RÅDETS BESLUT (EU) 2018/1926

av den 19 november 2018

om den ståndpunkt som ska intas på Europeiska unionens vägnar i FN:s ekonomiska kommission för Europas expertgrupp för den europeiska överenskommelsen om arbetsförhållanden för fordonsbesättningar vid internationella vägtransporter

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt, särskilt artikel 91 jämförd med artikel 218.9,

med beaktande av Europeiska kommissionens förslag, och

av följande skäl:

(1) Den europeiska överenskommelsen om arbetsförhållanden för fordonsbesättningar vid internationella vägtransporter (AETR) ([1]) trädde i kraft den 5 januari 1976.

(2) En expertgrupp för AETR har inrättats av FN:s ekonomiska kommission för Europa (Unece) inom ramen för AETR. Den gruppen är ett organ som har befogenhet att utarbeta och lägga fram förslag om ändring av AETR till Uneces arbetsgrupp för vägtransporter.

(3) Expertgruppen för AETR diskuterar för närvarande ändringar av AETR, på grundval av ett unionsförslag som följer på en ståndpunkt på unionens vägnar som antogs genom rådets beslut (EU) 2016/1877 ([2]). En ytterligare ändring av AETR förefaller nödvändig för att säkerställa att avtalsslutande parter i AETR utanför EU kan delta i utbyte av uppgifter på förarkort baserat på harmoniserade standarder för säkerhet och dataskydd.

(4) I Europaparlamentets och rådets förordning (EU) nr 165/2014 ([3]) föreskrivs att medlemsstaterna ska sammankoppla sina elektroniska nationella register över förarkort genom att använda meddelandesystemet TACHOnet (Telematics Network for the Exchange of Information Concerning the Issuing of Tachograph Cards) eller, om ett kompatibelt system används, säkerställa att elektroniskt datautbyte med alla andra medlemsstater är möjligt genom meddelandesystemet TACHOnet. TACHOnet är en plattform för utbyte av information om förarkort mellan medlemsstaterna, för att säkerställa att förare inte innehar mer än ett förarkort.

(5) För att uppnå alleuropeisk harmonisering när det gäller elektroniskt utbyte av information om förarkort är det nödvändigt att TACHOnet används som enda plattform av alla avtalsslutande parter i AETR.

(6) Anslutningen till meddelandesystemet TACHOnet sker i dag antingen direkt genom en transeuropeisk telematiktjänst för myndigheter (Testa) eller indirekt genom en medlemsstat som redan är ansluten till Testa. Eftersom Testa är en tjänst som är begränsad till medlemsstaterna och unionens institutioner, kan avtalsslutande parter i AETR utanför EU endast ansluta sig till TACHOnet indirekt.

(7) Kommissionen har nyligen utvärderat de indirekta anslutningarna till TACHOnet-systemet och drog slutsatsen att de inte erbjuder samma skyddsnivå som Testa. I synnerhet finns det inte tillräcklig garanti för autenticiteten, integriteten och konfidentialiteten hos den information som utbyts genom indirekta anslutningar. De indirekta anslutningarna till TACHOnet bör därför ersättas med en säker anslutning.

(8) eDelivery är ett nätverk av anslutningsnoder för digital kommunikation som utvecklats av kommissionen där varje deltagare på nationell nivå blir en nod som använder standardiserade transportprotokoll och säkerhetsföreskrifter. eDelivery är ett flexibelt verktyg som kan anpassas till varje specifik tjänst.

(9) eDelivery utnyttjar brett tillämpad säkerhetsteknik såsom infrastruktur för kryptering med öppen nyckel (PKI) för att säkerställa autenticiteten, integriteten och konfidentialiteten hos den information som utbyts. Tillgång till TACHOnet för avtalsslutande parter i AETR utanför EU bör beviljas genom eDelivery.

([1]) EGT L 95, 8.4.1978, s. 1.

([2]) Rådets beslut (EU) 2016/1877 av den 17 oktober 2016 om den ståndpunkt som ska intas på Europeiska unionens vägnar i expertgruppen för Förenta nationernas ekonomiska kommission för den europeiska överenskommelsen om arbetsförhållanden för fordonsbesättningar vid internationella vägtransporter (AETR) och i arbetsgruppen för vägtransporter (EUT L 288, 22.10.2016, s. 49).

([3]) Europaparlamentets och rådets förordning (EU) nr 165/2014 av den 4 februari 2014 om färdskrivare vid vägtransporter, om upphävande av rådets förordning (EEG) nr 3821/85 om färdskrivare vid vägtransporter och om ändring av Europaparlamentets och rådets förordning (EG) nr 561/2006 om harmonisering av viss sociallagstiftning på vägtransportområdet (EUT L 60, 28.2.2014, s. 1).

(10) De avtalsslutande parterna i AETR bör följa ett särskilt förfarande för att få det digitala certifikat och tillhörande elektroniska nycklar som ger tillgång till TACHOnet.

(11) Anslutning till TACHOnet genom eDelivery innebär att de avtalsslutande parterna i AETR är skyldiga att säkerställa att de elektroniska nycklar och certifikat som ger tillträde till systemet är skyddade och inte kan användas av obehöriga parter. De avtalsslutande parterna i AETR bör också garantera att de nycklar som omfattas av certifikat som har löpt ut inte längre används.

(12) Det är nödvändigt att garantera skydd av de personuppgifter som är tillgängliga för parterna via TACHOnet i enlighet med konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter av den 28 januari 1981.

(13) De nationella myndigheter som är anslutna till TACHOnet är skyldiga att implementera de tekniska lösningar som krävs för att säkerställa att driften av TACHOnet kännetecknas av hög prestanda. Det är kommissionens uppgift att utforma de tester som ska bekräfta att dessa prestanda uppnås och att genomföra dem i samordning med de nationella behöriga myndigheterna.

(14) I sin dom av den 31 mars 1971 i mål 22/70 ([1]) slog Europeiska unionens domstol fast att frågor som rör arbetsförhållanden för fordonsbesättningar vid vägtransporter är ett område som omfattas av unionens externa befogenhet. Denna befogenhet har sedan dess utövats i flera rättsakter som antagits av unionen, inklusive Europaparlamentets och rådets förordning (EG) nr 561/2006 ([2]) och Europaparlamentets och rådets förordning (EU) nr 165/2014. Eftersom det sakområde som regleras i AETR omfattas av tillämpningsområdet för förordning (EG) nr 561/2006 ligger den exklusiva befogenheten att förhandla om och ingå det relevanta avtalet och ändringar av det hos unionen.

(15) Om de avtalsslutande parternas förslag godtagits av expertgruppen för AETR, kan de leda till en ändring av AETR, efter det att ett förfarande för revidering av AETR har inletts och slutförts. När förslagen godtagits av expertgruppen för AETR är, i ett andra steg, unionsmedlemsstaterna såsom avtalsslutande parter i AETR skyldiga att samarbeta vid användning av mekanismen för revidering av AETR, i överensstämmelse med kravet på lojalt samarbete enligt artikel 4.3 i fördraget om Europeiska unionen, med förbehåll för ett rådsbeslut i enlighet med artikel 218.6 i fördraget om Europeiska unionens funktionssätt. De föreslagna ändringarna av AETR kommer att få verkan först efter det att revideringen av AETR har slutförts.

(16) Det är lämpligt att fastställa den ståndpunkt som ska intas på unionens vägnar i expertgruppen för AETR, eftersom ändringen av AETR kommer att vara bindande för unionen.

(17) Eftersom unionen inte är en avtalsslutande part i AETR och dess status inte medger att den översänder de föreslagna ändringarna, bör medlemsstaterna, i unionens intresse, översända de föreslagna ändringarna till expertgruppen för AETR i en anda av lojalt samarbete i syfte att främja uppnåendet av unionens mål.

(18) Unionens ståndpunkt ska uttryckas gemensamt av dess medlemsstater som är medlemmar i expertgruppen för AETR och i Uneces arbetsgrupp för vägtransporter.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Den ståndpunkt som ska intas på unionens vägnar vid expertgruppen för Europa-avtalet om arbete som utförs av fordonsbesättningar vid internationella vägtransporter (AETR) ska förespråka de föreslagna ändringarna av AETR vilka anges i det dokument som bifogas detta beslut.

Artikel 2

Den ståndpunkt som avses i artikel 1 ska uttryckas gemensamt av de unionsmedlemsstater som är avtalsslutande parter i AETR.

Formella och mindre ändringar av den ståndpunkt som avses i artikel 1 får överenskommas utan att ståndpunkten behöver ändras.

([1]) ECLI:EU:C:1971:32.

([2]) Europaparlamentets och rådets förordning (EG) nr 561/2006 av den 15 mars 2006 om harmonisering av viss sociallagstiftning på vägtransportområdet och om ändring av rådets förordningar (EEG) nr 3821/85 och (EG) nr 2135/98 samt om upphävande av rådets förordning (EEG) nr 3820/85 (EUT L 102, 11.4.2006, s. 1).

Artikel 3

Detta beslut träder i kraft dagen efter det att det har antagits.

Utfärdat i Bryssel den 19 november 2018.

På rådets vägnar
E. KÖSTINGER
Ordförande

BILAGA

NYTT TILLÄGG TILL AETR

Tillägg 4

TACHOnet-specifikationer

1. **Tillämpningsområde och syfte**

1.1 I detta tillägg fastställs villkoren för anslutning av avtalsslutandende parter i AETR till TACHOnet via eDelivery.

1.2 Avtalsslutande parter som ansluter sig till TACHOnet via eDelivery ska följa bestämmelserna i detta tillägg.

2. **Definitioner**

a) avtalsslutande part eller part: en avtalsslutande part i AETR.

b) eDelivery: en tjänst som utvecklats av Europeiska kommissionen och som gör det möjligt att överföra uppgifter mellan tredje parter på elektronisk väg och som tillhandahåller bevis avseende de överförda uppgifternas hantering, inklusive bevis för uppgifternas sändning och mottagande, och som skyddar överförda uppgifter mot risken för eventuella otillåtna ändringar.

c) det system för elektroniskt utbyte av information om förarkort, mellan avtalsslutande parter, som avses i artikel 31.2 i förordning (EU) nr 165/2014.

d) centralenhet: det informationssystem som möjliggör dirigering av TACHOnet-meddelanden mellan begärande och svarande parter.

e) begärande part: den avtalsslutande part som skickar en TACHOnet-begäran eller en anmälan, vilken därefter dirigeras till rätt svarande part av centralenheten.

f) svarande part: den avtalsslutande part till vilken en TACHOnet-begäran eller en anmälan är riktad.

g) kortutfärdande myndighet: den enhet som är bemyndigad av en avtalsslutande part att utfärda och förvalta färdskrivarkort.

