Rådet for
Den Europæiske Union

Bruxelles, den 5. november 2018
(OR. en)

13711/18
ADD 1

Interinstitutionel sag:
2018/0339(NLE)

TRANS 488

NOTE

fra:	Generalsekretariatet for Rådet
til:	delegationerne
Tidl. dok. nr.:	ST 13711/18 TRANS 448
Komm. dok. nr.:	ST 12727/18 TRANS 426 + ADD 1
Vedr.:	Rådets afgørelse om den holdning, som på Den Europæiske Unions vegne skal indtages i Ekspertgruppen vedrørende den Europæiske Overenskomst om Arbejde, der Udføres af det Kørende Personale i International Vejtransport, under De Forenede Nationers Økonomiske Kommission for Europa

Bilag til ovennævnte rådsafgørelse.

BILAG

Nyt tillæg til AETR-overenskomsten

Tillæg 4

TACHOnet-specifikationer

1. Anvendelsesområde og formål

1.1. Dette tillæg fastlægger betingelserne for forbindelsen til TACHOnet for kontraherende parter i AETR-overenskomsten gennem eDelivery.

1.2. Kontraherende parter, der tilslutter sig TACHOnet gennem eDelivery, skal overholde bestemmelserne i dette tillæg.

2. Definitioner

a) "kontraherende part" eller "part": enhver kontraherende part i AETR-overenskomsten

b) "eDelivery": tjenesten udviklet af Kommissionen, der gør det muligt at sende data mellem tredjeparter ad elektronisk vej og dokumenterer behandlingen af de sendte data, herunder leverer bevis for afsendelse og modtagelse af dataene, og som beskytter de sendte data mod risikoen for uautoriseret ændring

c) "TACHOnet":systemet til elektronisk udveksling af informationer om førerkort mellem de kontraherende parter som omhandlet i artikel 31, stk. 2, i forordning (EU) nr. 165/2014.

d) "central hub": det informationssystem, der gør det muligt at route TACHOnet-meddelelser mellem anmodende og besvarende parter

e) "anmodende part": den kontraherende part, der afgiver en TACHOnet-anmodning eller -meddelelse, som derefter routes af den centrale hub til den relevante besvarende part

f) "besvarende part": den kontraherende part, som TACHOnet-anmodningen eller -meddelelsen er rettet til

g) "kortudstedende myndighed" eller "CIA": den enhed, en kontraherende part har bemyndiget til at udstede og administrere takografkort.

3. Generelt ansvar

3.1. Ingen af de kontraherende parter kan indgå aftale om adgang til TACHOnet på vegne af en anden part eller på anden måde repræsentere den anden kontraherende part på grundlag af dette tillæg. Ingen af de kontraherende parter kan fungere som den anden kontraherende parts underleverandør i forbindelse med de aktiviteter, der er omhandlet i dette tillæg.

3.2. De kontraherende parter giver adgang til deres nationale register over førerkort via TACHOnet, på den måde og med det serviceniveau, der er fastlagt i undertillæg 4.6.

3.3. De kontraherende parter underretter straks hinanden, hvis de observerer forstyrrelser eller fejl inden for deres ansvarsområde, som kan bringe den normale drift af TACHOnet i fare.

3.4. Parterne udpeger hver især kontaktpersoner til TACHOnet og oplyser AETR-sekretariatet om disse. Enhver ændring i kontaktpunkter oplyses skriftligt til AETR-sekretariatet.

4. Test med henblik på forbindelse til TACHOnet

4.1. En kontraherende parts forbindelse til TACHOnet etableres efter en vellykket afslutning af test af forbindelse, integration og ydeevne i overensstemmelse med Kommissionens instrukser og under dennes tilsyn.

4.2. Hvis de indledende test ikke bestås, kan Kommissionen midlertidigt stille testfasen i bero. Testene genoptages, når den kontraherende part har givet Kommissionen meddelelse om vedtagelsen af de nødvendige tekniske forbedringer på nationalt plan, som muliggør en vellykket gennemførelse af de indledende test.

4.3. De indledende test varer maksimalt seks måneder.

5. Sikker arkitektur

5.1. TACHOnet-meddelelsernes fortrolighed, integritet og uafviselighed sikres af den sikre TACHOnet-arkitektur.

5.2. Den sikre TACHOnet-arkitektur baseres på en Public Key Infrastructure (PKI) oprettet af Kommissionen; kravene til PKI'en er fastsat i undertillæg 4.8 og 4.9.

5.3. Følgende enheder inddrages i den sikre TACHOnet-arkitektur:

a) Certificeringsenhed: ansvarlig for generering af de digitale certifikater, som leveres af registreringsenheden til de kontraherende parters nationale myndigheder (via betroede kurerer udpeget af disse), samt for etablering af den tekniske infrastruktur for udstedelse, tilbagekaldelse og fornyelse af digitale certifikater.

b) Domæneejer: ansvarlig for driften af den centrale hub som omhandlet i undertillæg 4.1, og for valideringen og koordineringen af den sikre TACHOnet-arkitektur.

c) Registreringsenhed: ansvarlig for registrering og godkendelse af anmodninger om udstedelse, tilbagekaldelse og fornyelse af digitale certifikater og for verificering af de betroede kurerers identitet.

d) Betroet kurer: den person, der er udpeget af de nationale myndigheder, og som er ansvarlig for at overdrage den offentlige nøgle til registreringsenheden og for at få det pågældende certifikat, der genereres af certificeringsenheden.

e) Den kontraherende parts nationale myndighed, som:

i) genererer de private nøgler og de tilsvarende offentlige nøgler, som skal være omfattet af de certifikater, der genereres af certificeringsenheden

ii) anmoder certificeringsenheden om de digitale certifikater

iii) udpeger den betroede kurer.

5.4. Certificeringsenheden og registreringsenheden udpeges af Kommissionen.

5.5. Enhver kontraherende part, der tilslutter sig TACHOnet, skal anmode om udstedelse af et digitalt certifikat i henhold til undertillæg 4.9 med henblik på at kunne underskrive og kryptere en TACHOnet-meddelelse.

5.6. Et certifikat kan trækkes tilbage i henhold til undertillæg 4.9.

6. Databeskyttelse og tavshedspligt

6.1. Parterne skal i overensstemmelse med databeskyttelseslovgivningen på internationalt og nationalt plan og navnlig konventionen om beskyttelse af personer i forbindelse med automatisk behandling af personoplysninger vedtage alle nødvendige tekniske og organisatoriske foranstaltninger med henblik på at sikre TACHOnet-dataenes sikkerhed og forhindre ændring eller tab af eller uautoriseret behandling af eller adgang til disse data (navnlig meddelelsernes ægthed, datafortrolighed, sporbarhed, integritet, tilgængelighed, afviselighed og sikkerhed).

6.2. Parterne beskytter hver især deres egne nationale systemer mod ulovlig brug, ondsindet kode, vira, uautoriseret indtrængen i computersystemer, brud på datasikkerheden, ulovlig manipulation af data og andre lignende handlinger fra tredjeparters side. Parterne er enige om at anvende kommercielt rimelige metoder til at undgå overførsel af vira, tidsbomber, orme eller lignende genstande samt andre programmeringsrutiner, der kan forstyrre den anden parts computersystemer.

7. Omkostninger

7.1. De kontraherende parter afholder egne udviklings- og driftsomkostninger i forbindelse med deres egne datasystemer og procedurer, i det omfang det er nødvendigt for at opfylde forpligtelserne i henhold til dette tillæg.

7.2. De tjenester, der er angivet i undertillæg 4.1, og som leveres af den centrale hub, stilles til rådighed vederlagsfrit.

8. Underentreprise

8.1. Parterne kan give enhver af tjenesterne, som de er ansvarlige for i henhold til dette tillæg, i underentreprise.

8.2. En sådan underentreprise fritager ikke parten for det ansvar, der påhviler den i henhold til dette tillæg, herunder ansvaret for at sikre et passende serviceniveau i henhold til undertillæg 4.6.

Undertillæg 4.1

Generelle aspekter af TACHOnet

1. Generel beskrivelse

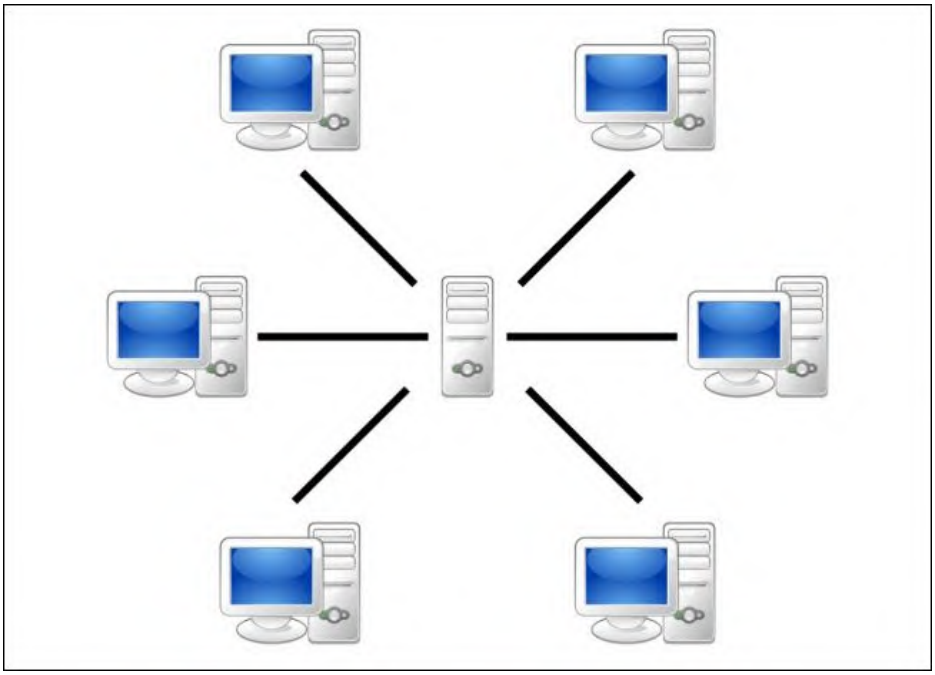
TACHOnet er et elektronisk system til udveksling af informationer om førerkort mellem kontraherende parter i AETR-overenskomsten. TACHOnet router anmodninger om information fra de anmodende parter til de besvarende parter, samt svar fra sidstnævnte til førstnævnte. Kontraherende parter, der er en del af TACHOnet, kobler deres nationale registre over førerkort til systemet.

