

Brussel, 5 november 2018  
(OR. en)

---

Interinstitutioneel dossier:  
2018/0339(NLE)

---

13711/18  
ADD 1

TRANS 488

**NOTA**

|                 |                                                                                                                                                                                                                                                                                                                                  |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| van:            | het secretariaat-generaal van de Raad                                                                                                                                                                                                                                                                                            |
| aan:            | de delegaties                                                                                                                                                                                                                                                                                                                    |
| nr. vorig doc.: | ST 13711/18 TRANS 448                                                                                                                                                                                                                                                                                                            |
| Nr. Comdoc.:    | ST 12727/18 TRANS 426 + ADD 1                                                                                                                                                                                                                                                                                                    |
| Betreft:        | Besluit van de Raad inzake het standpunt dat namens de Europese Unie moet worden ingenomen in de deskundigengroep inzake de Europese Overeenkomst nopens de arbeidsvoorwaarden voor de bemanningen van motorrijtuigen in het internationale vervoer over de weg van de Economische Commissie voor Europa van de Verenigde Naties |

Bijlage bij bovengenoemd besluit van de Raad.

**Nieuw aanhangsel bij de AETR**

**Aanhangsel 4**

**TACHOnet-specificaties**

1. Toepassingsgebied en doel
  - 1.1. In dit aanhangsel worden de voorwaarden uiteengezet voor de aansluiting op TACHOnet via eDelivery van de overeenkomstsluitende partijen bij de AETR.
  - 1.2. Overeenkomstsluitende partijen die via eDelivery op TACHOnet zijn aangesloten, houden zich aan de bepalingen van dit aanhangsel.
2. Definities
  - a) "overeenkomstsluitende partij" of "partij": elke overeenkomstsluitende partij bij de AETR;
  - b) "eDelivery": de door de Europese Commissie ontwikkelde dienst die het mogelijk maakt gegevens via elektronische middelen tussen derden over te brengen en die bewijs verschaft met betrekking tot de verwerking van de overgebrachte gegevens, met inbegrip van het bewijs van verzending en ontvangst van de gegevens, en die de overgebrachte gegevens beschermt tegen elk risico van onrechtmatige wijziging;
  - c) "TACHOnet": het systeem voor de elektronische uitwisseling van informatie over bestuurderskaarten tussen de overeenkomstsluitende partijen, zoals bedoeld in artikel 31, lid 2, van Verordening (EU) nr. 165/2014;
  - d) "centraal knooppunt": het informatiesysteem waarmee TACHOnet-berichten tussen de vragende en antwoordende partijen kunnen worden verstuurd;
  - e) "vragende partij": de overeenkomstsluitende partij die via TACHOnet een verzoek of mededeling verstuurt, welke vervolgens via het centraal knooppunt wordt verzonden naar de geschikte antwoordende partij;

- f) "antwoordende partij": de overeenkomstsluitende partij waaraan het verzoek of de mededeling via TACHOnet is gericht;
- g) "autoriteit die de kaarten afgeeft": de instantie die door een overeenkomstsluitende partij is gemachtigd voor de afgifte en het beheer van tachograafkaarten.

### 3. Algemene verantwoordelijkheden

- 3.1. Geen van de overeenkomstsluitende partijen mag namens een andere partij een overeenkomst voor de toegang tot TACHOnet sluiten of de andere overeenkomstsluitende partij op enige andere wijze vertegenwoordigen op grond van dit aanhangsel. Geen van de overeenkomstsluitende partijen mag optreden als subcontractant van de andere overeenkomstsluitende partij voor de in dit aanhangsel bedoelde verrichtingen.
  - 3.2. De overeenkomstsluitende partijen verschaffen via TACHOnet toegang tot hun nationaal register van bestuurderskaarten, op de wijze en met het dienstverleningsniveau zoals beschreven in subaanhangsel 4.6.
  - 3.3. De overeenkomstsluitende partijen stellen elkaar onverwijld in kennis van storingen of fouten die onder hun verantwoordelijkheid vallen en die de normale werking van TACHOnet in gevaar kunnen brengen.
  - 3.4. Elke partij benoemt een contactpersoon voor TACHOnet en stelt het AETR-secretariaat daarvan in kennis. Elke wijziging van het contactpunt moet schriftelijk aan het AETR-secretariaat worden meegedeeld.
- ### 4. Tests voor de aansluiting op TACHOnet
- 4.1. Een overeenkomstsluitende partij wordt op TACHOnet aangesloten nadat met succes verbindings-, integratie- en prestatietests zijn uitgevoerd volgens de instructies en onder het toezicht van de Europese Commissie.
  - 4.2. Als de voorafgaande tests mislukken, kan de Europese Commissie de testfase tijdelijk opschorten. De tests worden hernomen zodra de overeenkomstsluitende partij de Europese Commissie in kennis heeft gesteld van de vaststelling van de nodige technische verbeteringen op nationaal niveau, waardoor de voorafgaande tests met succes kunnen worden uitgevoerd.

4.3. De voorafgaande tests mogen maximaal zes maanden duren.

## 5. Trust-architectuur

5.1. De vertrouwelijkheid, de integriteit en de onweerlegbaarheid van de TACHOnet-berichten worden gewaarborgd door de trust-architectuur van TACHOnet.

5.2. De trust-architectuur van TACHOnet is gebaseerd op een door de Europese Commissie opgezette publieke-sleutelinfrastructuur (PKI) waarvan de vereisten zijn opgenomen in de subaanhangsels 4.8 en 4.9.

5.3. De volgende entiteiten zijn betrokken bij de trust-architectuur van TACHOnet:

- a) certificaatautoriteit, die verantwoordelijk is voor de aanmaak van de digitale certificaten die door de registratieautoriteit worden afgegeven aan de nationale autoriteiten van de overeenkomstsluitende partijen (via door hen aangestelde betrouwbare koeriers), en voor het opzetten van de technische infrastructuur voor de uitgave, de intrekking en de verlenging van digitale certificaten;
- b) domeineigenaar, die verantwoordelijk is voor de werking van het in subaanhangsel 4.1 bedoelde centrale knooppunt en voor de validering en de coördinatie van de trust-architectuur van TACHOnet;
- c) registratieautoriteit, die verantwoordelijk is voor de registratie en de goedkeuring van de verzoeken tot uitgave, intrekking en verlenging van digitale certificaten en voor de identiteitscontrole van de betrouwbare koeriers;
- d) betrouwbare koerier, de door de nationale autoriteiten aangestelde persoon die verantwoordelijk is voor de overhandiging van de publieke sleutel aan de registratieautoriteit en voor het verkrijgen van het overeenkomstige certificaat dat door de certificaatautoriteit wordt aangemaakt;
- e) nationale autoriteit van de overeenkomstsluitende partij, die:
  - i) de geheime sleutels en de overeenkomstige publieke sleutels aanmaakt die worden opgenomen in de certificaten die door de certificaatautoriteit worden aangemaakt;

- ii) de digitale certificaten opvraagt bij de certificatautoriteit;
- iii) de betrouwbare koerier aanstelt.

5.4. De certificatautoriteit en de registratieautoriteit worden aangesteld door de Europese Commissie.

5.5. Elke overeenkomstsluitende partij die op TACHOnet wordt aangesloten, moet in overeenstemming met subaanghangsel 4.9 verzoeken om de uitgave van een digitaal certificaat voor de ondertekening en versleuteling van een TACHOnet-bericht.

5.6. Een certificaat kan worden ingetrokken in overeenstemming met subaanghangsel 4.9.

## 6. Gegevensbescherming en vertrouwelijkheid

6.1. In overeenstemming met de gegevensbeschermingswetten op internationaal en nationaal niveau en in het bijzonder het Verdrag tot bescherming van personen met betrekking tot de geautomatiseerde verwerking van persoonsgegevens, stellen de partijen alle nodige technische en organisatorische maatregelen vast om de veiligheid van de TACHOnet-gegevens te waarborgen en de wijziging, het verlies en de onrechtmatige verwerking van of de onrechtmatige toegang tot dergelijke gegevens te voorkomen (met name de authenticiteit, vertrouwelijkheid, traceerbaarheid, integriteit, beschikbaarheid en onweerlegbaarheid van de gegevens en de beveiliging van de berichten).

6.2. Elke partij beschermt haar eigen nationale systeem tegen illegaal gebruik, kwaadaardige code, virussen, inbraak in computers, schendingen en geknoei met gegevens en andere soortgelijke daden van derden. De partijen stemmen ermee in commercieel redelijke inspanningen te leveren om de overdracht te vermijden van virussen, tijdbommen, wormen of soortgelijke items of computerprogramma's die de systemen van andere partijen kunnen verstoren.

## 7. Kosten

7.1. De overeenkomstsluitende partijen dragen zelf de ontwikkelings- en werkingskosten die nodig zijn om hun gegevenssystemen en -procedures te laten voldoen aan de verplichtingen van dit aanhangsel.

7.2. De in subaanhangsel 4.1 genoemde diensten van het centrale knooppunt zijn gratis.

## 8. Uitbesteding

8.1. De partijen mogen de diensten waarvoor zij volgens dit aanhangsel verantwoordelijk zijn, uitbesteden.

8.2. Uitbesteding ontslaat de partij niet van de verantwoordelijkheid uit hoofde van dit aanhangsel, met inbegrip van de verantwoordelijkheid voor een geschikt dienstverleningsniveau in overeenstemming met subaanhangsel 4.6.

## **Algemene aspecten van TACHOnet**

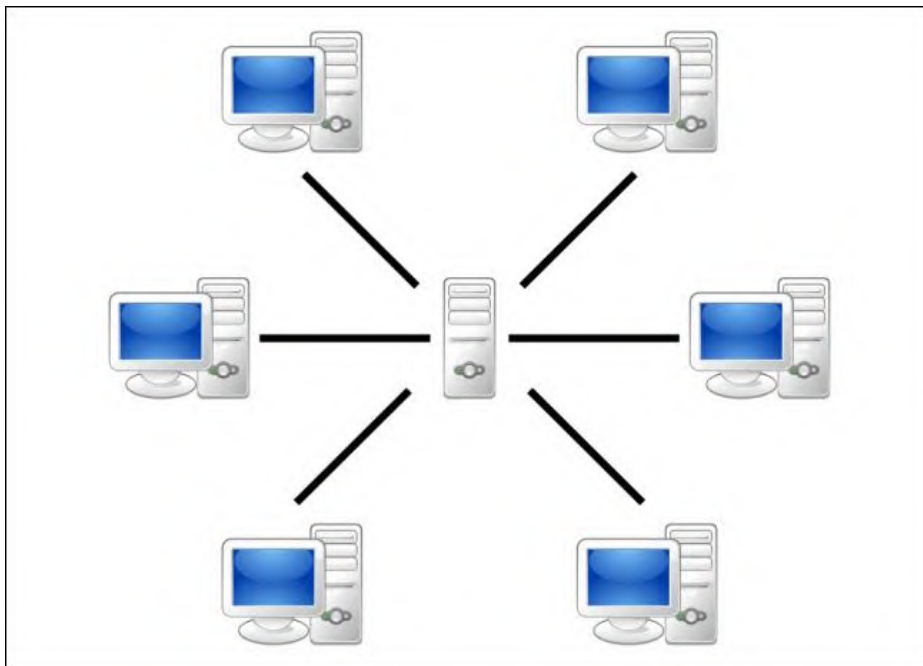
### **1. Algemene omschrijving**

TACHOnet is een elektronisch systeem voor de uitwisseling van informatie over bestuurderskaarten tussen de overeenkomstsluitende partijen van de AETR. TACHOnet verstuurt informatieverzoeken van vragende partijen naar antwoordende partijen, en verstuurt de antwoorden van de laatsten naar de eersten. Overeenkomstsluitende partijen die zijn aangesloten op TACHOnet, moeten hun nationale registers van bestuurderskaarten aansluiten op het systeem.

