Nations Unies ECE/TRANS/SC.1/GE.21/2019/1/Rev.3

Conseil économique et social

Distr. générale
30 juillet 2021
Français
Original : anglais

Commission économique pour l'Europe

Comité des transports intérieurs

Groupe de travail des transports routiers

Groupe d'experts de l'Accord européen relatif au travail des équipages des véhicules effectuant des transports internationaux par route (AETR)

Vingt-septième session
Genève, 12 octobre 2021
Point 4 de l'ordre du jour provisoire

Système TACHOnet

Communication du Portugal

Le présent document, soumis par le Portugal en sa qualité de pays occupant la présidence de l'Union européenne, contient la version révisée d'un projet de nouvel appendice à l'AETR concernant le système TACHOnet. Il est fondé sur le document informel n° 3 (juin 2021) portant modification du document ECE/TRANS/SC.1/GE.21/2019/Rev.2.

Nouvel appendice à l'AETR

Appendice 4

Spécifications du système d'échange électronique d'informations sur les cartes de conducteur ~~TACHOnet~~

1. Champ d'application et objet

1.1 Le présent appendice établit les modalités et les conditions de connexion des Parties contractantes à l'AETR au système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ par l'intermédiaire du service eDelivery.

1.2 Les Parties contractantes qui se connectent au système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ par l'intermédiaire du service eDelivery respectent les dispositions établies dans le présent appendice.

2. Définitions

Au sens du présent appendice, on entend :

a) Par « Partie contractante » ou « partie », toute Partie contractante à l'AETR ;

b) Par « eDelivery », le service, mis au point par la Commission européenne, qui permet à des tiers d'échanger des données par voie électronique, qui conserve une trace officielle du traitement des données transmises et, notamment, atteste de leur envoi et de leur réception, et qui empêche toute modification non autorisée de ces données ;

~~c) Par « système TACHOnet », le système d'échange électronique entre Parties contractantes d'informations sur les cartes de conducteur mis en place par la Commission européenne ;~~

c~~d~~) Par « 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) Par « partie demandeuse », la Partie contractante qui émet une demande ou une notification ~~TACHOnet~~, qui est ensuite acheminée par le système central jusqu'à la partie destinataire concernée ;

f) Par « partie destinataire », la Partie contractante à laquelle la demande ou la notification ~~TACHOnet~~ est destinée ;

g) Par « autorité de délivrance des cartes », une entité habilitée par une Partie contractante à délivrer et à gérer des cartes tachygraphiques ;

h)' Par « personne concernée », une personne physique dont les données sont échangées au moyen du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ ;

h) Par « donnée à caractère personnel », toute information échangée au moyen du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ pouvant conduire à l'identification de la personne concernée, comme un nom ou un numéro d'identification ;

i) Par « violation de données à caractère personnel », une violation de la sécurité entraînant accidentellement ou de manière illicite la destruction, la perte, l'altération, la divulgation ou l'accès non autorisés à des données à caractère personnel transmises, stockées ou autrement traitées ;

j) Par « traitement automatique », les opérations suivantes, effectuées en totalité ou en partie à l'aide de procédés automatisés : enregistrement des données, application à ces données d'opérations logiques et/ou arithmétiques, leur modification, effacement, extraction ou diffusion.

3. Responsabilités générales

3.1 Aucune des Parties contractantes n'est autorisée à conclure des accords visant à accéder au système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ au nom d'une autre partie ni à représenter de quelque manière que ce soit 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 par le présent appendice.

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

3.3 Les Parties contractantes doivent s'informer 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 du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~.

3.4 Chaque partie doit désigner des personnes à contacter concernant le système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ et en informer le secrétariat de l'AETR. Tout changement en la matière doit impérativement être notifié par écrit au secrétariat de l'AETR.

4. Essais de connexion au système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~

4.1 La connexion d'une Partie contractante au système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ sera établie après que les essais de connexion, d'intégration et de performance auront 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 seront repris une fois que la Partie contractante aura informé la Commission européenne que les améliorations techniques requises au niveau national pour le bon déroulement des essais préliminaires ont été effectuées.

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

5. Architecture sécurisée

5.1 La confidentialité, l'intégrité et la non-révocation des messages ~~TACHOnet~~ sont assurées par l'architecture sécurisée du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~.