2. Arkitektur

Meddelelsessystemet TACHOnet består af følgende dele:

2.1. En central hub, som er i stand til at modtage en anmodning fra den anmodende part, validere anmodningen og behandle den ved at videresende den til de besvarende parter. Den centrale hub afventer svar fra hver af de besvarende parter, samler alle svarene og videresender det samlede svar til den anmodende part.

2.2. Parternes nationale systemer, som er udstyret med en grænseflade, der både kan sende anmodninger til den centrale hub og modtage svar på disse. Nationale systemer kan bruge egenudviklet eller kommerciel software til at sende og modtage meddelelser fra den centrale hub.



3. Forvaltning

3.1. Den centrale hub forvaltes af Kommissionen, som er ansvarlig for dens tekniske drift og vedligeholdelse.

3.2. Data opbevares i den centrale hub i højst seks måneder med undtagelse af de logføringsdata og statistiske data, som er anført i undertillæg 4.7.

3.3. Den centrale hub giver ikke adgang til personoplysninger. Autoriseret personale i Kommissionen kan dog tildeles adgang, hvis det er nødvendigt i forbindelse med overvågning, vedligeholdelse og fejlfinding.

3.4. De kontraherende parter er hver især ansvarlige for:

3.4.1. Opsætning og forvaltning af deres nationale systemer, herunder grænsefladen med den centrale hub.

3.4.2. Installation og vedligeholdelse af deres nationale system, både hvad angår hardware og software, hvad enten det er egenudviklet eller kommercielt.

3.4.3. Korrekt interoperabilitet mellem deres nationale system og den centrale hub, herunder håndtering af fejlmeddelelser, som modtages fra den centrale hub.

3.4.4. At træffe alle nødvendige foranstaltninger for at sikre oplysningernes fortrolighed, integritet og tilgængelighed.

3.4.5. Driften af de nationale systemer i overensstemmelse med det serviceniveau, som er fastsat i undertillæg 4.6.

Undertillæg 4.2

TACHOnets funktioner

1. Følgende funktioner stilles til rådighed via meddelelsessystemet TACHOnet:

1.1. Check Issued Cards (CIC): Giver den anmodende part mulighed for at sende en anmodning om kontrol af udstedte kort (CIC-anmodning) til en af eller alle de besvarende parter med henblik på at fastslå, om en kortansøger i forvejen besidder et førerkort udstedt af de besvarende parter. De besvarende parter svarer på anmodningen ved at fremsende et CIC-svar.

1.2. Check Card Status (CCS): Giver den anmodende part mulighed for at anmode den besvarende part om nærmere oplysninger om et kort udstedt af sidstnævnte ved at sende en anmodning om kontrol af kortstatus (CCS-anmodning). Den besvarende part svarer på anmodningen ved at fremsende et CCS-svar.

1.3. Modify Card Status (MCS): Giver den anmodende part mulighed for at underrette den besvarende part, via en anmodning om ændring af kortstatus (MCS-anmodning), om, at status på et kort udstedt af sidstnævnte er ændret. Den besvarende part svarer på anmodningen med en MCS-bekræftelse.

1.4. Issued Card Driving License (ICDL): Giver den anmodende part mulighed for at underrette den besvarende part, via en anmodning om svar vedrørende kort udstedt på grundlag af kørekort (ICDL-anmodning), om, hvorvidt et kort er blevet udstedt af førstnævnte på grundlag af et kørekort udstedt af sidstnævnte. Den besvarende part svarer på anmodningen med et ICDL-svar.

2. Andre meddelelsestyper, som anses for at være nødvendige for TACHOnettets effektive funktion inkluderes, f.eks. fejlmeddelelser.

3. De nationale systemer skal anerkende de kortstatusser, som er opført på listen i tabel 1, når de anvender funktionerne i punkt 1. Parterne er dog ikke forpligtet til at indføre en administrativ procedure, som gør brug af samtlige statustyper på listen.

4. Hvis en part modtager et svar eller en meddelelse, som indeholder en status, der ikke anvendes i den administrative procedure, skal det nationale system omsætte statussen i meddelelsen til procedurens tilsvarende værdi. Meddelelsen må ikke afvises af den besvarende part, såfremt den status, der fremgår af meddelelsen, er opført på listen i tabel 1.

5. De kortstatusser, som er opført på listen i tabel 1, må ikke anvendes til at afgøre, om et førerkort er gyldigt. Når en part sender en forespørgsel til registret hos den kortudstedende nationale myndighed via CCS-funktionen, skal svaret indeholde det specifikke felt "gyldigt førerkort". De nationale administrative procedurer skal være udformet på en sådan måde, at CCS-svar altid indeholder en tilsvarende værdi for "gyldigt førerkort".

Tabel 1

Kortstatusser

Kortstatus	**Definition**
Ansøgning	Den kortudstedende myndighed har modtaget en ansøgning om udstedelse af et førerkort. Disse oplysninger er blevet registreret og lagret i databasen med de genererede søgenøgler.
Godkendt	Den kortudstedende myndighed har godkendt ansøgningen om et takografkort.
Afslået	Den kortudstedende myndighed har afslået ansøgningen.
Personligt tilpasset	Takografkortet er blevet personligt tilpasset.
Afsendt	Den nationale myndighed har afsendt førerkortet til den pågældende fører eller det pågældende leveringsorgan.
Overdraget	Den nationale myndighed har overdraget førerkortet til den pågældende fører.
Konfiskeret	Den kompetente myndighed har inddraget førerens førerkort.
Suspenderet	Førerens førerkortet er blevet midlertidigt inddraget.
Tilbagekaldt	Den kortudstedende myndighed har besluttet at tilbagekalde førerkortet. Kortet er blevet endegyldigt ugyldiggjort.
Afleveret	Takografkortet er blevet afleveret til den kortudstedende myndighed og erklæret som ikke længere nødvendigt.
Bortkommet	Takografkortet er blevet meldt bortkommet til den kortudstedende myndighed.
Stjålet	Takografkortet er blevet meldt stjålet til den kortudstedende myndighed. Et stjålet kort anses for at være tabt.
Uanvendeligt	Takografkortet er blevet meldt uanvendeligt til den kortudstedende myndighed.
Udløbet	Takografkortets gyldighedsperiode er udløbet.
Erstattet	Takografkortet, som er meldt bortkommet, stjålet eller uanvendeligt, er blevet erstattet med et nyt kort. Oplysningerne på det gamle kort og det nye kort er de samme med undtagelse af kortnummerets erstatningsindeks, som er blevet øget med én.

Fornyet	Takografkortet er blevet fornyet på grund af ændringer i de administrative data, eller fordi gyldighedsperioden er udløbet. Det nye kort har samme kortnummer som det gamle med undtagelse af kortnummerets erstatningsindeks, som er blevet øget med én.
Under udskiftning	Den kortudstedende myndighed, som har udstedt førerkortet, har modtaget en meddelelse om, at proceduren for at udskifte dette kort med et førerkort, som er udstedt af en anden parts kortudstedende myndighed, er påbegyndt.
Udskiftet	Den kortudstedende myndighed, som har udstedt førerkortet, har modtaget en meddelelse om, at proceduren for at udskifte dette kort med et førerkort, som er udstedt af en anden parts udstedende myndighed, er fuldført.

Undertillæg 4.3

Bestemmelser for TACHOnet-meddelelser

1. Generelle tekniske krav

1.1. Den centrale hub skal tilbyde både synkrone og asynkrone grænseflader til udveksling af meddelelser. Parterne kan udvælge den teknologi, der er mest egnet som grænseflade med deres egne applikationer.

1.2. Alle meddelelser, der udveksles mellem den centrale hub og de nationale systemer, skal indkodes med UTF-8.

1.3. De nationale systemer skal være i stand til at modtage og behandle meddelelser, der indeholder græske eller kyrilliske skrifttegn.

2. XML-meddelelsesstruktur og XML Schema Definition (XSD)

2.1. XML-meddelelsernes generelle struktur skal følge det format, som er defineret af de XSD-skemaer, der er installeret i den centrale hub.

2.2. Den centrale hub og de nationale systemer skal sende og modtage meddelelser, som er i overensstemmelse med meddelelsernes XSD-skema.

2.3. De nationale systemer skal være i stand til at sende, modtage og behandle alle meddelelser, som svarer til funktionerne i undertillæg 4.2.

2.4. XML-meddelelserne skal som minimum overholde de mindstekrav, som er opført i tabel 2.

Tabel 2

Mindstekrav til indholdet af XML-meddelelserne

Fælles header		**Obligatorisk**
Version	XML-specifikationernes officielle version specificeres i det navneområde, som er defineret i meddelelsens XSD, og i attributten *version* i headerelementet i alle XML-meddelelser. Versionsnummeret ("n.m") defineres som en fast værdi i hver version af XML Schema Definition-filen (xsd).	Ja
Testidentifikator	Valgfrit ID til testning. Testens ophavsmand udfylder ID'et, og alle deltagere i workflowet videresender/svarer med det samme ID. Der bør ses bort fra ID'et under produktionen, og det anvendes ikke, hvis det forekommer.	Nej
Teknisk identifikator	Et UUID, som entydigt identificerer hver enkelt meddelelse. Afsenderen genererer UUID'et og udfylder denne attribut. Denne oplysning bruges ikke i erhvervsøjemed.	Ja
Workflow-identifikator	Attributten workflowId er et UUID, som genereres af den anmodende part. Dette ID bruges derefter i alle meddelelser til at koordinere workflowet.	Ja
Afsendelsestidspunkt	Dato og tidspunkt (UTC) for afsendelse af meddelelsen.	Ja
Timeout	Dette er en valgfri attribut med dato og klokkeslæt (i UTC-format). Værdien fastsættes kun af den centrale hub i videresendte anmodninger. Hermed underrettes den besvarende part om, hvor lang tid der går, før anmodningen udløber. Denne værdi er ikke påkrævet i MS2TCN_<x>_Req eller nogen svarmeddelelser. Den er valgfri, så den samme headerdefinition kan anvendes for alle typer meddelelser, uanset om attributten timeoutValue kræves eller ej.	Nej
Fra	ISO 3166-1-alpha 2-koden for den part, som afsender meddelelsen, eller "EU".	Ja
Til	ISO 3166-1-alpha 2-koden for den part, som meddelelsen sendes til, eller "EU".	Ja

Undertillæg 4.4

Translitterations- og NYSIIS-tjenester (New York State Identification and Intelligence System)

1. NYSIIS-algoritmen, som er implementeret i den centrale hub, anvendes til at indkode navnene på alle førere i det nationale register.