### **2. Architectuur**

Het TACHOnet-berichtensysteem bestaat uit de volgende onderdelen:

- 2.1. een centraal knooppunt, waarin een verzoek van een vragende partij wordt ontvangen, gevalideerd en verwerkt door dat naar de antwoordende partijen door te sturen. In het centrale knooppunt worden de reacties van de antwoordende partijen afgewacht, worden alle antwoorden geconsolideerd en wordt het geconsolideerde antwoord naar de vragende partij gestuurd;
- 2.2. de nationale systemen van de partijen, die worden uitgerust met een interface waarmee vragen naar het centrale knooppunt kunnen worden verzonden en de antwoorden daarop kunnen worden ontvangen. Om berichten met het centrale knooppunt uit te wisselen, kunnen de nationale systemen propriëtaire of commerciële software gebruiken.



### 3. Beheer

- 3.1. Het centrale knooppunt wordt beheerd door de Europese Commissie, die verantwoordelijk is voor de technische exploitatie en het onderhoud ervan.
- 3.2. In het centrale knooppunt worden gegevens niet langer dan zes maanden bewaard, behalve de in subaanhangel 4.7 genoemde logbestanden en statistische gegevens.
- 3.3. De persoonsgegevens in het centrale knooppunt zijn niet toegankelijk, behalve voor gemachtigd personeel van de Europese Commissie en als dat noodzakelijk is voor controle, onderhoud en het oplossen van problemen.
- 3.4. Elke overeenkomstsluitende partij is verantwoordelijk voor:
  - 3.4.1. het opzetten en beheren van zijn nationaal systeem, met inbegrip van de interface met het centrale knooppunt;
  - 3.4.2. de installatie en het onderhoud van het nationale systeem, zowel hardware als propriëtaire of commerciële software;
  - 3.4.3. de goede interoperabiliteit tussen het nationale systeem en het centrale knooppunt, met inbegrip van het beheer van foutmeldingen van het centrale knooppunt;
  - 3.4.4. alle maatregelen die moeten worden genomen om de vertrouwelijkheid, integriteit en beschikbaarheid van de informatie te waarborgen;
  - 3.4.5. de werking van het nationale systeem overeenkomstig de dienstverleningsniveaus in subaanhangel 4.6.



## Subaanhangsel 4.2

### Functies van TACHOnet

1. Het TACHOnet-berichtensysteem heeft de volgende functies:
  - 1.1. Check Issued Cards (CIC) (controle van afgegeven kaarten): de vragende partij kan een CIC-verzoek naar één of alle antwoordende partijen sturen om na te gaan of een aanvrager van een kaart reeds een door de antwoordende partijen afgegeven bestuurderskaart bezit. De antwoordende partijen beantwoorden het verzoek door een CIC-antwoord te sturen;
  - 1.2. Check Card Status (CCS) (controle van de kaartstatus): de vragende partij kan de antwoordende partij om bijzonderheden vragen over een kaart die door die laatste is afgegeven door een CCS-verzoek te sturen. De antwoordende partij beantwoordt de vraag door een CCS-antwoord te sturen;
  - 1.3. Modify Card Status (MCS) (wijzig kaartstatus): de vragende partij kan de antwoordende partij via een MCS-verzoek op de hoogte brengen van een wijziging van de status van een kaart die door de antwoordende partij is afgegeven. De antwoordende partij antwoordt met een MCS-bevestiging;
  - 1.4. Issued Card Driving Licence (ICDL) (kaart afgegeven voor een rijbewijs): de vragende partij kan de antwoordende partij via een ICDL-verzoek ervan op hoogte brengen dat de eerste een kaart heeft afgegeven voor een rijbewijs dat is afgegeven door de laatste. De antwoordende partij antwoordt met een ICDL-antwoord.
2. TACHOnet bevat ook andere soorten berichten die geschikt worden geacht voor het efficiënt functioneren, bijvoorbeeld foutmeldingen.
3. Nationale systemen herkennen de kaartstatussen die zijn vermeld in tabel 1 wanneer gebruik wordt gemaakt van een van de functies die zijn beschreven in punt 1. De partijen zijn echter niet verplicht om een administratieve procedure in te voeren waarbij alle vermelde statussen worden gebruikt.

4. Als een partij een antwoord of bericht ontvangt waarin een status wordt vermeld die niet in haar administratieve procedure wordt gebruikt, wordt de status van het ontvangen bericht door het nationale systeem omgezet in de overeenkomstige waarde van de administratieve procedure. Als de status van het bericht wordt vermeld in tabel 1, mag de antwoordende partij het bericht niet afwijzen.
5. De kaartstatus in tabel 1 mag niet worden gebruikt om na te gaan of een bestuurderskaart geldig is voor het besturen van voertuigen. Als een partij via de CCS-functie informatie opvraagt uit het register van de nationale autoriteit die de kaart heeft afgegeven, moet het antwoord het specifieke veld "geldig voor het besturen van een voertuig" bevatten. De nationale administratieve procedures moeten zo zijn opgesteld dat CCS-antwoorden altijd de toepasselijke waarde "geldig voor het besturen van een voertuig" bevatten.

Tabel 1  
**Kaartstatussen**

| <b>Card Status<br/>(kaartstatus)</b> | <b>Definitie</b>                                                                                                                                                                                                                        |
|--------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Toepassing                           | De autoriteit die de kaarten afgeeft (card issuing authority, CIA) heeft een verzoek ontvangen om een bestuurderskaart af te geven. Die informatie is geregistreerd en opgeslagen in de gegevensbank met de gegenereerde zoek sleutels. |
| Goedgekeurd                          | De CIA heeft de aanvraag voor de tachograafkaart goedgekeurd.                                                                                                                                                                           |
| Afgewezen                            | De CIA heeft de aanvraag niet goedgekeurd.                                                                                                                                                                                              |
| Op naam                              | De tachograafkaart is gepersonaliseerd.                                                                                                                                                                                                 |
| Verzonden                            | De nationale autoriteit heeft de bestuurderskaart naar de desbetreffende bestuurder of het afgevend agentschap gestuurd.                                                                                                                |
| Overhandigd                          | De nationale autoriteit heeft de bestuurderskaart overhandigd aan de desbetreffende bestuurder.                                                                                                                                         |
| In beslag genomen                    | De bevoegde autoriteit heeft de bestuurderskaart van de bestuurder afgenomen.                                                                                                                                                           |
| Geschorst                            | De bestuurderskaart is tijdelijk van de bestuurder afgenomen.                                                                                                                                                                           |
| Ingetrokken                          | De CIA heeft besloten de bestuurderskaart in te trekken. De kaart is definitief ongeldig gemaakt.                                                                                                                                       |
| Ingeleverd                           | De tachograafkaart is naar de CIA teruggestuurd met de verklaring dat ze niet langer nodig is.                                                                                                                                          |
| Verloren                             | De tachograafkaart is als verloren aangegeven bij de CIA.                                                                                                                                                                               |
| Gestolen                             | De tachograafkaart is als gestolen aangegeven bij de CIA. Een gestolen kaart wordt als verloren beschouwd.                                                                                                                              |
| Defect                               | De tachograafkaart is als defect aangegeven bij de CIA.                                                                                                                                                                                 |
| Verlopen                             | De geldigheidsperiode van de tachograafkaart is verstreken.                                                                                                                                                                             |
| Vervangen                            | De tachograafkaart, die als verloren, gestolen of defect is opgegeven, is vervangen door een nieuwe kaart. De gegevens op de nieuwe kaart zijn dezelfde, behalve de vervangingsindex van het kaartnummer, die met één is vermeerderd.   |

|                   |                                                                                                                                                                                                                                                |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Verlengd          | De tachograafkaart is verlengd omdat de administratieve gegevens zijn gewijzigd of de geldigheidsduur is verstreken. Het nummer van de nieuwe kaart is hetzelfde, behalve de vervangingsindex van het kaartnummer, die met één is vermeerderd. |
| Wordt ingewisseld | De CIA die een bestuurderskaart heeft afgegeven, heeft een bericht ontvangen dat de procedure voor de inwisseling van die kaart voor een bestuurderskaart die is afgegeven door de CIA van een andere partij, is begonnen.                     |
| Ingewisseld       | De CIA die een bestuurderskaart heeft afgegeven, heeft een bericht ontvangen dat de procedure voor de inwisseling van die kaart voor een bestuurderskaart die is afgegeven door de CIA van een andere partij, is voltooid.                     |

### Subaanhangsel 4.3

#### **Bepalingen voor berichten van TACHOnet**

1. Algemene technische vereisten
  - 1.1. Het centrale knooppunt beschikt over zowel synchrone als asynchrone interfaces voor de uitwisseling van berichten. De partijen kunnen kiezen voor de technologie die het best communiceert met hun eigen toepassingen.
  - 1.2. Alle berichten die tussen het centrale knooppunt en de nationale systemen worden uitgewisseld, moeten in UTF-8 worden opgesteld.
  - 1.3. De nationale systemen moeten berichten met Griekse of Cyrillische lettertekens kunnen ontvangen en verwerken.
2. XML-structuur van berichten en XML-schemadefinitie (XSD)
  - 2.1. De algemene structuur van XML-berichten beantwoordt aan het formaat dat is vastgesteld door de XSD-schema's van het centrale knooppunt.
  - 2.2. Het centrale knooppunt en de nationale systemen sturen en ontvangen berichten die voldoen aan het XSD-schema voor berichten.
  - 2.3. De nationale systemen kunnen alle berichten verzenden, ontvangen en verwerken die overeenstemmen met een van de in subaanhangsel 4.2 genoemde functies.
  - 2.4. De XML-berichten bevatten minstens de minimumeisen in tabel 2.

