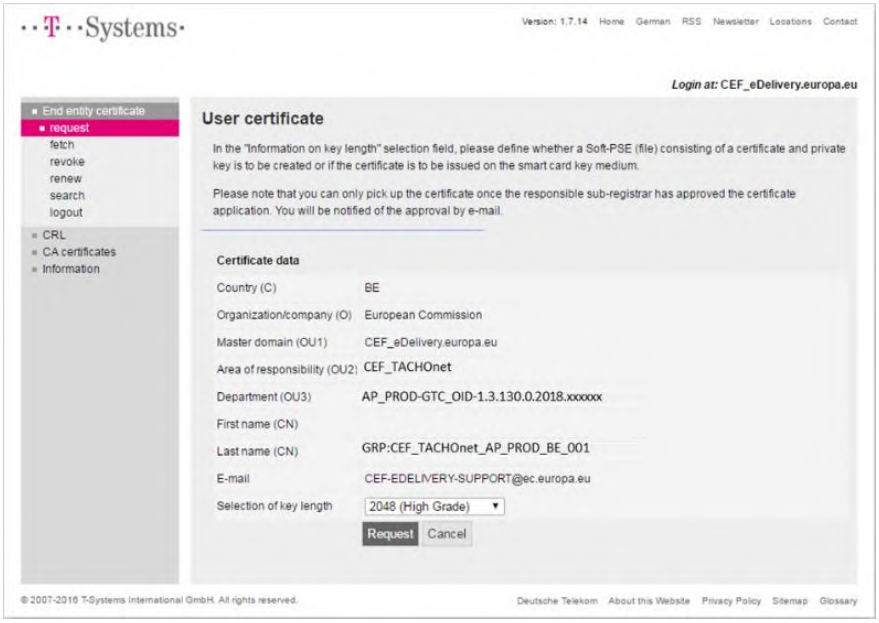


Figura 5

(e) organizația înregistrează numărul de referință pentru a recupera certificatul;

Figura 6

(f) echipa de asistență a MIE verifică dacă există noi cereri de certificate și dacă informațiile din cererile de certificate sunt valabile, adică dacă respectă convenția de denumire specificată în apendicele 5.1 „Convenție de denumire pentru certificat”;

(g) echipa de asistență a MIE verifică dacă informațiile introduse în cerere sunt într-un format valabil.

(h) Atunci când oricare dintre verificările de la punctele 5 sau 6 de mai sus eșuează, echipa de asistență a MIE transmite la adresa de e-mail furnizată în câmpul „Identification data” al formularului de cerere, punând în copie proprietarul domeniului, un e-mail prin care organizația este invitată să demareze din nou procesul. Cererea de certificat eșuată se anulează;

(i) echipa de asistență a MIE transmite autorității de înregistrare un e-mail cu privire la valabilitatea cererii. Acest e-mail trebuie să includă:

(1) denumirea organizației, disponibilă în câmpul „Organisation (O)” al cererii de certificat;

(2) datele certificatului, inclusiv denumirea PA pentru care urmează să fie eliberat certificatul, disponibilă în câmpul „Last Name (CN)” al cererii de certificat;

(3) numărul de referință al certificatului;

(4) adresa organizației, adresa de e-mail a acesteia și numele persoanei care o reprezintă.