3. **Allmänna skyldigheter**

3.1 Ingen av de avtalsslutande parterna får ingå avtal om tillgång till TACHOnet på en annan parts vägnar eller på något annat sätt företräda den andra avtalsslutande parten på grundval av detta tillägg. Ingen av de avtalsslutande parterna agerar som den andra avtalsslutande partens underleverantör i de verksamheter som avses i detta tillägg.

3.2 De avtalsslutande parterna ska ge tillgång till sina nationella register över förarkort via TACHOnet på det sätt och med den tjänstenivå som anges i undertillägg 4.6.

3.3 De avtalsslutande parterna ska utan dröjsmål underrätta varandra om de uppmärksammar störningar eller fel inom sina respektive ansvarsområden som kan äventyra den normala driften av TACHOnet.

3.4 Varje part ska utse kontaktpersoner för TACHOnet till AETR-sekretariatet. Varje ändring av kontaktpunkter ska meddelas AETR-sekretariatet skriftligen.

4. **Tester för anslutning till TACHOnet**

4.1 En avtalsslutande part ska anslutas till TACHOnet efter framgångsrikt slutförande av anslutnings-, integrations- och prestandatester i enlighet med instruktioner från och under överinseende av Europeiska kommissionen.

4.2 Om de preliminära testerna misslyckas får Europeiska kommissionen tillfälligt avbryta testfasen. Testerna ska återupptas så snart den avtalsslutande parten har meddelat Europeiska kommissionen att den antagit de tekniska förbättringar på nationell nivå som är nödvändiga för att de preliminära testerna ska kunna genomföras på ett tillfredsställande sätt.

4.3 Den maximala varaktigheten för de preliminära testerna ska vara sex månader.

5. **Förtroendearkitektur**

5.1 TACHOnet-meddelandenas konfidentialitet, integritet och oavvislighet ska säkerställas genom förtroendearkitekturen i TACHOnet.

5.2 Förtroendearkitekturen i TACHOnet ska baseras på en PKI-tjänst (Public Key Infrastructure) som inrättats av Europeiska kommissionen, och kraven för denna tjänst fastställs i undertilläggen 4.8 och 4.9.

5.3 Följande enheter ska medverka i förtroendearkitekturen i TACHOnet:

a) Certifieringsmyndighet, med ansvar för genereringen av de digitala certifikat som ska levereras av registreringsmyndigheten till de avtalsslutande parternas nationella myndigheter (via betrodda kurirer som de utser), samt för inrättandet av den tekniska infrastrukturen för utfärdande, återkallande och förnyelse av digitala certifikat.

b) Domänägare, med ansvar för driften av den centralenhet som avses i undertillägg 4.1 och för valideringen och samordningen av förtroendearkitekturen i TACHOnet.

c) Registreringsmyndighet, med ansvar för registrering och godkännande av begäran om utfärdande, återkallande och förnyelse av digitala certifikat, och för kontrollen av de betrodda kurirernas identitet.

d) Betrodd kurir, som är den person som utsetts av de nationella myndigheterna, med ansvar för att överlämna den öppna nyckeln till registreringsmyndigheten och för att ta emot motsvarande certifikat som genererats av certifieringsmyndigheten.

e) Nationell myndighet från den avtalsslutande parten, som ska

i) generera de privata nycklarna och motsvarande öppna nycklar som ska ingå i de certifikat som ska genereras av certifieringsmyndigheten,

ii) begära de digitala certifikaten från certifieringsmyndigheten,

iii) utse den betrodda kuriren.

5.4 Certifieringsmyndigheten och registreringsmyndigheten ska utses av Europeiska kommissionen.

5.5 En avtalsslutande part som ansluter sig till TACHOnet måste begära att ett digitalt certifikat utfärdas i enlighet med undertillägg 4.9 för att parten ska kunna signera och kryptera ett TACHOnet-meddelande.

5.6 Ett certifikat får återkallas i enlighet med undertillägg 4.9.

6. **Dataskydd och konfidentialitet**

6.1 Parterna ska i enlighet med nationella och internationella dataskyddslagar, och i synnerhet med konventionen om skydd för enskilda vid automatisk databehandling av personuppgifter, vidta alla tekniska och organisatoriska åtgärder som är nödvändiga för att garantera säkerheten för TACHOnet-data och förhindra ändring eller förlust av, eller obehörig behandling av eller tillgång till, sådana data (i synnerhet meddelandenas autenticitet, datasekretess, spårbarhet, integritet, tillgänglighet och oavvislighet samt säkerhet).

6.2 Varje part ska skydda sina egna nationella system mot olaglig användning, skadlig kod, virus, datorintrång, överträdelser och olaglig manipulering av data och andra jämförbara åtgärder som vidtas av tredje part. Parterna samtycker till att göra kommersiellt rimliga ansträngningar för att undvika överföring av virus, tidsinställda bomber, maskar eller liknande företeelser eller andra programmeringsrutiner som kan störa den andra partens datorsystem.

7. **Kostnader**

7.1 De avtalsslutande parterna ska stå för sina egna utvecklings- och driftskostnader för egna datasystem och förfaranden i den utsträckning som krävs för att de ska kunna fullgöra sina skyldigheter enligt detta tillägg.

7.2 De tjänster som anges i undertillägg 4.1, vilka tillhandahålls av centralenheten, är kostnadsfria.

8. **Underentreprenad**

8.1 Parterna får lägga ut alla tjänster, som de ansvarar för enligt detta tillägg, på underleverantörer.

8.2 Sådan underentreprenad befriar inte parten från ansvaret enligt detta tillägg, inklusive ansvaret för lämplig tjänstenivå i enlighet med undertillägg 4.6.

Undertillägg 4.1

Allmänna aspekter av TACHOnet

1. **Allmän beskrivning**

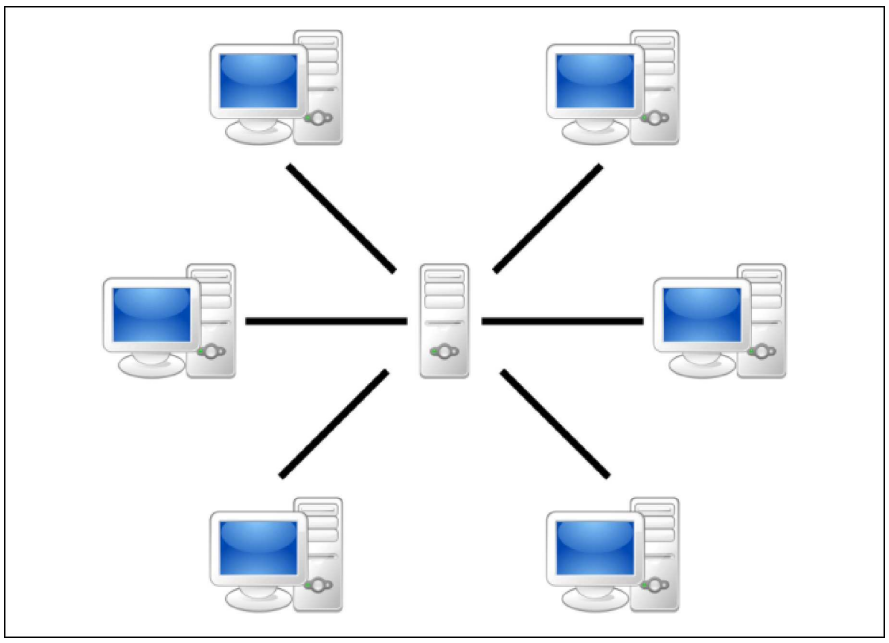
TACHOnet är ett elektroniskt system för utbyte av information om förarkort mellan avtalsslutandende parter i AETR. TACHOnet dirigerar begäran om information från de begärande parterna till de svarande parterna, och svaren från de sistnämnda till de förstnämnda. Avtalsslutande parter som är en del av TACHOnet måste ansluta sina nationella register över förarkort till systemet.

2. **Arkitektur**

Meddelandesystemet TACHOnet ska bestå av följande delar:

2.1 En centralenhet som ska kunna ta emot en begäran från den begärande parten, och validera och behandla den genom att vidarebefordra den till de svarande parterna. Centralenheten ska vänta på svar från varje svarande part, konsolidera samtliga svar och vidarebefordra det konsoliderade svaret till den begärande parten.

2.2 Parternas nationella system, som ska vara utrustade med ett gränssnitt som både kan sända begäran till centralenheten och ta emot motsvarande svar. Nationella system får använda egen eller kommersiell programvara för att sända och ta emot meddelanden från centralenheten.



3. **Förvaltning**

3.1 Centralenheten ska förvaltas av Europeiska kommissionen, som ska ansvara för teknisk drift och underhåll av centralenheten.

3.2 Centralenheten får inte lagra data under en längre period än sex månader, utom loggningsuppgifter och statistiska uppgifter enligt undertillägg 4.7.

3.3 Centralenheten ska inte ge tillgång till personuppgifter, med undantag för Europeiska kommissionens behöriga personal när det är nödvändigt för övervakning, underhåll och felsökning.

3.4 Varje avtalsslutande part ska ansvara för följande:

3.4.1 Inrättande och förvaltning av sina nationella system, inbegripet gränssnittet mot centralenheten.

3.4.2 Installation och underhåll av sina nationella system, både maskinvara och programvara, egen eller kommersiell.

3.4.3 En korrekt driftskompatibilitet mellan de nationella systemen och centralenheten, inbegripet hanteringen av felmeddelanden från centralenheten.

3.4.4 Åtgärder för att säkerställa informationens konfidentialitet, integritet och tillgänglighet.

3.4.5 Driften av de nationella systemen i enlighet med de tjänstenivåer som anges i undertillägg 4.6.

Undertillägg 4.2

Funktioner i TACHOnet

1. Följande funktioner ska tillhandahållas via meddelandesystemet TACHOnet:

1.1 Check Issued Cards (CIC): ger den begärande parten möjlighet att sända en CIC-begäran om kontroll av utfärdade kort till en eller alla svarande parter, i syfte att fastställa om en person som ansöker om kort redan innehar ett förarkort utfärdat av de svarande parterna. De svarande parterna ska besvara begäran genom att sända ett CIC-svar.

