Rat der
Europäischen Union

Brüssel, den 5. November 2018
(OR. en)

13711/18
ADD 1

Interinstitutionelles Dossier:
2018/0339(NLE)

TRANS 488

VERMERK

Absender:	Generalsekretariat des Rates
Empfänger:	Delegationen
Nr. Vordok.:	ST 13711/18 TRANS 448
Nr. Komm.dok.:	ST 12727/18 TRANS 426 + ADD 1
Betr.:	Beschluss des Rates zur Festlegung des gemeinsamen Standpunkts, der im Namen der Europäischen Union in der Sachverständigengruppe zum Europäischen Übereinkommen über die Arbeit des im internationalen Straßenverkehr beschäftigten Fahrpersonals der Wirtschaftskommission für Europa der Vereinten Nationen zu vertreten ist

Anhang zum oben genannten Beschluss des Rates.

ANHANG

Neue Anlage des AETR

Anlage 4

TACHOnet-Spezifikationen

1. Anwendungsbereich und Zweck

1.1. Diese Anlage enthält die Bedingungen für die Anbindung der AETR-Vertragsparteien an TACHOnet durch elektronische Zustellung (eDelivery).

1.2. Vertragsparteien, die sich durch eDelivery mit TACHOnet vernetzen, müssen die in dieser Anlage festgelegten Bestimmungen einhalten.

2. Begriffsbestimmungen

a) "Vertragspartei" (contracting party) oder "Partei" (party): eine AETR-Vertragspartei;

b) "elektronische Zustellung" (eDelivery): ein von der Europäischen Kommission entwickelter Dienst, der die Übermittlung von Daten zwischen Dritten mit elektronischen Mitteln ermöglicht und einen Nachweis der Handhabung der übermittelten Daten erbringt, darunter den Nachweis der Absendung und des Empfangs der Daten, und der die übertragenen Daten vor unbefugter Veränderung schützt;

c) "TACHOnet": das System für den elektronischen Austausch von Informationen über Fahrerkarten zwischen den Vertragsparteien im Sinne von Artikel 31 Absatz 2 der Verordnung (EU) Nr. 165/2014;

d) "Zentralstelle" (central hub): das Informationssystem, mit dessen Hilfe die TACHOnet-Benachrichtigungen zwischen den anfragenden und antwortenden Parteien ausgetauscht werden können;

e) "anfragende Partei" (requesting party): die Vertragspartei, die eine TACHOnet-Anfrage oder -Mitteilung abschickt, die dann über die Zentralstelle an die entsprechende antwortende Partei geleitet wird;

f) "antwortende Partei" (responding party): die Vertragspartei, an die die TACHOnet-Anfrage oder -Mitteilung gerichtet ist;

g) "Karten ausstellende Behörde" ("card issuing authority", CIA): die Stelle, die von einer Vertragspartei ermächtigt wurde, Fahrtenschreiberkarten auszustellen und zu verwalten.

3. Allgemeine Zuständigkeiten

3.1. Keine Vertragspartei kann Vereinbarungen über den Zugang zu TACHOnet im Namen einer anderen Partei treffen oder auf eine andere Art und Weise die andere Vertragspartei auf der Grundlage dieser Anlage vertreten. Keine Vertragspartei handelt im Zusammenhang mit dem in dieser Anlage genannten Tätigkeiten als Unterauftragnehmer der anderen Vertragspartei

3.2. Die Vertragsparteien gewähren über TACHOnet Zugang zu ihrem nationalen Fahrerkartenregister und zwar in einer Art und Weise und mit einem Leistungsniveau wie in Unteranlage 4.6 festgelegt.

3.3. Die Vertragsparteien unterrichten sich gegenseitig und unverzüglich über Störungen oder Fehler in ihrem Zuständigkeitsbereich, die den normalen Betrieb von TACHOnet gefährden könnten.

3.4. Jede Partei meldet dem AETR-Sekretariat Ansprechpartner für TACHOnet. Jede Änderung der Ansprechpartner ist dem AETR-Sekretariat schriftlich mitzuteilen.

4. Tests für die Anbindung an TACHOnet

4.1. Die Anbindung einer Vertragspartei an TACHOnet gilt als hergestellt, wenn die Verbindungs-, Integrations- und Leistungstests nach den Anweisungen und unter der Aufsicht der Europäischen Kommission erfolgreich abgeschlossen wurden.

4.2. Bei einem Nichtbestehen der Vortests kann die Europäische Kommission die Testphase vorübergehend anhalten. Die Tests werden fortgesetzt, sobald die Vertragspartei der Europäischen Kommission mitgeteilt hat, dass die für eine erfolgreiche Durchführung der Vortests erforderlichen technischen Verbesserungen auf nationaler Ebene vorgenommen worden sind.

4.3. Die Höchstdauer der Vortests beträgt sechs Monate.

5. Vertrauensarchitektur

5.1. Die TACHOnet-Vertrauensarchitektur muss die Vertraulichkeit, Integrität und Nichtabstreitbarkeit von TACHOnet-Benachrichtigungen gewährleisten.

5.2. Die TACHOnet-Vertrauensarchitektur beruht auf einer von der Europäischen Kommission eingerichteten Public Key Infrastruktur (PKI), deren Anforderungen in den Teilanlagen 4.8 und 4.9 festgelegt sind.

5.3. Folgende Stellen werden innerhalb der TACHOnet-Vertrauensarchitektur tätig:

a) Die Zertifizierungsbehörde, die für die Generierung der digitalen Zertifikate, die von der Registrierungsbehörde den nationalen Behörden der Vertragsparteien (über die von ihnen ernannten vertrauenswürdigen Kuriere) übermittelt werden, sowie für den Aufbau der technischen Infrastruktur für die Ausstellung, die Sperrung und die Erneuerung der digitalen Zertifikate zuständig ist.

b) Inhaber von Domänen, die für den Betrieb der in Unteranlage 4.1 genannten Zentralstelle sowie für die Validierung und Koordinierung der TACHOnet-Vertrauensarchitektur zuständig sind.

c) Die Registrierungsbehörde, die für die Registrierung und Genehmigung der Anträge auf Ausstellung, Sperrung und Erneuerung digitaler Zertifikate sowie für die Überprüfung der Identität vertrauenswürdiger Kuriere zuständig ist.

d) Vertrauenswürdiger Kurier ist eine von den nationalen Behörden für die Übermittlung des öffentlichen Schlüssels an die Registrierungsbehörde und für die Entgegennahme des entsprechenden von der Zertifizierungsbehörde generierten Zertifikats benannte Person.

e) Die Nationale Behörde der Vertragspartei, die

i) private Schlüssel und die entsprechenden öffentlichen Schlüssel generiert, die in die von der Zertifizierungsbehörde generierten Zertifikate eingetragen werden;

ii) bei der Zertifizierungsbehörde die digitalen Zertifikate beantragt;

iii) den vertrauenswürdigen Kurier benennt.

5.4. Die Zertifizierungsbehörde und die Registrierungsbehörde werden von der Europäischen Kommission benannt.

5.5. Jede Vertragspartei, die sich an das TACHOnet anbindet, muss zur Zeichnung und Verschlüsselung einer TACHOnet-Benachrichtigung die Ausstellung eines digitalen Zertifikats nach Unteranlage 4.9 beantragen.

5.6. Ein Zertifikat kann nach Unteranlage 4.9 gesperrt werden.

6. Datenschutz und Vertraulichkeit

6.1. Im Einklang mit den Datenschutzbestimmungen auf internationaler und nationaler Ebene und insbesondere mit dem Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten müssen die Parteien alle erforderlichen technischen und organisatorischen Maßnahmen ergreifen, um die Sicherheit der TACHOnet-Daten zu gewährleisten und um die Änderung, den Verlust, die unbefugte Verarbeitung dieser Daten oder den unbefugten Zugang zu diesen Daten zu verhindern (insbesondere im Hinblick auf Authentizität, Vertraulichkeit, Rückverfolgbarkeit, Integrität, Verfügbarkeit, Nichtabstreitbarkeit und Sicherheit der Benachrichtigungen).

6.2. Jede Partei schützt ihre eigenen Systeme gegen unbefugte Nutzung, schädliche Programmcodes, Viren, unbefugte Computerzugriffe, Verstöße gegen den Datenschutz und die Manipulation von Daten sowie sonstige vergleichbare Handlungen Dritter. Die Parteien vereinbaren, wirtschaftlich angemessene Anstrengungen zu unternehmen, um die Übertragung von Viren, Zeitbomben, Würmern oder ähnlicher Schadsoftware sowie sonstiger Computerprogrammroutinen zu verhindern, die in die Computersysteme anderer Parteien eindringen können.

7. Kosten

7.1. Die Vertragsparteien tragen ihre eigenen Entwicklungs- und Betriebskosten, die bei ihren eigenen Datensystemen und Verfahren anfallen, die sie für die Erfüllung ihrer Verpflichtungen nach dieser Anlage benötigen.

7.2. Die in Unteranlage 4.1 genannten Dienste werden von der Zentralstelle kostenfrei zur Verfügung gestellt.

8. Vergabe von Unteraufträgen

8.1. Die Parteien können über alle Dienste, für die sie nach dieser Anlage zuständig sind, Unteraufträge vergeben.

8.2. Solche Unteraufträge befreien die Partei nicht von ihrer Zuständigkeit nach dieser Anlage, auch nicht von der Zuständigkeit für ein nach Unteranlage 4.6 angemessenes Leistungsniveau.

Unteranlage 4.1

Allgemeine Aspekte des TACHOnet

1. Allgemeine Beschreibung

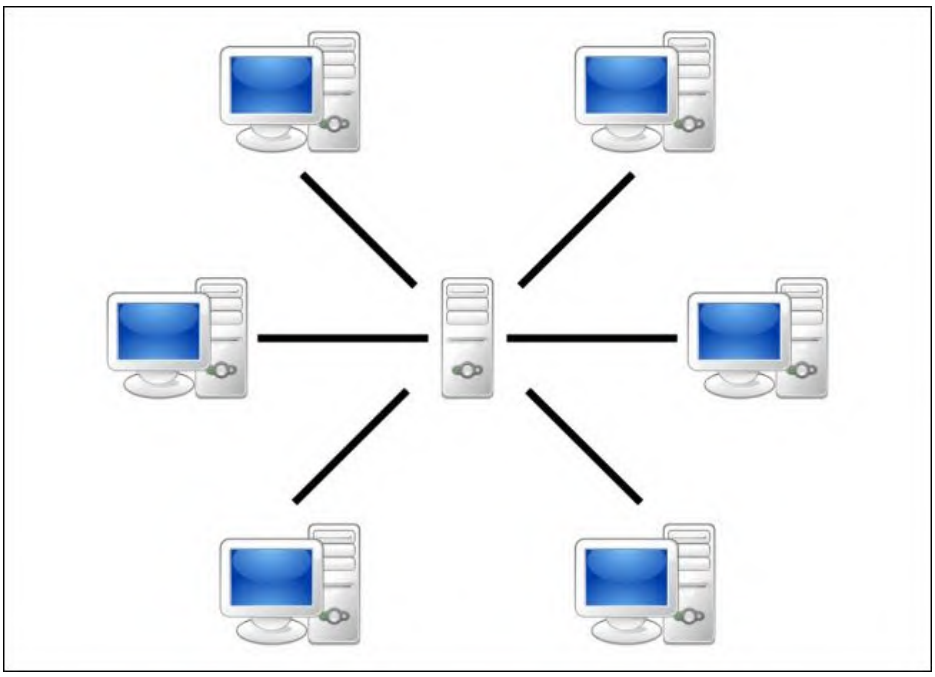
TACHOnet ist ein System für den elektronischen Austausch von Informationen über Fahrerkarten zwischen den AETR-Vertragsparteien. TACHOnet leitet Informationsanfragen von der anfragenden Partei an die antwortende Partei ebenso weiter wie die Antwort der Letzteren an die Erstere. Vertragsparteien, die Teil von TACHOnet sind, müssen ihre nationalen Fahrerkartenregister an das System anbinden.