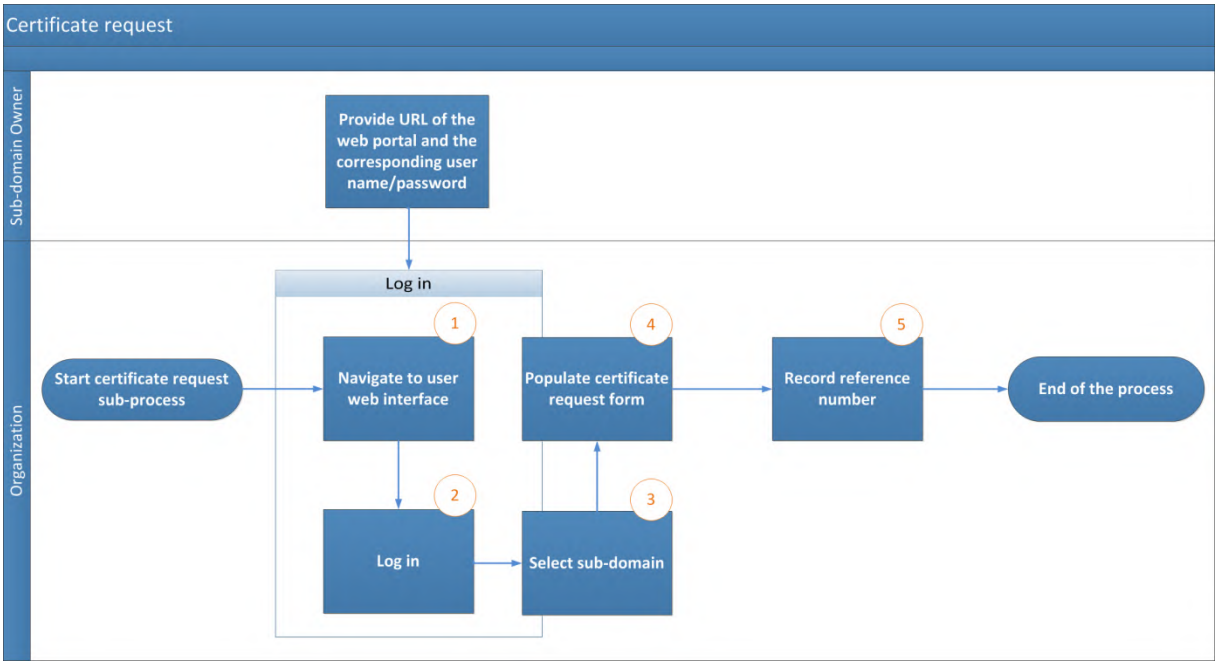


Figura 7 – Procesul de solicitare a certificatului

2.2.4. etapa 3: înregistrarea la autoritatea de înregistrare (aprobarea certificatului)

2.2.4.1. Curierul de încredere sau punctul de contact face o programare la autoritatea de înregistrare prin intermediul unui schimb de e-mailuri, identificând curierul de încredere care va participa la întâlnirea față în față.

2.2.4.2. Organizația pregătește pachetul de documente, care constă în:

(a) procura completată și semnată;

(b) o copie a pașaportului valabil al curierului de încredere care va participa la întâlnirea față în față. Această copie trebuie semnată de unul dintre punctele de contact ale organizației, identificate în cadrul etapei 1;

(c) formularul de cerere a certificatului pe hârtie, semnat de unul dintre punctele de contact ale organizației.

2.2.4.3. Autoritatea de înregistrare îl primește pe curierul de încredere după ce identitatea acestuia a fost verificată la recepția clădirii. Autoritatea de înregistrare efectuează înregistrarea față în față a cererii de certificat prin:

(a) identificarea și autentificarea curierului de încredere;

(b) verificarea înfățișării fizice a curierului de încredere pe baza pașaportului prezentat de curierul de încredere;

(c) verificarea valabilității pașaportului prezentat de curierul de încredere;

(d) verificarea pașaportului validat prezentat de curierul de încredere pe baza copiei pașaportului valabil al curierului de încredere semnate de unul dintre punctele de contact identificate ale organizației. Semnătura este autentificată pe baza originalului formularului de identificare a punctelor de contact și a curierilor de încredere;

(e) verificarea procurii completate și semnate;

(f) verificarea formularului de cerere a certificatului pe hârtie și a semnăturii sale, pe baza originalului formularului de identificare a punctelor de contact și a curierilor de încredere;

(g) apelarea punctului de contact semnatar pentru dubla verificare a identității curierului de încredere și a conținutului cererii de certificat.

