Conseil de
l'Union européenne

Bruxelles, le 5 novembre 2018
(OR. en)

13711/18
ADD 1

Dossier interinstitutionnel:
2018/0339(NLE)

TRANS 488

NOTE

Origine:	Secrétariat général du Conseil
Destinataire:	délégations
Nº doc. préc.:	ST 13711/18 TRANS 448
N° doc. Cion:	ST 12727/18 TRANS 426 + ADD 1
Objet:	Décision du Conseil relative à la position à adopter, au nom de l'Union européenne, au sein du groupe d'experts sur l'accord européen relatif au travail des équipages des véhicules effectuant des transports internationaux par route de la Commission économique des Nations unies pour l'Europe

Appendice à la décision du Conseil susvisée.

PIÈCE JOINTE

Nouvel appendice relatif à l'AETR

Appendice 4

Spécifications TACHOnet

1. Champ d'application et objet

1.1. Le présent appendice établit les modalités et les conditions relatives à la connexion des parties contractantes à l'AETR à TACHOnet par l'intermédiaire d'eDelivery.

1.2. Les parties contractantes qui se connectent à TACHOnet par l'intermédiaire d'eDelivery respectent les dispositions établies dans le présent appendice.

2. Définitions

a) "Partie contractante" ou "partie", toute partie contractante à l'AETR;

b) "eDelivery", le service, mis au point par la Commission européenne, qui permet de transmettre des données entre des tiers par voie électronique, qui fournit des preuves concernant le traitement des données transmises, y compris la preuve de leur envoi et de leur réception, et qui protège les données transmises contre le risque d'altération non autorisée;

c) "TACHOnet", le système d'échange électronique d'informations sur les cartes de conducteur entre parties contractantes visé à l'article 31, paragraphe 2, du règlement (UE) n° 165/2014;

d) "système central", le système d'information qui permet le routage des messages sur le système TACHOnet entre les parties demandeuses et les parties destinataires;

e) "partie demandeuse", la partie contractante qui émet une demande ou une notification TACHOnet, laquelle est ensuite acheminée par le système central jusqu'à la partie destinataire concernée;

f) "partie destinataire", la partie contractante à laquelle la demande ou la notification TACHOnet est destinée;

g) "autorité de délivrance des cartes", une entité habilitée par une partie contractante pour la délivrance et la gestion des cartes tachygraphiques.

3. Responsabilités générales

3.1. Aucune des parties contractantes n'est autorisée à conclure des accords visant à accéder à TACHONET au nom d'une autre partie ou ne peut représenter d'une autre manière l'autre partie contractante sur la base du présent appendice. Aucune des parties contractantes n'agit en tant que sous-traitant de l'autre partie contractante dans le cadre des opérations visées dans le présent appendice.

3.2. Les parties contractantes donnent accès à leur registre national d'informations sur les cartes de conducteur par l'intermédiaire de TACHOnet, de la manière et avec le niveau de service définis au sous-appendice 4.6.

3.3. Les parties contractantes s'informent mutuellement sans délai si elles constatent des perturbations ou des erreurs relevant de leur domaine de responsabilité qui sont susceptibles de compromettre le fonctionnement normal de TACHOnet.

3.4. Chaque partie désigne des personnes de contact pour TACHOnet et en informe le secrétariat de l'AETR. Tout changement dans les points de contact doit être transmis par écrit au secrétariat de l'AETR.

4. Essais de connexion à TACHOnet

4.1. La connexion à TACHOnet d'une partie contractante est considérée comme établie après que les essais de connexion, d'intégration et de performance ont été menés à bien conformément aux instructions et sous le contrôle de la Commission européenne.

4.2. En cas d'échec des essais préliminaires, la Commission européenne peut suspendre temporairement la phase d'essai. Les essais sont repris après que la partie contractante a informé la Commission européenne que les améliorations techniques requises au niveau national pour le bon déroulement des essais préliminaires ont été adoptées.

4.3. La durée maximale de ces essais préliminaires est de six mois.

5. Architecture de confiance

5.1. La confidentialité, l'intégrité et la non-répudiation des messages TACHOnet sont assurées par l'architecture de confiance de TACHOnet.

5.2. L'architecture de confiance de TACHOnet est fondée sur un service d'infrastructure à clé publique (ICP) mis en place par la Commission européenne, dont les exigences sont définies aux sous-appendices 4.8 et 4.9.

5.3. Les entités suivantes interviennent dans l'architecture de confiance de TACHOnet:

a) autorité de certification, responsable de la génération des certificats numériques devant être délivrés par l'autorité d'enregistrement aux autorités nationales des parties contractantes (par l'intermédiaire de coursiers de confiance désignés par celles-ci), ainsi que de la mise en place de l'infrastructure technique concernant la délivrance, la révocation et le renouvellement des certificats numériques;

b) propriétaire du domaine, responsable de l'exploitation du système central visé au sous-appendice 4.1 et de la validation et de la coordination de l'architecture de confiance de TACHOnet;

c) autorité d'enregistrement, chargée d'enregistrer et d'approuver les demandes de délivrance, de révocation et de renouvellement des certificats numériques, et de vérifier l'identité des coursiers de confiance;

d) le coursier de confiance est la personne désignée par les autorités nationales, chargée de remettre la clé publique à l'autorité d'enregistrement et d'obtenir le certificat correspondant généré par l'autorité de certification;

e) autorité nationale de la partie contractante, qui devra:

i) générer les clés privées et les clés publiques correspondantes à inclure dans les certificats à générer par l'autorité de certification;

ii) demander les certificats numériques à l'autorité de certification;

iii) désigner le coursier de confiance.

5.4. L'autorité de certification et l'autorité d'enregistrement sont désignées par la Commission européenne.

5.5. Toute partie contractante qui se connecte à TACHOnet doit demander la délivrance d'un certificat numérique conformément au sous-appendice 4.9, afin de signer et de crypter un message TACHOnet.

5.6. Un certificat peut être révoqué conformément au sous-appendice 4.9.

6. Protection des données et confidentialité

6.1. Les parties, dans le respect des législations internationales et nationales en matière de protection des données, et notamment de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, adoptent toutes les mesures techniques et organisationnelles nécessaires pour garantir la sécurité des données de TACHOnet et empêcher la modification, la perte ou le traitement non autorisé de ces données ou l'accès non autorisé à celles-ci (notamment en ce qui concerne l'authenticité, la confidentialité des données, la traçabilité, l'intégrité, la disponibilité et la non-répudiation ainsi que la sécurité des messages).

6.2. Chaque partie protège ses propres systèmes nationaux contre l'utilisation illicite, les codes malveillants, les virus, les intrusions informatiques, les infractions et la falsification illégale de données et contre d'autres actions comparables commises par des tiers. Les parties conviennent de déployer des efforts commercialement raisonnables pour éviter la transmission de virus, de bombes à retardement, de vers ou d'éléments similaires ou de toute routine de programmation informatique qui pourraient interférer avec les systèmes informatiques de l'autre partie.

7. Coûts

7.1. Les parties contractantes supportent leurs propres coûts de développement et d'exploitation en rapport avec leurs propres systèmes et procédures de données, selon les besoins, pour remplir les obligations découlant du présent appendice.

7.2. Les services spécifiés dans le sous-appendice 4.1, fournis par le système central, sont gratuits.

8. Sous-traitance

8.1. Les parties peuvent sous-traiter tout service dont elles sont responsables en vertu de du présent appendice.

8.2. Une telle sous-traitance ne dégage pas la partie de la responsabilité qui lui incombe en vertu du présent appendice, y compris la responsabilité pour le niveau de service approprié conformément au sous-appendice 4.6.

Sous-appendice 4.1

Aspects généraux de TACHOnet

1. Description générale

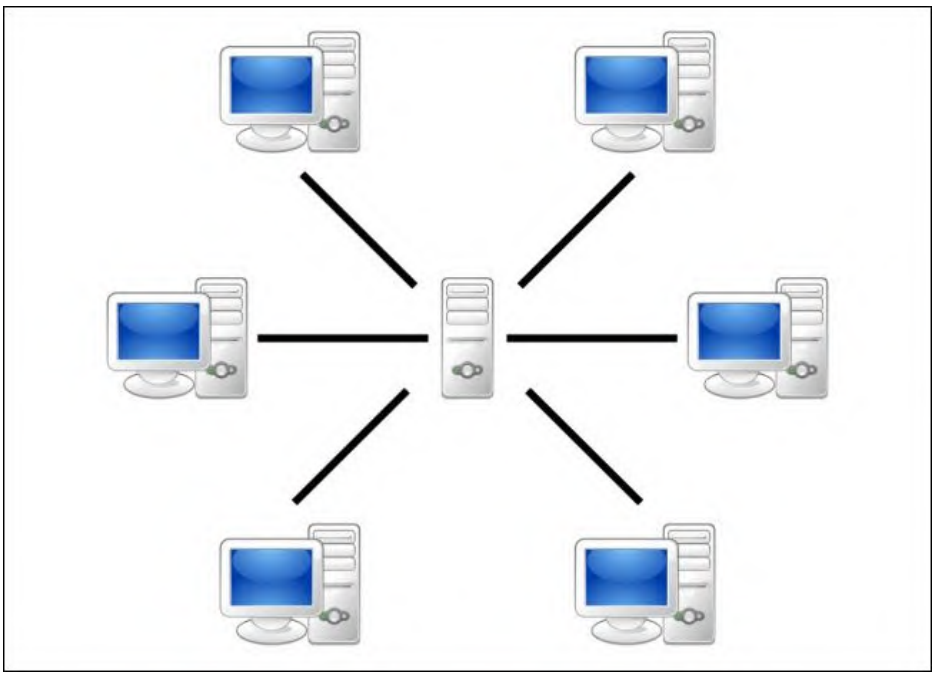
TACHOnet est un système électronique d'échange d'informations sur les cartes de conducteur entre les parties contractantes à l'AETR. TACHOnet achemine les demandes d'information des parties demandeuses aux parties destinataires, ainsi que les réponses de ces dernières aux premières. Les parties contractantes qui utilisent TACHOnet doivent connecter leurs registres nationaux d'informations sur les cartes de conducteur au système.