2. Når der søges efter et kort via CIC-funktionen, anvendes NYSIIS-nøglerne som den primære søgemekanisme.

3. Derudover kan parterne anvende en egen algoritme for at opnå flere resultater.

4. Søgeresultaterne viser, hvilken søgemekanisme der blev anvendt til at finde en given post: enten NYSIIS eller partens egen.

5. Hvis en part vælger at registrere ICDL-meddelelser, skal NYSIIS-nøglerne i disse meddelelser registreres som en del af ICDL-dataene. Ved søgning i ICDL-data anvender parten NYSIIS-nøglen for ansøgerens navn.

Undertillæg 4.5

Sikkerhedskrav

1. HTTPS anvendes til udveksling af meddelelser mellem den centrale hub og de nationale systemer.

2. De nationale systemer skal anvende de digitale certifikater som omhandlet i undertillæg 4.8 og 4.9 med det formål at sikre overførslen af meddelelser mellem det nationale system og den centrale hub.

3. De nationale systemer skal som minimum anvende certifikater, der bruger SHA-2 (SHA-256) som hashalgoritme for signatur og en offentlig nøgle med en længde på 2048 bit.

Undertillæg 4.6

Serviceniveau

1. De nationale systemer skal opfylde følgende minimumskrav til deres serviceniveau:

1.1. De skal være tilgængelige 24 timer i døgnet, 7 dage om ugen.

1.2. Deres tilgængelighed skal overvåges ved hjælp af en impulsmeddelelse fra den centrale hub.

1.3. Deres tilgængelighedsgrad skal være på 98 % i henhold til følgende tabel (tallene er blevet afrundet til den nærmeste praktiske enhed):

Tilgængelighed på	svarer til, at systemet ikke er tilgængeligt		
	Dagligt	Månedligt	Årligt
98 %	0,5 timer	15 timer	7,5 dage

Parterne opfordres til at overholde den daglige tilgængelighedsgrad. Det anerkendes dog, at visse nødvendige aktiviteter, såsom systemvedligeholdelse, kræver, at systemet bliver utilgængeligt i mere end 30 minutter ad gangen. De månedlige og årlige tilgængelighedsgrader er dog stadig obligatoriske.

1.4. De skal som minimum besvare 98 % af de anmodninger, som tilsendes dem i løbet af en kalendermåned.

1.5. De skal besvare en anmodning inden for 10 sekunder.

1.6. Den globale timeout for anmodninger (den øverste tidsgrænse for svar til den anmodende bruger) må ikke overstige 20 sekunder.

1.7. De skal som minimum kunne håndtere 6 anmodninger pr. sekund.

1.8. De nationale systemer må ikke sende flere end 2 anmodninger til TACHOnet-hubben pr. sekund.

1.9. Alle nationale systemer skal være i stand til at håndtere eventuelle tekniske problemer med den centrale hub eller de nationale systemer hos andre parter. De omfatter, men er ikke begrænset til:

a) tab af forbindelsen til den centrale hub

b) manglende svar på en anmodning

c) modtagelse af svar efter meddelelsens timeout

d) modtagelse af meddelelser, som der ikke er anmodet om

e) modtagelse af ugyldige meddelelser

2. Den centrale hub skal:

2.1. have en tilgængelighedsgrad på 98 %

2.2. underrette de nationale systemer om enhver fejl via enten en svarmeddelelse eller en særskilt fejlmeddelelse. De nationale systemer skal til gengæld modtage disse fejlmeddelelser og have etableret en fejlafhjælpningsprocedure, der kan håndtere og rette fejlen.

3. Vedligeholdelse

Parterne underretter via webapplikationen de andre parter og Kommissionen om rutinemæssige vedligeholdelsesaktiviteter, mindst én uge før disse aktiviteter påbegyndes, hvis det er teknisk muligt.

Undertillæg 4.7

Logning af og statistik over data, som indsamles på den centrale hub

1. For at sikre beskyttelsen af personoplysninger skal data til statistiske formål være anonyme. Data, som kan identificere et specifikt kort, en specifik fører eller et specifikt kørekort, må ikke være tilgængelige til statistiske formål.

2. Logning af oplysninger anvendes til at holde kontrol med alle transaktioner af hensyn til overvågning og fejlretning og for at kunne generere statistik om disse transaktioner.

3. Personoplysninger opbevares i loggen i maksimalt seks måneder. Statistiske oplysninger opbevares på ubestemt tid.

4. De statistiske rapporteringsdata omfatter:

   a) den anmodende part

   b) den besvarende part

   c) meddelelsestypen

   d) svarets statuskode

   e) meddelelsernes dato og klokkeslæt

   f) svartiden.

Undertillæg 4.8

Generelle bestemmelser for digitale nøgler og certifikater til TACHOnet

1. Kommissionens Generaldirektorat for Informationsteknologi (DIGIT) stiller en PKI-tjeneste[1] (benævnt "CEF PKI-tjeneste") til rådighed for de kontraherende parter i AETR-overenskomsten, der tilslutter sig TACHOnet, (herefter de nationale myndigheder) gennem eDelivery.

2. Processen for anmodning og tilbagekaldelse af digitale certifikater samt de detaljerede betingelser for anvendelsen af disse er defineret i tillægget.

3. Anvendelse af certifikater:

3.1. Når et certifikat er udstedt, anvender den nationale myndighed[2] udelukkende certifikatet i forbindelse med TACHOnet. Certifikatet kan anvendes til at:

a) bekræfte datas oprindelse

b) kryptere data

c) sikre påvisning af integritetsbrud på data.

3.2. Enhver anvendelse, der ikke er udtrykkeligt godkendt som en af certifikatets tilladte anvendelsesmuligheder, er forbudt.

4. De kontraherende parter:

a) beskytter deres private nøgle mod uautoriseret brug

b) undgår at overdrage eller oplyse deres private nøgle til tredjeparter, også som repræsentanter

---

1 En PKI (Public Key Infrastructure) er en række roller, politikker, procedurer og systemer, der er nødvendige for at oprette, administrere, distribuere og tilbagekalde digitale certifikater.

2 Identificeret ved attributværdien "O=" i det udstedte certifikats Subject Distinguished Name.

c) sikrer fortroligheden, integriteten og tilgængeligheden af de private nøgler, der genereres, opbevares og anvendes i forbindelse med TACHOnet

d) undgår fortsat brug af den private nøgle efter gyldighedsperiodens udløb eller certifikatets tilbagekaldelse, bortset fra med det formål at få vist krypterede data (f.eks. dekryptering af e-mails). Udløbne nøgler skal enten tilintetgøres eller opbevares på en måde, der forhindrer brugen af dem

e) indsender til registreringsenheden identifikation for de autoriserede repræsentanter, der er autoriseret til at anmode om tilbagekaldelse af certifikater udstedt til organisationen (anmodninger om tilbagekaldelse skal omfatte en adgangskode til anmodning om tilbagekaldelse samt oplysninger om de hændelser, der medfører tilbagekaldelse)

f) forebygger misbrug af den private nøgle ved at anmode om tilbagekaldelse af det hermed forbundne PKI-certifikat i tilfælde af kompromittering af den private nøgle eller af aktiveringsdataene for den private nøgle

g) er ansvarlige for og forpligtet til at anmode om tilbagekaldelse af certifikatet i de tilfælde, der er identificeret i certificeringsenhedens certificeringspolitik (CP) og certificeringspraksis (CPS)

h) underretter straks registreringsenheden om tab, tyveri eller potentiel kompromittering af en AETR-nøgle anvendt i forbindelse med TACHOnet.

5. Ansvar

Uden at det berører Europa-Kommissionens ansvar på en måde, der strider mod eventuelle krav ifølge gældende national ret, eller ansvar i tilfælde, hvor ansvar ikke kan udelukkes ifølge den pågældende ret, er Europa-Kommissionen ikke ansvarlig for:

a) certifikatets indhold; ansvaret for dette er udelukkende certifikatindehaverens. Det er certifikatindehaverens ansvar at kontrollere certifikatindholdets nøjagtighed

b) certifikatindehaverens anvendelse af certifikatet.

Undertillæg 4.9

Beskrivelse af PKI-tjenesten for TACHOnet

1. Indledning

En PKI (Public Key Infrastructure) er en række roller, politikker, procedurer og systemer, der er nødvendige for at oprette, administrere, distribuere og tilbagekalde digitale certifikater[3]. CEF PKI-tjenesten i eDelivery gør det muligt at udstede og administrere digitale certifikater, der anvendes til at sikre fortroligheden, integriteten og afviseligheden af informationer, som udveksles via adgangspunkter (AP).

PKI-tjenesten i eDelivery er baseret på Trust Center Services TeleSec Shared Business CA (certificeringsenhed), som er underlagt certificeringspolitikken (CP)/certificeringspraksissen (CPS) i T-Systems International GmbH's Trust Center Services TeleSec Shared Business CA[4].

PKI-tjenesten udsteder certifikater, der er egnede til at sikre forskellige forretningsprocesser internt og eksternt i virksomheder, organisationer, offentlige myndigheder og institutioner, der kræver et middel sikkerhedsniveau for at dokumentere slutenhedens ægthed, integritet og troværdighed.