2.2.4.4. Autoritatea de înregistrare confirmă echipei de asistență a MIE că autoritatea națională este într-adevăr autorizată să exploateze componentele pentru care solicită certificatele și că procesul de înregistrare față în față corespunzător s-a încheiat cu succes. Confirmarea trebuie transmisă printr-un email securizat cu un certificat de tip „CommiSign”, atașând o copie scanată a pachetului de documente autentificat prin procesul de înregistrare față în față și o copie scanată a listei semnate de verificare a procesului care a fost utilizată de autoritatea de înregistrare.

2.2.4.5. Dacă autoritatea de înregistrare confirmă valabilitatea cererii, procesul se desfășoară în continuare în conformitate cu indicațiile de la punctele 2.2.4.6 și 2.2.4.7. În caz contrar, se respinge eliberarea certificatului și se informează organizația în acest sens.

2.2.4.6. Echipa de asistență a MIE aprobă cererea de certificat și notifică autorității de înregistrare aprobarea certificatului.

2.2.4.7. Autoritatea de înregistrare informează organizația că certificatul poate fi recuperat prin intermediul portalului pentru utilizatori.

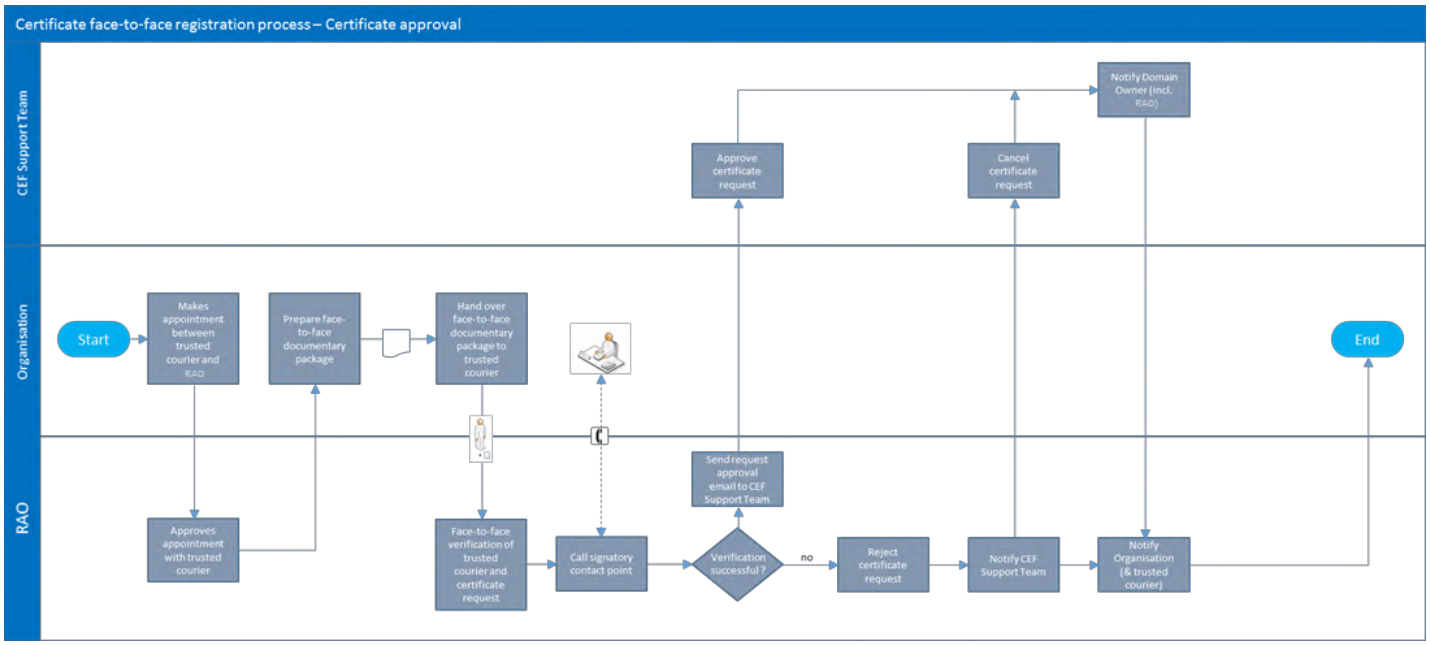


Figura 8 - Aprobarea certificatului

2.2.5. etapa 4: generarea certificatului

Odată aprobată cererea de certificat, certificatul este generat.