1.2 Check Card Status (CCS): ger den begärande parten möjlighet att fråga den svarande parten om detaljerna för ett kort som den sistnämnda utfärdat genom att sända en CCS-begäran. Den svarande parten ska besvara begäran genom att sända ett CCS-svar.

1.3 Modify Card Status (MCS): ger den begärande parten möjlighet att med en MCS-begäran informera den svarande parten om att statusen ändrats för ett kort som den sistnämnda utfärdat. Den svarande parten ska svara med en MCS-kvittering.

1.4 Issued Card Driving License (ICDL): ger den begärande parten möjlighet att med en ICDL-begäran informera den svarande parten om att ett kort utfärdats av den förstnämnda på grundval av ett körkort utfärdat av den sistnämnda. Den svarande parten ska svara med ett ICDL-svar.

2. Andra meddelandetyper som anses behövas för ett effektivt fungerande TACHOnet ska inkluderas, t.ex. felanmälningar.

3. Nationella system ska känna igen de kortstatusar som anges i tabell 1 när någon av de funktioner som beskrivs i punkt 1 används. Parterna är emellertid inte skyldiga att tillämpa ett förvaltningsförfarande som utnyttjar alla de förtecknade statustyperna.

4. När en part tar emot ett svar eller en anmälan med en status som inte används i de egna förvaltningsförfarandena ska det nationella systemet översätta statusen i det mottagna meddelandet till motsvarande värde i det egna förfarandet. Meddelandet får inte avvisas av den svarande parten, så länge som statusen i meddelandet finns förtecknad i tabell 1.

5. De kortstatusar som anges i tabell 1 får inte användas för att avgöra om ett förarkort är giltigt för körning. När en part skickar en förfrågan till registret vid den kortutfärdande nationella myndigheten via CCS-funktionen ska svaret innehålla det därför avsedda fältet ”valid for driving” (giltigt för körning). De nationella administrativa förfarandena ska vara sådana att CCS-svar alltid innehåller lämpligt ”valid for driving”-värde.

Tabell 1

Kortstatus

Card Status (Kortstatus)	Definition
Application (Ansökan)	Den kortutfärdande myndigheten har mottagit en ansökan om att utfärda ett förarkort. Denna information har registrerats och lagrats i databasen med de genererade söknycklarna.
Approved (Godkänt)	Den kortutfärdande myndigheten har godkänt ansökan om färdskrivarkortet.
Rejected (Avvisat)	Den kortutfärdande myndigheten har avslagit ansökan.
Personalised (Personaliserat)	Färdskrivarkortet har personaliserats.

Card Status (Kortstatus)	Definition
Dispatched (Avsänt)	Den nationella myndigheten har sänt förarkortet till den berörda föraren eller det berörda utlämningsstället.
Handed over (Överlämnat)	Den nationella myndigheten har lämnat över förarkortet till den berörda föraren.
Confiscated (Konfiskerat)	Föraren har fråntagits sitt förarkort av den behöriga myndigheten.
Suspended (Indraget)	Förarkortet har tillfälligt fråntagits föraren.
Withdrawn (Återkallat)	Den kortutfärdande myndigheten har beslutat att återkalla förarkortet. Kortet har permanent makulerats.
Surrendered (Inlämnat)	Färdskrivarkortet har återsänts till den kortutfärdande myndigheten med en förklaring att det inte längre behövs.
Lost (Förlorat)	Färdskrivarkortet har anmälts som förlorat till den kortutfärdande myndigheten.
Stolen (Stulet)	Färdskrivarkortet har anmälts som stulet till den kortutfärdande myndigheten. Ett stulet kort anses vara förlorat.
Malfunctioning (Ej fungerande)	Färdskrivarkortet har anmälts som ej fungerande till den kortutfärdande myndigheten.
Expired (Ej längre giltigt)	Färdskrivarkortets giltighetstid har löpt ut.
Replaced (Ersatt)	Färdskrivarkortet som har anmälts som förlorat, stulet eller ej fungerande har ersatts med ett nytt kort. Uppgifterna på det nya kortet är desamma, med undantag för kortnumrets ersättningsindex, som ökats med ett steg.
Renewed (Förnyat)	Färdskrivarkortet har förnyats på grund av en förändring av administrativa uppgifter eller på grund av att dess giltighetstid löpt ut. Uppgifterna på det nya kortet är desamma, med undantag för kortnumrets förnyelseindex, som ökats med ett steg.
In Exchange (Under utbyte)	Den kortutfärdande myndighet som utfärdade förarkortet har mottagit en anmälan om att förfarandet för utbyte av kortet mot ett förarkort utfärdat av en kortutfärdande myndighet i en annan part har inletts.
Exchanged (Utbytt)	Den kortutfärdande myndighet som utfärdade förarkortet har mottagit en anmälan om att förfarandet för utbyte av kortet mot ett förarkort utfärdat av en kortutfärdande myndighet i en annan part har slutförts.

Undertillägg 4.3

Föreskrifter om meddelanden i TACHOnet

1. **Allmänna tekniska krav**

1.1 Centralenheten ska tillhandahålla både synkrona och asynkrona gränssnitt för utbyte av meddelanden. Parterna får välja den lämpligaste tekniken som gränssnitt mot sina egna tillämpningar.

1.2 Alla meddelanden som utbyts mellan centralenheten och de nationella systemen måste vara UTF-8-kodade.

1.3 Nationella system ska kunna ta emot och behandla meddelanden med grekiska eller kyrilliska tecken.

2. **XML-meddelandestruktur och XML-schemadefinition (XSD)**

2.1 Den allmänna XML-meddelandestrukturen ska följa det format som definieras av de XML-scheman (XSD) som är installerade i centralenheten.

2.2 Centralenheten och de nationella systemen ska sända och ta emot meddelanden som överensstämmer med XML-schemat för respektive meddelande.

2.3 Nationella system ska kunna skicka, ta emot och behandla alla meddelanden som motsvarar någon av de funktioner som anges i undertillägg 4.2.

2.4 XML-meddelanden ska uppfylla åtminstone de minimikrav som fastställs i tabell 2.

Tabell 2

Minimikrav för innehållet i XML-meddelanden

Gemensam startdel (header)		**Obligatoriskt**
Version	Den officiella versionen av XML-specifikationerna kommer att anges i den namnrymd (namespace) som anges i meddelandets XML-schema och i version-attributet i header-elementet i varje XML-meddelande. Versionsnumret (n.m) kommer att definieras som ett fast värde i varje release av XML-schemafilen (xsd).	Ja
Test-ID (Test Identifier)	Frivilligt ID för test. Den som initierar testet ger värdet för detta ID, och alla som deltar i arbetsflödet vidarebefordrar/skickar tillbaka samma ID. I drift bör det ignoreras och det kommer inte att användas om det tillhandahålls.	Nej
Tekniskt ID (Technical Identifier)	Ett UUID som unikt identifierar varje enskilt meddelande. Avsändaren genererar ett UUID och ger det som värde för detta attribut. Dessa data används endast internt.	Ja
Arbetsflödes-ID (Workflow Identifier)	Arbetsflödes-ID är ett UUID och bör genereras av den begärande parten. Detta ID används sedan i alla meddelanden för att korrelera arbetsflödet.	Ja
Avsändningstid (Sent At)	Datum och tidpunkt (UTC) då meddelandet sändes.	Ja
Tidsfrist (Timeout)	Detta attribut med datum och tidpunkt (i UTC-format) är frivilligt. Detta värde kommer enbart att ges av centralenheten för vidarebefordrade begäran. Därigenom informeras den svarande parten om tidpunkten då tidsfristen för en begäran löper ut. Detta värde krävs inte i MS2TCN_<x>_Req eller i svarsmeddelanden. Det är frivilligt, så att samma header-definition kan användas för alla typer av meddelanden, oberoende av om attributet för tidsfrist krävs eller ej.	Nej
Från (From)	ISO 3166-1 tvåbokstavskod för den part som skickar meddelandet, eller ”EU”.	Ja
Till (To)	ISO 3166-1 tvåbokstavskod för den part till vilken meddelandet skickas, eller ”EU”.	Ja

Undertillägg 4.4

Translitterering och NYSIIS-tjänster (New York State Identification and Intelligence System)

1. Den NYSIIS-algoritm som är införd i centralenheten ska användas för att koda namnen på alla förare i det nationella registret.

2. Vid sökning efter ett kort via CIC-funktionen ska NYSIIS-nycklar användas som primär sökmekanism.

3. Dessutom får parterna tillämpa en anpassad algoritm för att få ytterligare resultat.

4. Sökresultaten ska visa vilken sökmekanism som har använts, antingen NYSIIS eller den anpassade.

5. Om en part väljer att registrera ICDL-anmälningar ska de NYSIIS-nycklar som ingår i anmälan registreras som en del av ICDL-data. Vid sökning efter ICDL-data ska parten använda NYSIIS-nyckeln för sökandens namn.

Undertillägg 4.5

Säkerhetskrav

1. HTTPS ska användas för utbyte av meddelanden mellan centralenheten och de nationella systemen.

2. Nationella system ska använda de digitala certifikat som avses i undertilläggen 4.8 och 4.9 för att säkerställa överföring av meddelanden mellan de nationella systemen och centralenheten.

3. Nationella system ska minst tillämpa certifikat som använder hashalgoritmen SHA-2 (SHA-256) för signaturer och öppna nycklar med en längd av 2 048 bitar.

Undertillägg 4.6

Tjänstenivåer

1. Nationella system ska uppfylla följande lägsta tjänstenivå:

1.1 De ska vara tillgängliga dygnet runt, året runt.

1.2 Deras tillgänglighet ska övervakas av ett Heartbeat-meddelande från centralenheten.

1.3 Deras tillgänglighet ska uppgå till 98 %, i enlighet med nedanstående tabell (värdena har avrundats till närmaste lämpliga enhet):

Tillgänglighet på	innebär att systemet inte är tillgängligt		
	Per dag	Per månad	Per år
98 %	0,5 timmar	15 timmar	7,5 dagar

Medlemsstaterna uppmuntras att respektera de dagliga tillgänglighetskraven. Det är dock uppenbart att vissa nödvändiga verksamheter, t.ex. systemunderhåll, kräver längre avbrott än 30 minuter. Den månatliga och årliga tillgängligheten förblir emellertid bindande.