2. Proces for anmodning om certifikat

2.1. Roller og ansvarsområder

2.1.1. "Organisation" eller "national myndighed", der anmoder om certifikatet

2.1.1.1. Den nationale myndighed anmoder om certifikaterne inden for rammerne af TACHOnet-projektet.

2.1.1.2 Den nationale myndighed:

a) anmoder om certifikaterne hos CEF PKI-tjenesten

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

[4] Den nyeste version af CP og CPS kan downloades på https://www.telesec.de/en/sbca-en/support/download-area/.

b) genererer de private nøgler og de tilsvarende offentlige nøgler, der skal være omfattet af de certifikater, som udstedes af certificeringsenheden

c) downloader certifikatet, når det er blevet godkendt

d) underskriver og returnerer til registreringsenheden:

i) identifikationsformularen for kontaktpersoner og betroede kurerer

ii) den underskrevne individuelle fuldmagt[5].

2.1.2. Betroet kurer

2.1.2.1. Den nationale myndighed udpeger en betroet kurer.

2.1.2.2. Den betroede kurer:

a) overdrager den offentlige nøgle til registreringsenheden via en proces, der omfatter identifikation og registrering ved personligt fremmøde

b) modtage det pågældende certifikat fra registreringsenheden.

2.1.3. Domæneejer

2.1.3.1. DG MOVE er domæneejer.

2.1.3.2. Domæneejeren:

a) validerer og koordinerer TACHOnet-netværket og den sikre TACHOnet-arkitektur, herunder foretager validering af procedurerne for udstedelse af certifikaterne

b) driver den centrale hub for TACHOnet og koordinerer parternes aktivitet med hensyn til TACHOnets funktion

c) gennemfører sammen med de nationale myndigheder testene af forbindelsen til TACHOnet.

[5] En fuldmagt er et juridisk dokument, med hvilket organisationen bemyndiger Kommissionen, repræsenteret ved den identificerede officielle ansvarlige for CEF PKI-tjenesten til at anmode T-Systems International GmbH's TeleSec Shared Business CA om at generere et certifikat på dennes vegne. Se også punkt 6.

2.1.4. Registreringsenhed

2.1.4.1. Det Fælles Forskningscenter (JRC) er registreringsenhed.

2.1.4.2. Registreringsenheden er ansvarlig for at verificere den betroede kurers identitet samt for registrering og godkendelse af anmodningerne om udstedelse, tilbagekaldelse og fornyelse af digitale certifikater.

2.1.4.3. Registreringsenheden:

a) tildeler den nationale myndighed en unik identifikator

b) bekræfter den nationale myndigheds identitet, kontaktpunkter og betroede kurerer

c) kommunikerer med CEF Support om den nationale myndigheds ægthed, kontaktpunkter og betroede kurerer

d) underretter den nationale myndighed om godkendelse eller afvisning af certifikatet.

2.1.5. Certificeringsenhed

2.1.5.1. Certificeringsmyndigheden er ansvarlig for at stille den tekniske infrastruktur til anmodning, udstedelse og tilbagekaldelse af digitale certifikater til rådighed.

2.1.5.2. Certificeringsenheden:

a) stiller den tekniske infrastruktur til nationale myndigheders certifikatanmodninger til rådighed

b) validerer eller afviser certifikatanmodninger

c) kommunikerer efter behov med registreringsenheden om verificering af identiteten på den anmodende organisation.

2.2. Udstedelse af certifikat

2.2.1. Udstedelsen af certifikater skal finde sted i henhold til følgende sekventielle trin, vist i figur 1:

a) **Trin 1:** Identifikation af betroet kurer

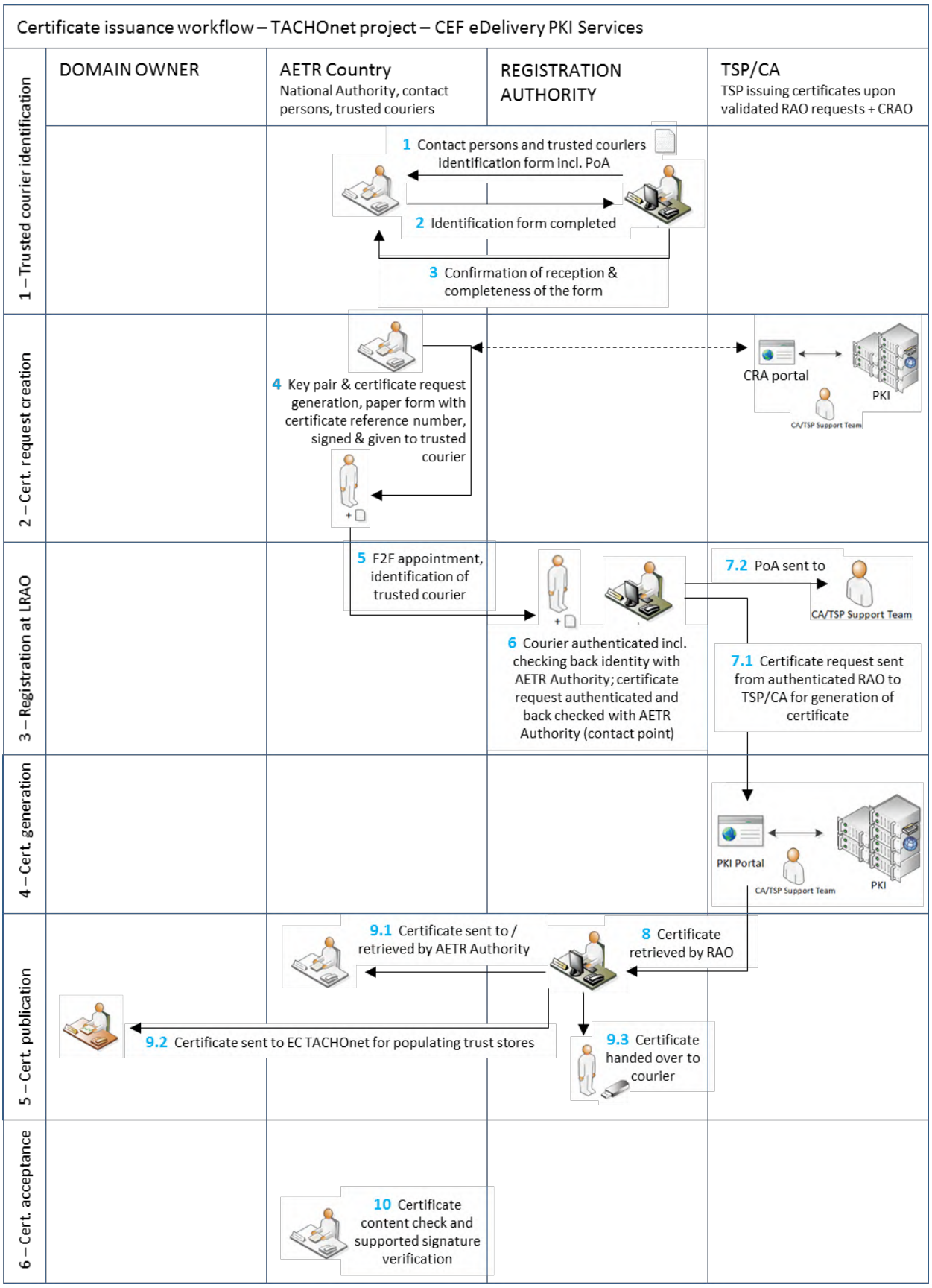
b) **Trin 2:** Udarbejdelse af anmodning om certifikat

c) **Trin 3**: Registrering hos registreringsenheden

d) **Trin 4:** Generering af certifikat

e) **Trin 5:** Offentliggørelse af certifikat

f) **Trin 6:** Accept af certifikat.



Figur 1 - Workflow for udstedelse af certifikat

2.2.2. Trin 1: Identifikation af betroet kurer

Følgende proces gennemføres med henblik på identifikation af en betroet kurer:

a) Registreringsenheden sender kontaktpersonernes og de betroede kurerers identifikationsformular til den nationale myndighed[6]. Formularen ledsages af en fuldmagt (PoA), som organisationen (AETR-myndigheden) underskriver.

b) Den nationale myndighed returnerer den udfyldte formular og underskrevne PoA til registreringsenheden.

c) Registreringsenheden bekræfter at have modtaget formularen, og at den er udfyldt.

d) Registreringsenheden sender en opdateret kopi af listen over kontaktpersoner og betroede kurerer til domæneejeren.

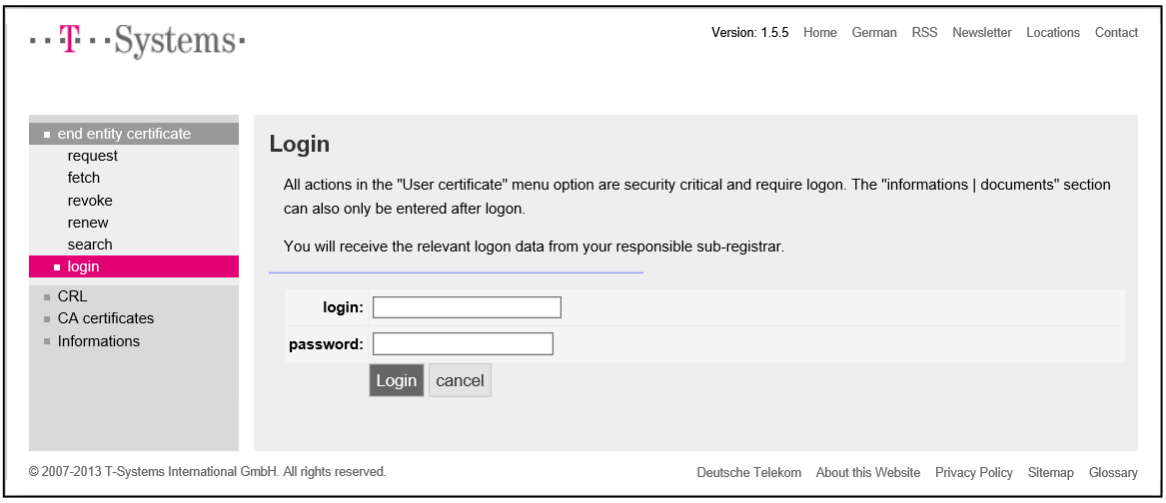
2.2.3. Trin 2: Udarbejdelse af anmodning om certifikat

2.2.3.1. Anmodningen og hentningen af certifikatet skal foretages på samme computer og med samme browser.

2.2.3.2. Følgende proces gennemføres med henblik på udarbejdelse af en anmodning om certifikat:

a) Organisationen navigerer til brugerens web-interface for at anmode om certifikatet via følgende URL: https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: og indtaster herefter brugernavnet "**sbca/CEF_eDelivery.europa.eu**" og adgangskoden "**digit.333**".