Tabel 2

**Minimumeisen voor de inhoud van XML-berichten**

| <b>Gemeenschappelijke header</b>                    |                                                                                                                                                                                                                                                                                                                                                                                                                                                               | <b>Verplicht</b> |
|-----------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| Version (versie)                                    | De officiële versie van de XML-specificaties wordt bepaald door de namespace die is gedefinieerd in de XSD van het bericht en in het attribuut version in de header van een XML-bericht. Het versienummer ("n.m") wordt gedefinieerd als een vaste waarde in elke release van het XML-schemadefinitiebestand (XSD).                                                                                                                                           | Yes              |
| Test Identifier (identificatiecode van de test)     | Facultatieve identificatiecode voor tests. De initiator van de test vult de identificatiecode in; iedereen die aan de workflow deelneemt, stuurt dezelfde identificatiecode door/terug. Tijdens de productie wordt de identificatiecode genegeerd en niet gebruikt.                                                                                                                                                                                           | Nee              |
| Technical Identifier (technische identificatiecode) | Een UUID die elk afzonderlijk bericht op een unieke wijze identificeert. De afzender genereert een UUID en vult dat attribuut met gegevens. Die gegevens worden niet gebruikt in zakelijke omstandigheden.                                                                                                                                                                                                                                                    | Ja               |
| Workflow Identifier (identificatiecode workflow)    | De identificatiecode van de workflow is een UUID die wordt gegenereerd door de vragende partij. Vervolgens wordt die identificatiecode in alle berichten gebruikt om de workflow te correleren.                                                                                                                                                                                                                                                               | Ja               |
| Sent at (verzonden op)                              | De datum en het tijdstip (UTC) waarop het bericht is verzonden.                                                                                                                                                                                                                                                                                                                                                                                               | Ja               |
| Timeout (onderbreking)                              | Facultatief datum- en tijdattribuut (in UTC-formaat). Het knooppunt bepaalt die waarde alleen voor doorgestuurde vragen. Daardoor wordt de antwoordende partij verwittigd van het tijdstip waarop het verzoek verloopt. Deze waarde is niet vereist in MS2TCN_<x>_Req en alle antwoordberichten. De waarde is facultatief, zodat dezelfde headerdefinitie kan worden gebruikt voor alle soorten berichten, ongeacht of het attribuut timeoutValue is vereist. | Nee              |
| From (van)                                          | ISO 3166-1 Alpha 2-code van de partij die het bericht verzendt of "EU".                                                                                                                                                                                                                                                                                                                                                                                       | Ja               |
| To (aan)                                            | ISO 3166-1 Alpha 2-code van de partij waaraan het bericht wordt verzonden of "EU".                                                                                                                                                                                                                                                                                                                                                                            | Ja               |

#### Subaanhangsel 4.4

##### **Transliteratie- en NYSIIS-diensten (New York State Identification and Intelligence System)**

1. Het NYSIIS-algoritme van het centrale knooppunt wordt gebruikt om de namen van alle bestuurders in het nationale register te coderen.
2. Als een kaart via de CIC-functie wordt gezocht, worden de NYSIIS-sleutels als voornaamste zoekmechanisme gebruikt.
3. Daarnaast kunnen de partijen een algoritme op maat gebruiken om aanvullende resultaten terug te sturen.
4. In de zoekresultaten wordt aangegeven welk zoekmechanisme (NYSIIS of op maat) is gebruikt om een record te vinden.
5. Als een partij ervoor kiest ICDL-berichten op te slaan, worden de in het bericht vervatte NYSIIS-sleutels geregistreerd als onderdeel van de ICDL-gegevens. Als een partij de ICDL-gegevens zoekt, gebruikt zij de NYSIIS-sleutels van de naam van de aanvrager.

## Subaanhangsel 4.5

### **Beveiligingseisen**

1. Voor de uitwisseling van berichten tussen het centrale knooppunt en de nationale systemen wordt HTTPS gebruikt.
2. De nationale systemen gebruiken de in de subaanhangsels 4.8 en 4.9 bedoelde digitale certificaten voor de veilige verzending van berichten tussen het nationale systeem en het centrale knooppunt.
3. De nationale systemen gebruiken ten minste certificaten met het hash-algoritme SHA-2 (SHA-256) voor de handtekening en een publieke sleutel met een lengte van 2048 bits.



## Subaanhangsel 4.6

### Dienstverleningsniveaus

1. Nationale systemen voldoen aan de volgende minimale dienstverleningsniveaus:
  - 1.1. zij zijn 24 uur per dag en 7 dagen per week beschikbaar;
  - 1.2. hun beschikbaarheid wordt gecontroleerd door een hartslagbericht vanuit het centrale knooppunt;
  - 1.3. de beschikbaarheidsgraad bedraagt 98 %, overeenkomstig de volgende tabel (de cijfers zijn afgerond op de dichtstbijzijnde geschikte eenheid):

| Een beschikbaarheid van | betekent een onbeschikbaarheid van |             |           |
|-------------------------|------------------------------------|-------------|-----------|
|                         | Dagelijks                          | Maandelijks | Jaarlijks |
| 98%                     | 0,5 uur                            | 15 uur      | 7,5 dag   |

De partijen worden aangespoord om zich aan de dagelijkse beschikbaarheidsgraad te houden, hoewel wordt erkend dat voor bepaalde noodzakelijke activiteiten, zoals onderhoud van het systeem, een wachttijd van meer dan 30 minuten nodig is. De maandelijkse en jaarlijkse beschikbaarheidsgraden zijn echter bindend;

- 1.4. zij beantwoorden ten minste 98 % van de verzoeken die in een kalendermaand worden doorgestuurd;
- 1.5. zij beantwoorden verzoeken binnen 10 seconden;
- 1.6. de algemene vraag-time-out (de tijd dat de verzoeker op een antwoord wacht) bedraagt niet meer dan 20 seconden;
- 1.7. zij kunnen zes verzoeken per seconde behandelen;
- 1.8. de nationale systemen mogen niet meer dan twee verzoeken per seconde naar het TACHOnet-knooppunt sturen;

1.9. elk nationaal systeem moet eventuele technische problemen in het centrale knooppunt of de nationale systemen van andere partijen kunnen opvangen. Daaronder vallen onder andere maar niet uitsluitend:

- a) verbroken verbinding met het centrale knooppunt;
- b) geen antwoord op een verzoek;
- c) ontvangst van antwoorden na een bericht-time-out;
- d) ontvangst van ongevraagde berichten;
- e) ontvangst van ongeldige berichten.

2. Het centrale knooppunt:

2.1. heeft een beschikbaarheidsgraad van 98 %;

2.2. brengt nationale systemen op de hoogte van fouten via een antwoordbericht of een speciale foutmelding. De nationale systemen ontvangen op hun beurt die specifieke foutmeldingen en beschikken over een escalatieworkflow om alle nodige maatregelen te treffen om de gemelde fout te corrigeren.

3. Onderhoud

Indien technisch mogelijk brengen de partijen ten minste één week vóór de start van een routine-onderhoud de andere partijen en de Europese Commissie via de webtoepassing op de hoogte van dat onderhoud.

## Subaanhangsel 4.7

### **Logbestanden en statistieken van de door het centrale knooppunt verzamelde gegevens**

1. Om de privacy te garanderen zijn de gegevens die voor statistische doeleinden worden gebruikt anoniem. Gegevens voor het identificeren van een specifieke kaart, bestuurder of rijbewijs zijn niet beschikbaar voor statistische doeleinden.
2. Via logbestanden worden alle transacties gevolgd met het oog op toezicht en het verwijderen van bugs en om statistieken over deze transacties te kunnen opstellen.
3. Persoonsgegevens worden niet langer dan zes maanden in de logbestanden bewaard. Statistische gegevens worden voor onbepaalde tijd bewaard.
4. De statistische gegevens voor de rapportage bevatten:
  - a) de vragende partij;
  - b) de antwoordende partij;
  - c) het soort bericht;
  - d) de statuscode van het antwoord;
  - e) de datum en het tijdstip van de berichten;
  - f) de responstijd.

## Subaanhangsel 4.8

### **Algemene bepalingen betreffende digitale sleutels en certificaten voor TACHOnet**

1. Het directoraat-generaal Informatica van de Europese Commissie (DIGIT) stelt een PKI-dienst<sup>1</sup> ("CEF PKI-dienst" genoemd) ter beschikking van de overeenkomstsluitende partijen bij de AETR om zich via eDelivery te kunnen aansluiten op TACHOnet (voortaan de nationale autoriteiten).
2. De procedure voor het aanvragen en intrekken van digitale certificaten, evenals de gedetailleerde voorwaarden voor het gebruik ervan, zijn beschreven in het aanhangsel.
3. Gebruik van certificaten
  - 3.1. Zodra het certificaat is uitgegeven, gebruikt de nationale autoriteit<sup>2</sup> het alleen voor TACHOnet. Het certificaat kan worden gebruikt om:
    - a) de oorsprong van de gegevens te authenticeren;
    - b) gegevens te versleutelen;
    - c) de opsporing van integriteitsinbreuken van gegevens te waarborgen.
  - 3.2. Elk gebruik van het certificaat dat niet uitdrukkelijk is goedgekeurd als onderdeel van het toegestane gebruik, is verboden.
4. De overeenkomstsluitende partijen:
  - a) beschermen hun geheime sleutel tegen onrechtmatig gebruik;
  - b) sturen de geheime sleutels niet door of delen die niet mee aan derden, zelfs als vertegenwoordigers;

---

<sup>1</sup> Een PKI (publieke-sleutelinfrastructuur) is een reeks rollen, principes, procedures en systemen voor het aanmaken, beheren, verdelen en intrekken van digitale certificaten.

<sup>2</sup> Geïdentificeerd door de attribuutwaarde "O=" in de Subject Distinguished Name van het uitgegeven certificaat.

- c) waarborgen de vertrouwelijkheid, de integriteit en de beschikbaarheid van de geheime sleutels die voor TACHOnet zijn aangemaakt, opgeslagen en gebruikt;
- d) gebruiken de geheime sleutel niet langer nadat de geldigheidsduur is verstreken of het certificaat is ingetrokken, behalve om versleutelde gegevens te bekijken (bv. om e-mails te ontsleutelen). Vervallen sleutels worden vernietigd of op zodanige wijze bewaard dat zij niet kunnen worden gebruikt;
- e) bezorgen de registratieautoriteit de identiteit van de vertegenwoordigers die gemachtigd zijn om de intrekking van de aan de organisatie afgegeven certificaten te vragen (intrekkingsverzoeken bevatten een intrekkingswachtwoord en gegevens over de gebeurtenissen die tot de intrekking hebben geleid);
- f) voorkomen misbruik van de geheime sleutel door om de intrekking van het bijbehorende certificaat te verzoeken als de geheime sleutel of de activeringsgegevens zijn aangetast;
- g) hebben de verantwoordelijkheid en de plicht om tot de intrekking van een certificaat te verzoeken onder de omstandigheden die zijn vermeld in het certificatiebeleid (certification policies, CP) en de certificatiepraktijkverklaring (certification practices statement, CPS) van de certificatautoriteit;
- h) brengen de registratieautoriteit onverwijld op de hoogte van verlies, diefstal of mogelijke aantasting van AETR-sleutels die voor TACHOnet worden gebruikt.