1.4 De ska ge svar på minst 98 % av de begäranden som vidarebefordras till dem under en kalendermånad.

1.5 Begäran ska besvaras inom 10 sekunder.

1.6 Den sammanlagda väntetiden för en begäran (den tid som den som skickat begäran väntar på ett svar) får inte överstiga 20 sekunder.

1.7 De ska kunna hantera 6 begäran per sekund.

1.8 Nationella system får inte sända begäran till TACHOnet i en takt som överstiger 2 begäran per sekund.

1.9 Alla nationella system ska kunna klara eventuella tekniska problem i centralenheten eller i nationella system hos andra parter. Sådana problem kan bland annat handla om

a) förlorad kontakt med centralenheten,

b) uteblivet svar på en begäran,

c) mottagande av svar efter det att meddelandets tidsfrist löpt ut,

d) mottagande av oönskade meddelanden,

e) mottagande av ogiltiga meddelanden.

2. Centralenheten ska

2.1 ha en tillgänglighet på 98 %,

2.2 anmäla eventuella fel till de nationella systemen, antingen via svarsmeddelandet eller via ett särskilt felmeddelande. De nationella systemen ska i sin tur ta emot dessa särskilda felmeddelanden och ha ett ”upptrappningsflöde” (escalation workflow) för att åtgärda det anmälda felet.

3. Underhåll

Parterna ska minst en vecka innan sådana verksamheter inleds, om det är tekniskt möjligt, underrätta övriga parter och Europeiska kommissionen om eventuellt rutinmässigt underhåll via webbtillämpningen.

Undertillägg 4.7

Loggning och statistik om de data som samlats in i centralenheten

1. Av integritetsskäl ska alla data som används för statistiska ändamål vara anonyma. Data som identifierar ett specifikt kort, en viss förare eller ett visst körkort ska inte vara tillgängliga för statistiska ändamål.

2. Alla transaktioner som sker i övervaknings- och felsökningssyfte ska synas i loggningsuppgifterna och det ska vara möjligt att ta fram statistik om sådana transaktioner.

3. Personuppgifter får finnas kvar i loggarna i högst 6 månader. Statistiska uppgifter ska finnas kvar på obestämd tid.

4. De statistiska data som används för rapportering ska inbegripa

   a) begärande part,

   b) svarande part,

   c) meddelandetyp,

   d) svarets statuskod,

   e) datum och tidpunkt för meddelandena,

   f) svarstid.

Undertillägg 4.8

Allmänna bestämmelser om digitala nycklar och certifikat för TACHOnet

1. Europeiska kommissionens generaldirektorat för informationsteknik (DIGIT) ska tillhandahålla en PKI-tjänst ([1]) (nedan kallad ”CEF PKI-tjänst”) för de avtalsslutande parter i AETR som ansluter sig till TACHOnet (nedan kallade de nationella myndigheterna) via eDelivery.

2. Förfarandet för att begära och återkalla digitala certifikat, samt detaljerade villkor för dess användning, fastställs i tillägget.

3. Användning av certifikat:

3.1 När certifikatet har utfärdats ska den nationella myndigheten ([2]) använda det endast inom ramen för TACHOnet. Certifikatet kan användas för att

   a) autentisera uppgifternas ursprung,

   b) kryptera data,

   c) säkerställa upptäckt av integritetsöverträdelser som rör data.

3.2 All användning som inte uttryckligen godkänts som en del av den tillåtna användningen av certifikatet är förbjuden.

4. Avtalsslutande parter ska göra följande:

   a) Skydda sin privata nyckel mot obehörig användning.

   b) Avstå från att överföra sin privata nyckel till tredje part, eller avslöja sin privata nyckel för tredje part, även som företrädare.

([1]) En PKI (Public Key Infrastructure) är en uppsättning roller, policyer, förfaranden och system som behövs för att skapa, förvalta, distribuera och återkalla digitala certifikat.

([2]) Identifieras med värdet på attributet ”O=” i ”Subject Distinguished Name” för det utfärdade certifikatet.

c) Säkerställa konfidentialitet, integritet och tillgänglighet för de privata nycklar som genereras, lagras och används för TACHOnet.

d) Avstå från fortsatt användning av den privata nyckeln efter det att certifikatets giltighetsperiod har löpt ut eller efter det att certifikatet har återkallats, annat än i syfte att visa krypterade data (t.ex. dekryptering av e-postmeddelanden). Nycklar som upphört att gälla ska antingen förstöras eller bevaras på ett sätt som förhindrar deras användning.

e) Tillhandahålla registreringsmyndigheten identifikation av de auktoriserade företrädare som bemyndigats att begära återkallande av certifikat som utfärdats till organisationen (begäran om återkallande ska inbegripa ett lösenord för begäran om återkallande samt närmare uppgifter om de händelser som lett till återkallandet).

f) Förhindra missbruk av den privata nyckeln genom att begära återkallande av det tillhörande PKI-certifikatet (certifikat för öppen nyckel) om den privata nyckeln eller aktiveringsuppgifterna för den privata nyckeln röjs.

g) Ha ansvar för och skyldighet att begära återkallande av certifikat under de omständigheter som anges i certifieringsmyndighetens certifieringspolicy (Certification Policies, CP) och riktlinjer för certifiering (Certification Practices Statement, CPS).

h) Utan dröjsmål underrätta registreringsmyndigheten om förlust, stöld eller potentiellt röjande av någon AETR-nyckel som används inom ramen för TACHOnet.

5. Ansvar

Utan att det påverkar Europeiska kommissionens ansvar i strid mot tillämplig nationell lagstiftning eller i fall som inte får undantas enligt sådan lagstiftning, ska Europeiska kommissionen inte hållas ansvarig eller skadeståndsskyldig med avseende på följande:

a) Certifikatets innehåll, för vilket endast certifikatinnehavaren har ansvaret. Det ska vara certifikatinnehavarens ansvar att kontrollera riktigheten i certifikatets innehåll.

b) Certifikatinnehavarens användning av certifikatet.

Undertillägg 4.9

Beskrivning av PKI-tjänsten för TACHOnet

1. **Inledning**

En PKI (Public Key Infrastructure) är en uppsättning roller, policyer, förfaranden och system som behövs för att skapa, förvalta, distribuera och återkalla digitala certifikat ([1]). CEF PKI-tjänsten via eDelivery möjliggör utfärdande och förvaltning av digitala certifikat som används för att säkerställa konfidentialitet, integritet och oavvislighet i fråga om den information som utbyts mellan accesspunkter (Access Points, AP).

PKI-tjänsten i eDelivery är baserad på Trust Center Services TeleSec Shared Business CA (Certification Authority) för vilken CP (Certificate Policy) / CPS (Certification Practices Statement) hos TeleSec Shared-Business-CA inom T-Systems International GmbH ([2]) gäller.

PKI-tjänsten utfärdar certifikat som är lämpliga för att säkra olika verksamhetsprocesser inom och utanför företag, organisationer, myndigheter och institutioner som kräver en medelhög skyddsnivå för att styrka slutmottagarens autenticitet, integritet och tillförlitlighet.

2. **Process för begäran om certifikat**

2.1 Roller och ansvarsområden

2.1.1 ”Organisation” eller ”nationell myndighet” som begär certifikatet

2.1.1.1 Den nationella myndigheten ska begära certifikaten inom ramen för TACHOnet-projektet.

2.1.1.2 Den nationella myndigheten ska

a) begära certifikaten från CEF PKI-tjänsten,

([1]) https://en.wikipedia.org/wiki/Public_key_infrastructure
([2]) Den senaste versionen av CP och CPS kan laddas ner från https://www.telesec.de/en/sbca-en/support/download-area/

b) generera de privata nycklarna och motsvarande öppna nycklar som ska ingå i de certifikat som utfärdas av certifieringsmyndigheten,

c) ladda ner certifikatet efter godkännande,

d) underteckna och till registreringsmyndigheten returnera

i) formuläret för identifiering av kontaktpersoner och betrodda kurirer,

ii) den undertecknade individuella fullmakten ([1]).

2.1.2 Betrodd kurir

2.1.2.1. Den nationella myndigheten ska utse en betrodd kurir.

2.1.2.2. Den betrodda kuriren ska

a) överlämna den öppna nyckeln till registreringsmyndigheten under ett identifierings- och registreringsförfarande med personligt möte,

b) hämta motsvarande certifikat från registreringsmyndigheten.

2.1.3 Domänägare

2.1.3.1 GD MOVE ska vara domänägare.

2.1.3.2 Domänägaren ska

a) validera och samordna TACHOnet-nätverket och förtroendearkitekturen i TACHOnet, inbegripet valideringen av förfarandena för utfärdande av certifikaten,

b) driva centralenheten i TACHOnet och samordna parternas verksamhet med avseende på TACHOnets funktion,

c) tillsammans med nationella myndigheter utföra tester av anslutningen till TACHOnet.

2.1.4 Registreringsmyndighet

2.1.4.1 Gemensamma forskningscentret (GFC) ska vara registreringsmyndighet.

2.1.4.2 Registreringsmyndigheten ska ha ansvar för att kontrollera den betrodda kurirens identitet, för att registrera och godkänna begäran om utfärdande, återkallande och förnyelse av digitala certifikat.

2.1.4.3 Registreringsmyndigheten ska

a) tilldela den nationella myndigheten ett unikt ID,

b) autentisera den nationella myndighetens identitet, kontaktpunkter och betrodda kurirer,

c) kommunicera med CEF Support angående den nationella myndighetens autenticitet, kontaktpunkter och betrodda kurirer,

d) informera den nationella myndigheten om godkännande eller avvisande av certifikat.

2.1.5 Certifieringsmyndighet

2.1.5.1 Certifieringsmyndigheten ska ha ansvar för att tillhandahålla den tekniska infrastrukturen för begäran, utfärdande och återkallande av digitala certifikat.

2.1.5.2 Certifieringsmyndigheten ska

a) tillhandahålla den tekniska infrastrukturen för nationella myndigheters begäran om certifikat,

b) validera eller avslå begäran om certifikat,

c) vid behov kommunicera med registreringsmyndigheten avseende kontroll av den begärande organisationens identitet.