2. Architektur

Das TACHOnet-Benachrichtigungssystem umfasst folgende Komponenten:

2.1. eine Zentralstelle, die in der Lage ist, die Anfrage einer anfragenden Partei entgegenzunehmen, sie zu validieren und sie an die antwortenden Parteien weiterzuleiten. Die Zentralstelle wartet auf die Beantwortung durch die antwortenden Parteien, konsolidiert alle Antworten und leitet die konsolidierte Antwort an die anfragende Partei weiter.

2.2. die nationalen Systeme der Parteien, die über eine Schnittstelle verfügen, über die sowohl Anfragen an die Zentralstelle gesendet als auch die Antworten von dieser empfangen werden können. Für die nationalen Systeme kann urheberrechtlich geschützte oder kommerzielle Software verwendet werden, um Benachrichtigungen der Zentralstelle zu empfangen oder an diese zu senden.



3. Verwaltung

3.1. Die Zentralstelle wird von der Europäischen Kommission verwaltet, die für den technischen Betrieb und die Instandhaltung der Zentralstelle zuständig ist.

3.2. Die Zentralstelle speichert alle Daten höchstens sechs Monate lang, es sei denn, es handelt sich um die in Unteranlage 4.7 genannten Protokolldaten und statistischen Daten.

3.3. Die Zentralstelle erlaubt keinen Zugriff auf personenbezogene Daten, es sei denn, hierzu befugtes Personal der Europäischen Kommission benötigt diesen Zugang für die Zwecke der Überwachung, der Instandhaltung und der Fehlerbehebung.

3.4. Jede Vertragspartei ist zuständig für

3.4.1. die Einrichtung und Verwaltung ihrer nationalen Systeme, einschließlich der Schnittstellen mit der Zentralstelle;

3.4.2. die Installation und Instandhaltung der Hardware und Software ihrer nationalen urheberrechtlich geschützten oder kommerziellen Systeme;

3.4.3. die funktionierende Interoperabilität ihrer nationalen Systeme mit der Zentralstelle, darunter die Bearbeitung von Fehlermeldungen der Zentralstelle;

3.4.4. die Ergreifung aller Maßnahmen, die für die Wahrung der Vertraulichkeit, Integrität und Verfügbarkeit der Informationen notwendig sind;

3.4.5. den Betrieb der nationalen Systeme gemäß den in Unteranlage 4.6 festgelegten Leistungsanforderungen.

Unteranlage 4.2

TACHOnet-Benachrichtigungen

1. Das TACHOnet-Benachrichtigungssystem muss folgende Funktionen bieten:

1.1. "Check Issued Cards (CIC)" (Überprüfung der ausgestellten Karten): Mit Hilfe dieser Funktion kann die anfragende Vertragspartei einer oder allen antwortenden Partei(en) eine Anfrage zur Überprüfung der ausgestellten Karten übermitteln, um festzustellen, ob ein Antragsteller bereits über eine in einer antwortenden Parteien ausgestellte Fahrerkarte verfügt. Die antwortenden Parteien reagieren auf die Anfrage mit einer Antwort nach der Überprüfung der ausgestellten Karten "Check Issued Cards Response".

1.2. "Check Card Status (CCS)" (Überprüfung des Kartenstatus): Mit dieser Funktion kann die anfragende Partei bei der antwortenden Partei Einzelheiten zu der von letzterer ausgestellten Karte abfragen, indem sie eine Anfrage zur Überprüfung des Kartenstatus "Check Card Status Request" schickt. Die antwortende Partei reagiert auf die Anfrage mit einer Antwort nach Überprüfung des Kartenstatus "Check Card Status Response".

1.3. "Modify Card Status (MCS)" (Änderung des Kartenstatus): Mit dieser Funktion kann die anfragende Partei der antwortenden Partei eine Mitteilung über die Änderung des Kartenstatus schicken, um ihr mitzuteilen, dass sich der Status einer von ihr ausgestellten Karte geändert hat. Die antwortende Partei reagiert auf die Mitteilung mit einer Bestätigung der Änderung des Kartenstatus "Modify Card Status Acknowledgement".

1.4. "Issued Card Driving Licence (ICDL)" (Ausstellung einer Karte anhand des Führerscheins): Mit dieser Funktion kann die anfragende Partei der antwortenden Partei mitteilen, dass sie auf der Grundlage einer von der antwortenden Partei ausgestellten Fahrerlaubnis eine Karte ausgestellt hat. Die antwortende Partei reagiert auf diese Mitteilung mit einer "Issued Card Driving Licence Response".

2. Weitere Arten von Benachrichtigungen, wie etwa Fehlermeldungen, die für das reibungslose Funktionieren des TACHOnet als geeignet empfunden werden, sind aufzunehmen.

3. Die nationalen Systeme müssen bei der Nutzung der in Nummer 1 erläuterten Funktionen den in Tabelle 1 aufgeführten Kartenstatus erkennen. Die Parteien sind jedoch nicht verpflichtet, ein Verwaltungsverfahren einzuführen, das alle aufgeführten Statusmeldungen nutzt.

4. Erhält eine Partei eine Antwort oder Mitteilung über einen Status, der in ihren Verwaltungsverfahren nicht verwendet wird, überträgt das nationale System den in der eingegangenen Benachrichtigung angegebenen Status in den entsprechenden Status dieses Verfahrens. Die Benachrichtigung darf von der antwortenden Partei nicht abgewiesen werden, sofern der in der Benachrichtigung angegebene Status in Tabelle 1 aufgeführt ist.

5. Der in Tabelle 1 aufgeführte Kartenstatus darf nicht dazu verwendet werden, die Gültigkeit der Fahrerlaubnis festzustellen. Fragt eine Partei das Register der Karten ausstellenden nationalen Behörde über die CCS-Funktion ab, muss die Antwort ein spezielles Feld "valid for driving" (gültig als Fahrerlaubnis) enthalten. Die nationalen Verwaltungsverfahren müssen so ausgelegt sein, dass die CCS-Antworten stets den entsprechenden Wert für "valid for driving" (gültig als Fahrerlaubnis) enthalten.

Tabelle 1

Kartenstatusmeldungen

"Card Status" (Kartenstatus)	**Begriffsbestimmung**
"Application" (Beantragung)	Bei der CIA geht ein Antrag auf Ausstellung einer Fahrerkarte ein. Diese Information wird registriert und mit den generierten Suchschlüsseln in die Datenbank eingegeben.
"Approved" (genehmigt)	Die CIA hat den Antrag auf Ausstellung einer Fahrtenschreiberkarte genehmigt.
"Rejected" (abgelehnt)	Die CIA hat den Antrag nicht genehmigt.
"Personalised" (personalisiert)	Die Fahrtenschreiberkarte wurde personalisiert.
"Dispatched" (versandt)	Die nationale Behörde hat die Fahrerkarte an den betreffenden Fahrer oder an die Ausgabestelle versandt.
"Handed Over" (ausgehändigt)	Die nationale Behörde hat die Fahrerkarte an den betreffenden Fahrer ausgehändigt.
"Confiscated" (eingezogen)	Die Fahrerkarte wurde von der zuständigen Behörde eingezogen.
"Suspended" (ausgesetzt)	Die Fahrerkarte wurde vorübergehend eingezogen.
"Withdrawn" (entzogen)	Die CIA hat entschieden, dem Fahrer die Fahrerkarte zu entziehen. Die Karte wurde endgültig für ungültig erklärt.
"Surrendered" (zurückgegeben)	Die Fahrtenschreiberkarte wurde mit der Erklärung an die CIA zurückgegeben, dass sie nicht mehr benötigt wird.
"Lost" (verloren)	Die Fahrtenschreiberkarte wurde von der CIA als verloren gemeldet.
"Stolen" (gestohlen)	Die Fahrtenschreiberkarte wurde von der CIA als gestohlen gemeldet. Eine gestohlene Karte gilt als verloren.
"Malfunctioning" (schlecht funktionierend)	Die Fahrtenschreiberkarte wurde von der CIA als schlecht funktionierend gemeldet.
"Expired" (abgelaufen)	Die Gültigkeitsdauer der Fahrtenschreiberkarte ist abgelaufen.
"Replaced" (ersetzt)	Die Fahrtenschreiberkarte, die als verloren, gestohlen oder schlecht funktionierend gemeldet ist, wurde durch eine neue Karte ersetzt. Die Daten der neuen Karte sind mit denen der alten Karte bis auf die Kartennummer identisch, deren Ersatzindex um eine Stelle erhöht ist.

"Renewed" (erneuert)	Die Fahrtenschreiberkarte wurde erneuert, da sich Verwaltungsdaten geändert haben oder die Gültigkeitsdauer abgelaufen war. Die Daten der neuen Karte sind mit denen der alten Karte bis auf die Kartennummer identisch, deren Erneuerungsindex um eine Stelle erhöht ist.
"In Exchange" (im Austausch)	Die CIA, die eine Fahrerkarte ausgestellt hat, hat eine Mitteilung erhalten, dass ein Verfahren eingeleitet wurde, diese Karte gegen eine von der CIA einer anderen Partei ausgestellte Karte auszutauschen.
"Exchanged" (ausgetauscht)	Die CIA, die eine Fahrerkarte ausgestellt hat, hat eine Mitteilung über den Abschluss des Verfahrens erhalten, mit dem diese Karte gegen eine von der CIA einer anderen Partei ausgestellte Karte ausgetauscht wurde.

Unteranlage 4.3

TACHOnet-Benachrichtigungen

1. Allgemeine technische Anforderungen

1.1. Die Zentralstelle verfügt sowohl über synchrone als auch asynchrone Schnittstellen für den Austausch von Benachrichtigungen. Die Parteien können die für ihre eigenen Anwendungen am besten geeignete Technologie einsetzen.

1.2. Alle zwischen der Zentralstelle und den nationalen Systemen ausgetauschten Benachrichtigungen müssen UTF-8 verschlüsselt sein.

1.3. Die nationalen Systeme müssen in der Lage sein, Benachrichtigungen mit griechischen oder kyrillischen Zeichen entgegenzunehmen und zu verarbeiten.

2. XML-Schema der Benachrichtigungen und Schemadefinition (XSD)

2.1. Das allgemeine XML-Schema der Benachrichtigungen folgt dem Format der XSD-Schemadefinition der Zentralstelle.

2.2. Die Zentralstelle und die nationalen Systeme senden und empfangen Benachrichtigungen, die dem XSD-Schema entsprechen.

2.3. Die nationalen Systeme müssen in der Lage sein, alle Benachrichtigungen im Zusammenhang mit einer der in Unteranlage 4.2 genannten Funktionen zu senden, zu empfangen und zu verarbeiten.