## 5. Aansprakelijkheden

Onverminderd de aansprakelijkheid van de Europese Commissie in strijd met de in de toepasselijke wetgeving van de Europese Unie of nationale wetgeving vervatte voorschriften, of betreffende haar aansprakelijkheid voor aangelegenheden die uit hoofde van die wetgeving niet mogen worden uitgesloten, is de Europese Commissie niet verantwoordelijk of aansprakelijk voor:

- a) de inhoud van het certificaat, die uitsluitend bij de houder van het certificaat ligt.  
Het is de verantwoordelijkheid van de houder van het certificaat om de nauwkeurigheid van de inhoud van het certificaat te controleren;
- b) het gebruik van het certificaat door de houder ervan.

## Beschrijving van de PKI-dienst voor TACHOnet

### 1. Inleiding

Een PKI (publieke-sleutelinfrastructuur) is een reeks rollen, principes, procedures en systemen voor het aanmaken, beheren, verdelen en intrekken van digitale certificaten<sup>3</sup>. De CEF PKI-dienst van eDelivery maakt de uitgave en het beheer mogelijk van digitale certificaten die worden gebruikt om de vertrouwelijkheid, de integriteit en de onweerlegbaarheid te waarborgen van de informatie die tussen toegangspunten wordt uitgewisseld.

De PKI-dienst van eDelivery is gebaseerd op de Trust Center Services TeleSec Shared Business CA (certificaatautoriteit) waarop het certificatiebeleid (CP) en de certificatiepraktijkverklaring (CPS) van TeleSec Shared Business CA van T-Systems International GmbH<sup>4</sup> van toepassing zijn.

De PKI-dienst geeft certificaten uit die geschikt zijn voor de beveiliging van verschillende bedrijfsprocessen binnen en buiten ondernemingen, organisaties, openbare autoriteiten en instellingen waarvoor een gemiddeld beveiligingsniveau is vereist om de authenticiteit, de integriteit en de betrouwbaarheid van de eindentiteit te bewijzen.

### 2. Aanvraagprocedure voor certificaten

#### 2.1. Taken en verantwoordelijkheden

##### 2.1.1. "Organisatie" of "nationale autoriteit" die het certificaat aanvraagt

2.1.1.1. De nationale autoriteit vraagt de certificaten aan in het kader van het TACHOnet-project.

2.1.1.2 De nationale autoriteit:

- a) vraagt de certificaten aan bij de CEF PKI-dienst;

---

<sup>3</sup> [https://nl.wikipedia.org/wiki/Public\\_key\\_infrastructure](https://nl.wikipedia.org/wiki/Public_key_infrastructure)

<sup>4</sup> De recentste versie van het CP en de CPS kan worden gedownload van <https://www.telesec.de/en/sbca-en/support/download-area/>

- b) genereert de geheime sleutels en de overeenkomstige publieke sleutels die worden opgenomen in de door de certificaatautoriteit uitgegeven certificaten;
- c) downloadt het goedgekeurde certificaat;
- d) ondertekent en stuurt het volgende terug naar de registratieautoriteit:
  - i) het identificatieformulier met de contactpersonen en betrouwbare koeriers,
  - ii) de ondertekende individuele volmacht<sup>5</sup>.

#### 2.1.2. Betrouwbare koerier

2.1.2.1. De nationale autoriteit stelt een betrouwbare koerier aan.

2.1.2.2. De betrouwbare koerier:

- a) overhandigt de publieke sleutel aan de registratieautoriteit tijdens een persoonlijke identificatie- en registratieprocedure;
- b) ontvangt het overeenkomstige certificaat van de registratieautoriteit.

#### 2.1.3. Domeineigenaar

2.1.3.1. De domeineigenaar is DG MOVE.

2.1.3.2. De domeineigenaar:

- a) valideert en coördineert het TACHOnet-netwerk en de trust-architectuur van TACHOnet, met inbegrip van de validering van de procedures voor de uitgave van certificaten;
- b) exploiteert het centrale knooppunt van TACHOnet en coördineert de activiteiten van de partijen met betrekking tot de werking van TACHOnet;
- c) voert samen met de nationale autoriteiten de aansluitingstest van TACHOnet uit.

---

<sup>5</sup> Een volmacht is een juridisch document waarbij de organisatie de Europese Commissie, vertegenwoordigd door de geïdentificeerde ambtenaar die verantwoordelijk is voor de CEF PKI-dienst, machtigt om namens haar TeleSec Shared Business CA van T-Systems International GmbH te verzoeken om een certificaat aan te maken. Zie ook punt 6.

#### 2.1.4. Registratieautoriteit

2.1.4.1. De registratieautoriteit is het Joint Research Centre (JRC).

2.1.4.2. De registratieautoriteit is verantwoordelijk voor de controle van de identiteit van de betrouwbare koerier en voor de registratie en goedkeuring van de verzoeken tot uitgave, intrekking en verlenging van digitale certificaten.

2.1.4.3. De registratieautoriteit:

- a) wijst de unieke identificatiecode toe aan de nationale autoriteit;
- b) authenticceert de identiteit van de nationale autoriteit, haar contactpunten en betrouwbare koeriers;
- c) communiceert met de CEF-ondersteuning over de authenticiteit van de nationale autoriteit, haar contactpunten en betrouwbare koeriers;
- d) informeert de nationale autoriteit over de goedkeuring of afkeuring van certificaten.

#### 2.1.5. Certificaatautoriteit

2.1.5.1. De certificaatautoriteit is verantwoordelijk voor het verschaffen van de technische infrastructuur voor de aanvraag, de uitgave en de intrekking van digitale certificaten.

2.1.5.2. De certificaatautoriteit:

- a) levert de technische infrastructuur voor certificaataanvragen door nationale autoriteiten;
- b) valideert of verwierpt certificaataanvragen;
- c) communiceert met de registratieautoriteit desgevraagd over de identiteitsverificatie van de aanvragende autoriteit.

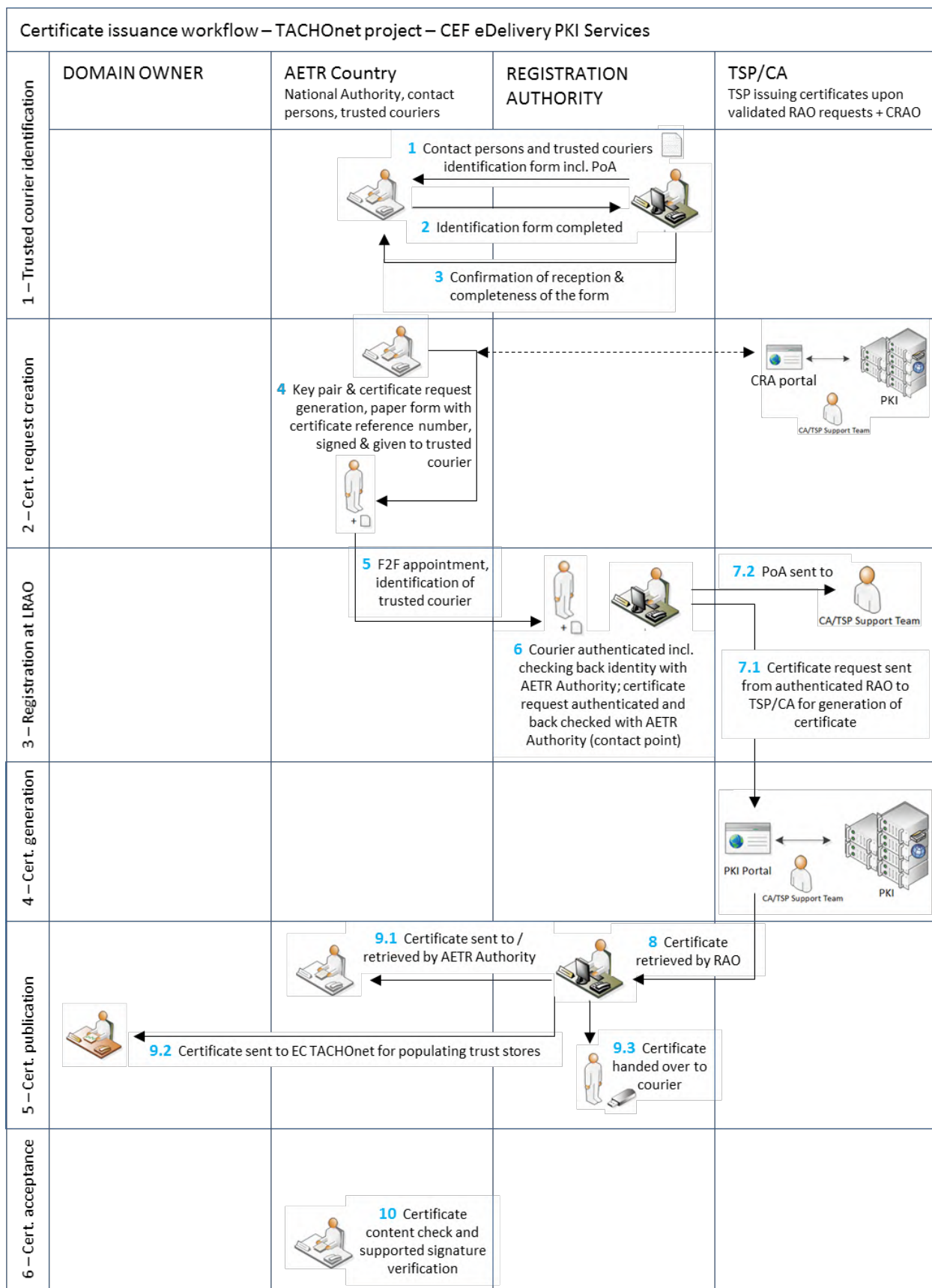
#### 2.2. Uitgave van certificaten

2.2.1. De uitgave van certificaten gebeurt volgens de stappen in figuur 1:

- a) **Stap 1:** Identificatie van de betrouwbare koerier



- b) **Stap 2:** Aanmaken van de aanvraag van het certificaat
- c) **Stap 3:** Registratie door de registratieautoriteit
- d) **Stap 4:** Aanmaak van het certificaat
- e) **Stap 5:** Publicatie van het certificaat
- f) **Stap 6:** Aanvaarding van het certificaat



Figuur 1 - Workflow voor de uitgave van een certificaat

### 2.2.2. Stap 1: Identificatie van de betrouwbare koerier

De identificatie van de betrouwbare koerier verloopt volgens deze procedure:

- a) de registratieautoriteit stuurt de nationale autoriteit een identificatieformulier voor de contactpersonen en betrouwbare koeriers<sup>6</sup>. Dat formulier bevat ook een volmacht die moet worden ondertekend door de organisatie (AETR-autoriteit);
- b) de nationale autoriteit stuurt het ingevulde formulier en de ondertekende volmacht terug naar de registratieautoriteit;
- c) de registratieautoriteit bevestigt de goede ontvangst en volledigheid van het formulier;
- d) de registratieautoriteit bezorgt een bijgewerkte lijst van contactpersonen en betrouwbare koeriers aan de domeineigenaar.