6 Se punkt 5.

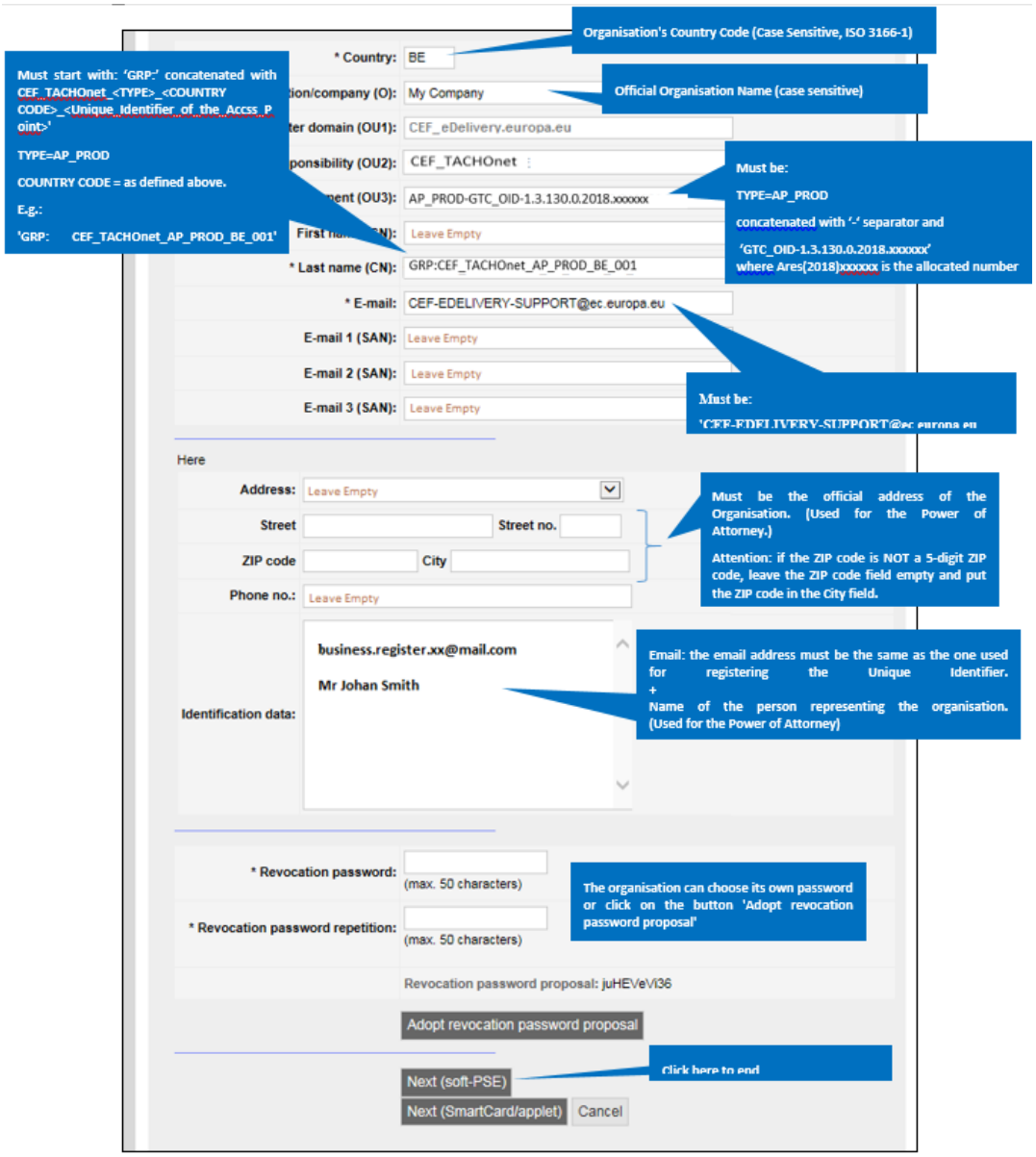


Figur 2

b) Organisationen klikker på "request" i panelets venstre side og vælger "CEF_TACHOnet" i rullemenuen.

Figur 3

c) Organisationen udfylder formularen til anmodning om certifikat som vist i figur 4 med oplysningerne i tabel 3 og klikker på "Next (soft-PSE)" for at afslutte processen.


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

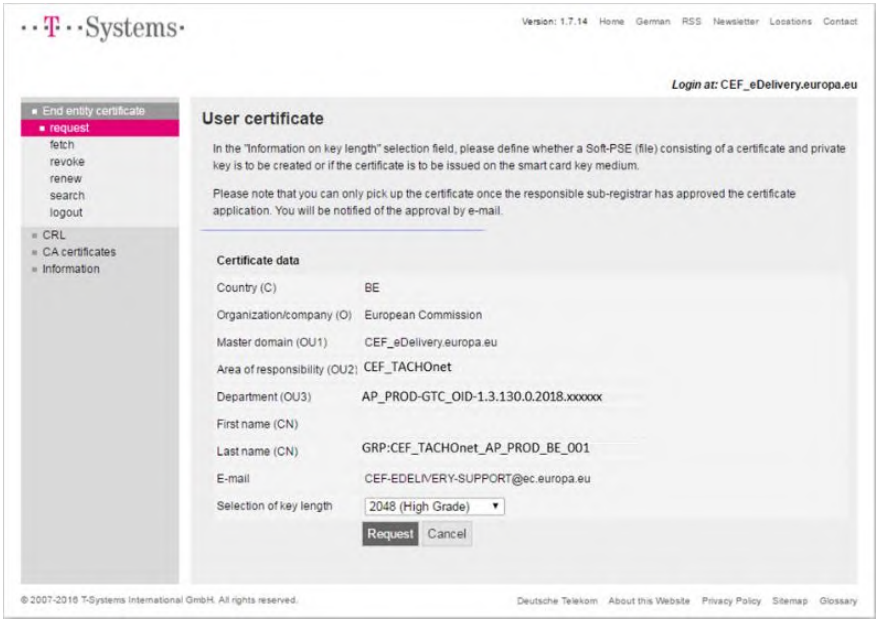
Figur 4

Felter til udfyldelse	Beskrivelse
Land	**C=landekode**, certifikatindehaverens hjemsted, verificeret ved hjælp af et offentligt register Begrænsninger: 2 tegn, i henhold til ISO 3166-1-alpha-2, forskel på små og store bogstaver Eksempler: DE, BE, NL Særlige tilfælde: UK (for Det Forenede Kongerige), EL (for Grækenland)
Organisation/Virksomhed (O)	**O=navnet på certifikatindehaverens organisation**
Masterdomæne (OU1)	**OU=CEF_eDelivery.europa.eu**
Ansvarsområde (OU2)	**OU=CEF_TACHOnet**
Afdeling (OU3)	Obligatorisk værdi pr. "ANSVARSOMRÅDE" Indholdet skal kontrolleres ved hjælp af en positivliste (hvidliste), når anmodningen om certifikatet er indsendt. Hvis informationen ikke er i overensstemmelse med listen, afvises anmodningen. Format: **OU=<TYPE>-<GTC_NUMBER>** Hvis "<TYPE>" erstattes af AP_PROD: Adgangspunkt i produktionsomgivelser. Og hvis <GTC_NUMBER> er **GTC_OID-1.3.130.0.2018.xxxxxx**, hvor Ares(2018)xxxxxx er GTC-nummeret for TACHOnet-projektet. f.eks.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
Fornavn (CN)	Skal være tomt
Efternavn (CN)	Skal begynde med "GRP:", efterfulgt af et fællesnavn. Format: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** f.eks.: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
E-mail 1 (SAN)	Skal være tomt
E-mail 2 (SAN)	Skal være tomt
E-mail 3 (SAN)	Skal være tomt

Adresse	Skal være tomt
Gade	Skal være den officielle adresse for certifikatindehaverens organisation. (Anvendes til fuldmagten.)
Husnr.	Skal være den officielle adresse for certifikatindehaverens organisation. (Anvendes til fuldmagten.)
Postnummer	Skal være den officielle adresse for certifikatindehaverens organisation. (Anvendes til fuldmagten.) **Bemærk**: Hvis postnummeret ikke er femcifret, efterlades feltet til postnummer tomt, og postnummeret anføres i feltet for by.
By	Skal være den officielle adresse for certifikatindehaverens organisation. (Anvendes til fuldmagten.) **Bemærk**: Hvis postnummeret ikke er femcifret, efterlades feltet til postnummer tomt, og postnummeret anføres i feltet for by.
Telefonnr.	Skal være tomt
Identifikationsdata	E-mailadressen skal være den samme som den, der anvendes til registrering af den unikke identifikator. + Skal være navnet på den person, der repræsenterer organisationen. (Anvendes til fuldmagten) + **Virksomhedsregisternr.** (kun obligatorisk for private virksomheder) **Registreret ved retten i** (kun påkrævet for tyske og østrigske private virksomheder)
Adgangskode til tilbagekaldelse	Obligatorisk felt valgt af den anmodende bruger
Gentagelse af adgangskode til tilbagekaldelse	Gentagelse af obligatorisk felt valgt af den anmodende bruger