2.4. Die XML-Benachrichtigungen müssen den in Tabelle 2 festgelegten Mindestanforderungen genügen.

Tabelle 2

Mindestanforderungen an den Inhalt von XML-Benachrichtigungen

"Common Header" (Gemeinsamer Header)		**Pflichtfelder**
"Version" (Version)	Die offizielle Version der XML-Spezifikationen wird durch den Namensraum spezifiziert, der in der XSD-Benachrichtigung und in dem Attribut *Version* des Header-Elements jeder XML-Benachrichtigung definiert ist. Die Versionsnummer ("n.m") wird in jeder Freigabe der Datei mit der XML-Schemadefinition (xsd) als fester Wert definiert.	Ja
"Test Identifier" (Testkennung)	Fakultative Kennung für Tests. Der Veranlasser des Tests vervollständigt die Kennung, und alle am Workflow Beteiligten müssen dieselbe Kennung weitergeben bzw. zurücksenden. Bei der Erzeugung sollte sie ignoriert und, soweit angegeben, nicht verwendet werden.	Nein
"Technical Identifier" (Technische Kennung)	Eine UUID dient der eindeutigen Identifizierung jeder einzelnen Benachrichtigung. Der Sender generiert eine UUID und vervollständigt dieses Attribut. Diese Daten werden in keiner Betriebssituation verwendet.	Ja
"Workflow Identifier" (Workflowkennung)	Die Workflowkennung ist eine UUID und sollte von dem anfragenden Mitgliedstaat generiert werden. Diese Kennung wird dann in allen Benachrichtigungen benutzt, die mit diesem Workflow zusammenhängen.	Ja
"Sent At"	(Versendet am) Datum und Uhrzeit (UTC) des Versands der Benachrichtigung	Ja
"Timeout"	(Zeit abgelaufen) Dieses Datums- und Zeitattribut (im UTC-Format) ist fakultativ. Der Wert wird nur von der Zentralstelle für weitergeleitete Anfragen festgelegt. Die antwortende Partei kann daran ablesen, wann die Zeit für die Anfrage abgelaufen sein wird. Für MS2TCN_<x>_Req und alle Antwort-Benachrichtigungen wird dieser Wert nicht benötigt. Er ist fakultativ, sodass dieselbe Headerdefinition für alle Arten von Benachrichtigungen verwendet werden kann, unabhängig davon, ob das Attribut für den Timeoutwert benötigt wird.	Nein
Von	Der ISO 3166-1 Alpha 2-Code der Partei, die die Benachrichtigung sendet, oder "EU".	Ja
An	Der ISO 3166-1 Alpha 2-Code der Partei, an die die Benachrichtigung gesendet wird, oder "EU".	Ja

Unteranlage 4.4

Transliterations- und NYSIIS-Dienste (New York State Identification and Intelligence System)

1. Für die Codierung der Namen aller Fahrer in den nationalen Registern ist der NYSIIS-Algorithmus der Zentralstelle zu verwenden.

2. Bei der Suche nach einer Karte mit Hilfe der CIC-Funktion sind die NYSIIS-Schlüssel als primärer Suchmechanismus zu verwenden.

3. Darüber hinaus können die Parteien einen eigenen Algorithmus verwenden, um zusätzliche Ergebnisse zu erhalten.

4. Die Suchergebnisse müssen Angaben dazu enthalten, ob für die Suche nach einem Datensatz der NYSIIS-Suchmechanismus oder ein eigener Suchmechanismus verwendet wurde.

5. Entscheidet sich eine Partei, die ICDL-Mitteilungen aufzuzeichnen, dann sind die in der Mitteilung enthaltenen NYSIIS-Schlüssel als Teil der ICDL-Daten zu speichern. Bei der Suche in den ICDL-Daten verwendet die Partei die NYSIIS-Schlüssel des Namens des Antragstellers.

Unteranlage 4.5

Sicherheitsanforderungen

1. Für den Austausch von Benachrichtigungen zwischen der Zentralstelle und den nationalen Systemen ist das Protokoll HTTPS zu verwenden.

2. Die nationalen Systeme verwenden die digitalen Zertifikate, die in den Unteranlagen 4.8 und 4.9 für die sichere Übertragung der Benachrichtigungen zwischen den nationalen Systemen und der Zentralstelle genannt werden.

3. Die nationalen Systeme haben als Mindestvorgabe Zertifikate zu implementieren, die den SHA-2 (SHA-256)-Signatur-Hash-Algorithmus nutzen und einen öffentlichen Schlüssel mit einer Länge von 2048 Bit haben.

Unteranlage 4.6

Leistungsanforderungen

1. Die nationalen Systeme müssen die folgenden Mindestleistungen erbringen:

1.1. Sie müssen täglich rund um die Uhr zur Verfügung stehen.

1.2. Ihre Verfügbarkeit wird über eine von der Zentralstelle ausgehende Heartbeat-Nachricht überwacht.

1.3. Ihre Verfügbarkeitsquote muss entsprechend folgender Tabelle bei 98 % liegen (die Zahlen sind auf die nächste Einerstelle gerundet):

Eine Verfügbarkeit von	bedeutet eine Nichtverfügbarkeit von		
	täglich	monatlich	jährlich
98 %	0,5 Stunden	15 Stunden	7,5 Tagen

Die Parteien sind aufgefordert, die tägliche Verfügbarkeitsquote einzuhalten, wenngleich eingeräumt wird, dass bestimmte unerlässliche Tätigkeiten, wie beispielsweise eine Systemwartung, eine Abschaltung von über 30 Minuten erfordern. Dennoch sind die monatlichen und jährlichen Verfügbarkeitsquoten nach wie vor verbindlich.

1.4. Sie müssen auf mindestens 98 % der Anfragen reagieren, die bei ihnen in einem Kalendermonat eingehen.

1.5. Sie müssen auf die Anfragen innerhalb von 10 Sekunden reagieren.

1.6. Generell darf bei Anfragen die Dauer bis zum Zeitablauf (die Wartezeit des Anfragenden auf eine Antwort) 20 Sekunden nicht überschreiten.

1.7. Sie müssen in der Lage sein, eine Anfragequote von 6 Benachrichtigungen pro Sekunde zu bearbeiten.

1.8. Nationale Systeme dürfen bei der Übermittlung von Anfragen an die Zentralstelle des TACHOnet eine Anfragequote von 2 Anfragen pro Sekunde nicht überschreiten.

1.9. Jedes nationale System muss in der Lage sein, mit technischen Problemen der Zentralstelle oder der nationalen Systeme anderer Parteien umzugehen. Hierzu zählen unter anderem:

a) Unterbrechung der Verbindung zur Zentralstelle,

b) keine Antwort auf eine Anfrage,

c) Eingang von Antworten nach Zeitablauf,

d) Eingang nicht angeforderter Benachrichtigungen,

e) Eingang ungültiger Benachrichtigungen.

2. Die Zentralstelle muss:

2.1. eine Verfügbarkeitsquote von 98 % gewährleisten;

2.2. den nationalen Systemen Fehlermeldungen übermitteln — entweder über eine Antwort-Benachrichtigung oder über eine spezielle Fehler-Benachrichtigung. Die nationalen Systeme, die diese speziellen Fehler-Benachrichtigungen erhalten, verfügen ihrerseits über einen abgestuften Reaktionsablauf, um die geeigneten Maßnahmen zur Behebung des gemeldeten Fehlers zu ergreifen.

3. Instandhaltung

Die Parteien teilen den anderen Parteien und der Europäischen Kommission, sofern technisch möglich, mindestens eine Woche im Voraus etwaige Routine-Instandhaltungstätigkeiten über die Internet-Anwendung mit.

Unteranlage 4.7

PROTOKOLLIERUNG UND STATISTIK DER IN DER ZENTRALSTELLE ERFASSTEN DATEN

1. Aus Datenschutzgründen müssen die für statistische Zwecke erhobenen Daten anonymisiert sein. Daten, die Rückschlüsse auf bestimmte Karten, Fahrer oder Fahrerlaubnisse zulassen, dürfen nicht zu statistischen Zwecken genutzt werden.

2. Für die Zwecke der Überwachung und Fehlerbehebung müssen die Protokolle alle Transaktionen erfassen und es ermöglichen, Statistiken über diese Transaktionen anzufertigen.

3. In den Protokollen dürfen personenbezogene Daten nicht länger als sechs Monate gespeichert werden. Statistische Informationen sind unbefristet aufzubewahren.

4. Die statistischen Daten für die Berichterstattung umfassen:

   a) die anfragende Partei;

   b) die antwortende Partei;

   c) die Art der Benachrichtigung;

   d) den Status-Code der Antwort;

   e) Datum und Uhrzeit der Benachrichtigungen;

   f) die Antwortzeit.

Unteranlage 4.8

Allgemeine Bestimmungen für digitale Schlüssel und Zertifikate für TACHOnet

1. Der Generaldirektor der Generaldirektion Informatik der Europäischen Kommission (DIGIT) stellt den AETR-Vertragsparteien, die sich mit TACHOnet über eDelivery vernetzen (im Folgenden die "nationalen Behörden") einen PKI-Dienst[1] zur Verfügung (der PKI-Dienst der Fazilität "Connecting Europe" im Folgenden "CEF-PKI-Dienst").

2. Das Verfahren für die Beantragung und Sperrung digitaler Zertifikate sowie die einzelnen Bedingungen für deren Verwendung sind in dieser Anlage erläutert.

3. Verwendung von Zertifikaten:

3.1. Sobald das Zertifikat ausgestellt wurde, darf die nationale Behörde[2] das Zertifikat nur im Zusammenhang mit TACHOnet verwenden. Das Zertifikat kann verwendet werden, um

   a) die Herkunft der Daten zu authentifizieren;

   b) Daten zu verschlüsseln;

   c) sicherzustellen, dass eine Verletzung der Integrität der Daten erkannt wird.

3.2. Jede Verwendung, die im Rahmen der erlaubten Verwendungen des Zertifikats nicht ausdrücklich genehmigt wird, ist untersagt.

4. Die Vertragsparteien

   a) schützen ihren privaten Schlüssel vor unbefugter Nutzung;

   b) geben ihren privaten Schlüssel auch nicht als Vertreter an Dritte weiter oder legen diesen privaten Schlüssel gegenüber Dritten offen;

---

1 Eine PKI (Public Key Infrastruktur) besteht aus Rollen, Richtlinien, Verfahren und Systemen für die Schaffung, Verwaltung und Sperrung digitaler Zertifikate.

2 Identifiziert durch den Attributwert "O=" "Subject" ist der "Distinguished Name" des ausgestellten Zertifikats.

c) gewährleisten die Vertraulichkeit, Integrität und Verfügbarkeit der privaten Schlüssel, die für TACHOnet generiert, gespeichert und verwendet werden;

d) verwenden den privaten Schlüssel nach Ablauf der Gültigkeit oder nach einer Sperrung des Zertifikats nicht weiter, ausgenommen ist die Sichtbarmachung verschlüsselter Daten (z. B. das Lesen verschlüsselter E-Mails). Abgelaufene Schlüssel müssen entweder vernichtet oder so aufbewahrt werden, dass sie nicht mehr verwendet werden können;

e) identifizieren gegenüber der Registrierungsbehörde die autorisierten Vertreter, die befugt sind, die Sperrung von Zertifikaten zu beantragen, die von der Organisation ausgestellt wurden (Anträge auf Sperrung müssen ein Sperrbeantragungspasswort sowie Angaben zu den Vorkommnissen enthalten, die zu der Sperrung geführt haben);

f) verhindern die missbräuchliche Nutzung des privaten Schlüssels, indem sie die Sperrung des entsprechenden Public-Key-Zertifikats beantragen, sofern der private Schlüssel oder die Aktivierungsdaten des privaten Schlüssels gefährdet wurden;

g) sind dafür verantwortlich und verpflichtet, die Sperrung eines Zertifikats zu beantragen, wenn die in dem Dokument "Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS)" der Zertifizierungsbehörde genannten Umstände vorliegen;

h) melden der Registrierungsbehörde unverzüglich jeden Verlust, Diebstahl oder jede potenzielle Gefährdung von AETR-Schlüsseln, die im Zusammenhang mit TACHOnet verwendet werden.