### 2.2.3. Stap 2: Aanmaken van de aanvraag van het certificaat

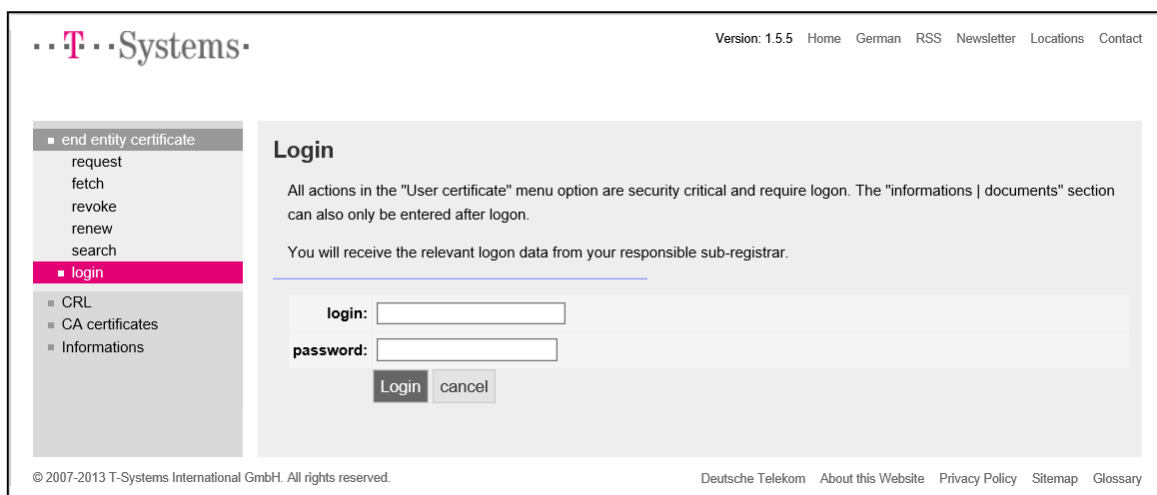
2.2.3.1. Het certificaat wordt op dezelfde computer en met dezelfde browser aangevraagd en opgehaald.

2.2.3.2. De aanvraag van het certificaat wordt aangemaakt volgens deze procedure:

- a) de organisatie gaat naar de gebruikerswebinterface om het certificaat aan te vragen via de URL <https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en> en vult als gebruikersnaam "**sbca/CEF\_eDelivery.europa.eu**" en als wachtwoord "**digit.333**" in;

---

<sup>6</sup> Zie punt 5.



Figuur 2

- b) de organisatie klikt aan de linkerkzijde van het scherm op "request" en kiest "CEF\_TACHOnet" in de vervolgkeuzelijst;



Figuur 3

- c) de organisatie vult het aanvraagformulier voor het certificaat onder figuur 4 in met de informatie van tabel 3 en klikt op "Next (soft-PSE)" om te procedure te voltooien;

Must start with: 'GRP:' concatenated with CEF\_TACHOnet\_<TYPE>\_<COUNTRY CODE>\_<Unique\_Identifier\_of\_the\_Accss\_P oint>'  
E.g.:  
'GRP: CEF\_TACHOnet\_AP\_PROD\_BE\_001'

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

Official Organisation Name (case sensitive)

Must be:  
TYPE=AP\_PROD  
concatenated with '-' separator and  
'GTC\_OID-1.3.130.0.2018.xxxxxx'  
where Ares(2018)xxxxxx is the allocated number

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

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

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

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

Click here to end

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

Country: BE

Organisation/company (O): My Company

Internet domain (OU1): CEF\_eDelivery.europa.eu

Responsibility (OU2): CEF\_TACHOnet

Unique Identifier (OU3): AP\_PROD-GTC\_OID-1.3.130.0.2018.xxxxxx

First name (CN): Leave Empty

Last name (CN): GRP:CEF\_TACHOnet\_AP\_PROD\_BE\_001

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

E-mail 1 (SAN): Leave Empty

E-mail 2 (SAN): Leave Empty

E-mail 3 (SAN): Leave Empty

Address: Leave Empty

Street: Street no.

ZIP code: City

Phone no.: Leave Empty

business.register.xx@mail.com

Mr Johan Smith

Revocation password: (max. 50 characters)

Revocation password repetition: (max. 50 characters)

Revocation password proposal: juHEVeV136

Adopt revocation password proposal

Figuur 4

| Vereiste velden              | Beschrijving                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Country                      | <p><b>C=Country Code</b>, land van de houder van het certificaat, geverifieerd aan de hand van een openbare gids.</p> <p>Restricties: 2 tekens, in overeenstemming met ISO 3166-1 Alpha-2, hoofdlettergevoelig.</p> <p>Voorbeelden: DE, BE, NL,</p> <p>Specifieke gevallen: UK (voor Groot-Brittannië), EL (voor Griekenland).</p>                                                                                                                                                                                                                                                                                                                             |
| Organisation/Company (O)     | <b>O=naam van de organisatie van de houder van het certificaat.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Master domain (OU1)          | <b>OU=CEF_eDelivery.europa.eu</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Area of responsibility (OU2) | <b>OU=CEF_TACHOnet</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Department (OU3)             | <p>Verplichte waarde per "AREA OF RESPONSIBILITY".</p> <p>De inhoud moet worden gecontroleerd aan de hand van een positieve lijst (witte lijst) wanneer het certificaat wordt aangevraagd. Als de informatie niet met de lijst overeenkomt, wordt de aanvraag verhinderd.</p> <p>Formaat:</p> <p><b>OU=&lt;TYPE&gt;-&lt;GTC_NUMBER&gt;</b></p> <p>Waarbij "&lt;TYPE&gt;" wordt vervangen door AP_PROD: Access Point in Production-omgeving.</p> <p>En waarbij &lt;GTC_NUMBER&gt; <b>GTC_OID-1.3.130.0.2018.xxxxxx</b> is, terwijl Ares(2018)xxxxxx het GTC-nummer voor het TACHOnet-project is.</p> <p>Bijv.:</p> <p>AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx</p> |
| First name (CN)              | Moet leeg blijven.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Last name (CN)               | <p>Moet beginnen met "GRP", gevolgd door een gewone naam.</p> <p>Formaat:</p> <p><b>CN=GRP:&lt;AREA OF RESPONSIBILITY&gt;_&lt;TYPE&gt;_&lt;COUNTRY CODE&gt;_&lt;UNIQUE IDENTIFIER&gt;</b></p> <p>Bijv.:</p> <p>GRP:CEF_TACHOnet_AP_PROD_BE_001</p>                                                                                                                                                                                                                                                                                                                                                                                                             |
| E-mail                       | <b>E=<a href="mailto:CEF-EDELIVERY-SUPPORT@ec.europa.eu">CEF-EDELIVERY-SUPPORT@ec.europa.eu</a></b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| E-mail 1 (SAN)               | Moet leeg blijven.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| E-mail 2 (SAN)               | Moet leeg blijven.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| E-mail 3 (SAN)               | Moet leeg blijven.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

|                                |                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Address                        | Moet leeg blijven.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Street                         | Het officiële adres van de organisatie of de houder van het certificaat. (Gebruikt voor de volmacht.)                                                                                                                                                                                                                                                                                                                                        |
| Street no.                     | Het officiële adres van de organisatie of de houder van het certificaat. (Gebruikt voor de volmacht.)                                                                                                                                                                                                                                                                                                                                        |
| Zip Code                       | Het officiële adres van de organisatie of de houder van het certificaat. (Gebruikt voor de volmacht.)<br><br><b><u>Let op:</u></b> als de postcode NIET uit vijf cijfers bestaat, het veld "ZIP code" open laten en de postcode invullen in het veld "City".                                                                                                                                                                                 |
| City                           | Het officiële adres van de organisatie of de houder van het certificaat. (Gebruikt voor de volmacht.)<br><br><b><u>Let op:</u></b> als de postcode NIET uit vijf cijfers bestaat, het veld "ZIP code" open laten en de postcode invullen in het veld "City".                                                                                                                                                                                 |
| Phone no                       | Moet leeg blijven.                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Identification data            | Het e-mailadres moet hetzelfde zijn als datgene dat wordt gebruikt om de unieke identificatiecode te registreren.<br>+<br>De naam van de persoon die de organisatie vertegenwoordigt. (Gebruikt voor de volmacht.)<br>+ <b>Handelsregisternummer</b> (alleen verplicht voor particuliere organisaties).<br><br><b>Ingeschreven bij de lokale rechtbank van</b> (alleen verplicht voor particuliere organisaties in Duitsland en Oostenrijk). |
| Revocation password            | Verplicht veld gekozen door de aanvrager.                                                                                                                                                                                                                                                                                                                                                                                                    |
| Revocation password repetition | Nogmaals verplicht veld gekozen door de aanvrager.                                                                                                                                                                                                                                                                                                                                                                                           |

Tabel 3 Alle gegevens van elk vereist veld.

- d) de gekozen sleutel heeft een lengte van 2048 bits (hoogwaardig);

The screenshot shows the 'User certificate' page on the T-Systems website. The left sidebar contains a menu with 'End entity certificate' expanded, showing 'request' (highlighted), 'fetch', 'revoke', 'renew', 'search', and 'logout'. Below this are 'CRL', 'CA certificates', and 'Information'. The main content area is titled 'User certificate' and contains instructions about key length and approval. The 'Certificate data' section includes fields for Country (C), Organization/company (O), Master domain (OU1), Area of responsibility (OU2), Department (OU3), First name (CN), Last name (CN), E-mail, and Selection of key length (set to 2048 (High Grade)). 'Request' and 'Cancel' buttons are at the bottom.