2.2.6. etapa 5: publicarea și recuperarea certificatului

2.2.6.1. În urma aprobării cererii de certificat, autoritatea de înregistrare recuperează certificatul și înmânează o copie curierului de încredere.

2.2.6.2. Organizația primește din partea autorității de înregistrare notificarea că certificatele pot fi recuperate.

2.2.6.3. Organizația trebuie să navigheze către portalul pentru utilizatori de la adresa https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en și să se autentifice folosind numele de utilizator „**sbca/CEF_eDelivery.europa.eu**” și parola „**digit.333**”.

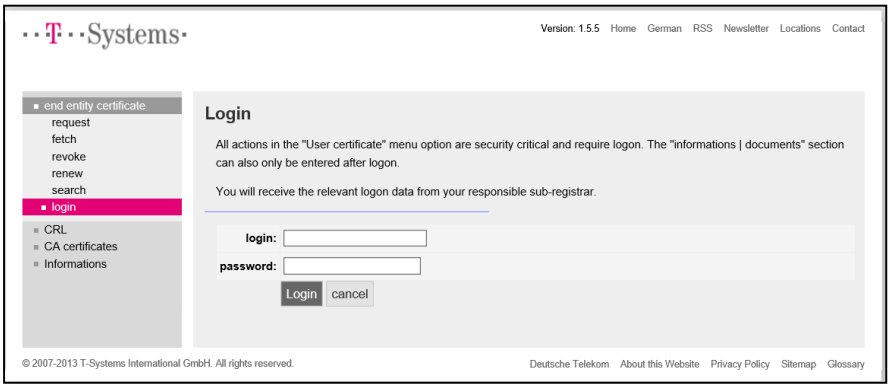


Figura 9

2.2.6.4. Organizația face clic pe butonul „fetch” din meniul din partea stângă și introduce numărul de referință înregistrat în timpul procesului de solicitare a certificatului.