5. Haftung

Unbeschadet der Haftung der Kommission bei einem Verstoß gegen einschlägige einzelstaatliche Rechtsvorschriften oder in Fällen, in denen ein Ausschluss nach diesen Rechtsvorschriften nicht möglich ist, übernimmt die Europäische Kommission keine Verantwortung oder Haftung für

a) den Inhalt des Zertifikats, die ausschließlich beim Inhaber des Zertifikats liegt. Es liegt in der Verantwortung des Zertifikatinhabers, die Richtigkeit des Zertifikatinhalts zu prüfen;

b) die Verwendung des Zertifikats durch seinen Inhaber.

Unteranlage 4.9

Beschreibung des PKI-Dienstes für TACHOnet

1. Einführung

Eine PKI (Public Key Infrastruktur) besteht aus Rollen, Richtlinien, Verfahren und Systemen für die Schaffung, Verwaltung und Sperrung digitaler Zertifikate[3]. Der CEF-PKI-Dienst "eDelivery" ermöglicht die Ausstellung und Verwaltung digitaler Zertifikate, die zur Gewährleistung der Vertraulichkeit, Integrität und Nichtabstreitbarkeit des Informationsaustauschs zwischen den Zugangspunkten (AP) verwendet werden.

Der PKI-Dienst "eDelivery" stützt sich auf den Dienst "TeleSec Shared Business CA", für den das Dokument "Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS)" des Trust-Center-Dienstes "TeleSec Shared-Business-CA" der T-Systems International GmbH[4] gilt.

Mit dem PKI-Dienst werden Zertifikate ausgestellt, die für die Absicherung verschiedener Geschäftsabläufe innerhalb und außerhalb von Unternehmen, Organisationen, öffentlichen Behörden und Institutionen geeignet sind und die ein mittleres Sicherheitsniveau benötigen, mit dem sich die Authentizität, Integrität und Vertrauenswürdigkeit der Endteilnehmer nachweisen lässt.

2. Verfahren zur Beantragung eines Zertifikats

2.1. Rollen und Zuständigkeiten

2.1.1. "Organisation" oder "nationale Behörde", die das Zertifikat beantragt

2.1.1.1. Die nationale Behörde beantragt Zertifikate im Zusammenhang mit dem TACHOnet-Projekt.

2.1.1.2. Die nationale Behörde

a) beantragt die Zertifikate beim CEF-PKI-Dienst;

---

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

4 Die aktuellen Versionen der CP und CPS können heruntergeladen werden unter: https://www.telesec.de/en/sbca-en/support/download-area/.

b) generiert private Schlüssel und die entsprechenden öffentlichen Schlüssel, die in die von der Zertifizierungsbehörde ausgestellten Zertifikate eingetragen werden;

c) lädt das Zertifikat nach Genehmigung herunter;

d) unterzeichnet und sendet an die Registrierungsbehörde zurück:

i) das Identifizierungsformular der Kontaktpersonen und des vertrauenswürdigen Kuriers,

ii) die unterzeichnete Einzelvollmacht[5].

2.1.2. Vertrauenswürdiger Kurier

2.1.2.1. Die nationale Behörde benennt einen vertrauenswürdigen Kurier.

2.1.2.2. Dieser

a) übergibt den öffentlichen Schlüssel der Registrierungsbehörde während des Verfahrens der persönlichen Identifizierung und Registrierung;

b) nimmt das entsprechende Zertifikat von der Registrierungsbehörde entgegen.

2.1.3. Domain-Inhaber

2.1.3.1. Domain-Inhaber ist die GD MOVE.

2.1.3.2. Der Domain-Inhaber

a) validiert und koordiniert das TACHOnet-Netz und die TACHOnet-Vertrauensarchitektur, einschließlich der Validierung der Verfahren für die Ausstellung von Zertifikaten;

b) betreibt die TACHOnet-Zentralstelle und koordiniert die Tätigkeiten der Parteien hinsichtlich der Funktionsweise des TACHOnet;

c) führt zusammen mit nationalen Behörden Tests zur Vernetzung mit TACHOnet durch.

[5] Eine Vollmacht ist ein Rechtsdokument, mit dem die Organisation die Person ermächtigt und autorisiert, die Generierung eines Zertifikats im Namen von T-Systems International GmbH für den Dienst TeleSec Shared Business CA zu beantragen, die von der Europäischen Kommission als für den CEF PKI-Dienst zuständige Person offiziell benannt wurde. Siehe auch Nummer 6.

2.1.4. Registrierungsbehörde

2.1.4.1. Registrierungsbehörde ist die Gemeinsame Forschungsstelle (JRC).

2.1.4.2. Die Registrierungsbehörde ist für die Überprüfung der Identität des vertrauenswürdigen Kuriers sowie für die Registrierung und Genehmigung der Anträge auf Ausstellung, Sperrung und Erneuerung digitaler Zertifikate zuständig.

2.1.4.3. Die Registrierungsbehörde muss

a) der nationalen Behörde die eindeutige Kennung zuweisen;

b) die Identität der nationalen Behörde, ihrer Ansprechpartner und vertrauenswürdigen Kuriere authentifizieren;

c) mit dem CEF-Support hinsichtlich der Authentizität der nationalen Behörde, ihrer Ansprechpartner und vertrauenswürdigen Kuriere kommunizieren;

d) die nationale Behörde über die Genehmigung oder Ablehnung eines Zertifikats unterrichten.

2.1.5. Zertifizierungsbehörde (Certification Authority)

2.1.5.1. Die Zertifizierungsbehörde ist für die Bereitstellung der technischen Infrastruktur für die Beantragung, Ausstellung und Sperrung digitaler Zertifikate zuständig.

2.1.5.2. Die Zertifizierungsbehörde muss

a) die technische Infrastruktur für die Beantragung von Zertifikaten durch nationale Behörden bereitstellen;

b) Zertifikatanträge validieren oder ablehnen;

c) mit der Registrierungsbehörde kommunizieren, um bei Bedarf die Identität einer anfragenden Organisation zu überprüfen.

2.2. Ausstellung von Zertifikaten

2.2.1. Zertifikate werden in der Reihenfolge der in Abbildung 1 dargestellten Schritte ausgestellt:

a) **Schritt 1:** Identifizierung des vertrauenswürdigen Kuriers;

b) **Schritt 2:** Beantragung eines Zertifikats;

c) **Schritt 3**: Registrierung bei der Registrierungsbehörde;

d) **Schritt 4:** Generierung des Zertifikats;

e) **Schritt 5:** Veröffentlichung des Zertifikats;

f) **Schritt 6:** Zertifikat wird akzeptiert.

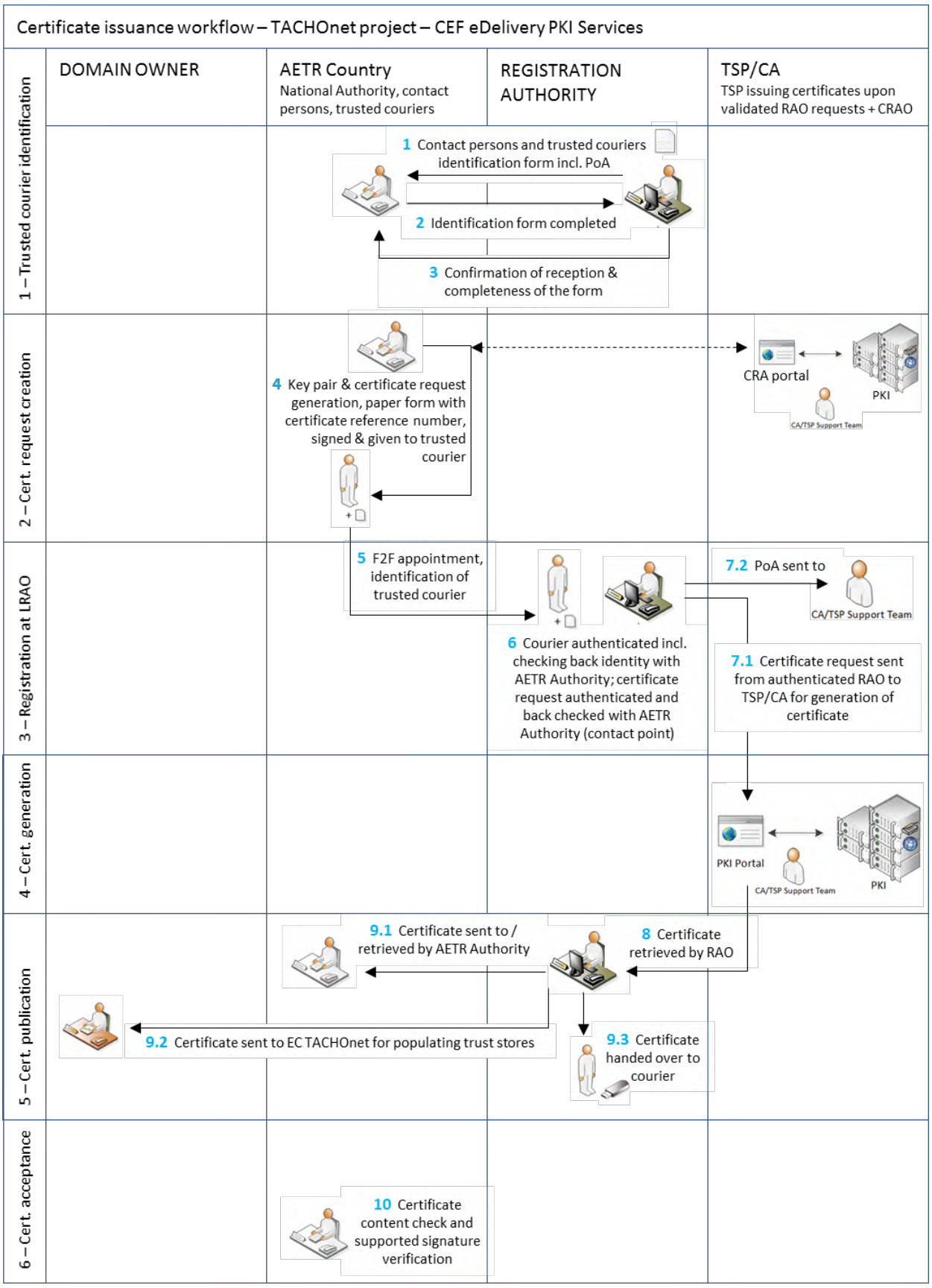


Abbildung1 - Ablaufschema der Zertifikatausstellung

2.2.2. Schritt 1: Identifizierung des vertrauenswürdigen Kuriers

Zur Identifizierung des vertrauenswürdigen Kuriers ist wie folgt zu verfahren:

a) Die Registrierungsbehörde sendet der nationalen Behörde das Identifizierungsformular zu den Ansprechpartnern und zum vertrauenswürdigen Kurier[6]. Dieses Formular enthält auch eine Vollmacht, die die Organisation (AETR-Behörde) unterzeichnet.

b) Die nationale Behörde sendet der Registrierungsbehörde das ausgefüllte Formular und die unterzeichnete Vollmacht zurück.

c) Die Registrierungsbehörde bestätigt den Empfang und die Vollständigkeit des Formulars.

d) Die Registrierungsbehörde stellt dem Domain-Inhaber eine aktuelle Liste der Ansprechpartner und vertrauenswürdigen Kuriere zur Verfügung.