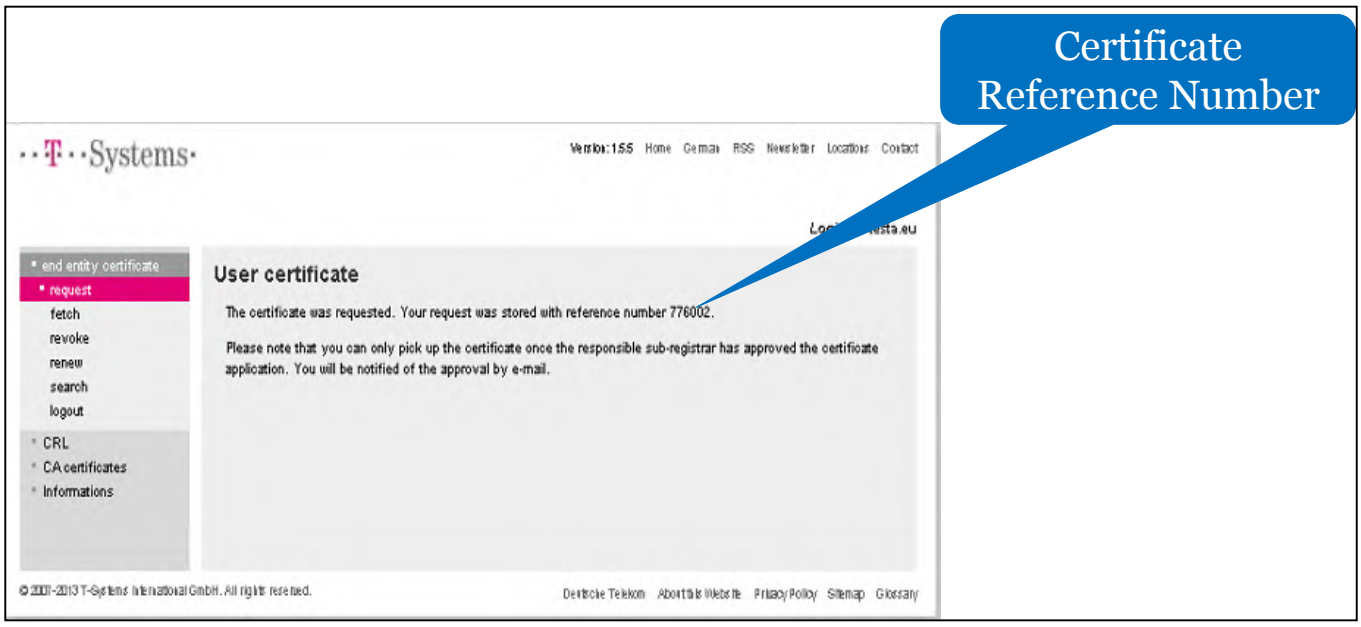
Tabel 3. Indførelse af oplysninger i alle påkrævede felter

d) Den valgte nøglelængde skal være 2048 (High Grade).



Figur 5

e) Organisationen skal registrere referencenummeret, der skal opgives ved afhentning af certifikatet.



Figur 6

f) CEF Support Team tjekker for nye anmodninger om certifikater og verificerer, om oplysningerne i certifikatanmodningen er gyldige, dvs. om de følger konventionen for navngivning i tillæg 5.1.

g) CEF Support Team verificerer, at oplysningerne i anmodningen er i et gyldigt format.

h) Viser tjekket i punkt 5 eller 6 ovenfor, at kravene ikke er opfyldt, sender CEF Support Team en e-mail til den e-mailadresse, der er anført under "Identifikationsoplysninger" i anmodningsformularen, med domæneejeren i cc, hvor organisationen anmodes om at påbegynde processen på ny. Den afviste certifikatanmodning annulleres.

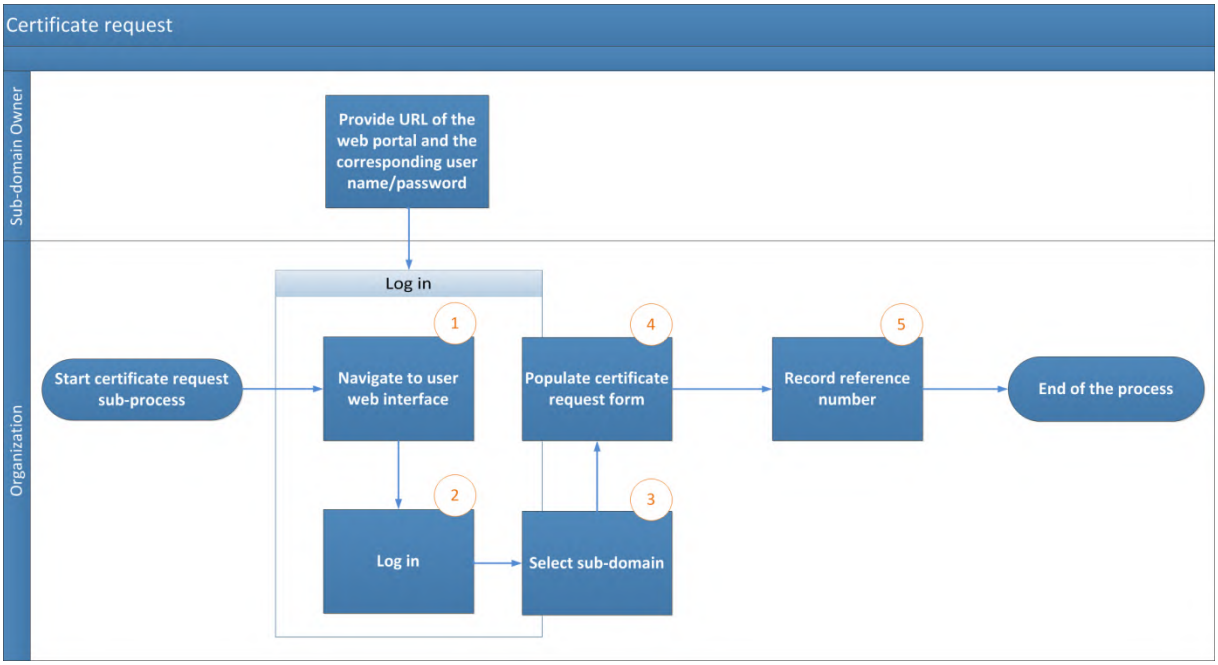
i) CEF Support Team sender en e-mail til registreringsenheden om anmodningens gyldighed. E-mailen skal omfatte:

   1) organisationens navn, som er anført i feltet "Organisation (O)" i certifikatanmodningen.

   2) certifikatoplysningerne, herunder navnet på det adgangspunkt, som certifikatet skal udstedes til, og som er anført i feltet "Efternavn (CN)" i certifikatanmodningen.

   3) certifikatets referencenummer

   4) organisationens adresse, e-mailadresse og navnet på den person, der repræsenterer den.



Figur 7 – Certifikatanmodningsproces

2.2.4. Trin 3: Registrering hos registreringsenhed (certifikatgodkendelse)

2.2.4.1. Den betroede kurer eller kontaktpunktet træffer via e-mail aftale med registreringsenheden om identifikation af den betroede kurer, som derefter giver personligt fremmøde.

2.2.4.2. Organisationen udarbejder dokumentationspakken bestående af:

a) den udfyldte og underskrevne fuldmagt

b) en kopi af gyldigt pas tilhørende den betroede kurer, der giver personligt fremmøde. Kopien skal være underskrevet af et af organisationens kontaktpunkter identificeret i trin 1.

c) en udskrift af certifikatanmodningen underskrevet af et af organisationens kontaktpunkter.

2.2.4.3. Registreringsenheden tager imod den betroede kurer, efter at dennes identitet er screenet i bygningens reception. Registreringsenheden gennemfører registreringen af certifikatanmodningen ved personligt fremmøde ved at:

a) identificere den betroede kurer

b) verificere den betroede kurers fysiske fremtræden i forhold til det pas, den betroede kurer forelægger

c) verificere gyldigheden af det pas, den betroede kurer forelægger

d) verificere det for gyldigt erklærede pas, som den betroede kurer forelægger, i forhold til kopien af det gyldige pas tilhørende den betroede kurer, som er underskrevet af et af organisationens identificerede kontaktpunkter. Underskriften bekræftes i forhold til den originale "identifikationsformular for betroede kurerer og kontaktpunkter"

e) verificere den udfyldte og underskrevne fuldmagt

f) verificere udskriften af certifikatanmodningen og dens underskrift i forhold til den originale "identifikationsformular for betroede kurerer og kontaktpunkter"

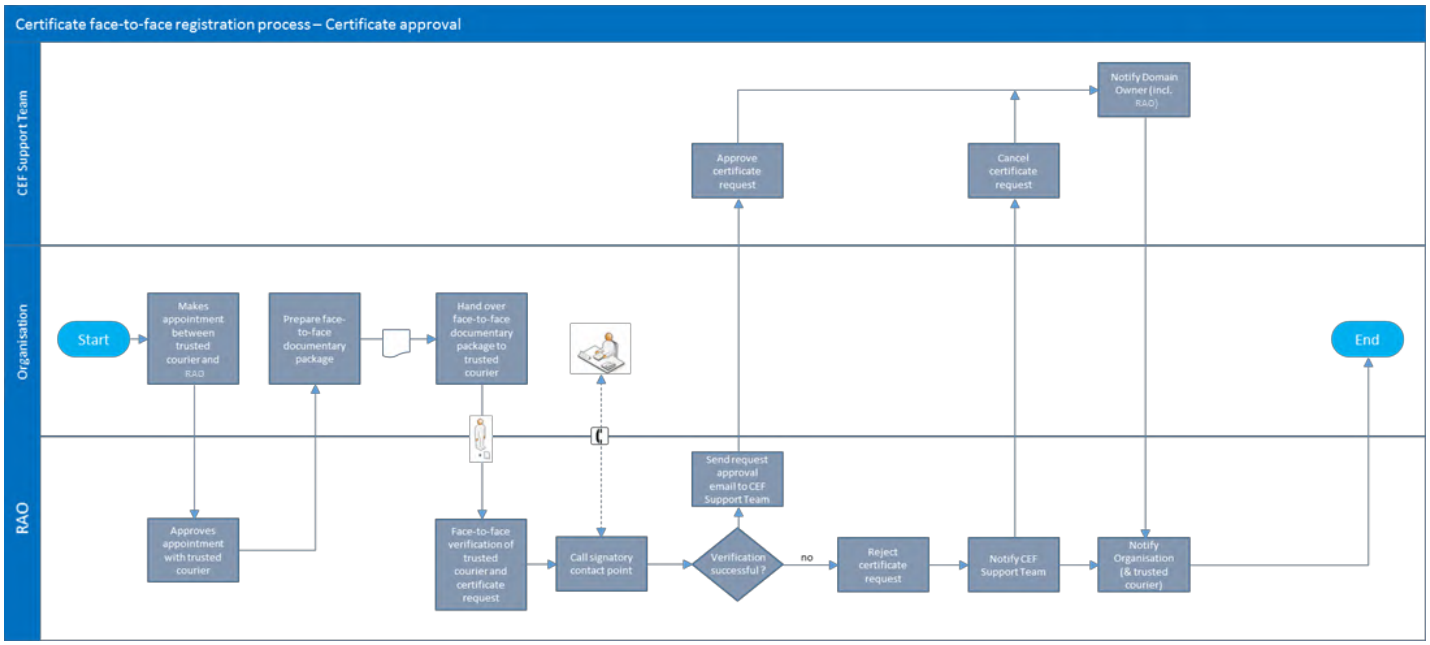
g) ringe til underskriverens kontaktpunkt for at dobbelttjekke den betroede kurers identitet samt indholdet af certifikatanmodningen.