2.2 Utfärdande av certifikat

2.2.1 Utfärdandet av certifikat ska genomföras i enlighet med följande sekventiella steg (se figur 1):

a) **Steg 1:** Identifiering av betrodd kurir.

([1]) En fullmakt är en rättslig handling genom vilken organisationen bemyndigar och auktoriserar Europeiska kommissionen, företrädd av den tjänsteman som utsetts att ansvara för CEF PKI-tjänsten, att för dess räkning begära generering av ett certifikat från T-Systems International GmbH TeleSec Shared Business CA. Se även punkt 6.

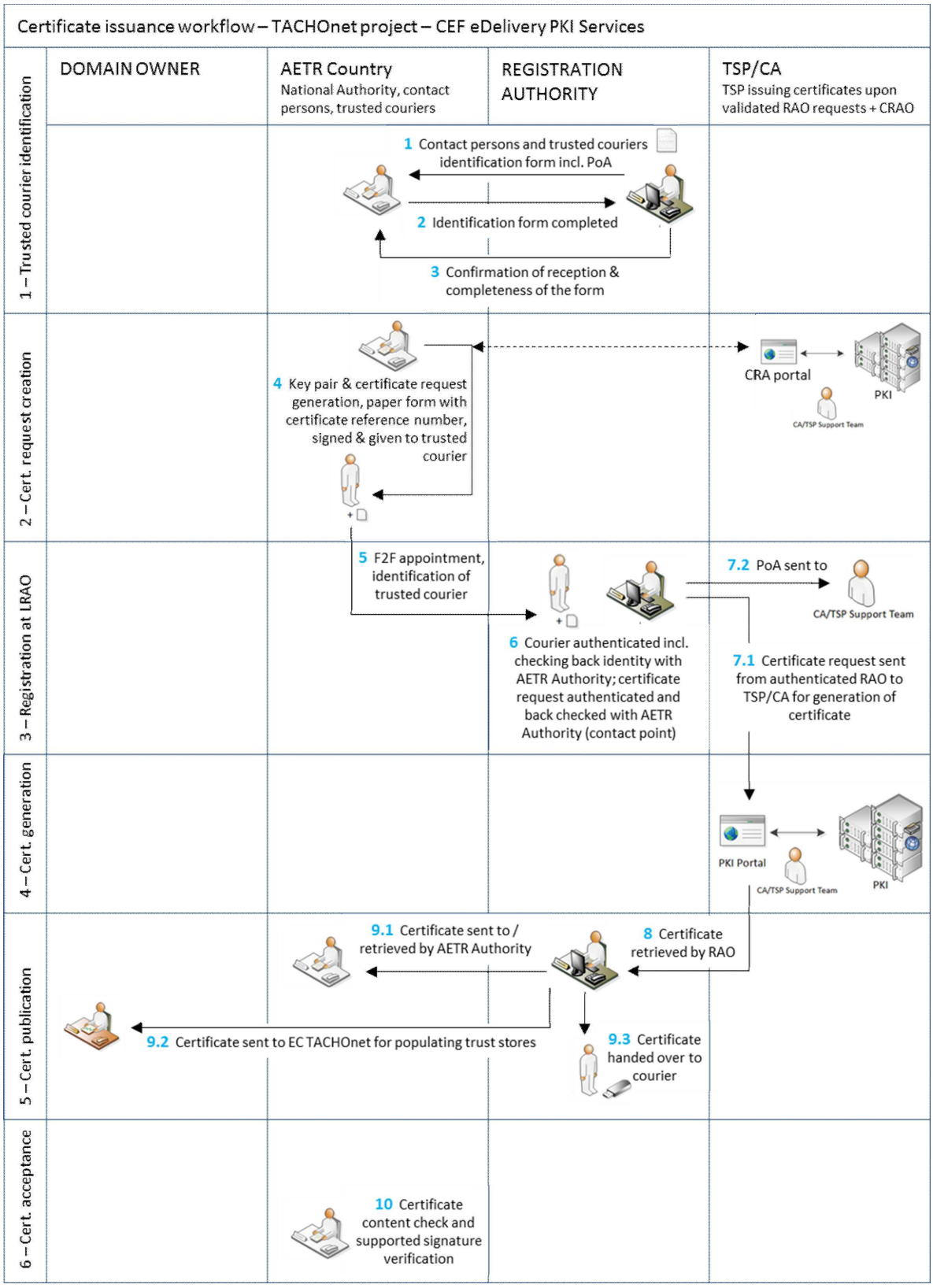
b) **Steg 2:** Skapande av begäran om certifikat.

c) **Steg 3:** Registrering vid registreringsmyndighet.

d) **Steg 4:** Generering av certifikat.

e) **Steg 5:** Offentliggörande av certifikat.

f) **Steg 6:** Godtagande av certifikat.



Figur 1 – **Arbetsflöde för utfärdande av certifikat**

2.2.2 Steg 1: Identifiering av betrodd kurir.

Följande process ska användas för identifieringen av betrodd kurir:

a) Registreringsmyndigheten ska skicka formuläret för identifiering av kontaktpersoner och betrodda kurirer till den nationella myndigheten ([1]). Detta formulär ska även innehålla en fullmakt som organisationen (AETR-myndigheten) ska underteckna.

b) Den nationella myndigheten ska skicka tillbaka det ifyllda formuläret och den undertecknade fullmakten till registreringsmyndigheten.

c) Registreringsmyndigheten ska bekräfta att formuläret mottagits samt att det är fullständigt.

d) Registreringsmyndigheten ska ge domänägaren en uppdaterad kopia av förteckningen över kontaktpersoner och betrodda kurirer.

2.2.3 Steg 2: Skapande av begäran om certifikat.

2.2.3.1 Begäran och hämtning av certifikatet ska göras från samma dator och med samma webbläsare.

2.2.3.2 Följande process ska användas för skapandet av begäran om certifikat:

a) Organisationen ska gå till webbgränssnittet för att begära certifikatet via webbadressen https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: och ska där ange användarnamnet "**sbca/CEF_eDelivery.europa.eu**" och lösenordet "**digit.333**".

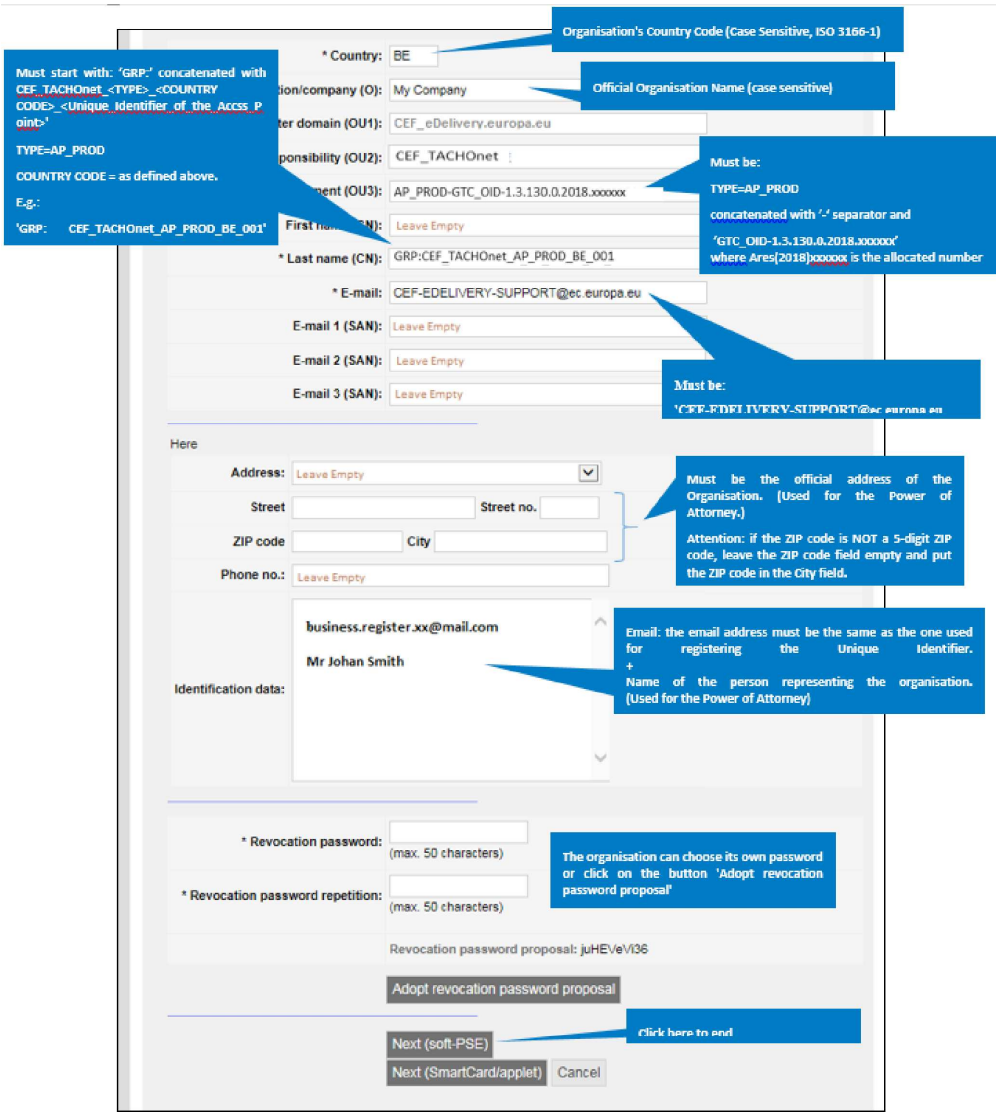
Figur 2

b) Organisationen ska klicka på "request" på panelens vänstra sida och välja "CEF_TACHOnet" i rullgardinsmenyn.

Figur 3

c) Organisationen ska i formuläret för begäran om certifikat (se figur 4) ange den information som beskrivs i tabell 3 och klicka på "Next (soft-PSE)" för att slutföra processen.

([1]) Se punkt 5.