2.2.3. Schritt 2: Beantragung eines Zertifikats

2.2.3.1. Die Beantragung und Entgegennahme des Zertifikats erfolgt auf demselben Computer und mit demselben Browser.

2.2.3.2. Für die Beantragung eines Zertifikats ist wie folgt zu verfahren:

a) Die Organisation beantragt das Zertifikat über die URL https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en und gibt als Login "**sbca/CEF_eDelivery.europa.eu**" und als Passwort "**digit.333**" ein.

6 Vgl. Nummer 5.

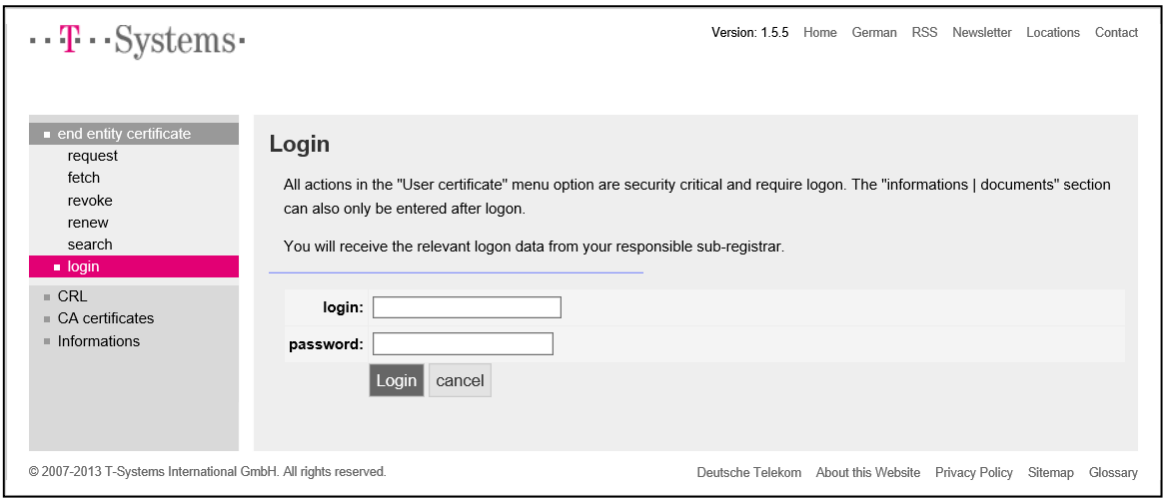


Abbildung 2

b) Die Organisation klickt auf der linken Seite "request" an und wählt dann "CEF_TACHOnet" in der Dropdown-Liste aus.

Abbildung 3

c) Die Organisation füllt das Formular zur Beantragung des Zertifikats (Abbildung 4) mit den Angaben von Tabelle 3 aus und klickt dann auf "Next (soft-PSE)", um den Prozess abzuschließen.

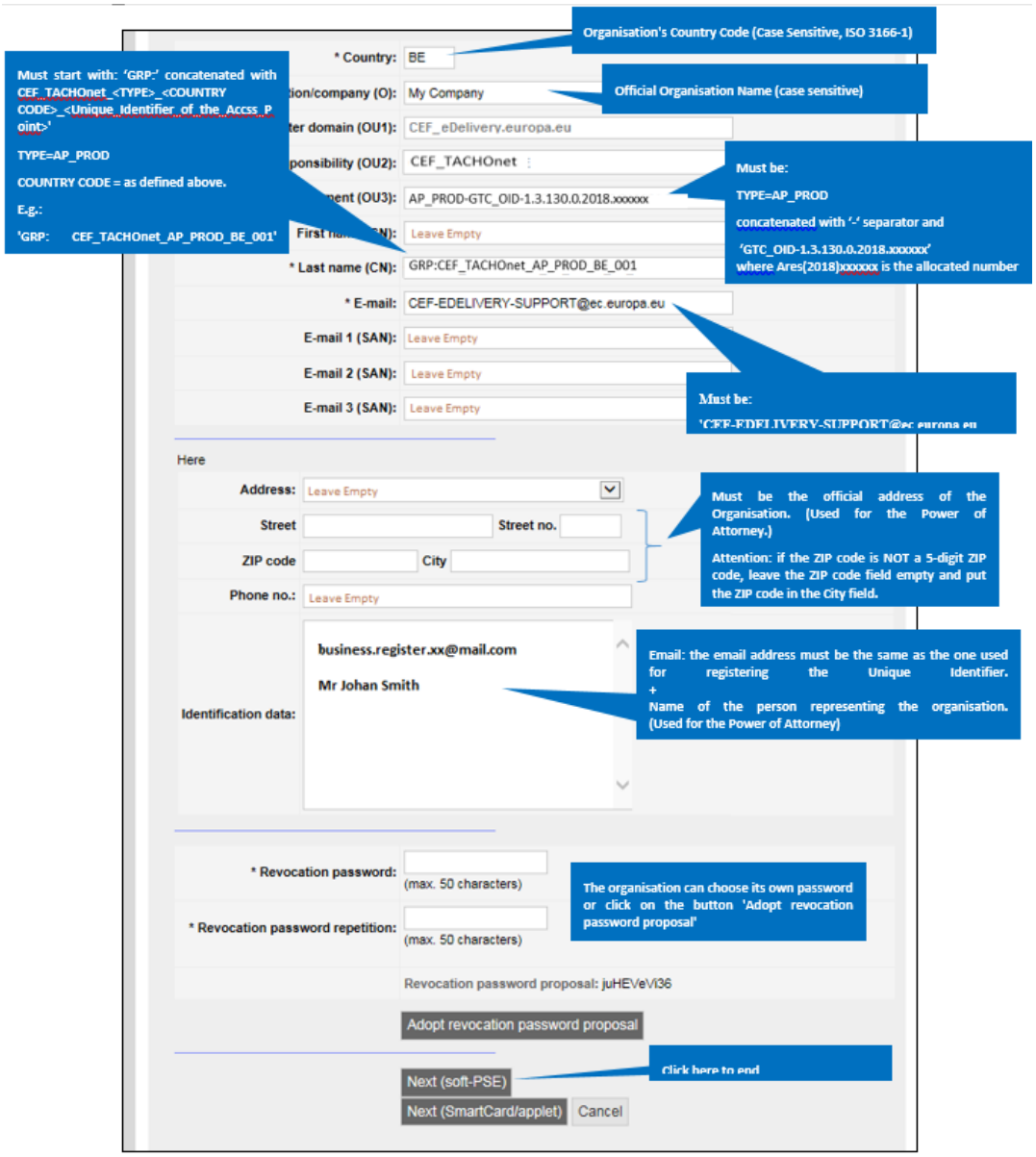

Organisation's Country Code (Case Sensitive, ISO 3166-1)
Official Organisation Name (case sensitive)
Must start with: 'GRP:' concatenated with CEF_TACHOnet_<TYPE>_<COUNTRY CODE>_<Unique_Identifier_of_the_Accss_Point>'
TYPE=AP_PROD
COUNTRY CODE = as defined above.
E.g.:
'GRP: CEF_TACHOnet_AP_PROD_BE_001'
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
E-mail 1 (SAN):
E-mail 2 (SAN):
E-mail 3 (SAN):
Here
Address:
Street
Street no.
ZIP code
City
Phone no.:
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

Abbildung 4

Auszufüllende Felder	Beschreibung
Land	**C=Country Code,** Sitz des Inhabers des Zertifikats, überprüft anhand eines öffentlichen Verzeichnisses; Beschränkungen: 2 Zeichen nach ISO 3166-1, Alpha-2, Groß- und Kleinschreibung Beispiele: DE, BE, NL, Besondere Fälle: UK (für Großbritannien), EL (für Griechenland)
Organisation/Unternehmen (O)	**O= Name der Organisation des Zertifikatinhabers**
Master Domain (OU1)	**OU=CEF_eDelivery.europa.eu**
"Area of responsibility" (OU2) (Zuständigkeitsbereich)	**OU=CEF_TACHOnet**
"Department" (OU3) (Abteilung)	Obligatorischer Wert je "AREA OF RESPONSIBILITY" Der Inhalt ist mit Hilfe einer Positivliste (weißen Liste) bei Antragstellung zu prüfen. Stimmen die Angaben mit der Liste nicht überein, wird die Beantragung verhindert. Format: **OU=<TYPE>-<GTC_NUMBER>** Dabei wird "<TYPE>" durch AP_PROD ersetzt: Zugangspunkt in Produktionsumgebung. und <GTC_NUMBER> ist **GTC_OID-1.3.130.0.2018**.xxxxxx, dabei ist Ares(2018)xxxxxx die GTC-Nummer für das TACHOnet-Projekt. z. B.: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
"First name (CN)" (Vorname)	Nicht ausfüllen
"Last name (CN)" (Nachname)	Muss mit "GRP" anfangen, gefolgt von einer Trivialbezeichnung Format: **CN=GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** z. B.: GRP:CEF_TACHOnet_AP_PROD_BE_001
"E-Mail" (E-Mail)	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
"E-mail 1 (SAN)"	Nicht ausfüllen
"E-mail 2 (SAN)"	Nicht ausfüllen
"E-mail 3 (SAN)"	Nicht ausfüllen

"Address" (Anschrift)	Nicht ausfüllen
"Street" (Straße)	Offizielle Anschrift der Organisation des Zertifikatinhabers. (Verwendet für die Vollmacht)
"Street no." (Hausnr.)	Offizielle Anschrift der Organisation des Zertifikatinhabers. (Verwendet für die Vollmacht)
"Zip Code" (PLZ)	Offizielle Anschrift der Organisation des Zertifikatinhabers. (Verwendet für die Vollmacht) **Achtung**: Ist die Postleitzahl nicht fünfstellig, das PLZ-Feld frei lassen und die PLZ in das "City"-Feld eintragen.
"City" (Ort)	Offizielle Anschrift der Organisation des Zertifikatinhabers. (Verwendet für die Vollmacht) **Achtung**: Ist die Postleitzahl nicht fünfstellig, das PLZ-Feld frei lassen und die PLZ in das "City"-Feld eintragen.
"Phone no." (Tel.-Nr.)	Nicht ausfüllen
"Identification data" (Identifizierungsdaten)	Die E-Mail-Adresse muss dieselbe sein wie für die Registrierung der eindeutigen Kennung. + Name der Person, die die Organisation vertritt. (Verwendet für die Vollmacht) + **Handelsregister Nr.** (nur obligatorisch für private Organisationen) **Eingetragen beim Amtsgericht von** (nur obligatorisch für deutsche und österreichische Organisationen)
"Revocation password" (Sperrpasswort)	vom Antragsteller gewähltes obligatorisches Feld
"Revocation password repetition" (Wiederholung des Sperrpassworts)	vom Antragsteller gewähltes obligatorisches Feld (Wiederholung)