2.2.4.4. Registreringsenheden bekræfter over for CEF Support Team, at den nationale myndighed er bemyndiget til at varetage driften af de komponenter, for hvilke den anmoder om certifikater, og at registreringsprocessen med personligt fremmøde var vellykket. Bekræftelsen sendes med krypteret e-mail ved brug af et "CommiSign"-certifikat, og der vedhæftes en scannet kopi af den bekræftede dokumentpakke fra det personlige fremmøde samt af registreringsenhedens underskrevne procestjekliste.

2.2.4.5. Hvis registreringsenheden bekræfter anmodningens gyldighed, fortsætter processen som fastlagt i 2.2.4.6 og 2.2.4.7. I modsat fald afvises det at udstede et certifikat, hvorefter organisationen informeres.

2.2.4.6. CEF Support Team godkender certifikatanmodningen og underretter registreringsenheden om, at certifikatet er godkendt.

2.2.4.7. Registreringsenheden underretter organisationen om, at certifikatet kan hentes via brugerportalen.



Figur 8 – Godkendelse af certifikat

2.2.5. Trin 4: Generering af certifikat

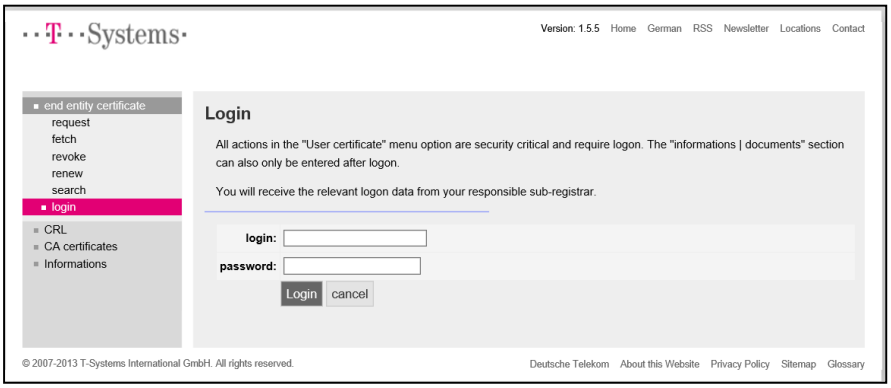
Certifikatet genereres, når certifikatanmodningen er godkendt.

2.2.6. Trin 5: Offentliggørelse og hentning af certifikat

2.2.6.1. Når certifikatanmodningen er blevet godkendt, henter registreringsenheden certifikatet og overdrager en kopi til den betroede kurer.

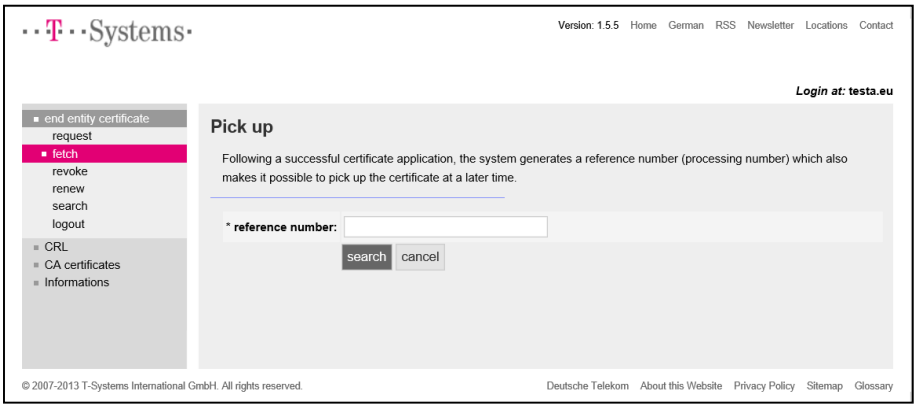
2.2.6.2. Organisationen modtager underretningen fra registreringsenheden om, at certifikaterne kan hentes.

2.2.6.3. Organisationen navigerer til brugerportalen på https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en og logger ind med brugernavnet "**sbca/CEF_eDelivery.europa.eu**" og adgangskoden "**digit.333**".



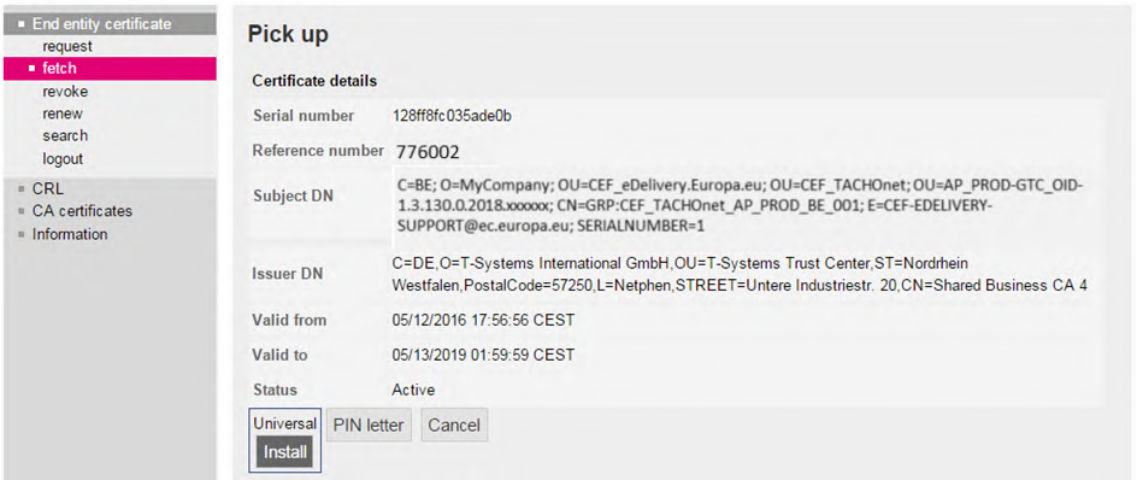
Figur 9

2.2.6.4. Organisationen klikker på "fetch" i venstre side og angiver det referencenummer, der blev registreret i certifikatanmodningsprocessen.



Figur 10

2.2.6.5. Organisationen installerer certifikaterne ved at klikke på knappen "Install".



Figur 11

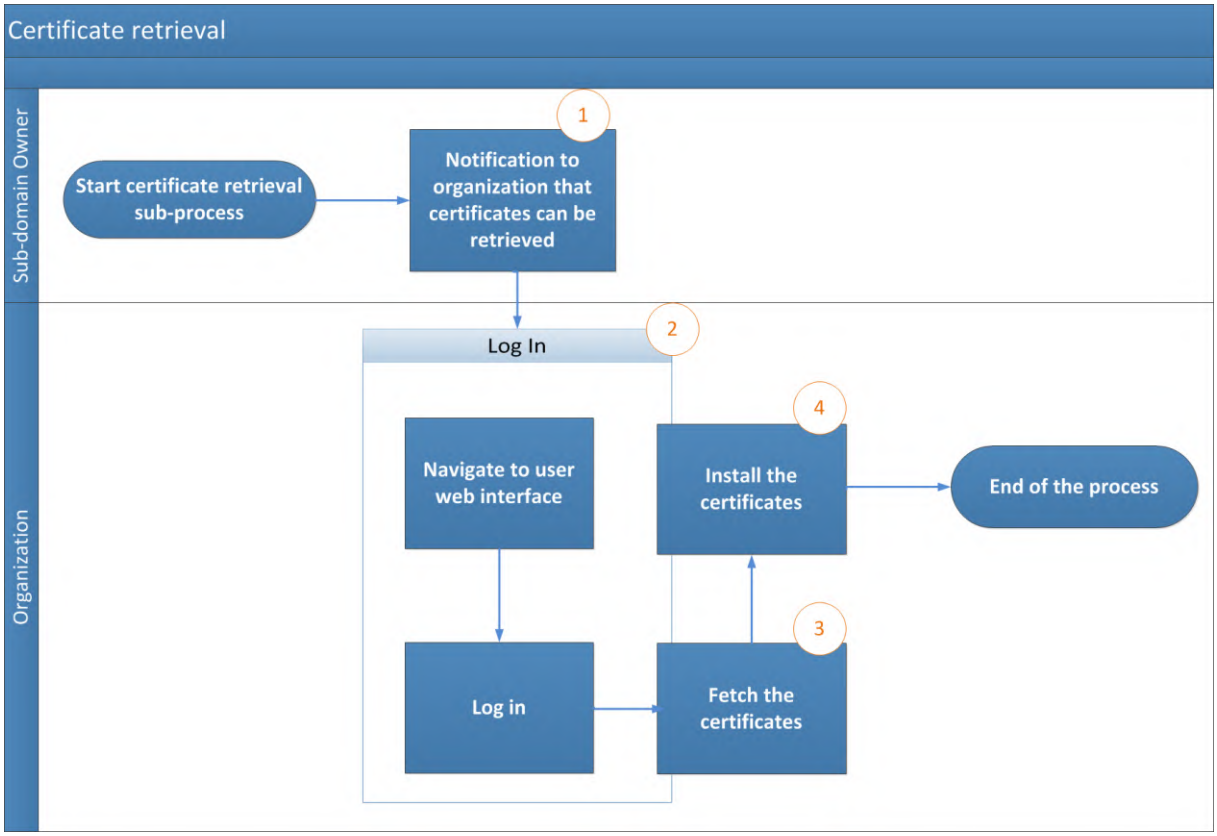
2.2.6.6. Certifikatet installeres på adgangspunktet. Da dette er implementeringsspecifikt, skal organisationen kontakte sit adgangspunkt for at få beskrivelsen af denne proces.