2. Architecture

Le système de messagerie TACHOnet se compose des éléments suivants:

2.1. un système central, capable de recevoir une demande de la partie demandeuse, de la valider et de la traiter en la transmettant aux parties destinataires. Le système central attend que chaque partie destinataire réponde, puis regroupe toutes les réponses et transmet la réponse ainsi consolidée à la partie demandeuse;

2.2. les systèmes nationaux des parties, équipés d'une interface capable à la fois d'envoyer les demandes au système central et de recevoir les réponses correspondantes. Ils peuvent utiliser un logiciel propriétaire ou commercial pour transmettre et recevoir les messages en provenance du système central.



3. Gestion

3.1. Le système central est géré par la Commission européenne, qui en assure l'exploitation technique et la maintenance.

3.2. Le système central ne conserve pas les données pendant plus de six mois, à l'exception des données statistiques et d'enregistrement définies au sous-appendice 4.7.

3.3. Le système central n'autorise pas l'accès aux données à caractère personnel, sauf au personnel de la Commission européenne dûment autorisé, si nécessaire aux fins de contrôle, de maintenance et de dépannage.

3.4. Les parties contractantes sont chargées:

3.4.1. d'assurer la configuration et la gestion de leurs systèmes nationaux, notamment de l'interface avec le système central;

3.4.2. de veiller à l'installation et à la maintenance de leurs systèmes nationaux, matériel et logiciels compris, qu'ils soient propriétaires ou commerciaux;

3.4.3. d'assurer l'interopérabilité adéquate de leurs systèmes nationaux avec le système central, y compris la gestion des messages d'erreur envoyés par le système central;

3.4.4. de prendre toutes les mesures nécessaires pour assurer la confidentialité, l'intégrité et la disponibilité de l'information;

3.4.5. d'assurer l'exploitation des systèmes nationaux conformément aux niveaux de service décrits au sous-appendice 4.6.

Sous-appendice 4.2

Fonctionnalités de TACHOnet

1. Les fonctionnalités suivantes sont accessibles via le système de messagerie TACHOnet:

1.1. Vérification des cartes délivrées (Check issued cards — CIC): permet à la partie demandeuse d'envoyer une "Demande de vérification des cartes délivrées" à une ou à toutes les parties destinataires, afin de déterminer si un demandeur de carte est déjà en possession d'une carte de conducteur délivrée par ces dernières. Les parties destinataires donnent suite à la demande en envoyant une "Réponse à la demande de vérification des cartes délivrées".

1.2. Vérification du statut de la carte (Check card status — CCS): permet à la partie demandeuse de solliciter auprès de la partie destinataire les informations sur une carte délivrée par cette dernière en lui envoyant une "Demande de vérification du statut de la carte". La partie destinataire donne suite à la demande en envoyant une "Réponse à la demande de vérification du statut de la carte".

1.3. Modification du statut de la carte (Modify card status — MCS): permet à la partie demandeuse de notifier à la partie destinataire, au moyen d'une "Demande de modification du statut de la carte", la modification du statut d'une carte délivrée par cette dernière. La partie destinataire y donne suite par un "Accusé de réception de la demande de modification du statut de la carte".

1.4. Permis de conduire à la base d'une carte délivrée (Issued card driving license — ICDL): permet à la partie demandeuse de notifier à la partie destinataire, via une "Demande concernant un permis de conduire à la base d'une carte délivrée", qu'une carte a été délivrée par la partie demandeuse sur la base d'un permis de conduire délivré par la partie destinataire. Cette dernière y donne suite par une "Réponse concernant un permis de conduire à la base d'une carte délivrée".

2. D'autres types de messages jugés nécessaires au bon fonctionnement du système de messagerie TACHOnet sont inclus, comme les notifications d'erreur.

3. Les systèmes nationaux reconnaissent les statuts des cartes énumérées dans le tableau 1 lors de l'utilisation de toutes les fonctionnalités décrites au point 1. Toutefois, les parties ne sont pas tenues de mettre en œuvre une procédure administrative faisant usage de tous les statuts figurant sur la liste.

4. Lorsqu'une partie reçoit une réponse ou une notification indiquant un statut non utilisé dans ses procédures administratives, le système national traduit le statut mentionné dans le message reçu en la valeur appropriée dans cette procédure. La partie destinataire ne doit pas rejeter le message dès lors que le statut signalé dans ce message est mentionné dans le tableau 1.

5. Le statut de la carte mentionné dans le tableau 1 ne doit pas être utilisé pour déterminer si une carte de conducteur est valable pour la conduite. Lorsqu'une partie interroge le registre de l'autorité nationale qui délivre la carte via la fonctionnalité CCS, la réponse contient le champ prévu à cet effet "valable pour la conduite". Les procédures administratives nationales sont telles que les réponses CCS contiennent toujours la valeur appropriée "valable pour la conduite".

Tableau 1

Statuts des cartes

Statut de la carte	**Définition**
Demande	L'autorité de délivrance des cartes a reçu une demande de délivrance d'une carte de conducteur. Cette information est enregistrée et sauvegardée dans la base de données à l'aide des clés de recherche générées.
Approuvé	L'autorité de délivrance des cartes a approuvé la demande de carte tachygraphique.
Rejeté	L'autorité de délivrance des cartes n'a pas approuvé la demande.
Personnalisée	La carte tachygraphique a été personnalisée.
Transmise	L'autorité nationale a livré la carte de conducteur au conducteur ou à l'organisme de délivrance concerné.
Remise	L'autorité nationale a remis la carte de conducteur au conducteur concerné.
Confisquée	L'autorité compétente a privé le conducteur de la carte de conducteur.
Suspendue	Le conducteur est temporairement privé de la carte de conducteur.
Retirée	L'autorité de délivrance des cartes a décidé de retirer la carte de conducteur. La carte a été définitivement annulée.
Restituée	La carte tachygraphique a été renvoyée à l'autorité de délivrance des cartes et déclarée ne plus être nécessaire.
Perdue	La carte tachygraphique a été déclarée perdue à l'autorité de délivrance des cartes.
Volée	La carte tachygraphique a été déclarée volée à l'autorité de délivrance des cartes. Une carte volée est considérée comme perdue.
Défectueuse	La carte tachygraphique a été déclarée défectueuse à l'autorité de délivrance des cartes.
Expirée	La période de validité de la carte tachygraphique est arrivée à expiration.
Remplacée	La carte tachygraphique ayant été déclarée perdue, volée ou défectueuse a été remplacée par une nouvelle carte. Les données de la nouvelle carte restent les mêmes, excepté l'indice de remplacement du numéro de la carte qui a été incrémenté d'une unité.

Renouvelée	La carte tachygraphique a été renouvelée à cause d'une modification des données administratives ou de l'expiration de la période de validité. Le numéro de carte de la nouvelle carte reste le même, excepté l'indice de renouvellement du numéro de la carte qui a été incrémenté d'une unité.
En cours d'échange	L'autorité de délivrance des cartes ayant délivré une carte de conducteur a reçu une notification signalant le début de la procédure d'échange de cette carte contre une carte de conducteur délivrée par l'autorité de délivrance des cartes d'une autre partie.
Échangée	L'autorité de délivrance des cartes ayant délivré une carte de conducteur a reçu une notification signalant la fin de la procédure d'échange de cette carte contre une carte de conducteur délivrée par l'autorité de délivrance des cartes d'une autre partie.

Sous-appendice 4.3

Dispositions régissant les messages de TACHOnet

1. Prescriptions techniques générales

1.1. Le système central fournit des interfaces synchrones et asynchrones pour l'échange des messages. Les parties peuvent choisir l'interface la plus appropriée pour interagir avec leurs propres applications.

1.2. Tous les messages échangés entre le système central et les systèmes nationaux doivent être encodés en UTF-8.

1.3. Les systèmes nationaux peuvent recevoir et traiter les messages contenant des caractères grecs ou cyrilliques.

2. Structure des messages XML et définition du schéma (XSD)

2.1. La structure générale des messages XML est conforme au format défini par les schémas XSD installés sur le système central.

2.2. Le système central et les systèmes nationaux transmettent et reçoivent les messages conformes au schéma XSD du message.

2.3. Les systèmes nationaux peuvent également envoyer, recevoir et traiter tous les messages correspondant à l'une des fonctionnalités décrites au sous-appendice 4.2.