Tabelle 3: Die Angaben sind für jedes Feld zu vervollständigen.

d) Für die ausgewählten Schlüssel gilt eine Länge von 2048 (High Grade)

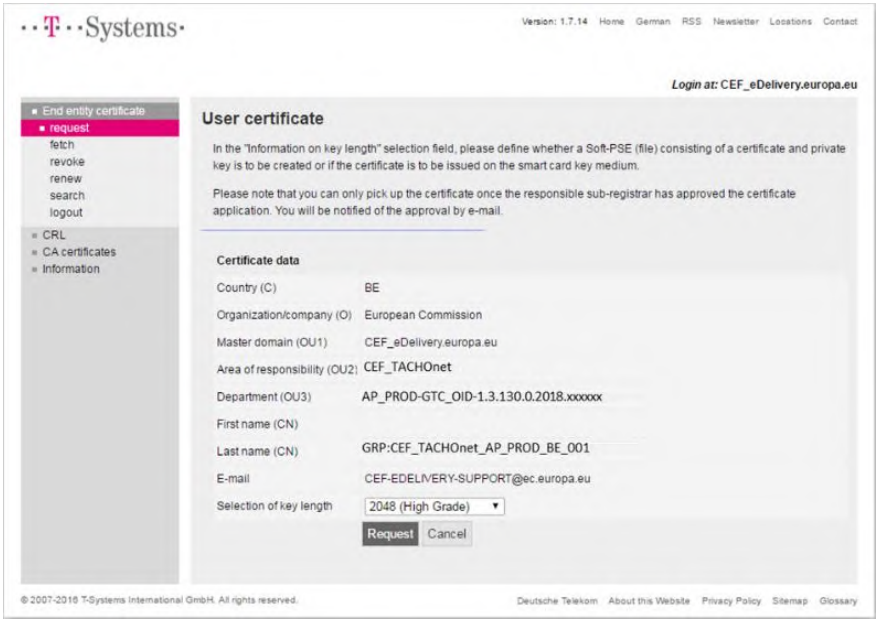


Abbildung 5

e) Die Organisation notiert die Referenznummer für den Abruf des Zertifikats.

Abbildung 6

f) Das CEF-Support-Team prüft den Eingang neuer Zertifikatsanträge und überprüft, ob die Angaben des Antrags gültig sind, d. h., ob sie mit der in Anlage 5.1 angegeben Bezeichnungsregelung übereinstimmen.

g) Das CEF-Support-Team überprüft, ob das Format der im Antrag gemachten Angaben gültig ist.

h) Verläuft eine der in den Nummern 5 oder 6 durchgeführten Überprüfungen negativ, sendet das CEF-Support-Team an die unter "Identification data" des Antragsformulars angegebene E-Mail-Adresse eine E-Mail mit Kopie an den Domain-Inhaber, in der sie die Organisation auffordert, den Vorgang neu zu starten. Der erfolglose Zertifikatantrag ist zu stornieren.

i) Das CEF-Support-Team sendet an die Registrierungsbehörde eine E-Mail zur Gültigkeit des Antrags. Die E-Mail enthält

   (1) den Namen der Organisation, wie im Feld "Organisation (O)" des Zertifikatantrags angegeben;

   (2) die Zertifikatsdaten, einschließlich des im Feld "Last Name (CN)" des Zertifikatantrags angegebenen Namens des AP, für den das Zertifikat ausgestellt wird;

   (3) Referenznummer des Zertifikats;

   (4) die Anschrift der Organisation, ihre E-Mail-Adresse und den Namen ihres Vertreters.

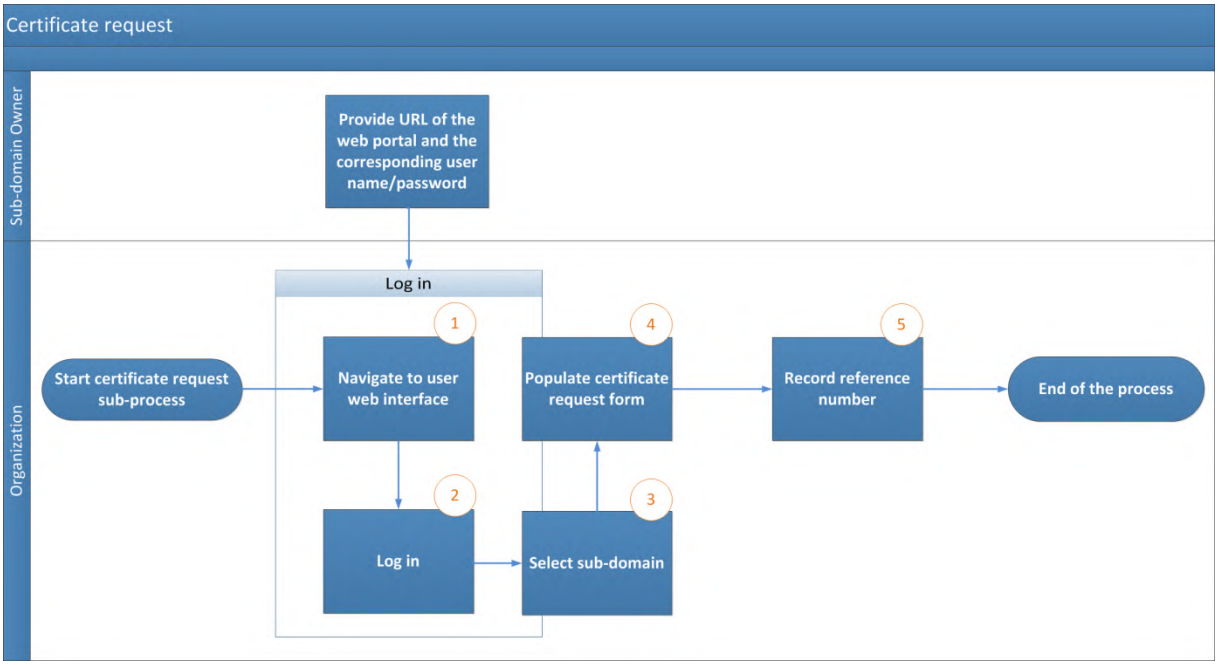


Abbildung 7 – Ablauf des Zertifikatantrags

2.2.4. Schritt 3: Registrierung bei der Registrierungsbehörde (Genehmigung des Zertifikats)

2.2.4.1. Der vertrauenswürdige Kurier oder Ansprechpartner vereinbart per E-Mail einen Termin bei der Registrierungsbehörde unter Angaben zur Person des vertrauenswürdigen Kuriers, der persönlich diesen Termin wahrnimmt.

2.2.4.2. Die Organisation stellt folgende Dokumente zusammen:

a) die ausgefüllte und unterzeichnete Vollmacht;

b) eine Kopie des gültigen Reisepasses des vertrauenswürdigen Kuriers, der persönlich den Termin wahrnimmt. Diese Kopie ist von einem der in Schritt 1 genannten Ansprechpartner der Organisation zu unterzeichnen;

c) den von einem Ansprechpartner der Organisation unterzeichneten Papierausdruck des Zertifikatantrags.

2.2.4.3. Die Registrierungsbehörde empfängt den vertrauenswürdigen Kurier, nachdem dessen Identität am Empfang des Gebäudes kontrolliert wurde. Die Registrierungsbehörde führt in persönlicher Anwesenheit des vertrauenswürdigen Kuriers eine Registrierung des Zertifikatantrags durch mittels

a) Identifizierung und Authentifizierung des vertrauenswürdigen Kuriers;

b) Überprüfung der physischen Erscheinung des vertrauenswürdigen Kuriers anhand des von diesem vorgelegten Reisepasses;

c) Überprüfung der Gültigkeit des vom vertrauenswürdigen Kurier vorgelegten Reisepasses;

d) Überprüfung des vom vertrauenswürdigen Kurier vorgelegten Reisepasses anhand der Kopie des gültigen Reisepasses des vertrauenswürdigen Kuriers, die von einem der Ansprechpartner der Organisation unterzeichnet wurde. Die Echtheit der Unterschrift wird anhand des Identifizierungsformulars zu den Ansprechpartnern und zum vertrauenswürdigen Kurier überprüft;

e) Überprüfung der ausgefüllten und unterzeichneten Vollmacht;

f) Überprüfung des Papierausdrucks des Zertifikatsantrags und der Unterschrift anhand des Originals des Identifizierungsformulars zu den Ansprechpartnern und zum vertrauenswürdigen Kurier;

g) Anruf beim unterzeichnenden Ansprechpartner zur Gegenprüfung der Identität des vertrauenswürdigen Kuriers und des Inhalts des Zertifikatantrags.

2.2.4.4. Die Registrierungsbehörde bestätigt dem CEF-Support-Team, dass die nationale Behörde tatsächlich befugt ist, die Komponenten zu bedienen, für die die Zertifikate beantragt werden und dass der entsprechende Registrierungsvorgang in persönlicher Anwesenheit des vertrauenswürdigen Kuriers erfolgreich verlief. Die Bestätigung ist mit einer mit Hilfe des "CommiSign"-Zertifikats gesicherten E-Mail zu versenden, der eine eingescannte Kopie der persönlich authentifizierten Dokumente sowie der unterzeichneten Ablauf-Checkliste, die von der Registrierungsbehörde abgearbeitet wurde, beigefügt ist.

2.2.4.5. Bestätigt die Registrierungsbehörde die Gültigkeit des Antrags, wird der Vorgang wie in den Nummern 2.2.4.6 und 2.2.4.7 beschrieben fortgesetzt. Ansonsten wird die Ausstellung des Zertifikats abgelehnt und die Organisation hierüber in Kenntnis gesetzt.

2.2.4.6. Das CEF-Support-Team genehmigt den Zertifikatantrag und unterrichtet die Registrierungsbehörde über die Genehmigung des Zertifikats.

2.2.4.7. Die Registrierungsbehörde teilt der Organisation mit, dass das Zertifikat über das Nutzerportal abgerufen werden kann.