Figur 4

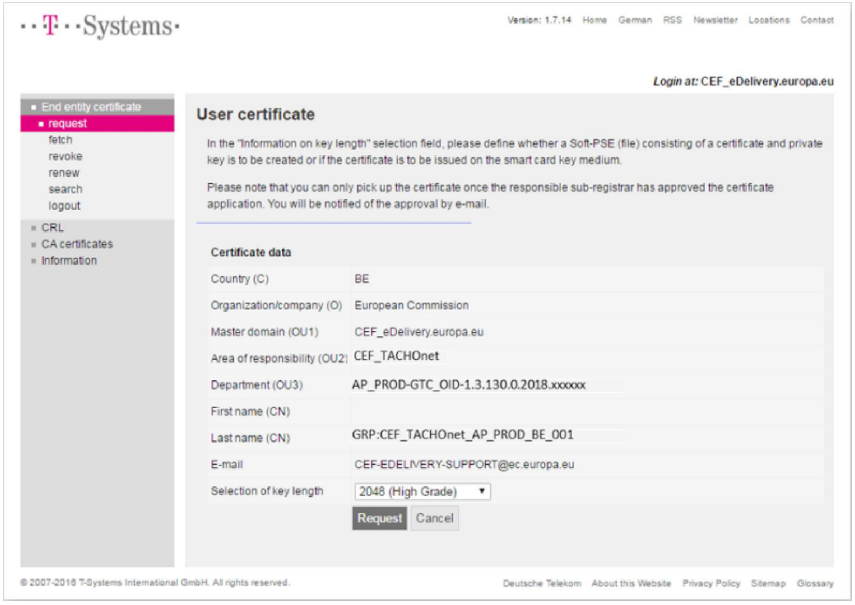
Begärda fält	Beskrivning
Country (land)	**C = Country Code**, certifikatinnehavarens lokalisering, verifierad med hjälp av ett allmänt register. Begränsningar: 2 tecken, i enlighet med ISO 3166-1, tvåbokstavskod, skiftlägeskänslig. Exempel: DE, BE, NL Specialfall: UK (för Storbritannien), EL (för Grekland)
Organisation/Company (O) (organisation/företag)	**O = Namnet på certifikatinnehavarens organisation**
Master domain (OU1) (huvuddomän)	**OU = CEF_eDelivery.europa.eu**
Area of responsibility (OU2) (ansvarsområde)	**OU = CEF_TACHOnet**

Begärda fält	Beskrivning
Department (OU3) (avdelning)	Obligatoriskt värde per ”AREA OF RESPONSIBILITY” Innehållet ska kontrolleras med hjälp av en positiv lista (vit lista) när certifikatet begärs. Om uppgifterna inte överensstämmer med listan avvisas begäran. Format: **OU=<TYPE>-<GTC_NUMBER>** Där ”<TYPE>” ersätts med AP_PROD: Access Point in Production environment (accesspunkt i produktionsmiljö). Och där <GTC_NUMBER> är **GTC_OID-1.3.130.0.2018.xxxxxx**, där Ares(2018)xxxxxx är GTC-numret för TACHOnet-projektet. t.ex.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN) (förnamn)	Måste vara tomt
Last name (CN) (efternamn)	Måste börja med ”GRP:”, följt av ett vedertaget namn. Format: **CN = GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** t.ex.: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-post: (e-post)	**E = CEF-EDELIVERY-SUPPORT@ec.europa.eu**
E-post: 1 (SAN)	Måste vara tomt
E-post: 2 (SAN)	Måste vara tomt
E-post: 3 (SAN)	Måste vara tomt
Address (adress)	Måste vara tomt
Street (gata)	Måste vara certifikatinnehavarens organisations officiella adress. (Används för fullmakten.)
Street no. (gatunummer)	Måste vara certifikatinnehavarens organisations officiella adress. (Används för fullmakten.)
Zip Code (postnummer)	Måste vara certifikatinnehavarens organisations officiella adress. (Används för fullmakten.) **Obs:** Om ZIP code INTE är en 5-siffrig kod ska fältet ZIP code lämnas tomt. Ange i så fall Zip code i fältet City.
City (ort)	Måste vara certifikatinnehavarens organisations officiella adress. (Används för fullmakten.) **Obs:** Om ZIP code INTE är en 5-siffrig kod ska fältet ZIP code lämnas tomt. Ange i så fall Zip code i fältet City.
Phone no (telefonnummer)	Måste vara tomt

Begärda fält	Beskrivning
Identification data (identifieringsuppgifter)	E-postadressen måste vara samma adress som användes för registrering av ”Unique Identifier” (unikt ID). + Måste vara namnet på den person som företräder organisationen. (Används för fullmakten.) + **Nr i handelsregister** (obligatoriskt endast för privata organisationer) **Registrerad vid lokal domstol i** (krävs endast för tyska och österrikiska privata organisationer)
Revocation password (lösenord för återkallande)	Obligatoriskt fält, väljs av den som lämnar in begäran
Revocation password repetition (upprepa lösenord för återkallande)	Obligatoriskt fält, väljs av den som lämnar in begäran (upprepning)

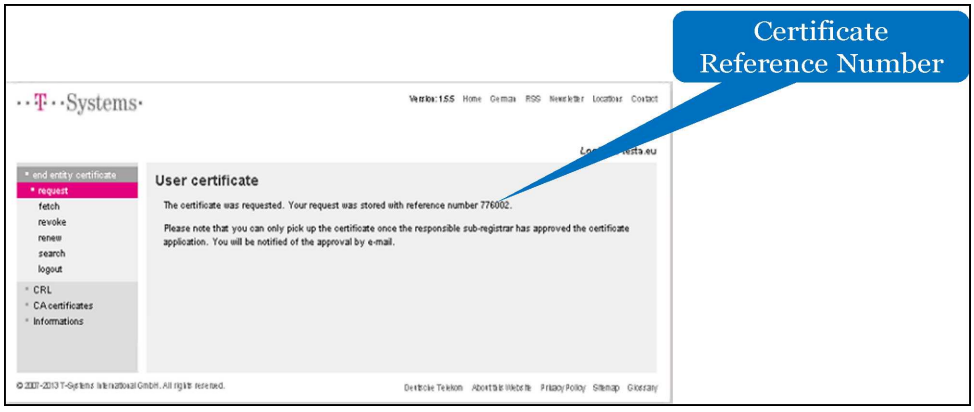
Tabell 3: **Fullständiga uppgifter om varje begärt fält**

d) Den valda nyckellängden ska vara 2 048 (High Grade).



Figur 5

e) Organisationen ska registrera referensnumret för hämtning av certifikatet.



Figur 6

f) CEF Support Team ska kontrollera om det finns nya begäran om certifikat och kontrollera att uppgifterna i begäran är giltiga, dvs. att de överensstämmer med de namngivningskonventioner som anges i tillägg 5.1 (Namngivningskonvention för certifikat).

g) CEF Support Team ska kontrollera att de uppgifter som lämnats i begäran har ett giltigt format.

h) När någon av kontrollerna i punkterna 5 eller 6 ovan ger negativt resultat ska CEF Support Team skicka ett e-postmeddelande till den e-postadress som angetts i ”Identification data” på formuläret för begäran, med kopia till domänägaren, och i meddelandet ska organisationen anmodas att starta processen på nytt. Den misslyckade begäran om certifikat ska annulleras.

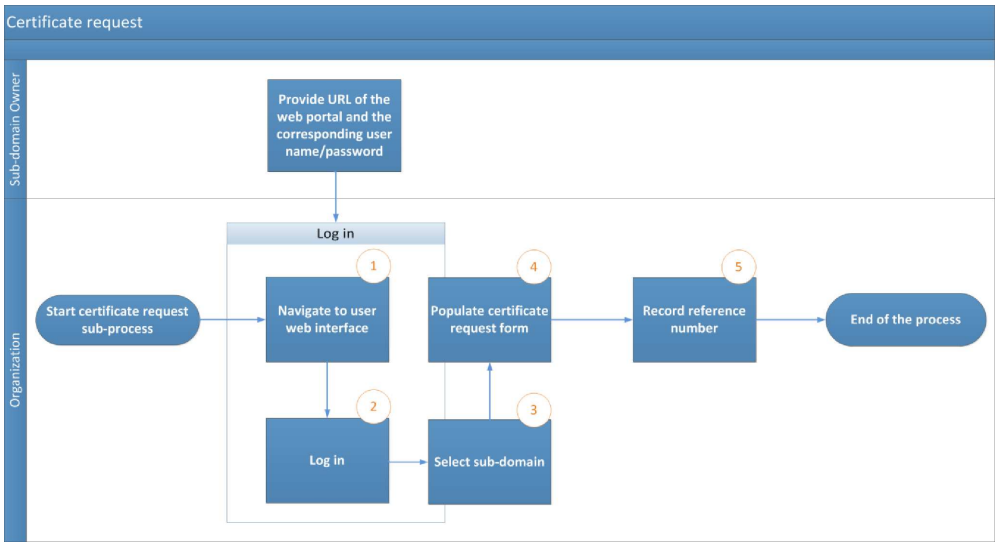
i) CEF Support Team ska skicka ett e-postmeddelande till registreringsmyndigheten om giltigheten för begäran. E-postmeddelandet ska inbegripa

1) namnet på organisationen, enligt fältet ”Organisation (O)” i begäran om certifikat,

2) uppgifter om certifikatet, inbegripet namnet på den AP för vilken certifikatet ska utfärdas, enligt fältet ”Last Name (CN)” i begäran om certifikat,

3) certifikatets referensnummer,

4) organisationens adress och e-postadress samt namnet på den person som företräder den.



Figur 7 – **Process för begäran om certifikat**

2.2.4 Steg 3: Registrering vid registreringsmyndighet (Godkännande av certifikat)

2.2.4.1 Den betrodda kuriren eller kontaktpunkten ska stämma möte med registreringsmyndigheten via e-post och därvid identifiera den betrodda kurir som kommer att delta i det personliga mötet.

2.2.4.2 Organisationen ska ta fram dokumentpaketet bestående av följande:

a) Ifylld och undertecknad fullmakt.

b) En kopia av ett giltigt pass som innehas av den betrodda kurir som kommer att delta i det personliga mötet. Denna kopia måste vara undertecknad av en av organisationens kontaktpunkter som identifieras i steg 1.

c) Pappersformuläret för begäran om certifikat, undertecknat av en av organisationens kontaktpunkter.