2.4. Les messages XML comprennent au moins les exigences minimales établies dans le tableau 2.

Tableau 2

Exigences minimales concernant le contenu des messages XML

En-tête commun		**Obligatoire**
Version	La version officielle des caractéristiques XML est indiquée dans l'espace de noms défini dans le XSD du message et dans l'attribut de version de l'élément d'en-tête de tout message XML. Le numéro de version ("n.m") est défini comme une valeur fixe dans chaque publication du fichier "Définition du schéma XML" (xsd).	Oui
Identifiant de test	Identifiant facultatif à des fins de test. L'initiateur du test saisit l'identifiant et tous les intervenants dans le flux de travail doivent transmettre/renvoyer le même identifiant. Il doit être ignoré dans la production et ne sera pas utilisé s'il est fourni.	Non
Identifiant technique	Il s'agit d'un UUID qui identifie de manière unique chaque message individuel. L'expéditeur crée un UUID et renseigne cet attribut. Ces données ne sont pas utilisées à des fins d'activité économique.	Oui
Identifiant du flux de travail	L'identifiant du flux de travail est un UUID et doit être créé par la partie demandeuse. Cet identifiant est ensuite utilisé dans tous les messages pour corréler le flux de travail.	Oui
Envoyé à	Date et heure (GMT) auxquelles le message a été envoyé.	Oui
Délai d'expiration	Il s'agit d'un attribut facultatif de date et d'heure (au format TUC). Cette valeur est définie par le système central uniquement pour les demandes transmises. Elle indique à la partie destinataire le délai d'expiration de la demande. Cette valeur n'est pas requise en MS2TCN_<x>_Req ni dans tous les messages de réponse. Elle est incluse en option afin de permettre l'utilisation de la même définition de l'en-tête dans tous les types de messages, que l'attribut "Valeur de délai d'expiration" soit requis ou non.	Non
De	Code ISO 3166-1 alpha 2 de la partie à l'origine du message ou "UE".	Oui
À	Code ISO 3166-1 alpha 2 de la partie destinataire du message ou "UE".	Oui

Sous-appendice 4.4

Translittération et services NYSIIS (New York State Identification and Intelligence System)

1. L'algorithme NYSIIS mis en œuvre dans le système central permet d'encoder les noms de tous les conducteurs dans le registre national.

2. Lors de la recherche d'une carte via la fonctionnalité CIC, les clés NYSIIS sont utilisées comme principal mécanisme de recherche.

3. Par ailleurs, les parties peuvent utiliser un algorithme personnalisé pour renvoyer des résultats supplémentaires.

4. Les résultats de la recherche précisent le mécanisme de recherche utilisé pour trouver une entrée, à savoir NYSIIS ou personnalisé.

5. Si une partie choisit d'enregistrer des notifications ICDL, les clés NYSIIS contenues dans la notification sont enregistrées comme faisant partie des données ICDL. La partie utilise les clés NYSIIS du nom du demandeur pour effectuer la recherche des données ICDL.

Sous-appendice 4.5

Exigences de sécurité

1. Le protocole HTTPS est utilisé pour l'échange des messages entre le système central et les systèmes nationaux.

2. Les systèmes nationaux utilisent les certificats numériques visés aux sous-appendices 4.8 et 4.9 afin de sécuriser la transmission des messages entre le système national et le système central.

3. Les systèmes nationaux mettent en œuvre, au minimum, des certificats utilisant l'algorithme de hachage de signature SHA-2 (SHA-256) et une longueur de clé publique de 2048 bits.

Sous-appendice 4.6

Niveaux de service

1. Les systèmes nationaux satisfont le niveau de service minimal suivant:

1.1. Ils sont disponibles 24 heures sur 24, 7 jours sur 7.

1.2. Leur disponibilité est contrôlée par un message pulsion émis depuis le système central.

1.3. Leur taux de disponibilité est de 98 %, conformément au tableau suivant (les chiffres ont été arrondis à l'unité la plus proche appropriée):

Une disponibilité de	correspond à une indisponibilité de		
	par jour	par mois	par an
98 %	0,5 heure	15 heure	7,5 jours

Les parties sont invitées à respecter le taux de disponibilité quotidien. Toutefois, il est admis que certaines activités nécessaires, telles que la maintenance du système, requièrent un temps d'arrêt de plus de 30 minutes. En revanche, les taux de disponibilité mensuelle et annuelle demeurent obligatoires.

1.4. Les systèmes doivent répondre à un minimum de 98 % des demandes qui leur sont transmises en un mois calendaire.

1.5. Les systèmes doivent répondre aux demandes dans un délai de 10 secondes.

1.6. Le délai global d'expiration de la demande (temps pendant lequel le demandeur peut attendre une réponse) ne dépasse pas 20 secondes.

1.7. Les systèmes doivent être en mesure de répondre à un taux de demande de 6 messages par seconde.

1.8. Les systèmes nationaux ne devraient pas envoyer de demandes au système central TACHOnet à un taux supérieur à 2 demandes par seconde.

1.9. Chaque système national doit pouvoir faire face aux problèmes techniques potentiels du système central ou des systèmes nationaux des autres parties. Ces problèmes comprennent notamment, sans toutefois s'y limiter:

a) la perte de connexion au système central;

b) l'absence de réponse à une demande;

c) la réception de la réponse après le délai d'expiration du message;

d) la réception de messages non sollicités;

e) la réception de messages non valables.

2. Le système central doit:

2.1. présenter un taux de disponibilité de 98 %;

2.2. envoyer aux systèmes nationaux une notification des erreurs, soit par le message de réponse, soit par un message d'erreur dédié. Les systèmes nationaux, en retour, reçoivent ces messages d'erreur dédiés et disposent d'un flux de travail progressif permettant de prendre les mesures appropriées pour corriger l'erreur notifiée.

3. Maintenance

Les parties informent les autres parties et la Commission européenne de toutes les activités de maintenance de routine, via l'application web, au moins une semaine avant le début de ces activités, si cela s'avère techniquement possible.

Sous-appendice 4.7

Enregistrement et statistiques des données collectées au niveau du système central

1. Dans un souci de confidentialité, les données communiquées à des fins statistiques sont anonymes. Les données relatives à l'identification d'une carte, d'un conducteur ou d'un permis de conduire spécifique ne sont pas communiquées à des fins statistiques.

2. Les informations enregistrées permettent de conserver une trace de toutes les transactions exécutées à des fins de contrôle ou de débogage et de produire des statistiques relatives à ces transactions.

3. Les données à caractère personnel ne doivent pas être conservées dans les fichiers-journaux pendant plus de six mois. Les informations statistiques sont en revanche conservées pendant une durée indéterminée.

4. Les données statistiques utilisées pour la transmission de rapports comprennent:

   a) la partie demandeuse;

   b) la partie destinataire;

   c) le type de message;

   d) le code d'état de la réponse;

   e) la date et l'heure des messages;

   f) le temps de réponse.

Sous-appendice 4.8

Dispositions générales relatives aux clés et aux certificats numériques pour TACHOnet

1. La direction générale de l'informatique (DIGIT) de la Commission européenne met un service ICP[1] (dénommé ci-après le "service MIE ICP") à la disposition des parties contractantes à l'AETR qui se connectent à TACHOnet (désormais les autorités nationales) par l'intermédiaire d'eDelivery.

2. La procédure de demande et de révocation de certificats numériques, ainsi que les modalités et les conditions détaillées de leur utilisation, sont définies dans l'appendice.

3. Utilisation des certificats:

3.1. Une fois le certificat délivré, l'autorité nationale[2] utilise le certificat uniquement dans le contexte de TACHOnet. Le certificat peut être utilisé afin:

   a) d'authentifier l'origine des données;

   b) de chiffrer des données;

   c) de garantir la détection des atteintes à l'intégrité des données.

3.2. Toute utilisation non explicitement autorisée parmi les utilisations autorisées du certificat est interdite.

4. Les parties contractantes:

   a) protègent leurs clés privées contre toute utilisation non autorisée;

   b) s'abstiennent de transférer ou de révéler leurs clés privées à des tiers, même en tant que représentants;

---

[1] Une ICP (infrastructure à clé publique) est un ensemble de rôles, de politiques, de procédures et de systèmes nécessaires à la gestion, à la distribution et à la révocation des certificats numériques.

[2] Identifié par la valeur d'attribut "O=" dans le Subject Distinguished Name du certificat émis.

c) garantissent la confidentialité, l'intégrité et la disponibilité des clés privées générées, stockées et utilisées pour TACHOnet;

d) s'abstenir de poursuivre l'utilisation de la clé privée après l'échéance de la période de validité ou après la révocation du certificat, à des fins autres que la visualisation des données chiffrées (p.ex. déchiffrage de courriels); Les clés arrivées à échéance doivent être soit détruites soit conservées d'une manière en empêchant l'utilisation;

e) fournissent à l'autorité d'enregistrement l'identification des représentants autorisés qui sont habilités à demander la révocation des certificats délivrés à l'organisation (les demandes de révocation doivent inclure un mot de passe de demande de révocation et des détails sur les événements qui ont conduit à la révocation);

f) empêchent une utilisation abusive des clés privées en demandant la révocation du certificat de clé publique correspondant lorsque la clé privée ou les données d'activation de la clé privée sont compromises;

g) sont responsables et ont l'obligation de demander la révocation du certificat dans les circonstances définies dans les politiques de certification (PC) et la déclaration d'activité de certification (CPS) de l'autorité de certification;

h) informent sans délai l'autorité d'enregistrement de la perte, du vol ou de la compromission potentielle de toute clé AETR utilisée dans le cadre de TACHOnet.

5. Engagements

Sans préjudice de la responsabilité de la Commission européenne en violation de toute exigence prévue par le droit national applicable ou en ce qui concerne la responsabilité pour les questions qui ne peuvent être exclues en vertu de ce droit, la Commission européenne n'est pas responsable à l'égard des aspects suivants:

a) le contenu du certificat, qui appartient exclusivement au détenteur du certificat. Il incombe au détenteur du certificat de vérifier l'exactitude du contenu du certificat;

b) l'utilisation du certificat par son détenteur.

Sous-appendice 4.9

Description du service ICP pour TACHOnet

1. Introduction

Une ICP (infrastructure à clé publique) est un ensemble de rôles, de politiques, de procédures et de systèmes nécessaires à la gestion, à la distribution et à la révocation des certificats numériques[3]. Le service MIE ICP d'eDelivery permet l'émission et la gestion de certificats numériques utilisés afin de garantir la confidentialité, l'intégrité et la non-répudiation des informations échangées entre des points d'accès.

Le service ICP d'eDelivery est basé sur l'autorité de certification Trust Center Services TeleSec Shared Business à laquelle s'applique la politique de certification (PC) / la déclaration d'activité de certification (CPS) de l'autorité de certification TeleSec Shared-Business-CA de T-Systems International GmbH[4].