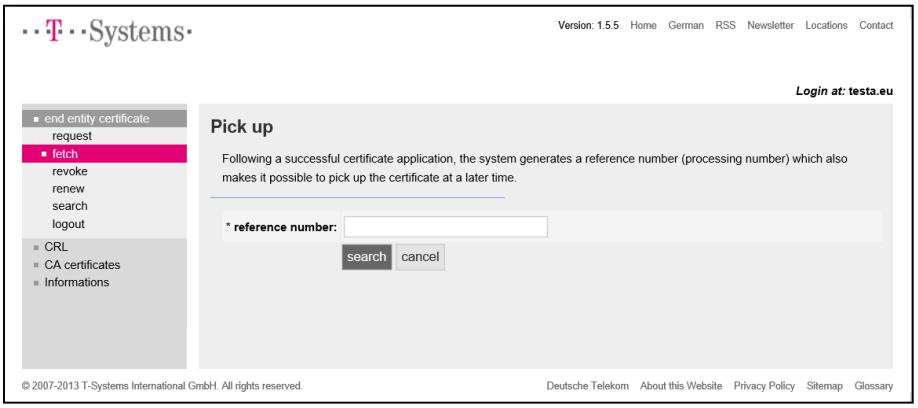


Figura 10

2.2.6.5. Organizația instalează certificatele făcând clic pe butonul „install”.

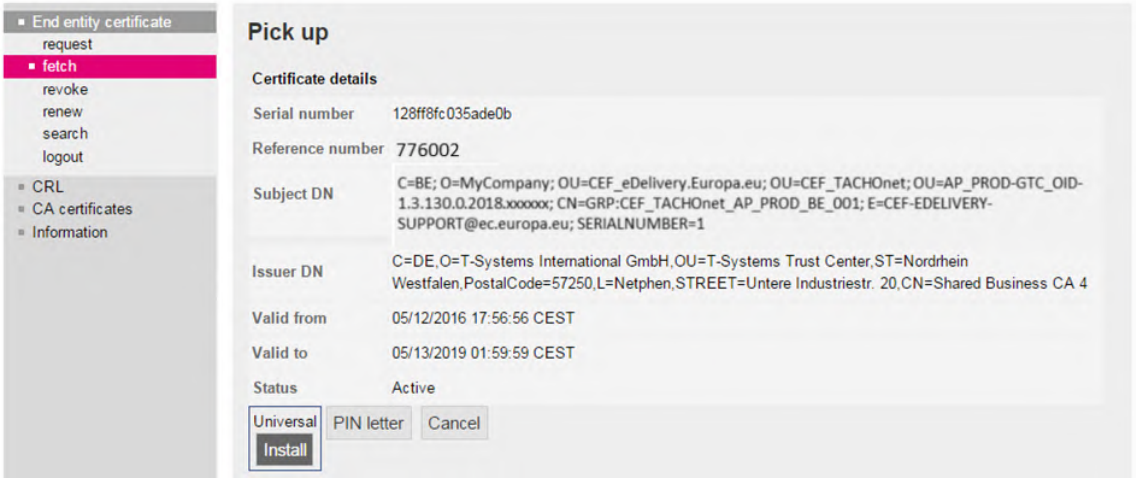


Figura 11

2.2.6.6. Certificatul trebuie instalat la punctul de acces. Deoarece instalarea este specifică implementării, organizația se consultă cu furnizorul său de punct de acces pentru a obține descrierea acestui proces.

2.2.6.7. Următoarele etape sunt necesare pentru instalarea certificatului la punctul de acces:

(a) exportarea cheii private și a certificatului;

(b) crearea registrului de chei (keystore) și a registrului de încredere (truststore);

(c) instalarea registrului de chei și a registrului de încredere la punctul de acces.