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

Figuur 5

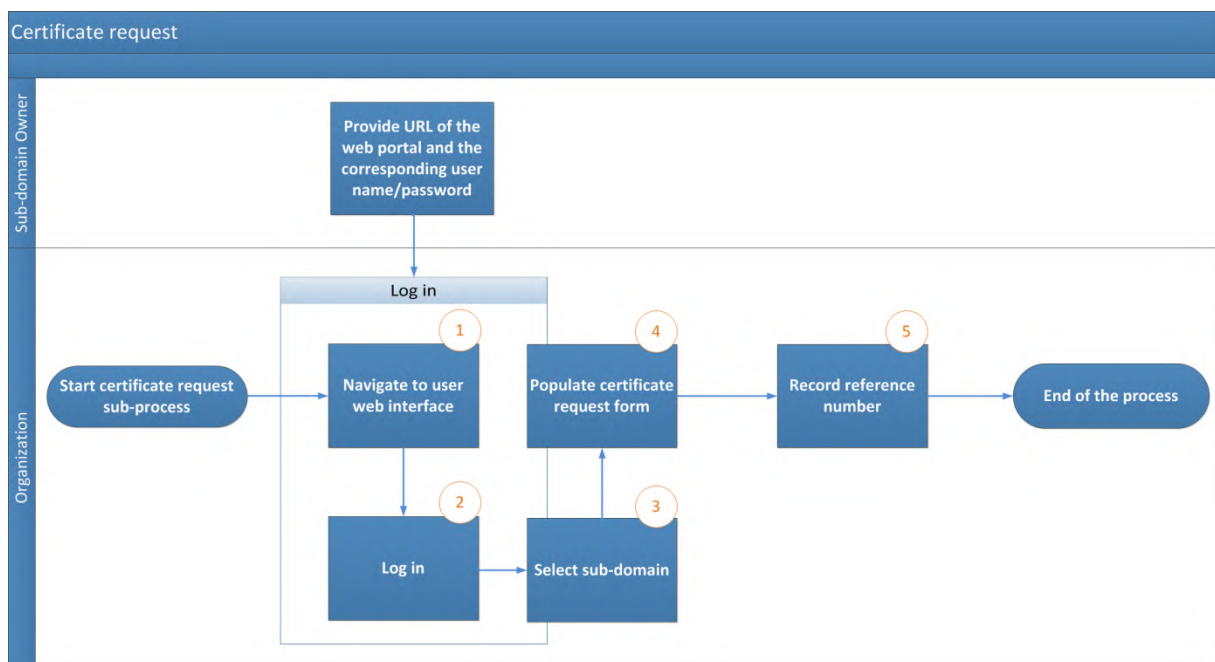
- e) de organisatie moet het referentienummer opslaan om het certificaat op te kunnen halen;

The screenshot shows the 'User certificate' page after a request. The message states: 'The certificate was requested. Your request was stored with reference number 776002.' A blue callout bubble points to this number with the text 'Certificate Reference Number'. The sidebar and footer are identical to Figure 5.

Figuur 6



- f) het CEF-ondersteuningsteam bekijkt nieuwe aanvragen voor certificaten en controleert of de informatie in de aanvraag geldig is, d.w.z. of die voldoet aan de naamgeving zoals gespecificeerd in aanhangsel 5.1: Naamgeving voor certificaten;
- g) het CEF-ondersteuningsteam controleert of de informatie in de aanvraag in een geldig formaat is ingevuld;
- h) als niet is voldaan aan punt 5 of 6, stuurt het CEF-ondersteuningsteam een e-mail naar het adres dat is ingevuld in het veld "Identification data" van het aanvraagformulier, met de domeineigenaar in CC, waarin het de organisatie vraagt om de procedure opnieuw te doorlopen. De foute aanvraag wordt geannuleerd.
- i) Het CEF-ondersteuningsteam stuurt de registratieautoriteit een e-mail over de geldigheid van de aanvraag. In die e-mail wordt het volgende vermeld:
  - 1) de naam van de organisatie, in het veld "Organisation (O)" van de aanvraag;
  - 2) de gegevens van het certificaat, met inbegrip van de naam van het toegangspunt waarvoor het certificaat wordt uitgegeven, in het veld "Last name (CN)" van de aanvraag;
  - 3) het referentienummer van het certificaat;
  - 4) het adres en het e-mailadres van de organisatie en de naam van haar vertegenwoordiger.



Figuur 7 – Procedure voor de aanvraag van een certificaat.

#### 2.2.4. Stap 3: Registratie door de registratieautoriteit (goedkeuring van het certificaat)

2.2.4.1. De betrouwbare koerier of het contactpunt maakt via e-mail een afspraak met de registratieautoriteit en identificeert de betrouwbare koerier die zich persoonlijk zal aanmelden.

2.2.4.2. De organisatie stelt het documentair pakket samen, dat bestaat uit:

- a) de ingevulde en ondertekende volmacht;
- b) een kopie van het geldige paspoort van de betrouwbare koerier die zich persoonlijk zal aanmelden. De kopie moet ondertekend zijn door een van de onder stap 1 geïdentificeerde contactpunten van de organisatie;
- c) het papieren aanvraagformulier voor het certificaat, ondertekend door een van de contactpunten van de organisatie.

2.2.4.3. De registratieautoriteit ontvangt de betrouwbare koerier nadat zijn identiteit is gecontroleerd aan de ingang van het gebouw. De registratieautoriteit voert de persoonlijke registratie van de aanvraag van het certificaat uit door:

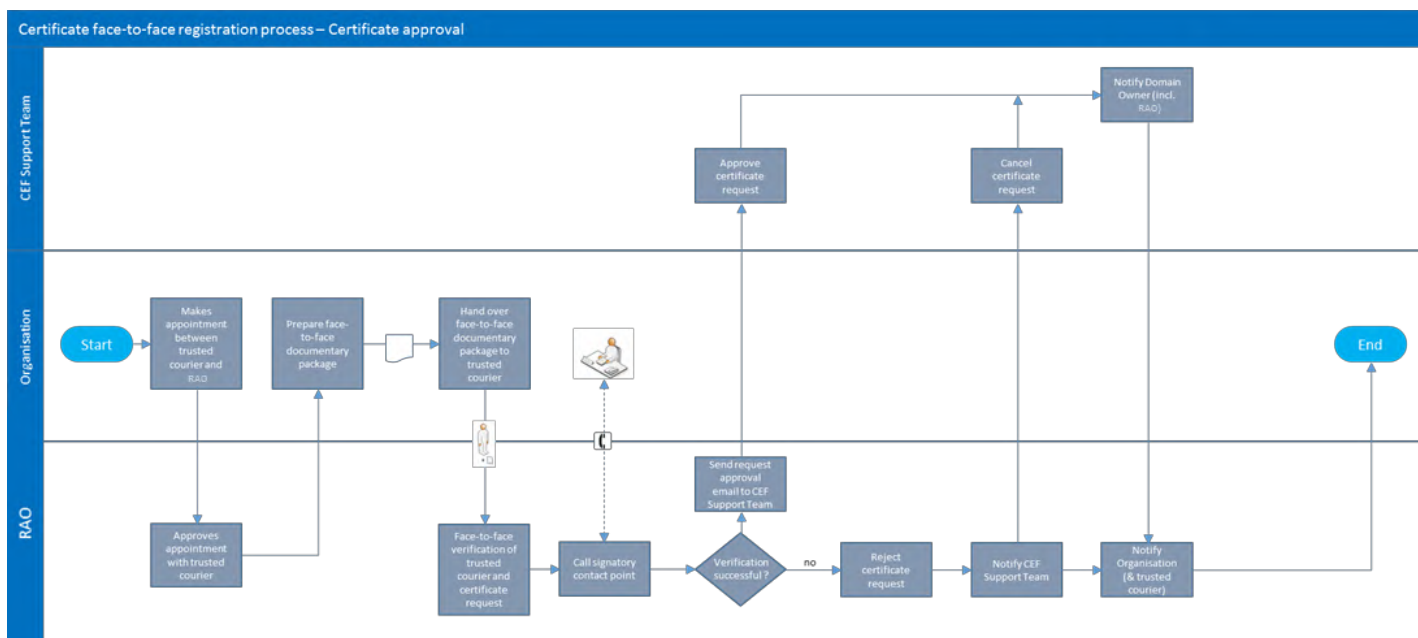
- a) de betrouwbare koerier te identificeren en te authenticeren;
- b) het fysieke voorkomen van de betrouwbare koerier te toetsen aan het paspoort dat door deze wordt voorgelegd;
- c) de geldigheid te controleren van het paspoort dat door de betrouwbare koerier wordt voorgelegd;
- d) het gevalideerde paspoort dat door de betrouwbare koerier wordt voorgelegd te toetsen aan de kopie van het geldige paspoort van de betrouwbare koerier die is ondertekend door een van de geïdentificeerde contactpunten van de organisatie. De handtekening wordt geauthenticeerd aan de hand van het "identificatieformulier van betrouwbare koeriers en contactpunten";
- e) de ingevulde en ondertekende volmacht te controleren;
- f) het papieren aanvraagformulier voor het certificaat en de handtekening te toetsen aan het originele "identificatieformulier voor betrouwbare koeriers en contactpunten";
- g) het ondertekenende contactpunt op te bellen om te identiteit van de betrouwbare koerier en de inhoud van de aanvraag van het certificaat nogmaals te controleren.

2.2.4.4. De registratieautoriteit bevestigt aan het CEF-ondersteuningsteam dat de nationale autoriteit inderdaad gemachtigd is om de componenten te exploiteren waarvoor zij de certificaten aanvraagt en dat de overeenkomstige persoonlijke registratieprocedure met succes is doorlopen. De bevestiging wordt verstuurd in een met een "CommiSign"-certificaat beveiligde e-mail, met als bijlage een gescand exemplaar van het geauthenticeerde documentaire pakket en van de ondertekende checklist van de procedure die door de registratieautoriteit is uitgevoerd.

2.2.4.5. Als de registratieautoriteit de geldigheid van de aanvraag bevestigt, wordt de procedure verdergezet zoals beschreven onder 2.2.4.6 en 2.2.4.7. Zo niet wordt de uitgave van het certificaat verworpen en wordt de organisatie daarvan in kennis gesteld.

2.2.4.6. Het CEF-ondersteuningsteam keurt de aanvraag van het certificaat goed en stelt de registratieautoriteit in kennis van de goedkeuring van het certificaat.

2.2.4.7. De registratieautoriteit stelt de organisatie ervan in kennis dat het certificaat kan worden opgehaald via het gebruikersportaal.



Figuur 8 - Goedkeuring van het certificaat.