Le service ICP délivre des certificats adaptés à la sécurisation de divers processus opérationnels à l'intérieur et à l'extérieur des entreprises, des organisations, des autorités publiques et des institutions qui exigent un niveau de sécurité moyen pour prouver l'authenticité, l'intégrité et la fiabilité de l'entité finale.

2. Processus de demande de certificat

2.1. Rôles et responsabilités

2.1.1. "Organisation" ou "autorité nationale" demandant le certificat

2.1.1.1. L'autorité nationale introduit les demandes de certificats dans le contexte du projet TACHOnet.

2.1.1.2. L'autorité nationale:

a) demande les certificats auprès du service MIE ICP;

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

[4] La dernière version de la PC et de la CPS peut être téléchargée à l'adresse suivante: https://www.telesec.de/en/sbca-en/support/download-area/

b) génère les clés privées et les clés publiques correspondantes à inclure dans les certificats délivrés par l'autorité de certification;

c) télécharge le certificat dès son approbation;

d) signe et renvoie à l'autorité d'enregistrement:

i) le formulaire d'identification des personnes de contact et des coursiers de confiance,

ii) le mandat individuel signé[5].

2.1.2. Coursier de confiance

2.1.2.1. L'autorité nationale désigne un coursier de confiance.

2.1.2.2. Le coursier de confiance:

a) remet la clé publique à l'autorité d'enregistrement durant un processus d'identification et d'enregistrement en face-à-face;

b) obtient le certificat correspondant de l'autorité d'enregistrement.

2.1.3. Propriétaire de domaine

2.1.3.1. La DG MOVE est le propriétaire de domaine.

2.1.3.2. Le propriétaire de domaine:

a) valide et coordonne le réseau TACHOnet et l'architecture de confiance TACHOnet, notamment la validation des procédures de délivrance des certificats;

b) exploite le système central TACHOnet et coordonne l'activité des parties concernant le fonctionnement de TACHOnet;

c) réalise, avec les autorités nationales, les essais de connexion à TACHOnet.

[5] Un mandat est un document juridique par lequel l'organisation habilite et autorise la Commission européenne, représentée par le fonctionnaire identifié responsable du service MIE ICP, à demander la génération d'un certificat à l'autorité de certification TeleSec Shared Business de T-Systems International GmbH pour son propre compte. Voir également le point 6.

2.1.4. Autorité d'enregistrement

2.1.4.1. Le Centre commun de recherche (CCR) est l'autorité d'enregistrement.

2.1.4.2. L'autorité d'enregistrement est chargée de vérifier l'identité du coursier de confiance, d'enregistrer et d'approuver les demandes de délivrance, de révocation et de renouvellement des certificats numériques.

2.1.4.3. L'autorité d'enregistrement:

a) assigne l'identifiant unique à l'autorité nationale;

b) authentifie l'identité de l'autorité nationale, ses points de contact et ses coursiers de confiance;

c) communique avec l'équipe de soutien du MIE en ce qui concerne l'authenticité de l'autorité nationale, ses points de contact et ses coursiers de confiance;

d) informe l'autorité nationale concernant l'approbation ou le rejet du certificat.

2.1.5. Autorité de certification

2.1.5.1. L'autorité de certification est responsable de la fourniture de l'infrastructure technique nécessaire à l'introduction de la demande et à la délivrance et à la révocation de certificats numériques.

2.1.5.2. L'autorité de certification:

a) fournit l'infrastructure technique pour les demandes de certificat introduites par les autorités nationales;

b) valide ou rejette la demande de certificat;

c) communique avec l'autorité d'enregistrement pour la vérification de l'identité de l'organisation demandeuse, le cas échéant.

2.2. Délivrance du certificat

2.2.1. Le certificat est délivré conformément aux étapes consécutives suivantes, représentées dans l'illustration 1:

a) **Étape 1:** identification du coursier de confiance;

b) **Étape 2:** création de la demande de certificat;

c) **Étape 3:** enregistrement auprès de l'autorité d'enregistrement;

d) **Étape 4:** génération du certificat;

e) **Étape 5:** publication du certificat;

f) **Étape 6:** acceptation du certificat.

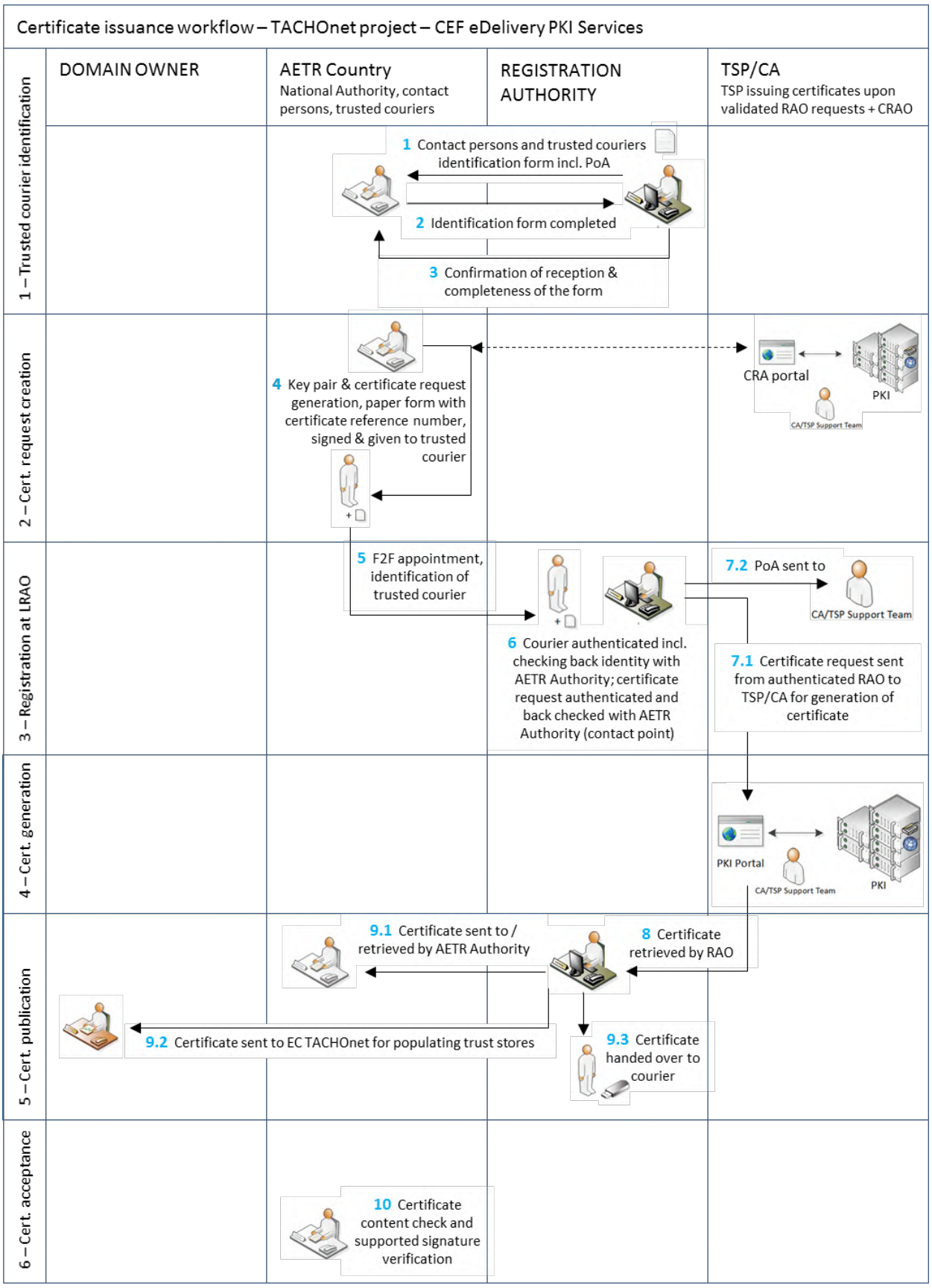


Illustration 1 - Flux de délivrance du certificat

2.2.2. Étape 1: identification du coursier de confiance

Le processus suivant est appliqué pour l'identification du coursier de confiance:

a) L'autorité d'enregistrement envoie à l'autorité nationale le formulaire d'identification des personnes de contact et des coursiers de confiance[6]. Ce formulaire inclut également un mandat que l'organisation (autorité AETR) signe.

b) L'autorité nationale renvoie le formulaire complété et le mandat signé à l'autorité d'enregistrement.

c) L'autorité d'enregistrement confirme la bonne réception et l'exhaustivité du formulaire.

d) L'autorité d'enregistrement fournit au propriétaire de domaine une copie mise à jour de la liste des personnes de contact et des coursiers de confiance.

2.2.3. Étape 2: création de la demande de certificat

2.2.3.1. La demande et la récupération du certificat se font sur le même ordinateur et avec le même navigateur.

2.2.3.2. Le processus suivant est appliqué pour la création de la demande de certificat:

a) L'organisation se rend sur l'interface utilisateur afin de demander le certificat via l'URL https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en: et saisit le nom d'utilisateur **"sbca/CEF_eDelivery.europa.eu"** et le mot de passe **"digit.333"**.

[6] Voir point 5.