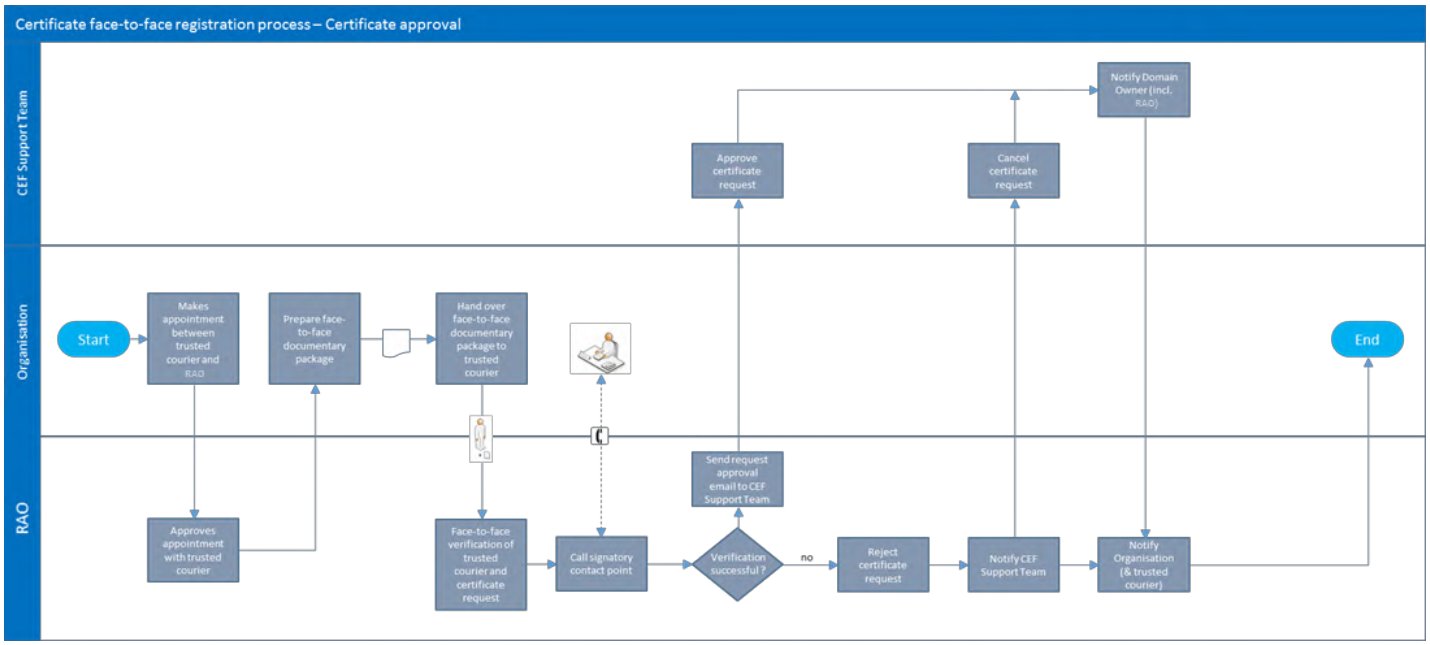


Abbildung 8 – Zertifikatgenehmigung

2.2.5. Schritt 4: Generierung eines Zertifikats

Nach Genehmigung des Zertifikatantrags wird das Zertifikat generiert.

2.2.6. Schritt 5: Veröffentlichung und Abruf von Zertifikaten

2.2.6.1. Nach Genehmigung des Zertifikatantrags ruft die Registrierungsbehörde das Zertifikat ab und übergibt dem vertrauenswürdigen Kurier eine Ausfertigung.

2.2.6.2. Die Organisation erhält von der Registrierungsbehörde eine Mitteilung, dass das Zertifikat abgerufen wurde.

2.2.6.3. Die Organisation ruft im Internet das Nutzerportal auf unter https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en und gibt das Login "**sbca/CEF_eDelivery.europa.eu**" sowie das Passwort "**digit.333**" ein.

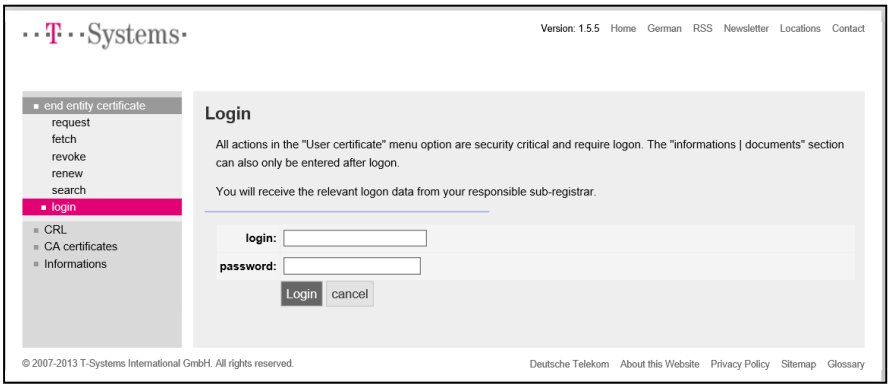


Abbildung 9

2.2.6.4. Die Organisation klickt in der Liste auf der linken Seite auf "fetch" (abholen) und gibt die während des Vorgangs der Zertifikatbeantragung notierte Referenznummer ein.

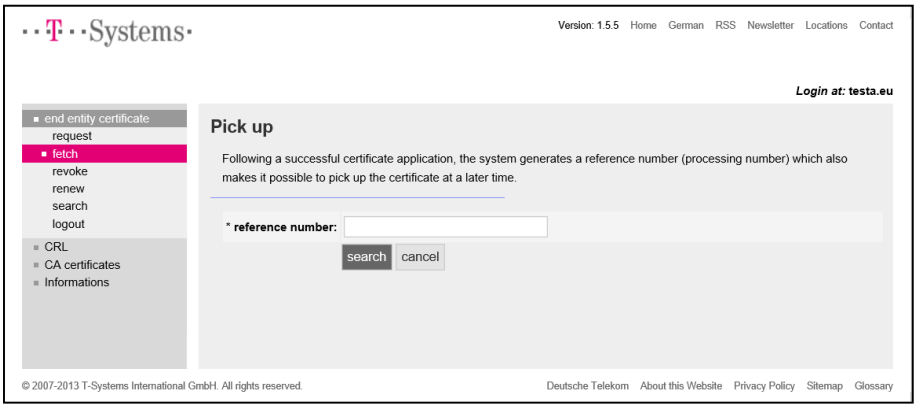


Abbildung 10

2.2.6.5. Die Organisation installiert die Zertifikate, indem sie auf die Schaltfläche "Install" (installieren) klickt.

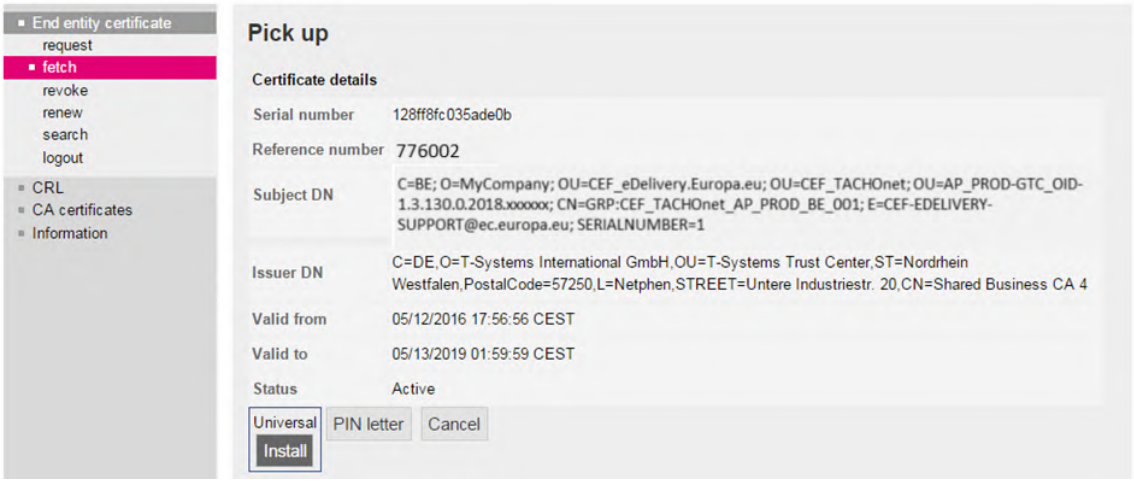


Abbildung 11

2.2.6.6. Das Zertifikat wird am Zugangspunkt installiert. Da dieser Vorgang implementierungsabhängig ist, muss sich die Organisation an den Anbieter ihres Zugangspunkts wenden, um sich diesen Vorgang erläutern zu lassen.

2.2.6.7. Folgende Schritte sind für die Installation am Zugangspunkt notwendig:

a) Export des privaten Schlüssels und des Zertifikats,

b) Erstellen des Schlüsselspeichers und des Vertrauensspeichers,

c) Installation des Schlüsselspeichers und des Vertrauensspeichers am Zugangspunkt.