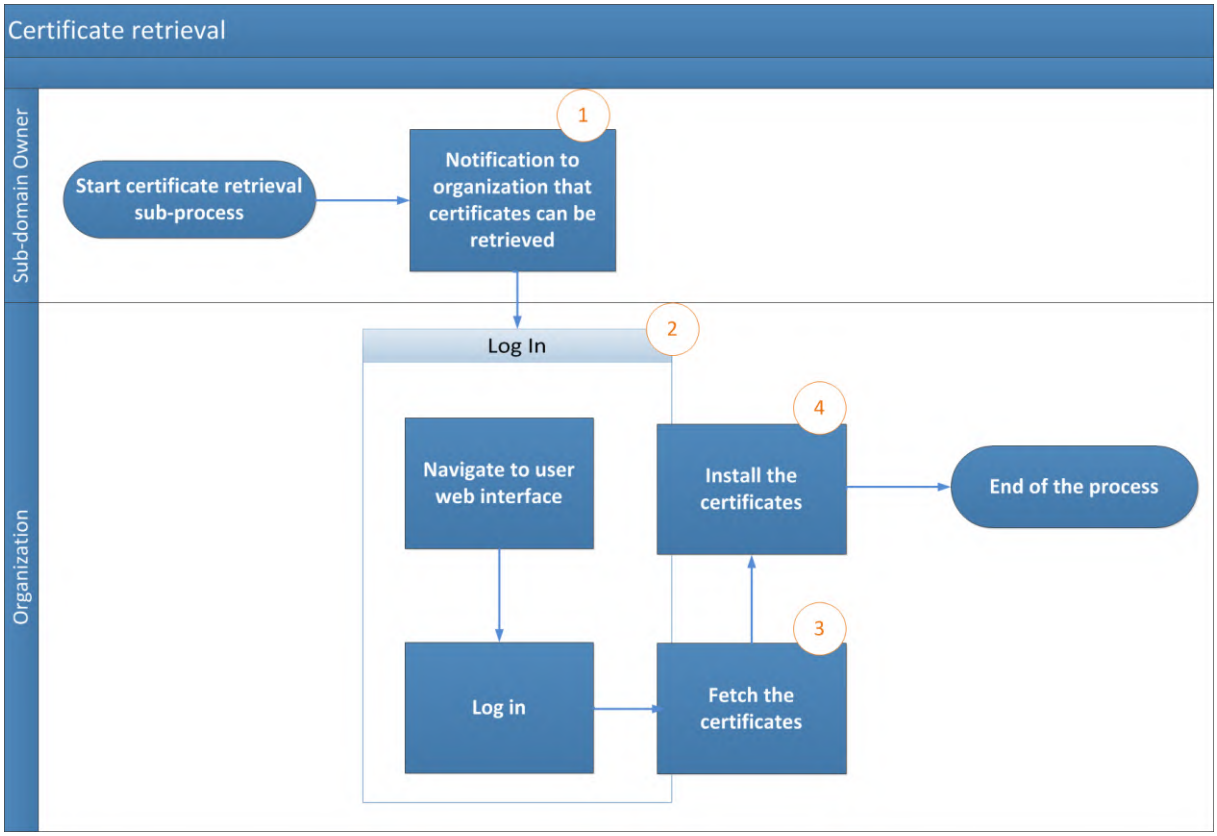


Figura 12 - Recuperarea certificatului

3. Procesul de revocare a certificatului

3.1. Organizația depune o cerere de revocare prin intermediul portalului pentru utilizatori.

3.2. Echipa de asistență a MIE execută revocarea certificatului.

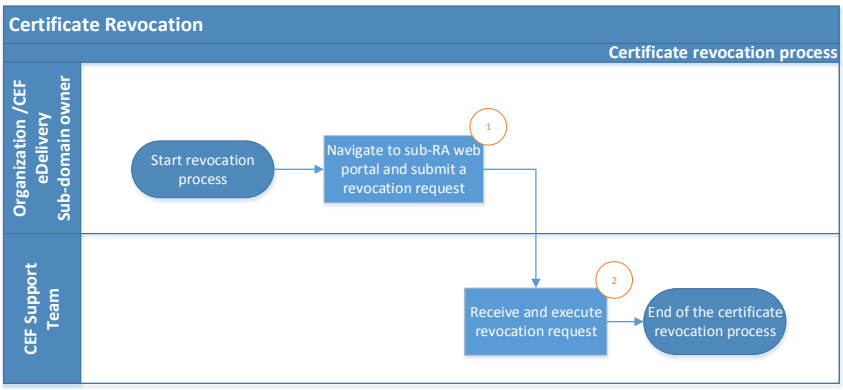


Figura 13 - Revocarea certificatului

4. Termenele și condițiile generale ale serviciului PKI MIE

4.1. Context

În calitatea sa de furnizor de soluție privind modulul e-Delivery al Mecanismului pentru interconectarea Europei, DIGIT pune la dispoziția părților contractante la AETR un serviciu PKI[7] („serviciul PKI MIE”). Serviciul PKI MIE trebuie utilizat de autoritățile naționale („utilizatorii finali”) care participă la TACHOnet.

DIGIT este un utilizator PKI în cadrul soluției TeleSec Shared-Business-CA („SBCA”) exploatate în cadrul Centrului de încredere (Trust Center) al grupului T-Systems International GmbH („T-Systems”[8]). DIGIT îndeplinește rolul de operator principal de registru (Master Registrar) al domeniului „CEF_eDelivery.europa.eu” al SBCA. În acest rol, DIGIT creează în cadrul domeniului „CEF_eDelivery.europa.eu” subdomenii pentru fiecare proiect care utilizează serviciul PKI MIE.