2.2.4.3 Registreringsmyndigheten ska ta emot den betrodda kuriren efter identitetskontroll vid receptionen i byggnaden. Registreringsmyndigheten ska utföra den personliga registreringen av begäran om certifikat genom att göra följande:

a) Identifiera och autentisera den betrodda kuriren.

b) Kontrollera att den betrodda kurirens utseende stämmer överens med det pass som den betrodda kuriren uppvisar.

c) Kontrollera att det pass som den betrodda kuriren uppvisar är giltigt.

d) Kontrollera att det validerade pass som uppvisas av den betrodda kuriren överensstämmer med den kopia av kurirens pass som undertecknats av en av organisationens kontaktpunkter som tidigare identifierats. Namnteckningen ska autentiseras med hjälp av det ursprungliga formuläret för identifiering av betrodd kurir och kontaktpunkter.

e) Kontrollera den ifyllda och undertecknade fullmakten.

f) Kontrollera pappersformuläret för begäran om certifikat och underskriften på detta med hjälp av det ursprungliga formuläret för identifiering av betrodd kurir och kontaktpunkter.

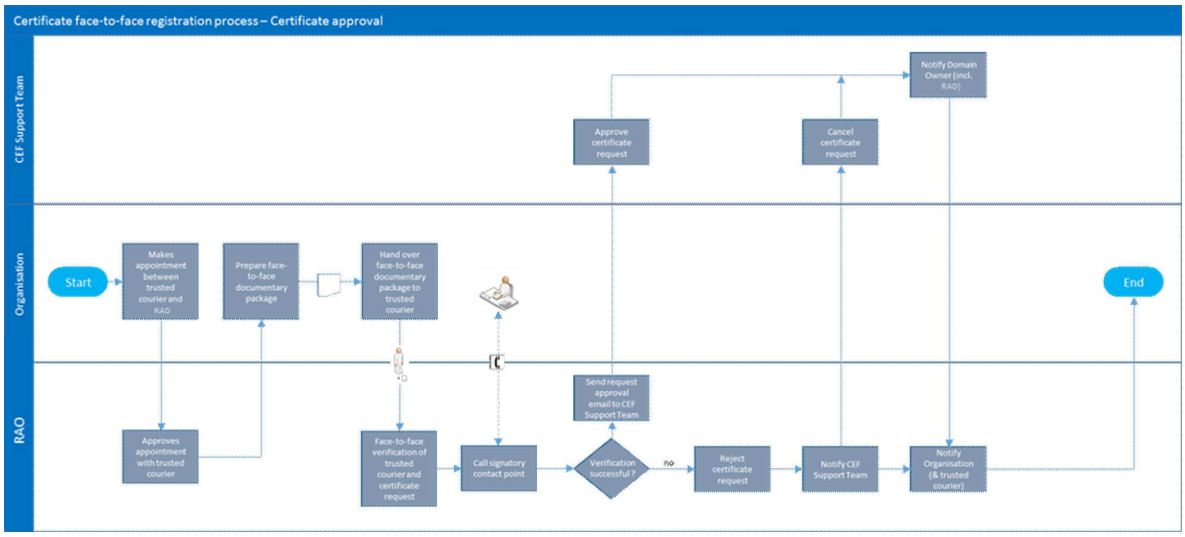
g) Uppmana den undertecknande kontaktpunkten att dubbelkontrollera den betrodda kurirens identitet och innehållet i begäran om certifikat.

2.2.4.4 Registreringsmyndigheten ska bekräfta för CEF Support Team att den nationella myndigheten verkligen är auktoriserad att handha de komponenter för vilka den begär certifikaten och att motsvarande process för personlig registrering har slutförts. Bekräftelsen ska skickas med ett säkert e-postmeddelande med hjälp av ett ”CommiSign”-certifikat, och som bilaga bifogas en inskannad kopia av det autentiserade dokumentpaketet avseende det personliga mötet och av den undertecknade processchecklista som använts av registreringsmyndigheten.

2.2.4.5 Om registreringsmyndigheten bekräftar att begäran är giltig ska processen fortsätta enligt punkterna 2.2.4.6 och 2.2.4.7. I annat fall ska begäran om utfärdandet av certifikatet avslås och organisationen ska informeras.

2.2.4.6 CEF Support Team ska godkänna begäran om certifikat och ska informera registreringsmyndigheten om godkännandet av certifikatet.

2.2.4.7 Registreringsmyndigheten ska underrätta organisationen om att certifikatet kan hämtas via användarportalen.



Figur 8 – **Godkännande av certifikat**

2.2.5 Steg 4: Generering av certifikat

Efter godkännande av begäran om certifikat ska certifikatet genereras.

2.2.6 Steg 5: Offentliggörande och hämtning av certifikat

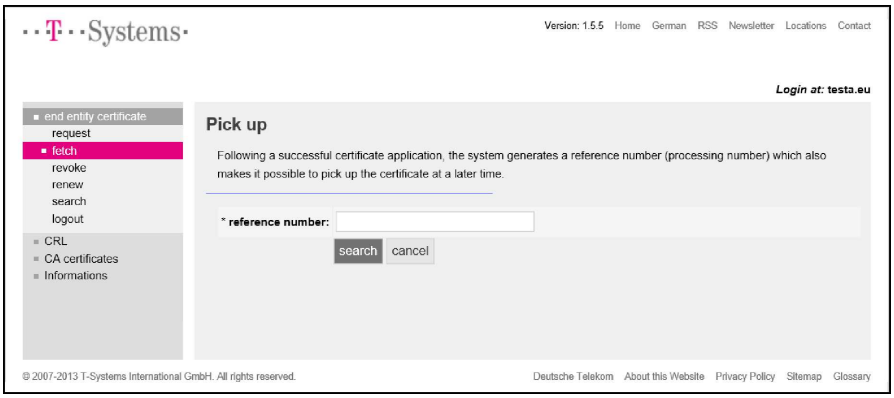
2.2.6.1 Efter det att begäran om certifikat har godkänts ska registreringsmyndigheten hämta certifikatet och överlämna en kopia till den betrodda kuriren.

2.2.6.2 Organisationen ska få ett meddelande från registreringsmyndigheten om att certifikaten kan hämtas.

2.2.6.3 Organisationen ska gå till användarportalen på https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en och logga in med användarnamnet ”**sbca/CEF_eDelivery.europa.eu**” och lösenordet ”**digit.333**”.

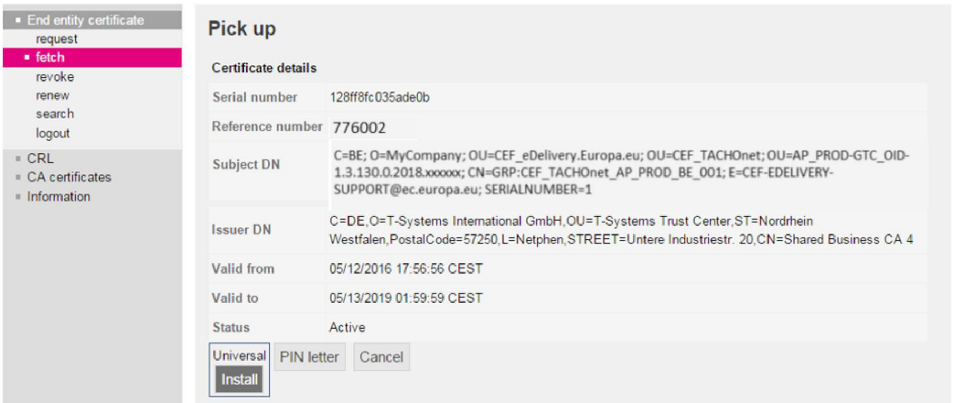
Figur 9

2.2.6.4 Organisationen ska klicka på ”fetch”-knappen på den vänstra sidan och ange det referensnummer som registrerats i samband med processen för begäran om certifikat.



Figur 10

2.2.6.5 Organisationen ska installera certifikaten genom att klicka på ”Install”-knappen.



Figur 11

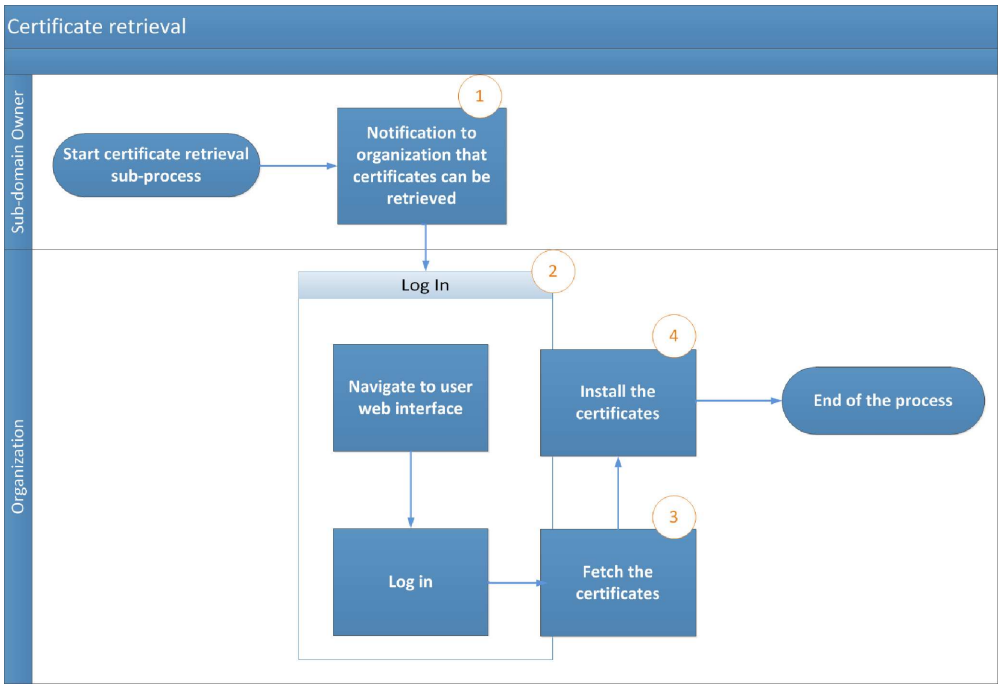
2.2.6.6 Certifikatet ska installeras på accesspunkten (AP). Eftersom detta är specifikt för det aktuella genomförandet ska organisationen vända sig till sin accesspunkt för att få en beskrivning av denna process.

2.2.6.7 Följande måste göras för installation av certifikatet på accesspunkten:

a) Exportera den privata nyckeln och certifikatet.

b) Skapa keystore och truststore.

c) Installera keystore och truststore på accesspunkten.