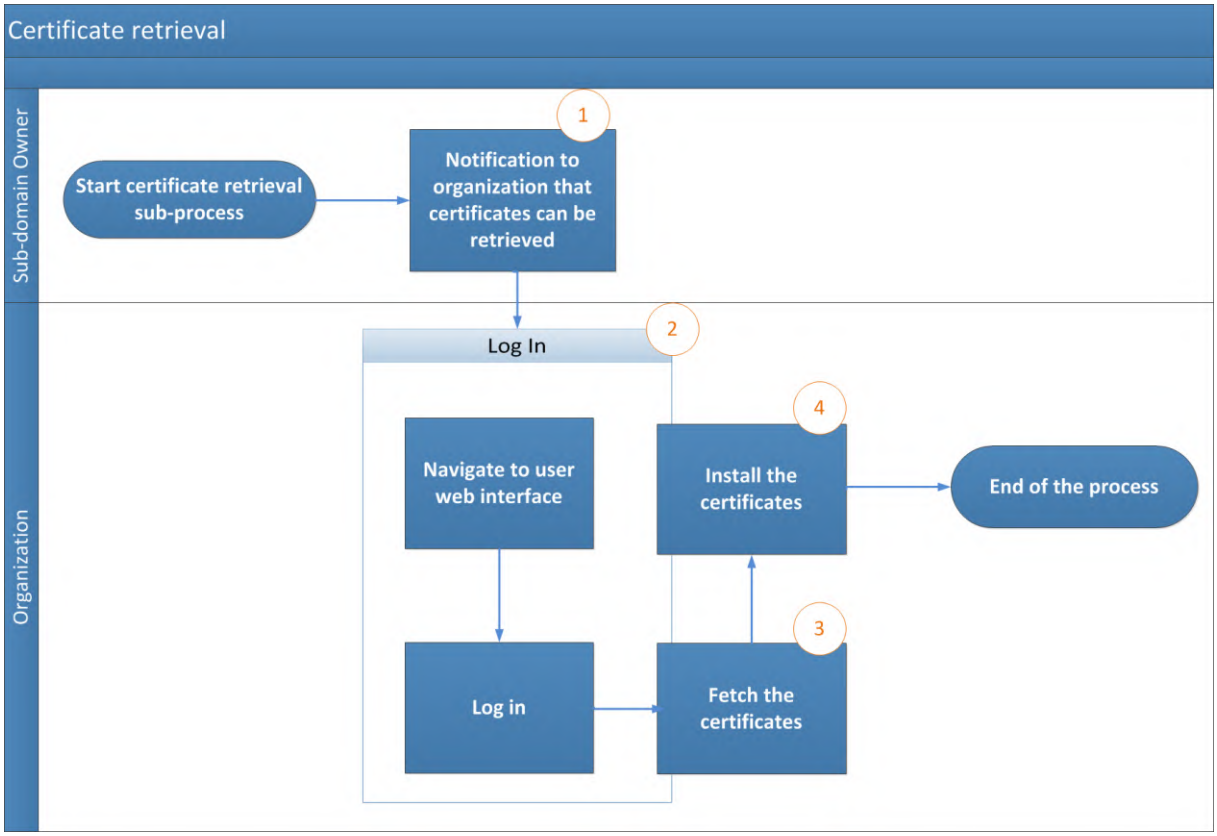


Abbildung 12 – Abruf von Zertifikaten

3. Verfahren zur Sperrung eines Zertifikats

3.1. Die Organisation reicht einen Sperrantrag über das Online-Nutzerportal ein.

3.2. Das CEF-Support-Team nimmt die Sperrung des Zertifikats vor.

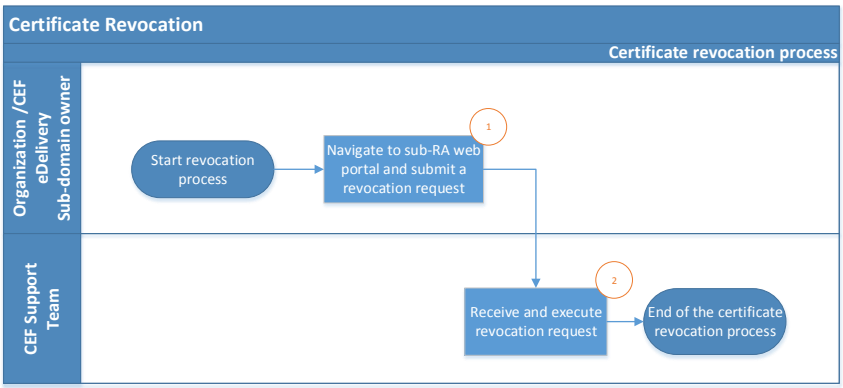


Abbildung 13 – Sperrung von Zertifikaten

4. Allgemeine Geschäftsbedingungen des CEF-PKI-Dienstes

4.1. Hintergrund

In ihrer Eigenschaft als Anbieter von Lösungen für den eDelivery-Baustein der Fazilität "Connecting Europe" wird die GD DIGIT den AETR-Vertragsparteien einen PKI-Dienst[7] ("CEF-PKI-Dienst") zur Verfügung stellen. Der CEF-PKI-Dienst wird von den nationalen Behörden (den "Endteilnehmern") genutzt, die sich an TACHOnet beteiligen.

Innerhalb der "TeleSec-Shared-Business-CA, (SBCA)"-Dienstleistung, die im Trust Center der Gruppen-Unit T-Systems International GmbH ("T-Systems"[8]) betrieben wird, ist die GD DIGIT ein PKI-Mandant. Die GD DIGIT hat die Rolle eines Master-Registrators der Domaine "CEF_eDelivery.europa.eu" der SBCA. In dieser Rolle kreiert die GD DIGIT innerhalb der "CEF_eDelivery.europa.eu"-Domäne für jedes Projekt, dass den CEF-PKI-Dienst nutzt, eine Sub-Domäne (einen Zuständigkeitsbereich).

Dieses Dokument enthält Angaben zu den Geschäftsbedingungen für die TACHOnet-Sub-Domäne. Die GD DIGIT hat die Rolle eines Sub-Registrators dieser Sub-Domäne. In dieser Eigenschaft stellt sie Zertifikate für dieses Projekt aus, sperrt und erneuert diese.

4.2. Haftungsausschluss

Die Europäische Kommission übernimmt keine Verantwortung oder Haftung für den Inhalt des Zertifikats, die ausschließlich beim Inhaber des Zertifikats liegen. Es liegt in der Verantwortung des Zertifikatinhabers, die Richtigkeit des Zertifikatinhalts zu prüfen.

Die Europäische Kommission übernimmt keine Verantwortung oder Haftung für die Verwendung des Zertifikats durch seinen Inhaber, bei dem es sich um eine dritte Rechtsperson außerhalb der Europäischen Kommission handelt.

---

7 Eine PKI (Public Key Infrastruktur) besteht aus Rollen, Richtlinien, Verfahren und Systemen für die Schaffung, Verwaltung undSperrung digitaler Zertifikate.

8 Der im T-Systems Trust Center lokalisierte Trust-Center-Operator nimmt in seiner vertrauenswürdigen Rolle auch die Aufgabe der internen Registrierungsbehörde wahr.

Mit der vorliegenden Haftungsausschlussklausel wird weder bezweckt, die Haftung der Europäischen Kommission entgegen den einschlägigen nationalen Rechtsvorschriften einzuschränken noch sie in Fällen auszuschließen, in denen ein Ausschluss nach diesen Rechtsvorschriften nicht möglich ist.

4.3. Genehmigte Verwendung/unzulässige Verwendung von Zertifikaten

4.3.1. Zulässige Verwendung von Zertifikaten

Sobald das Zertifikat ausgestellt ist, darf der Zertifikatinhaber[9] das Zertifikat nur im Zusammenhang mit TACHOnet verwenden. In diesem Zusammenhang kann das Zertifikat verwendet werden, um

- die Herkunft der Daten zu authentifizieren;
- Daten zu verschlüsseln;
- sicherzustellen, dass eine Verletzung der Integrität der Daten erkannt wird.

4.3.2. Unzulässige Verwendung von Zertifikaten

Jede Verwendung, die im Rahmen der erlaubten Verwendungen des Zertifikats nicht ausdrücklich genehmigt wird, ist untersagt.

4.4. Zusätzliche Pflichten des Zertifikatinhabers

Die Einzelheiten der Geschäftsbedingungen der SBCA werden von T-Systems in dem Dokument "Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS)" des SBCA-Dienstes festgelegt[10]. Dieses Dokument enthält Sicherheitsspezifikationen und Leitlinien zu den technischen und organisatorischen Aspekten sowie Erläuterungen zu den Tätigkeiten des Trust-Center-Betreibers in den Rollen der Zertifizierungsbehörde (CA) und der Registrierungsbehörde (RA) sowie von delegierten Dritten der Registrierungsbehörde (RA).

Nur zur Teilnahme an TACHOnet befugte Rechtspersonen können ein Zertifikat beantragen.

---

9 Identifiziert durch den Attributwert "O=" "Subject" ist der "Distinguished Name" des ausgestellten Zertifikats.

10 Die aktuellen Versionen der T-Systems SBCA CP/CPS können heruntergeladen werden unter: https://www.telesec.de/en/sbca-en/support/download-area/.

Hinsichtlich der Akzeptanz von Zertifikaten gilt Absatz 4.4.1 des SBCA-Dokuments "Zertifizierungsrichtlinie (Certificate Policy, CP) und Erklärung zum Zertifizierungsbetrieb (Certification Practice Statement, CPS)". Zudem gelten die im vorliegenden Dokument erläuterten Nutzungsbedingungen und Bestimmungen bei der erstmaligen Verwendung als von der Organisation akzeptiert, für die das Zertifikat ausgestellt wird ("O=").

Hinsichtlich der Veröffentlichung von Zertifikatinformationen gilt Absatz 2.2 des SBCA CP/CPS.

Alle Zertifikatinhaber müssen den folgenden Anforderungen genügen:

(1) schützen ihren privaten Schlüssel vor unbefugter Nutzung;

(2) sie geben ihren privaten Schlüssel auch nicht als Vertreter an Dritte weiter oder legen diesen privaten Schlüssel gegenüber Dritten offen;

(3) verwenden den privaten Schlüssel nach Ablauf der Gültigkeit oder nach einer Sperrung des Zertifikats nicht weiter, ausgenommen ist die Sichtbarmachung verschlüsselter Daten (z. B. das Lesen verschlüsselter E-Mails).

(4) Der Zertifikatinhaber ist dafür verantwortlich, den Schlüssel an die Endteilnehmer oder Teilnehmer weiterzuleiten.

(5) Der Zertifikatinhaber muss den Endteilnehmer/alle Endteilnehmer verpflichten, den vorliegenden Geschäftsbedingungen, auch den SBCA CP/CPS beim Umgang mit dem privaten Schlüssel zuzustimmen.

(6) Der Zertifikatinhaber muss die Angaben zur Person der autorisierten Vertreter zur Verfügung stellen, die befugt sind, die Sperrung von Zertifikaten zu beantragen, die von der Organisation ausgestellt wurden, wobei sie Angaben zu den Gründen machen müssen, die zur Sperrung und zum Sperrpasswort geführt haben.

(7) Der Zertifikatinhaber muss den Missbrauch privater Schlüssel durch die Sperrung von Zertifikaten verhindern, wenn diese Zertifikate für Gruppen von natürlichen Personen und Funktionen und/oder juristischen Personen ausgestellt wurden und eine Person die Gruppe der Endteilnehmer verlässt (z. B. infolge einer Beendigung des Beschäftigungsverhältnisses).

(8) Der Zertifikatinhaber ist für die Sperrung des Zertifikats verantwortlich und muss dessen Sperrung beantragen, wenn die in Absatz 4.9.1 des SBCA CP/CPS genannten Umstände eintreten.

Hinsichtlich der Erneuerung des Zertifikats oder neuer Schlüssel für das Zertifikat gilt Absatz 4.6 oder 4.7 des SBCA CP/CPS.

Bei einer Änderung des Zertifikats gilt Absatz 4.8 des SBCA CP/CPS.

Bei einer Sperrung des Zertifikats gilt Absatz 4.9 des SBCA CP/CPS.

5. Identifizierungsformular der Kontaktpersonen und des vertrauenswürdigen Kuriers (Muster)

Ich, *[Name und Anschrift des Vertreters der Organisation]*, **bestätige, dass für die Beantragung, Generierung und den Abruf der digitalen Zertifikate für öffentliche Schlüssel für TACHOnet-Zugangspunkte folgende Informationen zur Wahrung der Vertraulichkeit, Integrität und Nichtabstreitbarkeit der TACHOnet-Benachrichtigungen zu verwenden sind:**

Angaben zum Ansprechpartner:

– **Ansprechpartner 1:**	– **Ansprechpartner 2:**
– Name:	– Name:
– Vornamen:	– Vornamen:
– Telefon mobil:	– Telefon mobil:
– Tel.:	– Tel.:
– E-Mail:	– E-Mail:
– Handschriftliche Unterschriftsprobe: –	– Handschriftliche Unterschriftsprobe: – – –

Information zum vertrauenswürdigen Kurier:

– **Vertrauenswürdiger Kurier#1**	– **Vertrauenswürdiger Kurier#2**
– Name:	– Name:
– Vornamen:	– Vornamen:
– Telefon mobil:	– Telefon mobil:
– E-Mail:	– E-Mail:
– Ausstellungsland des Reisepasses:	– Ausstellungsland des Reisepasses:
– Reisepass-Nr.:	– Reisepass-Nr.:
– Ablauf der Gültigkeit des Reisepasses:	– Ablauf der Gültigkeit des Reisepasses:

Ort, Datum, Stempel des Unternehmens oder der Organisation:

(Unterschrift des bevollmächtigten Vertreters):

6. Dokumente

6.1. Persönliche Vollmacht (Muster)

Ein Muster der persönlichen Vollmacht, die unterzeichnet sein muss und vom vertrauenswürdigen Kurier bei der Registrierungsbehörde persönlich vorzulegen ist, ist hier abgelegt:

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. Zertifikatantrag in Papierform (Muster)

Ein Muster der persönlichen Vollmacht, die unterzeichnet sein muss und vom vertrauenswürdigen Kurier bei der Registrierungsbehörde persönlich vorzulegen ist, ist hier abgelegt:

7. Glossar

Die wichtigsten Begriffe dieser Unteranlage sind in den CEF-Begriffsbestimmungen auf dem Webportal der CEF-Digital abgelegt:

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

Die wichtigsten Akronyme, die in dieser Beschreibung der Komponente verwendet werden, sind im CEF-Glossar auf dem Webportal der CEF-Digital abgelegt:

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