Prezentul document oferă detalii cu privire la termenele și condițiile subdomeniului TACHOnet. DIGIT îndeplinește rolul de suboperator de registru al acestui subdomeniu. În această calitate, DIGIT eliberează, revocă și reînnoiește certificatele aferente acestui proiect.

4.2. Declinarea responsabilității

Comisia Europeană nu își asumă nicio responsabilitate sau răspundere cu privire la conținutul certificatului, care îi revine în exclusivitate proprietarului certificatului. Este responsabilitatea proprietarului certificatului să verifice exactitatea conținutului certificatului.

Comisia Europeană nu își asumă nicio responsabilitate sau răspundere cu privire la utilizarea certificatului de către proprietarul acestuia care este o entitate juridică terță din afara Comisiei Europene.

---

7 O PKI (infrastructură de chei publice) este un set de roluri, de politici, de proceduri și de sisteme necesare pentru crearea, gestionarea, distribuirea și revocarea certificatelor digitale.

8 În cadrul rolului său de încredere, operatorul Centrului de încredere, aflat în cadrul Centrului de încredere al T-Systems, îndeplinește, de asemenea, și sarcina de autoritate de înregistrare internă.

Prezenta declinare a responsabilității nu are ca scop limitarea răspunderii Comisiei Europene într-un mod care contravine cerințelor stabilite în legislația națională aplicabilă și nici excluderea răspunderii sale în ceea ce privește aspecte care nu pot fi excluse în temeiul legislației respective.

4.3. Utilizări autorizate/interzise ale certificatelor

4.3.1. Utilizări permise ale certificatelor

Odată eliberat certificatul, proprietarul certificatului[9] trebuie să îl utilizeze numai în contextul TACHOnet. În acest context, certificatul poate fi utilizat pentru:

- autentificarea originii datelor;
- criptarea datelor;
- asigurarea detectării cazurilor de violare a integrității datelor.

4.3.2. Utilizări interzise ale certificatelor

Orice utilizare care nu este autorizată în mod explicit în cadrul utilizărilor permise ale certificatului este interzisă.

4.4. Obligații suplimentare ale proprietarului certificatului

Termenele și condițiile detaliate ale SBCA sunt definite de T-Systems în politica de certificare (PC) / declarația de practici de certificare (DPC) pentru serviciul SBCA[10]. Acest document include specificații și orientări în materie de securitate privind aspectele tehnice și organizatorice și descrie activitățile operatorului Centrului de încredere în rolurile de autoritate de certificare (CA) și de autoritate de înregistrare (RA), precum și ale părții terțe delegate de autoritatea de înregistrare (RA).

Numai entitățile autorizate să participe la TACHOnet pot solicita un certificat.

---

9 Identificat prin valoarea atributului „O=” din câmpul Subject Distinguished Name al certificatului eliberat.

10 Cea mai recentă versiune a PC/DPC pentru SBCA T-Systems este disponibilă la adresa https://www.telesec.de/en/sbca-en/support/download-area/.

În ceea ce privește acceptarea certificatului, se aplică clauza 4.4.1 din politica de certificare și din declarația privind practicile de certificare („PC/DPC”) ale SBCA; în plus, se consideră că termenele de utilizare și dispozițiile descrise în prezentul document au fost acceptate de organizația căreia i se eliberează certificatul („O =”) atunci când acesta este utilizat pentru prima dată.

În ceea ce privește publicarea certificatului, se aplică clauza 2.2 din PC/DPC ale SBCA.