2.2.6.7. Certifikatet installeres på adgangspunktet ved at følge nedenstående trin:

a) eksport af den private nøgle og certifikatet

b) oprettelse af keystore og truststore

c) installation af keystore og truststore på adgangspunktet.

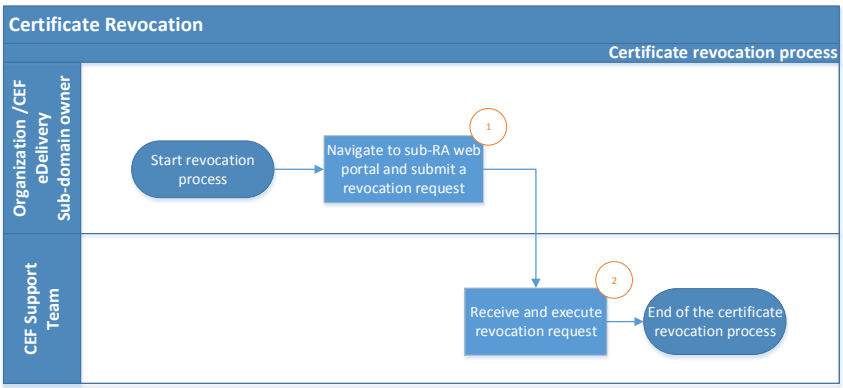


Figur 12 – Hentning af certifikat

3. Proces for tilbagekaldelse af certifikat

3.1. Organisationen indsender en anmodning om tilbagekaldelse via brugerwebportalen.

3.2. CEF Support Team gennemfører tilbagekaldelsen af certifikatet.



Figur 13 – Tilbagekaldelse af certifikat

4. Almindelige betingelser for CEF PKI-tjenesten

4.1. Baggrund

I sin egenskab af løsningsleverandør af eDelivery-modulet i Connecting Europe-faciliteten stiller DIGIT en PKI-tjeneste[7] ("CEF PKI-tjeneste") til rådighed for de kontraherende parter i AETR-overenskomsten. CEF PKI-tjenesten skal anvendes af nationale myndigheder ("slutbrugere"), der deltager i TACHOnet.

DIGIT er PKI-indehaver i TeleSec Shared-Business-CA-løsningen ("SBCA"), hvis drift varetages i Trust Center under koncernenheden T-Systems International GmbH ("T-Systems")[8]. DIGIT fungerer som hovedregistrator for SBCA's "CEF_eDelivery.europa.eu"-domæne. I denne egenskab opretter DIGIT underdomæner til "CEF_eDelivery.europa.eu"-domænet for hvert af de projekter, der benytter CEF PKI-tjenesten.

Dette dokument indeholder de nærmere betingelser for TACHOnet-underdomænet. DIGIT fungerer som underregistrator for dette underdomæne. I denne egenskab udsteder, tilbagekalder og fornyer DIGIT dette projekts certifikater.

4.2. Ansvarsfraskrivelse

Kommissionen er ikke ansvarlig for certifikatets indhold; ansvaret er alene certifikatindehaverens. Det er certifikatindehaverens ansvar at kontrollere certifikatindholdets nøjagtighed.

Kommissionen er ikke ansvarlig for, hvordan certifikatindehaveren som tredjeparts juridisk enhed uden for Kommissionen bruger certifikatet.

---

7 En PKI (Public Key Infrastructure) er en række roller, politikker, procedurer og systemer, der er nødvendige for at oprette, administrere, distribuere og tilbagekalde digitale certifikater.

8 Den betroede rolle, som Trust Center-operatøren (der er placeret i T-Systems Trust Center) har, omfatter også at varetage opgaven som intern registreringsenhed.

Hensigten med denne erklæring om ansvarsfraskrivelse er hverken at begrænse Kommissionens ansvar på en måde, der strider mod eventuelle krav ifølge gældende national ret eller at udelukke Kommissionens ansvar i tilfælde, hvor ansvar ikke kan udelukkes ifølge national ret.

4.3. Tilladt/Ikke-tilladt anvendelse af certifikater

4.3.1. Tilladt anvendelse af certifikater

Når et certifikat er udstedt, anvender certifikatindehaveren[9] udelukkende certifikatet i forbindelse med TACHOnet. I den forbindelse kan certifikatet anvendes til at:

- bekræfte datas oprindelse
- kryptere data
- sikre påvisning af integritetsbrud på data.

4.3.2. Ikke-tilladt anvendelse af certifikater

Enhver anvendelse, der ikke er udtrykkeligt godkendt som en af certifikatets tilladte anvendelsesmuligheder, er forbudt.

4.4. Certifikatindehaverens yderligere forpligtelser

SBCA's nærmere betingelser er defineret af T-Systems i SBCA-tjenestens certificeringspolitik (CP)/certificeringspraksis (CPS)[10]. Dette dokument omfatter sikkerhedsspecifikationer og retningslinjer vedrørende tekniske og organisatoriske aspekter og beskriver Trust Centre-operatørens aktiviteter i dennes egenskab af certificeringsenhed (CA) og registreringsenhed (RA) samt registreringsenhedens (RA) bemyndigede tredjepart.

Kun enheder, der er bemyndiget til at deltage i TACHOnet, kan anmode om et certifikat.

---

9 Identificeret ved attributværdien "O=" i det udstedte certifikats Subject Distinguished Name.

10 Den nyeste version af T-Systems SBCA CP/CPS kan findes på https://www.telesec.de/en/sbca-en/support/download-area/.

Med hensyn til accept af certifikat gælder punkt 4.4.1 i SBCA's certificeringspolitik og certificeringspraksis ("CP/CPS"), og derudover anses brugsvilkårene og bestemmelserne i nærværende dokument for at være accepteret af den organisation, som certifikatet er udstedt til ("O=") ved første anvendelse.

Med hensyn til offentliggørelse af certifikatet gælder punkt 2.2 i SBCA CP/CPS.

Alle certifikatejere skal opfylde følgende krav:

1) beskytter deres private nøgle mod uautoriseret brug

2) undgå at overdrage eller oplyse deres private nøgle til tredjeparter, også som repræsentanter

3) undgår fortsat brug af den private nøgle efter gyldighedsperiodens udløb eller certifikatets tilbagekaldelse, bortset fra med det formål at få vist krypterede data (f.eks. dekryptering af e-mails).

4) certifikatindehaveren er ansvarlig for at kopiere eller sende nøglen til slutenheden eller -enhederne.

5) certifikatindehaveren skal forpligte slutenheden/alle slutenheder til at overholde disse betingelser, herunder SBCA CP/CPS ved håndteringen af den private nøgle.

6) Certifikatindehaveren skal stille identifikation for de bemyndigede repræsentanter, som er bemyndiget til at anmode om tilbagekaldelse af certifikater udstedt til organisationen, til rådighed og i den forbindelse oplyse om de begivenheder, der har medført tilbagekaldelsen, og om adgangskoden til tilbagekaldelse.

7) for certifikater tilknyttet grupper af personer og funktioner og/eller juridiske personer, efter at en person har forladt gruppen af slutenheder (f.eks. ophør af ansættelsesforhold), skal certifikatindehaveren forebygge misbrug af den private nøgle ved at tilbagekalde certifikatet.

8) Certifikatindehaveren er ansvarlig for og skal anmode om tilbagekaldelse af certifikatet i de tilfælde, der er nævnt i punkt 4.9.1 i SBCA CP/CPS.

Med hensyn til fornyelse eller "rekey" af certifikater gælder punkt 4.6 eller 4.7 i SBCA CP/CPS.

Med hensyn til ændring af certifikater gælder punkt 4.8 i SBCA CP/CPS.

Med hensyn til tilbagekaldelse af certifikater gælder punkt 4.9 i SBCA CP/CPS.

5. Identifikationsformular for kontaktpersoner og betroede kurerer (eksempel)

Jeg, *[navn og adresse på organisationens repræsentant]***, erklærer, at nedenstående oplysninger er til brug i forbindelse med anmodning om, generering af og hentning af PKI-certifikater til TACHOnet-adgangspunkter til understøttelse af fortroligheden, integriteten og afviseligheden af TACHOnet-meddelelser:**

Oplysninger om kontaktperson:

– **Kontaktperson #1**	– **Kontaktperson #2**
– Navn:	– Navn:
– Fornavne:	– Fornavne:
– Mobiltelefon:	– Mobiltelefon:
– Telefon:	– Telefon:
– E-mail:	– E-mail:
– Underskriftsprøve: –	– Underskriftsprøve: – – –

Oplysninger om betroet kurer:

– **Betroet kurer #1**	– **Betroet kurer #2**
– Navn:	– Navn:
– Fornavne:	– Fornavne:
– Mobiltelefon:	– Mobiltelefon:
– E-mail:	– E-mail:
– Pasudstedende land:	– Pasudstedende land:
– Pasnummer:	– Pasnummer:
– Udløbsdato for pas:	– Udløbsdato for pas:

Sted og dato samt organisationens stempel eller segl:

Den bemyndigede repræsentants underskrift:

6. Dokumenter

6.1. Individuel fuldmagt (eksempel)

Et eksempel på en individuel fuldmagt, som skal underskrives og fremlægges af den betroede kurer under registreringen hos RAO ved personligt fremmøde, kan findes her:

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. Udskrift af anmodning om certifikat (eksempel)

Et eksempel på en udskrift af en anmodning om certifikat, som skal underskrives og fremlægges af den betroede kurer under registreringen hos RAO ved personligt fremmøde, kan findes her:

7. Glossar

De centrale termer, der er anvendt i dette undertillæg, er defineret i afsnittet CEF Definitions på CEF Digital Single Web Portal:

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

De centrale akronymer, der er anvendt i denne Component Offering Description, er defineret i CEF Glossary på CEF Digital Single Web Portal:

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