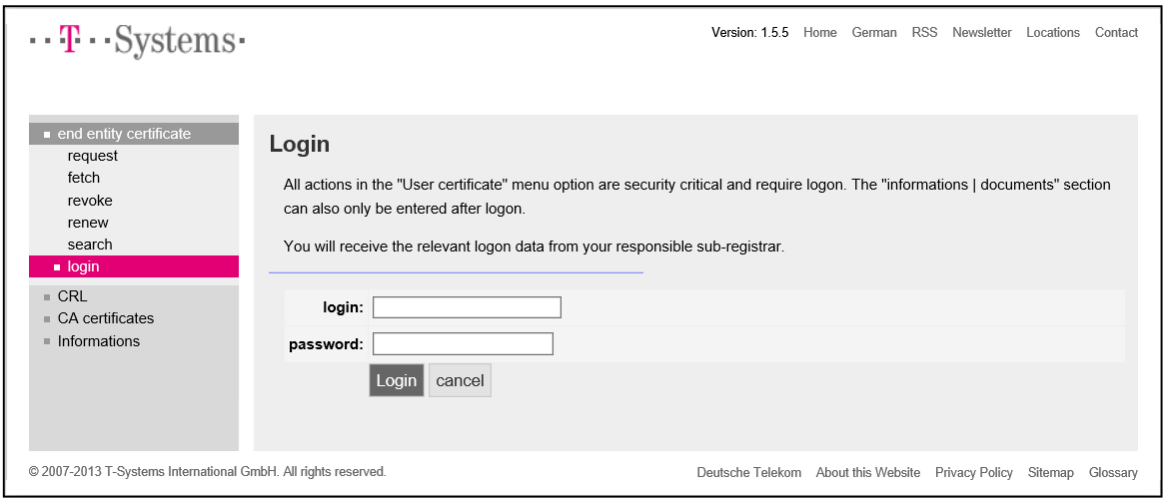


Illustration 2

b) L'organisation clique sur "request" (demander) dans le menu à gauche et sélectionne "CEF_TACHOnet" dans la liste déroulante.

Illustration 3

c) L'organisation complète le formulaire de demande de certificat figurant à l'illustration 4 avec les informations figurant dans le tableau 3. Elle clique ensuite sur "Next (soft-PSE)" pour finir le processus.

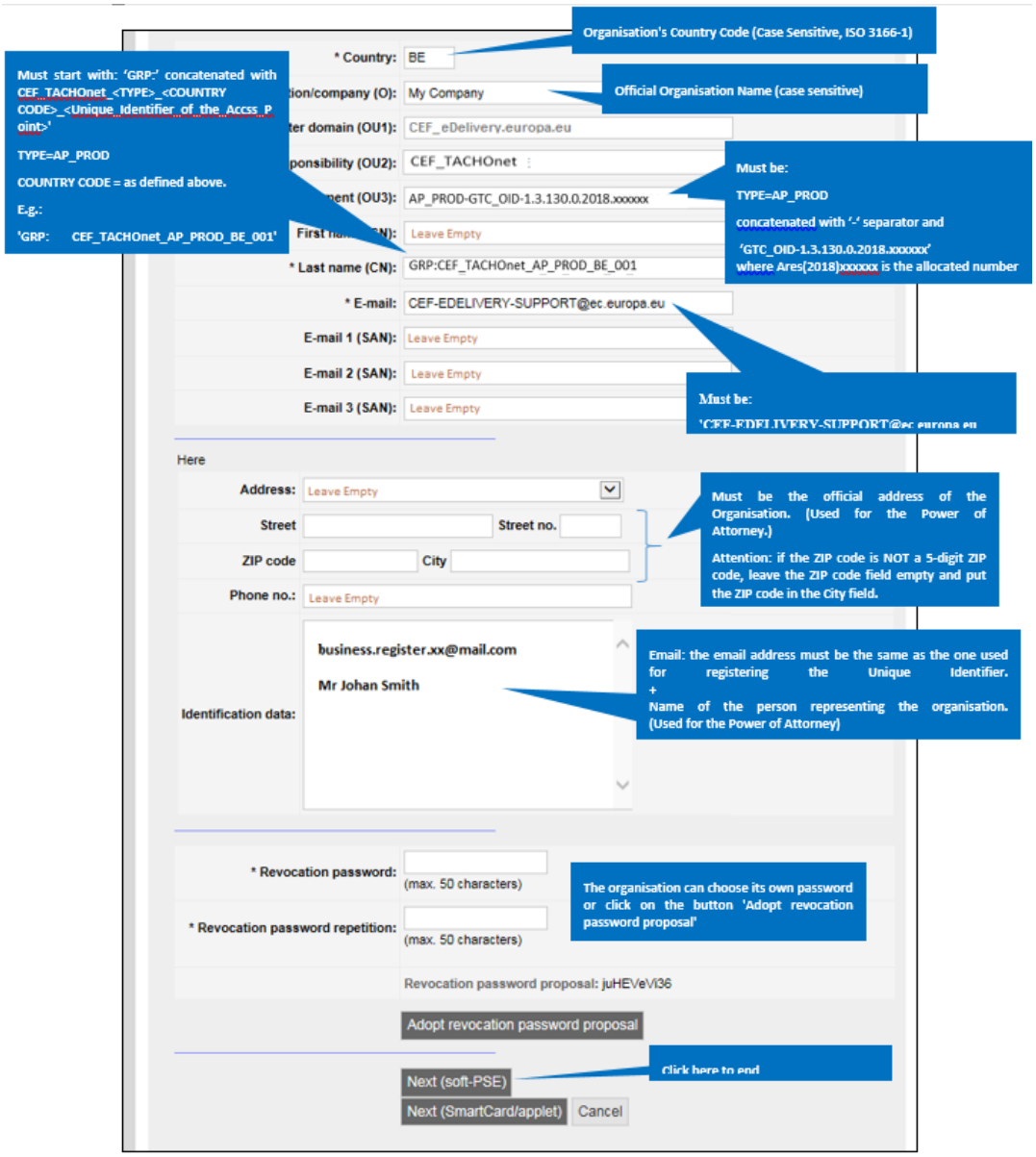


Illustration 4

Champs demandés	Description
Country (Pays)	**C = code pays**, localisation du détenteur du certificat, vérifiée à l'aide d'un annuaire public; contraintes: 2 caractères, conformément à la norme ISO 3166-1, alpha-2, sensible à la casse; exemples: DE, BE, NL, Cas particuliers UK (pour la Grande-Bretagne), EL (pour la Grèce)
Organisation/Company (O) (organisation/société)	**O = nom de l'organisation du détenteur du certificat**
Master domain (OU1) (domaine central)	**OU = CEF_eDelivery.europa.eu**
Area of responsibility (OU2) (Domaine de compétence)	**OU = CEF_TACHOnet**
Department (OU3) (Département)	Valeur obligatoire par "AREA OF RESPONSIBILITY" Le contenu doit être vérifié à l'aide d'une liste positive (liste blanche) lorsque le certificat est demandé. Si les informations ne correspondent pas à la liste, la demande est rejetée. Format: **OU = <TYPE>-<GTC_NUMBER>** où "<TYPE>" est remplacé par AP_PROD: Access Point in Production environment (point d'accès dans l'environnement de production); et où <GTC_NUMBER> est **GTC_OID-1.3.130.0.2018.xxxxxx**, où Ares(2018)xxxxxx est le numéro GTC pour le projet TACHOnet. Exemples: AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
First name (CN) (Prénom)	Doit rester vide
Last name (CN) (Nom de famille)	Doit commencer par "GRP", suivi d'un nom commun. Format: **CN = GRP:<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** Exemples: GRP:CEF_TACHOnet_AP_PROD_BE_001
E-mail	**E=CEF-EDELIVERY-SUPPORT@ec.europa.eu**
E-mail 1 (SAN)	Doit rester vide
E-mail 2 (SAN)	Doit rester vide
E-mail 3 (SAN)	Doit rester vide

Address (Adresse)	Doit rester vide
Street (Rue)	Doit être l'adresse officielle de l'organisation du détenteur du certificat (Utilisée pour le mandat).
Street no. (Numéro)	Doit être l'adresse officielle de l'organisation du détenteur du certificat (Utilisée pour le mandat).
Zip code (Code postal)	Doit être l'adresse officielle de l'organisation du détenteur du certificat (Utilisée pour le mandat). **Attention:** si le code postal n'est pas un code à 5 chiffres, laissez le champ vide et inscrivez le code postal dans le champ City (Ville).
City (Ville)	Doit être l'adresse officielle de l'organisation du détenteur du certificat (Utilisée pour le mandat). **Attention:** si le code postal n'est pas un code à 5 chiffres, laissez le champ vide et inscrivez le code postal dans le champ City (Ville).
Phone no (Numéro de téléphone)	Doit rester vide
Identification data (Données d'identification)	L'adresse e-mail doit être la même que celle utilisée pour enregistrer l'Unique Identifier (identifiant unique). + Doit être le nom de la personne représentant l'organisation. (utilisée pour le mandat). + **Numéro au registre du commerce** (obligatoire uniquement pour les organisations privées) **Inscrit au tribunal cantonal de** (obligatoire uniquement pour les organisations privées allemandes et autrichiennes)
Revocation password (Mot de passe de révocation)	Champ obligatoire choisi par le demandeur
Revocation password repetition (Répétition du mot de passe de révocation)	Répétition du champ obligatoire choisi par le demandeur

Tableau 3. Détails complets de chaque champ demandé

d) La longueur de clé est de 2048 (High Grade)

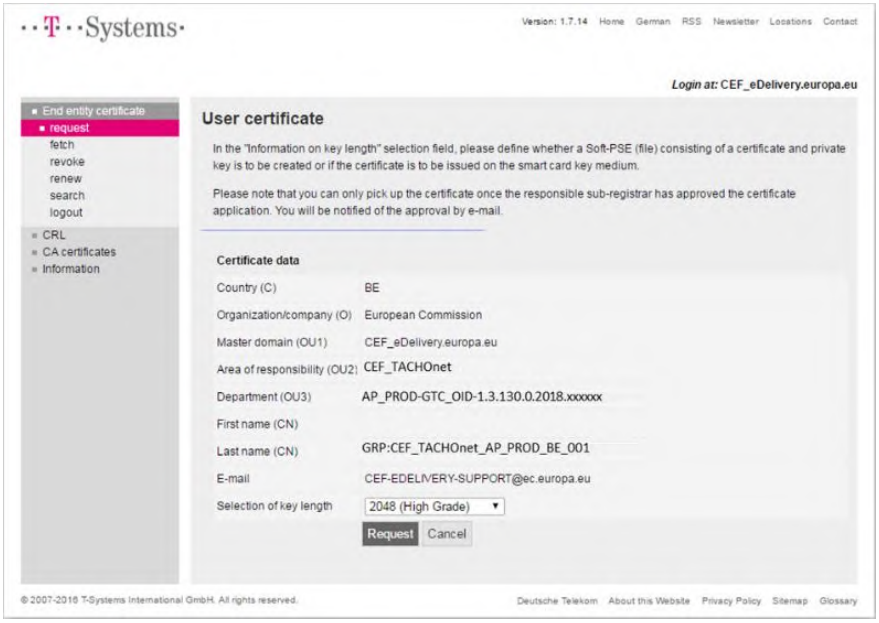


Illustration 5

e) L'organisation enregistre le numéro de référence afin de récupérer le certificat.