Toți proprietarii de certificate trebuie să respecte următoarele cerințe:

(1) să își protejeze cheia privată împotriva utilizării neautorizate;

(2) să evite transferarea sau dezvăluirea cheii lor private către terți, chiar dacă aceștia au calitatea de reprezentanți;

(3) să evite utilizarea în continuare a cheii private după expirarea perioadei de valabilitate sau după revocarea certificatului, în alte scopuri decât pentru a vizualiza date criptate (de exemplu pentru a decripta e-mailuri).

(4) proprietarul certificatului este responsabil pentru copierea sau transmiterea cheii către entitatea sau entitățile finale;

(5) proprietarul certificatului trebuie să oblige entitatea finală/toate entitățile finale să respecte prezentele termene și condiții, inclusiv PC/DPC ale SBCA, atunci când folosesc cheia privată;

(6) proprietarul certificatului trebuie să furnizeze datele de identificare ale reprezentanților autorizați care sunt autorizați să solicite revocarea certificatelor eliberate organizației pe baza detaliilor privind evenimentele care au dus la revocare și a parolei de revocare;

(7) pentru certificatele asociate unor grupuri de persoane și funcții și/sau persoane juridice, după ce o persoană părăsește grupul de entități finale (de exemplu la încetarea raportului de muncă), proprietarul certificatului trebuie să prevină utilizarea abuzivă a cheii private prin revocarea certificatului;

(8) proprietarul certificatului este responsabil și trebuie să solicite revocarea certificatului în circumstanțele menționate în clauza 4.9.1 din PC/DPC ale SBCA.

În ceea ce privește reînnoirea certificatului sau stabilirea altor chei pentru acesta, se aplică clauza 4.6 sau 4.7 din PC/DPC ale SBCA.

În ceea ce privește modificarea certificatului, se aplică clauza 4.8 din PC/DPC ale SBCA.

În ceea ce privește revocarea certificatului, se aplică clauza 4.9 din PC/DPC ale SBCA.

5. Formularul de identificare a persoanelor de contact și a curierilor de încredere (model)

Subsemnatul/a, [numele și adresa reprezentantului organizației], certific că următoarele informații trebuie utilizate în contextul solicitării, generării și recuperării certificatelor digitale de chei publice pentru punctele de acces TACHOnet care sprijină confidențialitatea, integritatea și nerepudierea mesajelor TACHOnet:

Informații privind persoana de contact**:**

– **Persoana de contact 1**	– **Persoana de contact 2**
– Nume:	– Nume:
– Prenume:	– Prenume:
– Telefon mobil:	– Telefon mobil:
– Telefon:	– Telefon:
– E-mail:	– E-mail:
– Specimen de semnătură olografă: –	– Specimen de semnătură olografă: – – –

Informații privind curierul de încredere**:**

– **Curierul de încredere 1**	– **Curierul de încredere 2**
– Nume:	– Nume:
– Prenume:	– Prenume:
– Telefon mobil:	– Telefon mobil:
– E-mail:	– E-mail:
– Țara care a eliberat pașaportul:	– Țara care a eliberat pașaportul:
– Pașaport nr.:	– Pașaport nr.:
– Data de expirare a valabilității pașaportului:	– Data de expirare a valabilității pașaportului:

Locul, data, ștampila companiei sau sigiliul organizației:

Semnătura reprezentantului autorizat:

6. Documente

6.1. Procură individuală (model)

Un model al procurii individuale care trebuie semnată și prezentată de curierul de încredere în cursul înregistrării față în față la autoritatea de înregistrare poate fi consultat la adresa:

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. Formular de cerere a certificatului pe hârtie (model)

Un model al formularului de cerere a certificatului pe hârtie care trebuie semnat și prezentat de curierul de încredere în cursul înregistrării față în față la autoritatea de înregistrare poate fi consultat la adresa:

7. Glosar

Termenii importanți utilizați în prezentul subapendice sunt definiți în secțiunea privind definițiile MIE a portalului web unic digital al MIE:

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

Acronimele importante utilizate în prezenta descriere a ofertei de componente sunt definite în glosarul MIE de pe portalul web unic digital al MIE:

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