5.2 L'architecture sécurisée du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ est fondée sur un service d'infrastructure à clef 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 doivent contribuer à l'architecture sécurisée du système ~~TACHOnet~~ :

a) L'autorité de certification, responsable de l'émission des certificats numériques devant être délivrés **(une fois que la demande a été validée par l'instance de validation des demandes)** ~~par l'autorité d'enregistrement aux~~ **pour téléchargement par les** autorités nationales des Parties contractantes (par l'intermédiaire ~~de messagers certifiés qu'elles auront désignés~~ **du portail en ligne du système d'ICP de l'autorité de certification**), ainsi que de la mise en place de l'infrastructure technique concernant la délivrance, la révocation et le renouvellement des certificats numériques ;

b) Le 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 sécurisée ~~du système TACHOnet~~ ;

c) ~~L'autorité d'enregistrement, chargée d'enregistrer et d'approuver les demandes de délivrance, de révocation et de renouvellement des certificats numériques, ainsi que de vérifier l'identité des messagers certifiés~~**L'instance de validation des demandes, chargée d'authentifier l'identité de l'organisme demandeur, de ses points de contact et de ses messagers certifiés. Dans le cadre des sessions ordinaires de l'ERCA, les autorités nationales compétentes pourront soumettre, par l'intermédiaire du messager certifié de l'ERCA, des demandes de certificat à valider. Le CCR validera les demandes de certificat au cours de l'appel téléphonique de validation passé au point de contact de l'ERCA (officiellement désigné par l'Autorité des États membres) à l'occasion des sessions de l'ERCA** ;

d) **Le messager certifié, personne physique désignée par l'autorité nationale et chargée d'authentifier la demande de certificat pour l'instance de validation des demandes et d'obtenir le certificat correspondant auprès de l'autorité de certification** ~~est la personne désignée par les autorités nationales pour remettre la clef publique à l'autorité d'enregistrement et obtenir le certificat correspondant émis par l'autorité de certification~~ ;

e) L'autorité nationale de la Partie contractante, qui devra :

i) Créer les clefs privées et les clefs publiques correspondantes qui doivent figurer dans les certificats émis par l'autorité de certification ;

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

iii) Désigner le messager certifié.

5.4 L'autorité de certification et ~~l'autorité d'enregistrement~~ **l'instance de validation des demandes** seront désignées par la Commission européenne.

5.5 Toute Partie contractante qui se connecte au système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ doit demander la délivrance d'un certificat numérique conformément au sous-appendice 4.9, afin de pouvoir signer et 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, doivent adopter toutes les mesures techniques et

organisationnelles nécessaires pour garantir la sécurité des données du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ et en empêcher la modification, la perte ou le traitement non autorisé ou encore l'accès non autorisé à ces données (notamment en ce qui concerne l'authenticité, la confidentialité, la traçabilité, l'intégrité, la disponibilité et la non-révocation des données, ainsi que la sécurité des messages).

6.2 Si une partie prend conscience d'une violation des données à caractère personnel, elle informera la Commission européenne dans les meilleurs délais et utilisera un moyen raisonnable et approprié pour remédier à cette violation et en minimiser les effets négatifs potentiels.

6.3 Les parties doivent permettre à la personne concernée dont les données à caractère personnel ont été obtenues au moyen du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ :

Article I a) D'obtenir la confirmation que les données à caractère personnel qui la concernent sont conservées dans un fichier ainsi que de se voir communiquer ces données sous une forme concise, transparente, intelligible et facilement accessible ;

Article II b) D'obtenir, le cas échéant, la rectification sans délai des données à caractère personnel inexactes ;

Article III c) D'obtenir, le cas échéant, l'effacement des données à caractère personnel si la personne concernée n'en a plus besoin ou si elles ont fait l'objet d'un traitement illicite ou en violation des principes de base énoncés dans les articles 5 et 6 de la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (ci-après « la Convention ») ;

Article IV d) S'opposer à tout moment, pour des raisons tenant à sa situation particulière, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement par une partie ;

Article V 6.4 Lorsque le traitement automatisé de données à caractère personnel obtenues au moyen du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ est nécessaire, il doit être effectué conformément à la Convention.