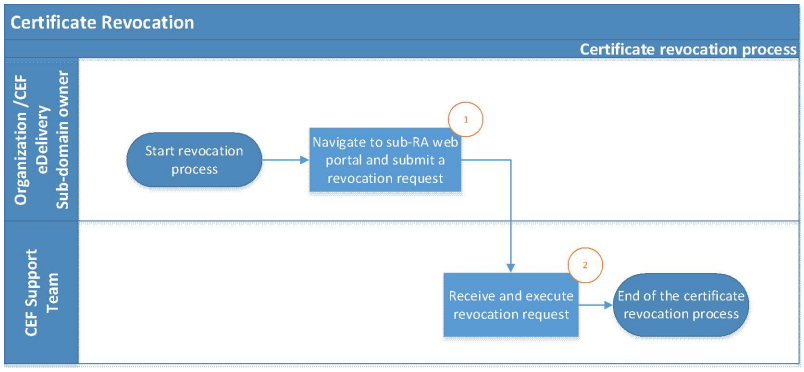


Figur 12 – **Hämtning av certifikat**

3. Process för återkallande av certifikat

3.1 Organisationen ska lämna en begäran om återkallande via den webbaserade användarportalen.

3.2 CEF Support Team ska verkställa återkallandet av certifikatet.



Figur 13 – **Återkallande av certifikat**

4. Allmänna villkor för CEF PKI-tjänsten

4.1 Bakgrund

DIGIT ska, i sin kapacitet som leverantör av lösningar för byggstenen eDelivery i Fonden för ett sammanlänkat Europa, tillhandahålla en PKI-tjänst ([1]) (”CEF PKI-tjänst”) för avtalsslutande parter i AETR. CEF PKI-tjänsten ska användas av nationella myndigheter (”slutanvändare”) som deltar i TACHOnet.

DIGIT är en PKI-innehavare inom TeleSec Shared-Business-CA-lösningen (”SBCA”) som används i Trust Center för Group unit T-Systems International GmbH (”T-Systems” ([2])). DIGIT har rollen som ”Master Registrar” i domänen ”CEF_eDelivery.europa.eu” i SBCA. I denna roll skapar DIGIT underdomäner inom domänen ”CEF_eDelivery.europa.eu” för varje projekt med hjälp av CEF PKI-tjänsten.

([1]) En PKI (Public Key Infrastructure) är en uppsättning roller, policyer, förfaranden och system som behövs för att skapa, förvalta, distribuera och återkalla digitala certifikat.

([2]) Trust Center-operatören, som är lokaliserad i T-Systems Trust Center, fullgör utöver sin roll som betrodd operatör också uppgiften som intern registreringsmyndighet.

Detta dokument innehåller närmare uppgifter om villkoren för underdomänen TACHOnet. DIGIT har rollen som ”sub-Registrar” i denna underdomän. Det är i denna kapacitet som DIGIT utfärdar, återkallar och förnyar certifikaten i detta projekt.

4.2 Ansvarsfriskrivning

Europeiska kommissionen frånsäger sig allt ansvar för certifikatets innehåll, för vilket endast certifikatinnehavaren har ansvaret. Det är certifikatinnehavarens ansvar att kontrollera riktigheten i certifikatets innehåll.

Europeiska kommissionen frånsäger sig allt ansvar för certifikatinnehavarens användning av certifikatet om innehavaren är en tredje rättslig enhet utanför Europeiska kommissionen.

Denna ansvarsfriskrivning är inte avsedd att begränsa Europeiska kommissionens ansvar i strid mot tillämplig nationell lagstiftning eller att befria kommissionen från ansvar i de fall där friskrivning inte får ske enligt sådan lagstiftning.

4.3 Auktoriserad/förbjuden användning av certifikat

4.3.1 Tillåten användning av certifikat

När certifikatet har utfärdats ska certifikatinnehavaren [1] använda det endast inom ramen för TACHOnet. I detta sammanhang kan certifikatet användas för att

— autentisera uppgifternas ursprung,

— kryptera data,

— säkerställa upptäckt av integritetsöverträdelser som rör data.

4.3.2 Förbjuden användning av certifikat

All användning som inte uttryckligen godkänts som en del av den tillåtna användningen av certifikatet är förbjuden.

4.4 Ytterligare skyldigheter för certifikatinnehavaren

De detaljerade villkoren för SBCA fastställs av T-Systems i CP/CPS (Certificate Policy/Certification Practice Statement) för SBCA-tjänsten [2]. Detta dokument innehåller säkerhetsspecifikationer och riktlinjer avseende tekniska och organisatoriska aspekter, och i dokumentet beskrivs de verksamheter som bedrivs av Trust Center-operatören i rollerna som certifieringsmyndighet (Certification Authority, CA) och registreringsmyndighet (Registration Authority, RA) samt registreringsmyndighetens (RA) delegerade tredje part.

Endast enheter som har rätt att delta i TACHOnet kan begära ett certifikat.

I fråga om godtagande av certifikat gäller klausul 4.4.1 i SBCA CP/CPS (Certificate Policy och Certification Practice Statement), och dessutom anses de användningsvillkor och bestämmelser som beskrivs i detta dokument vara godtagna av den organisation för vilken certifikatet utfärdats (”O=”) när det används för första gången.

I fråga om offentliggörande av certifikatet gäller klausul 2.2 i SBCA CP/CPS.

Alla certifikatinnehavare ska uppfylla följande krav:

1) Skydda sin privata nyckel mot obehörig användning.

2) Avstå från att överföra sin privata nyckel till tredje part, eller avslöja sin privata nyckel för tredje part, även som företrädare.

3) Avstå från fortsatt användning av den privata nyckeln efter det att certifikatets giltighetsperiod har löpt ut eller efter det att certifikatet har återkallats, annat än i syfte att visa krypterade data (t.ex. dekryptering av e-postmeddelanden).

4) Certifikatinnehavaren har ansvar för att kopiera eller vidarebefordra nyckeln till slutmottagaren eller slutmottagarna.

[1] Identifieras med värdet på attributet ”O=” i ”Subject Distinguished Name” för det utfärdade certifikatet.
[2] Den senaste versionen av T-Systems SBCA CP/CPS kan hämtas från https://www.telesec.de/en/sbca-en/support/download-area/

5) Certifikatinnehavaren måste ålägga slutmottagaren/alla slutmottagare att uppfylla aktuella villkor, inbegripet SBCA CP/CPS, när de har att göra med den privata nyckeln.

6) Certifikatinnehavaren måste tillhandahålla identifiering av de auktoriserade företrädare som bemyndigats att begära återkallande av certifikat som utfärdats till organisationen, med närmare uppgifter om händelser som lett till återkallandet samt lösenordet för återkallande.

7) För certifikat som är knutna till grupper av personer och funktioner och/eller juridiska personer, efter det att en person har lämnat en grupp av slutmottagare (t.ex. efter avslutat anställningsförhållande), ska certifikatinnehavaren förhindra missbruk av den privata nyckeln genom att begära återkallande av certifikatet.

8) Certifikatinnehavaren har ansvar för och ska begära återkallande av certifikatet under de omständigheter som avses i klausul 4.9.1 i SBCA CP/CPS.

I fråga om förnyelse av eller nya nycklar för certifikat gäller klausul 4.6 eller 4.7 i SBCA CP/CPS.

I fråga om ändring av certifikat gäller klausul 4.8 i SBCA CP/CPS.

I fråga om återkallande av certifikat gäller klausul 4.9 i SBCA CP/CPS.

5. **Formulär för identifiering av kontaktpersoner och betrodda kurirer (exempel)**

Jag, *[organisationsföreträdarens namn och adress]*, **intygar att följande information ska användas i samband med begäran om, generering av och hämtning av digitala certifikat för öppna nycklar för TACHOnet-accesspunkter som stöder TACHOnet-meddelandenas konfidentialitet, integritet och oavvislighet:**

Uppgifter om kontaktperson:

— **Kontaktperson #1**	— **Kontaktperson #2**
— Namn:	— Namn:
— Förnamn:	— Förnamn:
— Mobiltelefonnummer:	— Mobiltelefonnummer:
— Telefonnummer:	— Telefonnummer:
— E-post:	— E-post:
— Prov på egenhändig underskrift: —	— Prov på egenhändig underskrift: — — —

Uppgifter om betrodd kurir:

— **Betrodd kurir #1**	— **Betrodd kurir #2**
— Namn:	— Namn:
— Förnamn:	— Förnamn:
— Mobiltelefonnummer:	— Mobiltelefonnummer:
— E-post:	— E-post:
— Land som utfärdat passet:	— Land som utfärdat passet:
— Passnummer:	— Passnummer:
— Passets sista giltighetsdag:	— Passets sista giltighetsdag:

Ort, datum, organisationens stämpel eller sigill:

Auktoriserad företrädares underskrift:

6. **Dokument**

6.1 Individuell fullmakt (exempel)

Ett exempel på individuell fullmakt, som måste undertecknas och uppvisas av den betrodda kuriren i samband med personlig registrering vid registreringsmyndigheten, kan hittas här:

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 Pappersformulär för begäran om certifikat (exempel)

Ett exempel på pappersformulär för begäran om certifikat, som måste undertecknas och uppvisas av den betrodda kuriren i samband med personlig registrering vid registreringsmyndigheten, kan hittas här:

TACHOnet certificate request paper form

I, ***[name and address of the organisation representative]***, certifies that the following information are to be used in the context of the request, generation and retrieval of public key digital certificates for TACHOnet access points supporting the confidentiality, integrity and non-repudiation of the TACHOnet messages:

Please reproduce the certificate data information provided by CEF Support Team acknowledging the completeness of the electronic certificate request, e.g.:

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

Certificate request reference number: *insert reference number (e.g. 776002)*
Identification of the trusted courier proceeding to the face-to-face registration of the request: *please fill in*

Trusted courier #1
Name:
First names:
Mobile phone:
Email:
Passport issuing country:
Passport number:
Passport validity end date:

Place, date, company stamp or seal of the Organisation:

Signature of the authorised representative:

7. **Ordlista**

De centrala termer som används i detta undertillägg definieras i avsnittet ”CEF Definitions” på den gemensamma webbportalen CEF Digital:

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

De centrala akronymer som används i denna komponentbeskrivning definieras i avsnittet ”CEF Glossary” på den gemensamma webbportalen CEF Digital:

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