Illustration 6

f) L'équipe de soutien du MIE contrôle les nouvelles demandes de certificats et vérifie si les informations contenues dans la demande de certificat sont valides, c'est-à-dire si elles sont conformes à la convention de dénomination établie à l'appendice 5.1 Convention de dénomination du certificat.

g) L'équipe de soutien du MIE vérifie que les informations contenues dans la demande sont dans un format valide.

h) En cas d'échec de l'une ou l'autre des vérifications prévues aux points 5 ou 6 ci-dessus, l'équipe de soutien du MIE envoie un courrier électronique à l'adresse électronique fournie dans les "Données d'identification" du formulaire de demande, avec le propriétaire du domaine en copie, dans lequel l'organisation est invitée à recommencer la procédure. La demande de certificat rejetée est annulée.

i) L'équipe de soutien du MIE envoie un courrier électronique à l'autorité d'enregistrement concernant la validité de la demande. Le courrier électronique doit comprendre:

    1) le nom de l'organisation, qui se trouve dans le champ "Organisation (O)" de la demande de certificat;

    2) les données relatives au certificat, notamment le nom du PA pour lequel le certificat doit être délivré, disponible dans le champ "Last Name (CN)" (nom de famille) de la demande de certificat;

    3) le numéro de référence du certificat;

    4) l'adresse de l'organisation, son adresse de courrier électronique et le nom de la personne qui la représente.

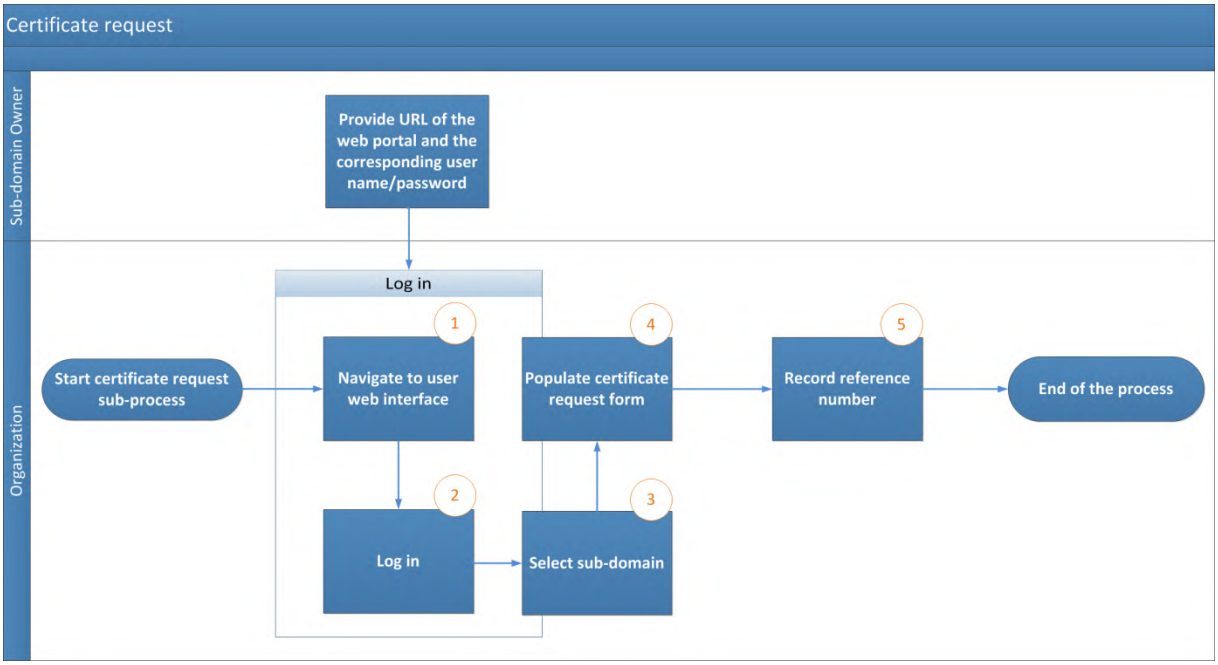


Illustration 7 – Processus de demande de certificat

2.2.4. Étape 3: Enregistrement auprès de l'autorité d'enregistrement (approbation du certificat)

2.2.4.1. Le coursier de confiance ou le point de contact prend rendez-vous avec l'autorité d'enregistrement par échange de courriels, et identifie le coursier de confiance qui participera à la réunion en face à face.

2.2.4.2. L'organisation prépare la documentation, qui consiste en:

a) le mandat complété et signé;

b) une copie du passeport en cours de validité du coursier de confiance qui participera à la réunion en face à face. Cette copie doit être signée par l'un des points de contact de l'organisation identifiés à l'étape 1;

c) le formulaire papier de demande de certificat, signé par l'un des points de contact de l'organisation.

2.2.4.3. L'autorité d'enregistrement reçoit le coursier de confiance après un contrôle d'identité à la réception du bâtiment. L'autorité d'enregistrement effectue l'enregistrement en face à face de la demande de certificat en:

a) identifiant et authentifiant le coursier de confiance;

b) comparant l'apparence physique du coursier de confiance avec la photo figurant sur le passeport présenté par le coursier de confiance;

c) vérifiant la validité du passeport présenté par le coursier de confiance;

d) comparant le passeport validé présenté par le coursier de confiance avec la copie du passeport valide du coursier de confiance qui a été signée par l'un des points de contact identifiés de l'organisation. La signature est authentifiée par comparaison avec le "formulaire d'identification du coursier de confiance et des points de contact" original;

e) vérifiant le mandat complété et signé;

f) vérifiant le formulaire papier de demande de certificat et sa signature en la comparant à celle figurant sur le "formulaire d'identification du coursier de confiance et des points de contact" original;

g) invitant le point de contact signataire à vérifier une nouvelle fois l'identité du coursier de confiance et le contenu de la demande de certificat.

2.2.4.4. L'autorité d'enregistrement confirme à l'équipe de soutien du MIE que l'autorité nationale est effectivement autorisée à exploiter les composants pour lesquels elle demande les certificats et que le processus d'enregistrement en face à face correspondant a été couronné de succès. La confirmation est envoyée par courrier électronique sécurisé au moyen d'un certificat "CommiSign", accompagné d'une copie scannée de la documentation authentifiée en face à face et de la liste de contrôle du processus signée et effectuée par l'autorité d'enregistrement.

2.2.4.5. Si l'autorité d'enregistrement confirme la validité de la demande, le processus se poursuit conformément aux points 2.2.4.6 et 2.2.4.7. Dans le cas contraire, la délivrance du certificat est rejetée et l'organisation en est informée.

2.2.4.6. L'équipe de soutien du MIE approuve la demande de certificat et informe l'autorité d'enregistrement de l'approbation du certificat.

2.2.4.7. L'autorité d'enregistrement informe l'organisation que le certificat peut être récupéré via le portail utilisateur.

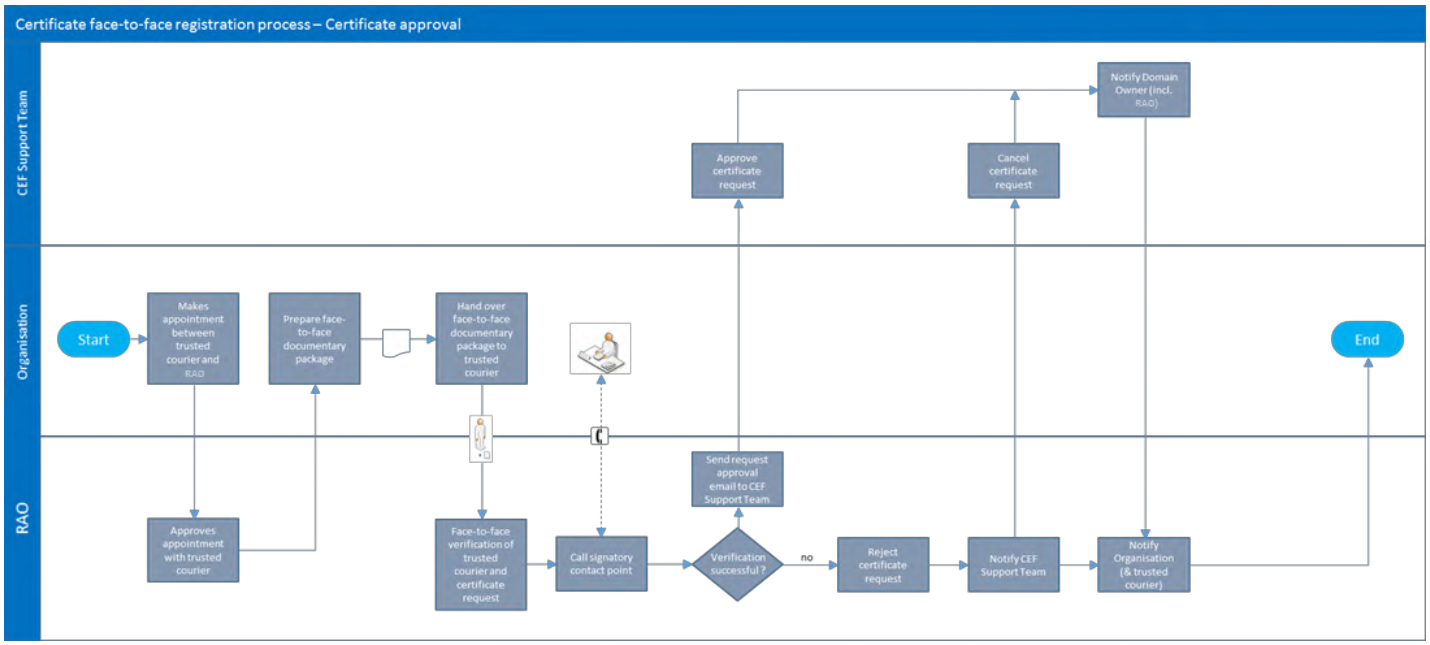


Illustration 8 – Approbation du certificat

2.2.5. Étape 4: Génération du certificat

Dès l'approbation de la demande de certificat, le certificat est généré.