6.5 Les parties doivent identifier toute donnée à caractère personnel transmise à une partie requérante par l'intermédiaire du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ et fournir des informations générales, comme par exemple sur un site Web, à propos des mesures de protection applicables aux transferts à d'autres parties.

6.6 La partie destinataire ne doit transférer des données à caractère personnel au moyen du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ que dans le but spécifique et légitime d'aider la partie demandeuse à s'acquitter de ses obligations au titre du présent Accord. La partie demandeuse ne procédera pas à un traitement ultérieur des données à caractère personnel d'une manière qui soit incompatible avec cet objectif.

6.7 La partie destinataire ne doit transférer des données à caractère personnel que conformément au présent Accord.

6.8 La partie demandeuse qui reçoit des données à caractère personnel par l'intermédiaire du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ ne doit transférer ces données qu'à une tierce partie qui soit un organisme national compétent chargé de contrôler et de faire respecter les temps de conduite et les périodes de repos conformément au présent Accord.

6.9 La partie demandeuse doit conserver les données à caractère personnel pendant une durée n'excédant pas celle qui est appropriée et nécessaire à la réalisation de la finalité pour laquelle elles sont traitées. Cette période de conservation doit être conforme aux lois, règles et règlements qui régissent la conservation de telles données dans la juridiction de la partie demandeuse.

7. Coûts

7.1 Les Parties contractantes supporteront à elles seules les coûts de développement et d'exploitation relatifs aux procédures et systèmes de données propres dont elles ont besoin pour s'acquitter des obligations découlant du présent appendice.

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

8. Sous-traitance

8.1 Les parties peuvent passer des contrats de sous-traitance pour tout service dont elles sont responsables en vertu du présent appendice.

8.2 Le recours à la sous-traitance ne dégage pas la partie de la responsabilité qui lui incombe en vertu du présent appendice, y compris en ce qui concerne le niveau de service approprié conformément au sous-appendice 4.6.

Sous-appendice 4.1

Aspects généraux du système d'échange électronique d'informations sur les cartes de conducteur ~~TACHOnet~~

1. Description générale

Le système **d'échange électronique d'informations sur les cartes de conducteur** ~~électronique TACHOnet~~ permet l'échange d'informations sur les cartes de conducteur. Il achemine les demandes d'information des parties demandeuses aux parties destinataires, ainsi que les réponses de ces dernières. Les Parties contractantes qui utilisent le système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ doivent connecter au système leurs registres nationaux d'informations sur les cartes de conducteur.

2. Architecture

Le système d'échange **électronique d'informations sur les cartes de conducteur** ~~de messages TACHOnet~~ se compose des éléments suivants :

2.1 Un système central qui peut recevoir une demande de la partie demandeuse, la valider et la traiter en la transmettant aux parties destinataires. Ce système attend que chaque partie destinataire ait répondu, puis elle procède à une synthèse des réponses, qu'elle transmet ensuite à la partie demandeuse ;

2.2 Les systèmes nationaux des parties possèdent une interface qui leur permet 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 sera géré par la Commission européenne, qui assurera son fonctionnement et sa maintenance.

3.2 Le système central ne conservera pas de données pendant plus de six mois, à l'exception du journal et des données statistiques définis au sous-appendice 4.7.

3.3 Le système central n'autorisera l'accès aux données à caractère personnel qu'au personnel de la Commission européenne dûment autorisé qui pourrait en avoir besoin pour des interventions de contrôle, de maintenance et de dépannage.

3.4 Il incombera aux Parties contractantes :

3.4.1 D'assurer la configuration et la gestion de leurs systèmes nationaux, y compris 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 de leurs systèmes nationaux avec le système central, y compris la gestion des messages d'erreur qu'il envoie ;

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 du système d'échange électronique d'informations sur les cartes de conducteur ~~TACHOnet~~

1. Le système d'échange **électronique d'informations sur les cartes de conducteur** ~~de messages TACHOnet~~ offrira les fonctionnalités ou informations suivantes :

1.1 Vérification des délivrances de cartes (Check Issued Cards − CIC) : permet à la partie demandeuse d'envoyer une « demande de vérification des délivrances de cartes » 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 qu'elles auraient délivrée. Les parties destinataires donnent suite à la demande en envoyant une « réponse à la demande de vérification des délivrances de cartes ».