#### 2.2.5. Stap 4: Aanmaak van het certificaat

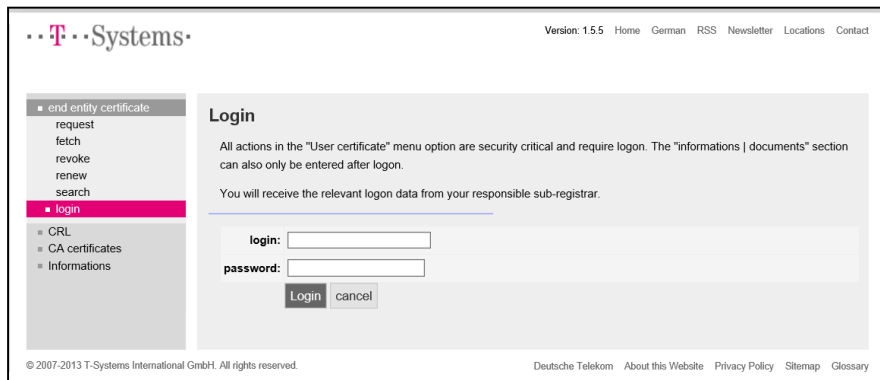
Na goedkeuring van de aanvraag van het certificaat, wordt het certificaat aangemaakt.

#### 2.2.6. Stap 5: Publiceren en ophalen van het certificaat

2.2.6.1. Nadat de aanvraag van het certificaat is goedgekeurd, ontvangt de registratieautoriteit het certificaat en overhandigt zij een exemplaar daarvan aan de betrouwbare koerier.

2.2.6.2. De registratieautoriteit deelt de organisatie mee dat de certificaten kunnen worden opgehaald.

2.2.6.3. De organisatie gaat naar het gebruikersportaal via <https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en> en logt in met gebruikersnaam "sbca/CEF\_eDelivery.europa.eu" en wachtwoord "digit.333".



..T..Systems·

Version: 1.5.5 Home German RSS Newsletter Locations Contact

■ end entity certificate  
request  
fetch  
revoke  
renew  
search  
■ login  
■ CRL  
■ CA certificates  
■ Informations

### Login

All actions in the "User certificate" menu option are security critical and require login. The "informations | documents" section can also only be entered after login.

You will receive the relevant login data from your responsible sub-registrar.

login:

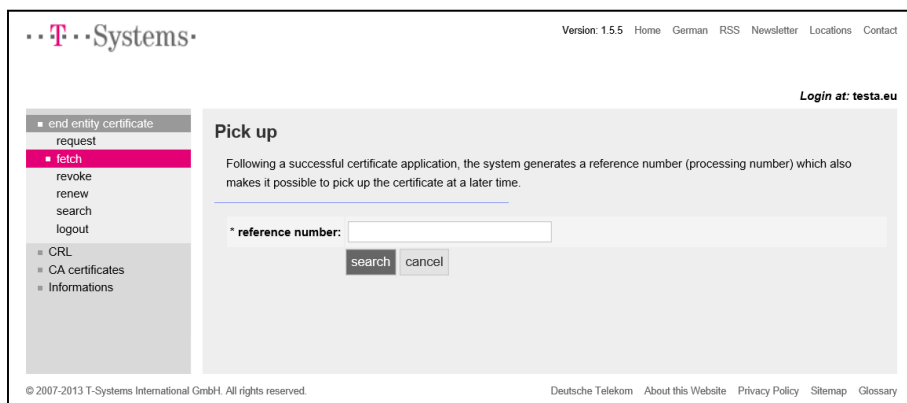
password:

Login cancel

© 2007-2013 T-Systems International GmbH. All rights reserved. Deutsche Telekom About this Website Privacy Policy Sitemap Glossary

Figuur 9

2.2.6.4. De organisatie klikt aan de linkerkzijde op de knop "fetch" en vult het referentienummer in dat tijdens de aanvraagprocedure van het certificaat is geregistreerd.



..T..Systems·

Version: 1.5.5 Home German RSS Newsletter Locations Contact

■ end entity certificate  
request  
■ fetch  
revoke  
renew  
search  
logout  
■ CRL  
■ CA certificates  
■ Informations

Login at: testa.eu

### Pick up

Following a successful certificate application, the system generates a reference number (processing number) which also makes it possible to pick up the certificate at a later time.

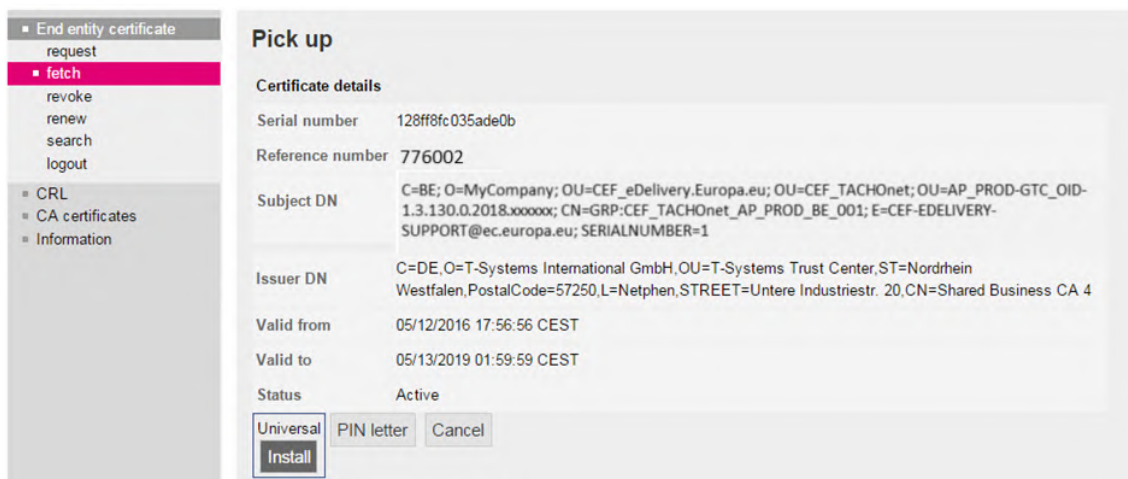
\* reference number:

search cancel

© 2007-2013 T-Systems International GmbH. All rights reserved. Deutsche Telekom About this Website Privacy Policy Sitemap Glossary

Figuur 10

2.2.6.5. De organisatie installeert de certificaten door op de knop "Install" te klikken.

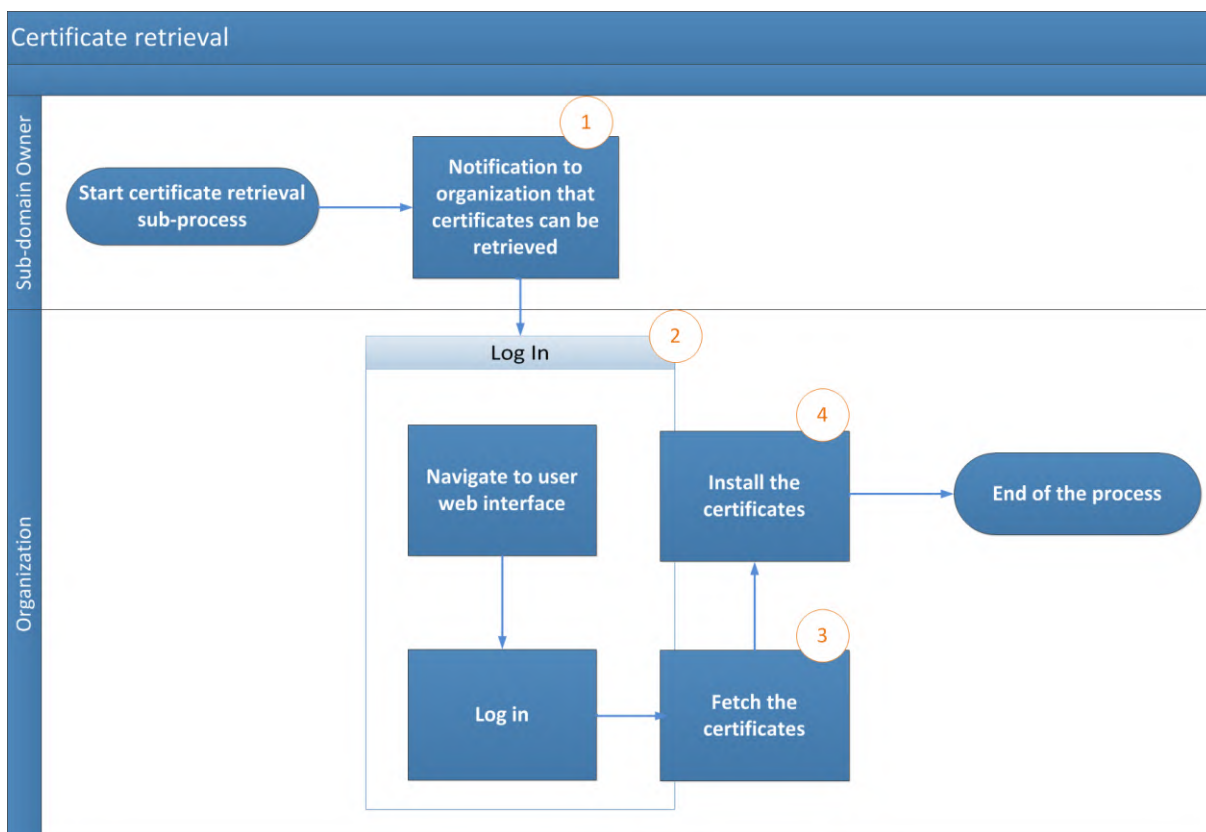


Figuur 11

2.2.6.6. Het certificaat wordt geïnstalleerd op het toegangspunt. Aangezien dit implementatie-specifiek is, verwijst de organisatie naar de provider van haar toegangspunt om de beschrijving van deze procedure te ontvangen.

2.2.6.7. Dit zijn de nodige stappen om het certificaat op het toegangspunt te installeren:

- a) de geheime sleutel en het certificaat exporteren;
- b) het sleutelbestand en het trustbestand aanmaken;
- c) het sleutelbestand en het trustbestand installeren op het toegangspunt.

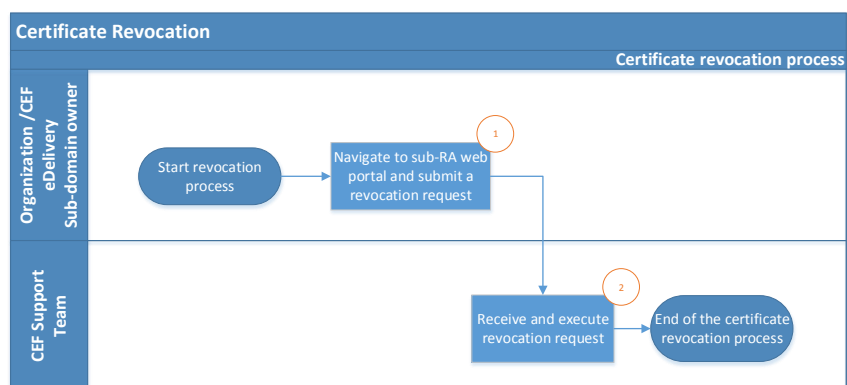


Figuur 12 - Ophalen van het certificaat.