2.2.6. Étape 5: Publication et récupération du certificat

2.2.6.1. Dès l'approbation de la demande de certificat, l'autorité d'enregistrement récupère le certificat et en remet une copie au coursier de confiance.

2.2.6.2. L'organisation est informée par l'autorité d'enregistrement que les certificats peuvent être récupérés.

2.2.6.3. L'organisation se rend sur le portail utilisateur, à l'adresse https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en et se connecte avec le nom d'utilisateur **"sbca/CEF_eDelivery.europa.eu"** et le mot de passe **"digit.333"**.

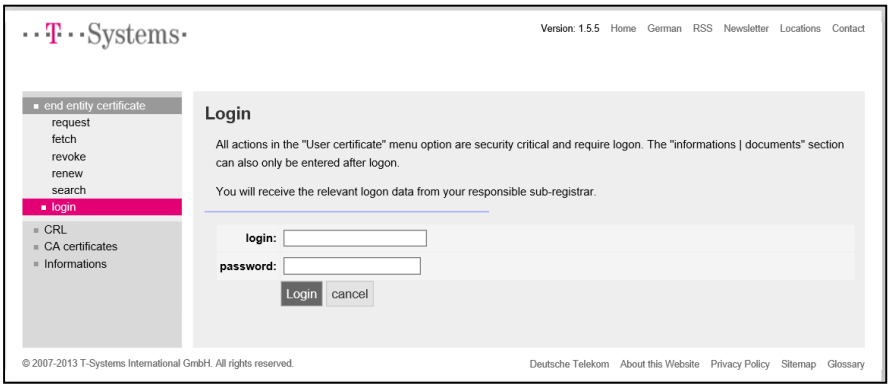


Illustration 9

2.2.6.4. L'organisation clique sur l'onglet "fetch" (récupérer) dans le menu à gauche et introduit le numéro de référence enregistré durant le processus de demande de certificat;

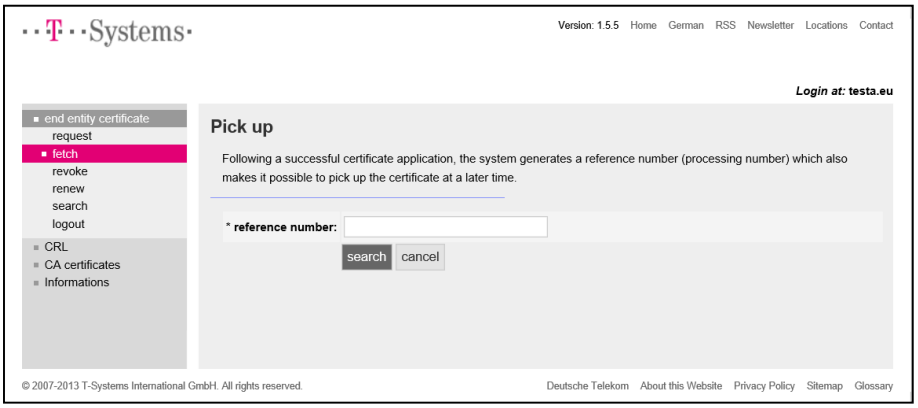


Illustration 10

2.2.6.5. l'organisation installe les certificats en cliquant sur l'onglet "install" (installer);

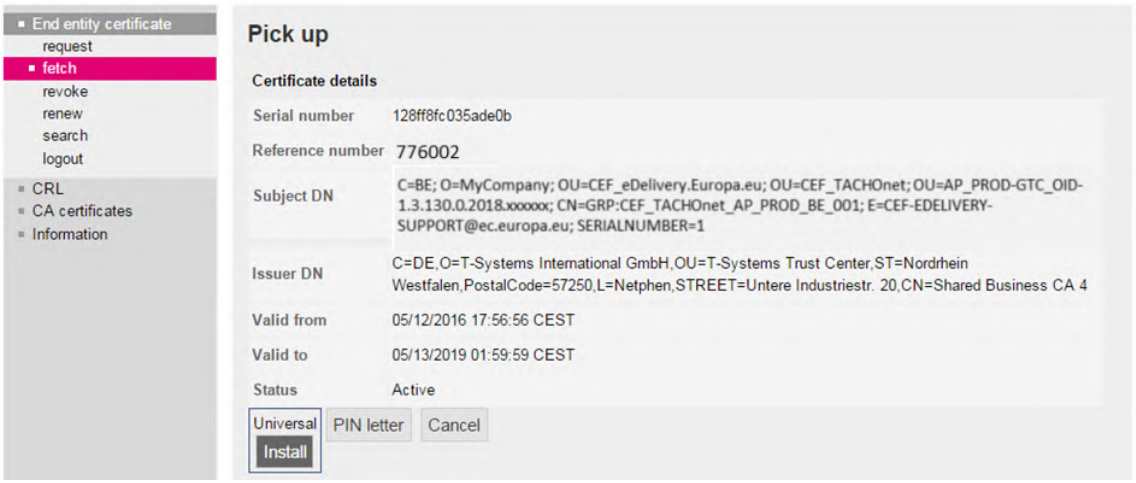


Illustration 11

2.2.6.6. le certificat est installé sur l'Access Point. Comme l'installation est spécifique à la mise en œuvre, l'organisation doit se référer à son fournisseur de point d'accès pour obtenir la description de ce processus.

2.2.6.7. Les étapes suivantes doivent être suivies pour installer le certificat sur le point d'accès:

a) exporter la clé privée et le certificat,

b) créer le keystore et le truststore,

c) installer le keystore et le truststore sur le point d'accès.

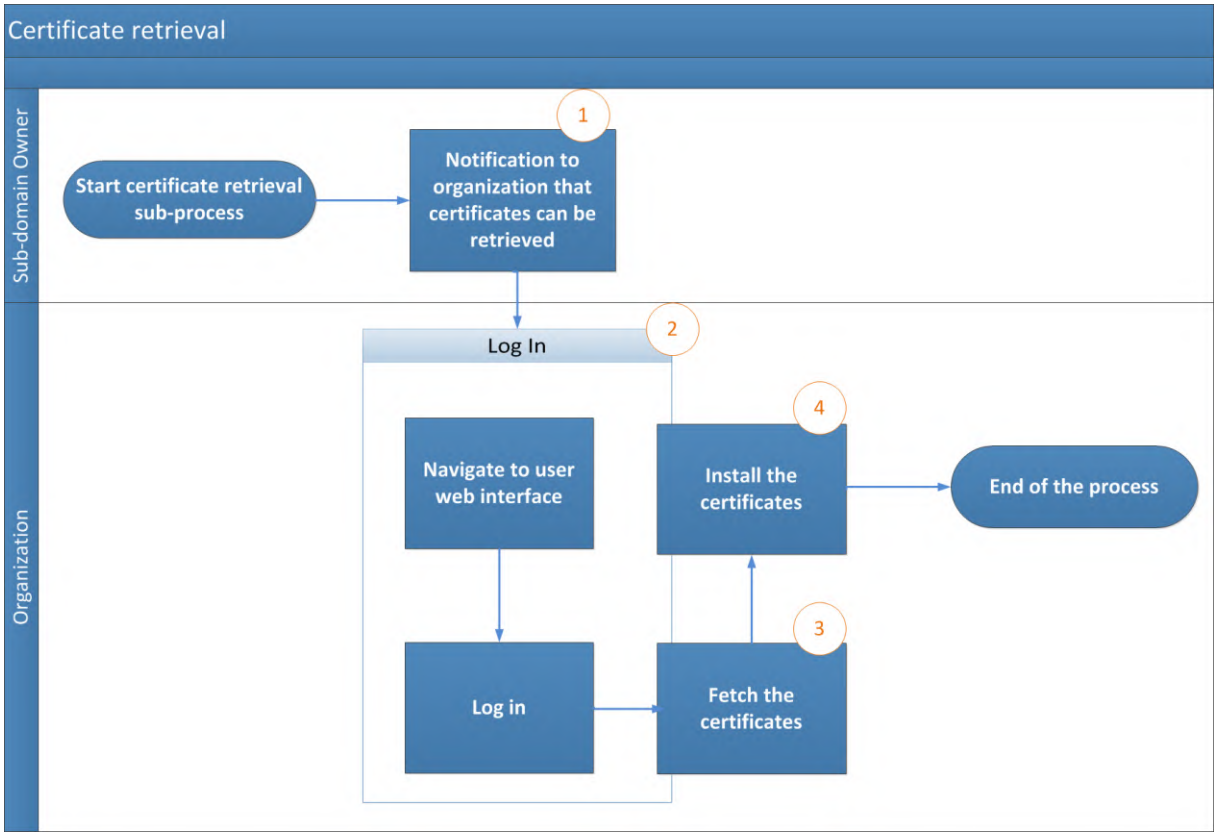


Illustration 12 – Récupération du certificat

3. Processus de révocation du certificat

3.1. L'organisation introduit une demande de révocation via le portail utilisateur;

3.2. l'équipe de soutien du MIE exécute la révocation du certificat.