1.2 Vérification de la situation de la carte (Check Card Status − CCS) : permet à la partie demandeuse de solliciter auprès de la partie destinataire des informations sur une carte qu'elle a délivrée en lui envoyant une « demande de vérification de la situation de la carte ». La partie destinataire donne suite à la demande en envoyant une « réponse à la demande de vérification de la situation de la carte ».

1.3 Modification de la situation 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 de la situation de la carte », la modification de la situation d'une carte qu'elle a délivrée. La partie destinataire y donne suite par un « accusé de réception de la demande de modification de la situation de la carte ».

1.4 Permis de conduire correspondant à la carte délivrée (Issued Card Driving License − ICDL) : permet à la partie demandeuse de notifier à la partie destinataire, via une « demande concernant le permis de conduire correspondant à la carte délivrée », qu'une carte a été délivrée par la partie demandeuse sur la foi d'un permis de conduire délivré par la partie destinataire. Cette dernière y donne suite par une « réponse concernant le permis de conduire correspondant à la carte délivrée ».

2. D'autres types de messages jugés nécessaires au bon fonctionnement du système d'échange **électronique d'informations sur les cartes de conducteur** ~~de messages TACHOnet~~ sont prévus, comme les notifications d'erreur.

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

4. Lorsqu'une partie reçoit une réponse ou une notification indiquant une situation que son système administratif national ne mentionne pas, ce système doit attribuer à la carte une situation appropriée qu'il reconnaît. La partie destinataire ne doit pas rejeter le message dès lors que la situation signalée dans ce message est mentionnée dans le tableau 1.

5. Les situations de cartes mentionnées dans le tableau 1 ne doivent pas servir à 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 un champ réservé à l'information « valable pour la conduite ». Les procédures administratives nationales sont telles que les réponses CCS contiennent toujours la valeur appropriée pour le champ « valable pour la conduite ».

Tableau 1
Les différentes situations d'une carte

Situation de la carte	**Définition**
Demandée	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 clefs de recherche générées.
Demande approuvée	L'autorité de délivrance des cartes a approuvé la demande de carte tachygraphique.
Demande rejetée	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, à laquelle il a été déclaré qu'elle n'était plus 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. Les données de la nouvelle carte restent les mêmes, excepté l'indice de renouvellement du numéro de la carte qui a été incrémenté d'une unité.

Situation de la carte	Définition
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 du système d'échange électronique d'informations sur les cartes de conducteur ~~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 la technologie 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.

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

2.4 Les messages XML doivent satisfaire au moins aux exigences minimales fixées 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
Identificateur d'essai	Identificateur facultatif à des fins d'essai. L'initiateur de l'essai saisira l'identificateur et tous les acteurs intervenant dans la succession des tâches devront transmettre/renvoyer le même identificateur. Dans la production il ne faut pas en tenir compte et il ne sera donc pas utilisé à cette fin s'il est fourni.	Non
Identificateur technique	Il s'agit d'un UUID qui ne sert à identifier qu'un seul message. L'expéditeur crée un UUID et renseigne cet attribut. Ces données ne sont pas utilisées à des fins opérationnelles.	Oui
Identificateur du flux d'information	L'identificateur du flux d'information est un UUID qui doit être créé par la partie demandeuse. Il est ensuite utilisé dans tous les messages pour corréler le flux d'information.	Oui
Envoyé à	Date et heure (GMT) auxquelles le message a été envoyé.	Oui

En-tête commun		*Obligatoire*
Délai d'expiration	Il s'agit d'un attribut de date et d'heure facultatif (au format TUC). Cette valeur ne sera définie par le système central que pour les demandes transmises. Elle indiquera à la partie destinataire le délai d'expiration de la demande. Elle n'est pas requise en MS2TCN_<x>_Req ni dans tous les messages de réponse. Elle est proposée en option afin de permettre l'utilisation de la même définition d'en-tête dans tous les types de messages, que l'attribut « Valeur de délai d'expiration » soit requis ou non.	Non
De	Le code pays ISO 3166-1 alpha 2 de la partie à l'origine du message ou « UE ».	Oui
À	Le code pays 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 du registre national.

2. Lors de la recherche d'une carte via la fonctionnalité CIC, les clefs 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 doivent préciser le mécanisme de recherche utilisé pour trouver une entrée, à savoir NYSIIS ou personnalisé.