### 3. Procedure voor de intrekking van certificaten

3.1. De organisatie dient een aanvraag tot intrekking in via het gebruikerswebportaal.

3.2. Het CEF-ondersteuningsteam trekt het certificaat in.



Figuur 13 - Intrekking van het certificaat.

## 4. Algemene voorwaarden van de CEF PKI-dienst.

### 4.1. Achtergrond

In zijn hoedanigheid van aanbieder van oplossingen van de bouwsteen eDelivery van de Connecting Europe Facility, stelt DIGIT een PKI-dienst<sup>7</sup> ("CEF PKI-dienst") ter beschikking van de overeenkomstsluitende partijen bij de AETR. De CEF PKI-dienst wordt gebruikt door de nationale autoriteiten ("eindgebruikers") die aan TACHOnet deelnemen.

DIGIT is een PKI-huurder binnen de TeleSec Shared Business CA-oplossing ("SBCA") die wordt geëxploiteerd in het trustcentrum van de groep T-Systems International GmbH ("T-Systems"<sup>8</sup>). DIGIT speelt de rol van hoofdregistrator van het domein "CEF\_eDelivery.europa.eu" van de SBCA. In die rol maakt DIGIT subdomeinen van het domein "CEF\_eDelivery.europa.eu" aan voor elk project dat de CEF PKI-dienst gebruikt.

Dit document bevat meer gegevens over de voorwaarden van het subdomein TACHOnet. DIGIT speelt de rol van subregistrator van dit subdomein. In die hoedanigheid is het verantwoordelijk voor de uitgave, intrekking en verlenging van certificaten voor dit project.

### 4.2. Uitsluiting van aansprakelijkheid

De Europese Commissie aanvaardt geen enkele verantwoordelijkheid of aansprakelijkheid met betrekking tot de inhoud van het certificaat, die uitsluitend bij de houder van het certificaat ligt. Het is de verantwoordelijkheid van de houder van het certificaat om de nauwkeurigheid van de inhoud van het certificaat te controleren.

De Europese Commissie aanvaardt geen enkele verantwoordelijkheid of aansprakelijkheid met betrekking tot het gebruik van het certificaat door de houder, die een derde partij buiten de Europese Commissie is.

---

<sup>7</sup> Een PKI (publieke-sleutelinfrastructuur) is een reeks rollen, principes, procedures en systemen voor het aanmaken, beheren, verdelen en intrekken van digitale certificaten.

<sup>8</sup> De betrouwbare trustcentrumexploitant, gevestigd in het trustcentrum van T-Systems, vervult ook de taak van interne registratieautoriteit.



Met deze afwijzing van aansprakelijkheid wordt niet beoogd de aansprakelijkheid van de Europese Commissie te beperken in strijd met de in de toepasselijke nationale wetgeving vervatte voorschriften, noch haar aansprakelijkheid uit te sluiten voor aangelegenheden die uit hoofde van die wetgeving niet mogen worden uitgesloten.

#### 4.3. Toegestaan/verboden gebruik van certificaten

##### 4.3.1. Toegestaan gebruik van certificaten

Zodra het certificaat is afgegeven, gebruikt de houder<sup>9</sup> het certificaat alleen voor TACHOnet. Het certificaat kan worden gebruikt om:

- de oorsprong van de gegevens te authenticeren;
- gegevens te versleutelen;
- de opsporing van integriteitsinbreuken van gegevens te waarborgen.

##### 4.3.2. Verboden gebruik van certificaten

Elk gebruik van het certificaat dat niet uitdrukkelijk is goedgekeurd als onderdeel van het toegestane gebruik, is verboden.

#### 4.4. Aanvullende verplichtingen van de houder van het certificaat

De gedetailleerde voorwaarden van de SBCA zijn gedefinieerd door T-Systems in het certificatiebeleid (CP) en de certificatiepraktijkverklaring (CPS) van de SBCA-dienst<sup>10</sup>. Dit document bevat beveiligingsspecificaties en richtsnoeren betreffende technische en organisatorische aspecten en beschrijft de activiteiten van de trustcentrumexploitant in de rol van certificaatautoriteit (CA) en registratieautoriteit (RA), evenals de gedelegeerde derde partij van de registratieautoriteit (RA).

Alleen partijen die gemachtigd zijn om deel te nemen aan TACHOnet, kunnen een certificaat aanvragen.

---

<sup>9</sup> Geïdentificeerd door de attribuutwaarde "O=" in de Subject Distinguished Name van het uitgegeven certificaat.

<sup>10</sup> De recentste versie van de CP/CPS van de SBCA van T-Systems is beschikbaar op <https://www.telesec.de/en/sbca-en/support/download-area/>.

Betreffende de aanvaarding van certificaten is punt 4.4.1 van het certificatiebeleid en de certificatiepraktijkverklaring (CP/CPS) van de SBCA van toepassing; bovendien worden de gebruiksvoorwaarden en bepalingen die zijn beschreven in het onderhavige document, geacht te zijn aangenomen door de organisatie waaraan het certificaat is afgegeven ("O=") zodra het certificaat een eerste keer wordt gebruikt.

Betreffende de publicatie van het certificaat is punt 2.2 van de CP/CPS van de SBCA van toepassing.

Alle houders van een certificaat moeten aan de volgende vereisten voldoen:

- 1) beschermen hun geheime sleutel tegen onrechtmatig gebruik;
- 2) zij sturen de geheime sleutels niet door of delen die niet mee aan derden, zelfs als vertegenwoordigers;
- 3) gebruiken de geheime sleutel niet langer nadat de geldigheidsduur is verstreken of het certificaat is ingetrokken, behalve om versleutelde gegevens te bekijken (bv. om e-mails te ontsleutelen).
- 4) de houder van het certificaat is verantwoordelijk voor het kopiëren of doorsturen van de sleutels naar de eindentiteit(en);
- 5) de houder van het certificaat moet de eindentiteit/alle eindentiteiten verplichten om aan deze voorwaarden te voldoen, met inbegrip van de CP/CPS van de SBCA, wanneer zij de geheime sleutel gebruiken;
- 6) de houder van het certificaat moet de vertegenwoordigers identificeren die gemachtigd zijn om de intrekking van de aan de organisatie afgegeven certificaten te vragen, met opgave van de gegevens over de gebeurtenissen die tot de intrekking hebben geleid en het intrekkingswachtwoord;
- 7) voor certificaten die zijn toegekend aan groepen personen en functies en/of rechtspersonen, moet de houder van het certificaat nadat een persoon de groep of eindentiteiten heeft verlaten (bv. bij stopzetting van de arbeidsovereenkomst) misbruik van de geheime sleutel voorkomen door het certificaat in te trekken;
- 8) de houder van het certificaat is verantwoordelijk en vraagt de intrekking van het certificaat aan onder de omstandigheden als bedoeld in punt 4.9.1 van de CP/CPS van de SBCA.

Wat betreft de verlenging of hersleuteling van certificaten is punt 4.6 of 4.7 van de CP/CPS van de SBCA van toepassing.

Wat betreft de wijziging van een certificaat is punt 4.8 van de CP/CPS van de SBCA van toepassing.

Wat betreft de intrekking van een certificaat is punt 4.9 van de CP/CPS van de SBCA van toepassing.

5. Identificatieformulier met contactpersonen en betrouwbare koeriers (voorbeeld)

**Ik, [naam en adres van de vertegenwoordiger van de organisatie], verklaar dat de volgende gegevens gebruikt moeten worden in het kader van de aanvraag, de aanmaak en de ophaling van digitale certificaten van publieke sleutels voor toegangspunten tot TACHOnet die de vertrouwelijkheid, de integriteit en de onweerlegbaarheid van de TACHOnet-berichten ondersteunen:**

Informatie over de contactpersoon:

| – Contactpersoon 1                 | – Contactpersoon 2                           |
|------------------------------------|----------------------------------------------|
| – Naam:                            | – Naam:                                      |
| – Voornamen:                       | – Voornamen:                                 |
| – Mobiele telefoon:                | – Mobiele telefoon:                          |
| – Telefoon:                        | – Telefoon:                                  |
| – E-mail:                          | – E-mail:                                    |
| – Voorbeeld van handtekening:<br>– | – Voorbeeld van handtekening:<br>–<br>–<br>– |

Informatie over de betrouwbare koerier:

| – Betrouwbare koerier 1          | – Betrouwbare koerier 2          |
|----------------------------------|----------------------------------|
| – Naam:                          | – Naam:                          |
| – Voornamen:                     | – Voornamen:                     |
| – Mobiele telefoon:              | – Mobiele telefoon:              |
| – E-mail:                        | – E-mail:                        |
| – Land van afgifte van paspoort: | – Land van afgifte van paspoort: |
| – Paspoortnummer:                | – Paspoortnummer:                |
| – Vervaldatum van het paspoort:  | – Vervaldatum van het paspoort:  |

**Plaats, datum, stempel van de onderneming of zegel van de organisatie:**

**Handtekening van de gemachtigde vertegenwoordiger:**

## 6. Documenten

### 6.1. Individuele volmacht (voorbeeld)

Een voorbeeld van de individuele volmacht die moet worden ondertekend en door de betrouwbare koerier moet worden voorgelegd tijdens de persoonlijke registratie bij de registratieautoriteit, kunt u hier vinden:

*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<sup>1</sup>: e.g. mail security (signature, encryption), virtual private network (VPN), TLS/SSL client

☐ server<sup>2</sup>: 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<sup>3</sup>: 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<sup>2</sup>** or **maximum of 36 months<sup>1,3</sup>** from date of issuance.

☐ The power of attorney is valid until \_\_\_\_\_ (mm.dd.yyyy), but up to a **maximum of 27 month<sup>2</sup>** months or **maximum of 36 months<sup>1,3</sup>** 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. Papieren aanvraagformulier voor een certificaat (voorbeeld)

Een voorbeeld van het papieren aanvraagformulier voor een certificaat dat moet worden ondertekend en door de betrouwbare koerier moet worden voorgelegd tijdens de persoonlijke registratie bij de registratieautoriteit, kunt u hier vinden:

## 7. Woordenlijst

De belangrijkste termen die in dit subaanhangsel worden gebruikt, zijn gedefinieerd onder CEF Definitions op de portaalsite CEF Digital:

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

De belangrijkste acroniemen die in deze beschrijving van componenten worden gebruikt, zijn gedefinieerd in het deel CEF Glossary op de portaalsite CEF Digital:

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

---