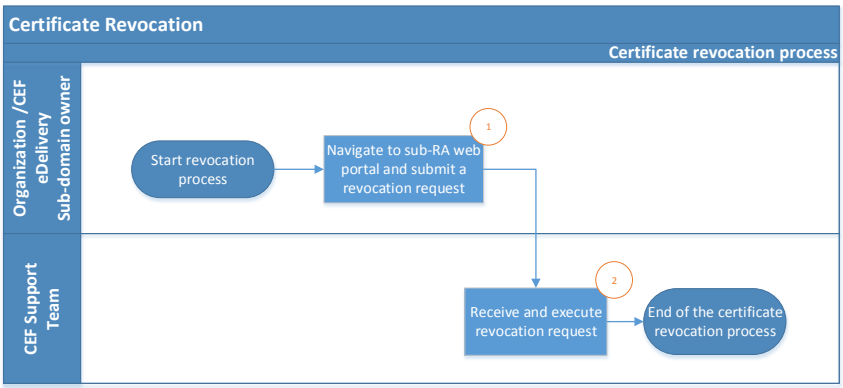


Illustration 13 – Révocation du certificat

4. Modalités et conditions générales du service CEF ICP

4.1. Contexte

En sa capacité de fournisseur de solution du module eDelivery du mécanisme pour l'interconnexion en Europe (MIE), la DIGIT met à la disposition des parties contractantes à l'AETR un service d'ICP[7] ("service MIE ICP"). Le service MIE ICP est utilisé par les autorités nationales ("utilisateurs finaux") participant à TACHOnet.

La DIGIT est un utilisateur de la solution TeleSec Shared-Business-CA ("SBCA") exploitée au sein du Trust Centerde l'unité de groupe T-Systems International GmbH ("T-Systems"[8]). La DIGIT joue le rôle de Master Registrar du domaine "CEF_eDelivery.europa.eu" de la SBCA. À ce titre, la DIGIT crée des sous-domaines au sein du domaine "CEF_eDelivery.europa.eu" pour chaque projet utilisant le service CEF ICP.

Le présent document fournit des détails sur les modalités et les conditions du sous-domaine TACHOnet. La DIGIT joue le rôle de sous-registraire de ce sous-domaine. En cette qualité, elle délivre, révoque et renouvelle les certificats de ce projet.

4.2. Exclusion de responsabilité

La Commission européenne décline toute responsabilité quant au contenu du certificat, qui relève exclusivement du détenteur du certificat. Il incombe au détenteur du certificat de vérifier l'exactitude du contenu du certificat.

La Commission européenne décline toute responsabilité quant à l'utilisation du certificat par son détenteur qui est une entité juridique tierce extérieure à la Commission européenne.

---

7 Une ICP (infrastructure à clé publique) est un ensemble de rôles, de politiques, de procédures et de systèmes nécessaires à la gestion, à la distribution et à la révocation des certificats numériques.

8 Le rôle de confiance de l'opérateur de Trust Center, situé dans le Trust Center de T-Systems, effectue également la tâche d'autorité d'enregistrement interne.

La présente clause de non-responsabilité n'a pas pour but de limiter la responsabilité de la Commission européenne de manière contraire aux exigences énoncées dans les législations nationales applicables ou d'exclure sa responsabilité dans les cas où elle ne peut l'être en vertu desdites législations.

4.3. Utilisations autorisées/interdites des certificats

4.3.1. Usage permis des certificats

Une fois le certificat délivré, le détenteur du certificat[9] utilisera le certificat uniquement dans le contexte de TACHOnet. Dans ce contexte, le certificat peut être utilisé afin:

- d'authentifier l'origine des données;
- de chiffrer des données;
- de garantir la détection des atteintes à l'intégrité des données.

4.3.2. Usage interdit des certificats

Toute utilisation non explicitement autorisée parmi les utilisations autorisées du certificat est interdite.

4.4. Autres obligations du détenteur de certificat

Les modalités et les conditions détaillées de la SBCA sont définies par T-Systems dans la politique de certification (PC)/la déclaration d'activité de certification (CPS) du service SBCA[10]. Le présent document comprend des spécifications et des lignes directrices en matière de sécurité concernant les aspects techniques et organisationnels et décrit les activités de l'opérateur du Trust Centre dans les rôles d'autorité de certification (AC) et d'autorité d'enregistrement (AE) ainsi que de tiers délégué par l'autorité d'enregistrement (AE).

Seules les entités autorisées à participer à TACHOnet peuvent demander un certificat.

[9] Identifié par la valeur d'attribut "O=" dans le Subject Distinguished Name du certificat émis.
[10] La dernière version de la PC et de la CPS du service SBCA de T-Systems est disponible sur https://www.telesec.de/en/sbca-en/support/download-area/.

En ce qui concerne l'acceptation du certificat, la clause 4.4.1 de la politique de certification et de la déclaration d'activité de certification ("PC/CPS") de la SBCA s'applique. En outre, les conditions d'utilisation et les dispositions décrites dans le présent document sont réputées acceptées par l'organisation à laquelle le certificat est délivré ("O=") lorsqu'elles sont utilisées pour la première fois.

En ce qui concerne la publication du certificat, la clause 2.2 de la PC/CPS de la SBCA s'applique.

Tous les détenteurs de certificat doivent satisfaire aux exigences suivantes:

1) protègent leurs clés privées contre toute utilisation non autorisée;

2) s'abstenir de transférer ou de révéler leurs clés privées à des tiers, même en tant que représentants;

3) s'abstenir de poursuivre l'utilisation de la clé privée après l'échéance de la période de validité ou après la révocation du certificat, à des fins autres que la visualisation des données chiffrées (p.ex. déchiffrage de courriels);

4) le détenteur de certificat est responsable de la copie ou du transfert de la clé à l'entité finale ou aux entités finales;

5) le détenteur de certificat doit obliger l'entité finale/toutes les entités finales à respecter les présentes modalités et conditions, dont la PC/la CPS de la SBCA, lorsqu'elles sont confrontées à la clé privée.

6) Le détenteur du certificat doit fournir l'identification des représentants autorisés qui sont habilités à demander la révocation des certificats délivrés à l'organisation ainsi que les détails des événements qui ont conduit à la révocation et le mot de passe de révocation;

7) pour les certificats associés à des groupes de personnes et des fonctions et/ou à des personnes morales, après qu'une personne quitte le groupe d'entités finales (par exemple, cessation de la relation de travail), le détenteur du certificat doit empêcher toute utilisation abusive de la clé privée en révoquant le certificat.

8) Le détenteur de certificat est responsable de la demande de révocation du certificat dans les conditions visées dans la clause 4.9.1 de la PC/CPS de la SBCA.

En ce qui concerne le renouvellement ou la création d'une nouvelle clé pour des certificats, la clause 4.6 ou 4.7 de la PC/CPS de la SBCA s'applique.

En ce qui concerne la modification du certificat, la clause 4.8 de la PC/CPS de la SBCA s'applique.

En ce qui concerne la révocation du certificat, la clause 4.9 de la PC/CPS de la SBCA s'applique.

5. Formulaire d'identification des personnes de contact et des coursiers de confiance (exemple)

Je soussigné, *[nom et adresse du représentant de l'organisation]***, certifie que les informations ci-après seront utilisées dans le contexte de la demande, de la génération et de la récupération de certificats numériques de clés publiques pour les points d'accès TACHOnet soutenant la confidentialité, l'intégrité et la non-répudiation des messages TACHOnet:**

Coordonnées de la personne de contact

– **Personne de contact #1**	– **Personne de contact #2**
– Nom:	– Nom:
– Prénom(s):	– Prénom(s):
– Téléphone portable:	– Téléphone portable:
– Téléphone:	– Téléphone:
– Courriel:	– Courriel:
– Signature manuscrite: –	– Signature manuscrite: – – –

Coordonnées du coursier de confiance:

– **Coursier de confiance #1**	– **Coursier de confiance #2**
– Nom:	– Nom:
– Prénom(s):	– Prénom(s):
– Téléphone portable:	– Téléphone portable:
– Courriel:	– Courriel:
– Pays de délivrance du passeport:	– Pays de délivrance du passeport:
– Numéro de passeport:	– Numéro de passeport:
– Date de fin de validité du passeport:	– Date de fin de validité du passeport:

Lieu, date, cachet de l'entreprise ou sceau de l'organisation:

Signature du représentant habilité:

6. Documents

6.1. Mandat individuel (modèle)

Un modèle de mandat individuel qui doit être signé et présenté par le coursier de confiance lors de l'enregistrement en face à face chez l'ordonnateur régional est disponible ici:

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. Formulaire papier de demande de certificat (modèle)

Un modèle de formulaire papier de demande de certificat qui doit être signé et présenté par le coursier de confiance lors de l'enregistrement en face à face chez l'ordonnateur régional est disponible ici:

7. Glossaire

Les principaux termes utilisés dans le présent sous-appendice sont définis dans la section "CEF Definitions" sur le portail web unique CEF Digital:

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

Les principaux acronymes utilisés dans le présent sous-appendice sont définis dans le glossaire CEF sur le portail web unique CEF Digital:

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