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

Sous-appendice 4.5

Exigences en matière de sécurité

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

2. Les systèmes nationaux utiliseront 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 mettront en œuvre, au minimum, des certificats utilisant l'algorithme de hachage de signature SHA-2 (SHA-256) et une longueur de clef publique de 2 048 bits.

Sous-appendice 4.6

Niveaux de service

1. Les systèmes nationaux doivent satisfaire au niveau de service minimal suivant :

1.1 Ils doivent être disponibles 24 heures sur 24, 7 jours sur 7.

1.2 Leur disponibilité doit être contrôlée par un message de pulsation émis depuis le système central.

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

	Correspond à une indisponibilité de		
Disponibilité de	*Par jour*	*Par mois*	*Par an*
98 %	0,5 heure	15 heures	7,5 jours

Les parties sont invitées à respecter le taux de disponibilité journalier. Toutefois, il est admis que certaines activités nécessaires, telles que la maintenance du système, requièrent un temps d'arrêt de plus de 30 min. Toutefois, les taux de disponibilité mensuel et annuel doivent rester stricts.

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

1.5 Ils doivent répondre aux demandes en moins de 10 s.

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

1.7 Les systèmes doivent être en mesure de répondre à 6 messages de demandes par seconde.

1.8 Les systèmes nationaux ne doivent pas envoyer plus de 2 demandes par seconde au **système central** ~~serveur TACHOnet~~.

1.9 Chaque système national doit pouvoir faire face aux problèmes techniques éventuels du système central ou des systèmes nationaux des autres parties. Ces problèmes peuvent être notamment :

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 valides.

2. Le système central doit :

2.1 Présenter un taux de disponibilité de 98 % ;

2.2 Notifier les erreurs aux systèmes nationaux, soit dans le message de réponse, soit par un message d'erreur spécifique. Les systèmes nationaux, en retour, doivent être en mesure de recevoir ces messages d'erreur spécifiques et disposer d'une procédure graduée permettant de prendre les mesures appropriées pour corriger l'erreur notifiée.

3. Maintenance

Les parties doivent prévenir les autres parties et la Commission européenne de toutes les activités de maintenance de routine, via l'application Web, une semaine au moins avant le début de ces activités, si c'est techniquement possible.

Sous-appendice 4.7

Informations de connexion et statistiques sur les données collectées au niveau du système central

1. Dans un souci de confidentialité, les données utilisées à des fins statistiques doivent être anonymes. Les données permettant d'identifier une carte, un conducteur ou un permis de conduire spécifique ne doivent pas être communiquées à des fins statistiques.

2. Les informations de connexion doivent permettre de conserver la trace de toutes les opérations effectuées, à des fins de contrôle ou de débogage, ainsi que de produire des statistiques relatives à ces opérations.

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

4. Les informations suivantes doivent être utilisées pour les statistiques :

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 clefs et aux certificats numériques ~~pour TACHOnet~~

1. La Direction générale de l'informatique (DIGIT) de la Commission européenne mettra un service ICP[1] (dénommé ci-après le « service MIE ICP ») à la disposition des Parties contractantes à l'AETR qui se connectent au système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ (désormais les autorités nationales) par l'intermédiaire du service 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 au sous-appendice 4.9.

3. Utilisation des certificats :

3.1 Une fois le certificat délivré, l'autorité nationale[2] doit l'utiliser uniquement dans le cadre du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~. Il peut être utilisé pour :

a) Authentifier l'origine des données ;

b) Chiffrer des données ;

c) Détecter des atteintes à l'intégrité des données.

3.2 Toute utilisation qui n'est pas explicitement mentionnée dans la liste des utilisations autorisées du certificat est interdite.

4. Les Parties contractantes doivent :

a) Protéger leurs clefs privées contre toute utilisation non autorisée ;

b) S'abstenir de transférer ou de révéler leurs clefs privées à des tiers, même s'ils les représentent ;

c) Garantir la confidentialité, l'intégrité et la disponibilité des clefs privées générées, stockées et utilisées ~~pour TACHOnet~~ ;

d) S'abstenir de continuer à utiliser la clef privée au-delà de la période de validité ou après la révocation du certificat, à des fins autres que la visualisation des données chiffrées (par exemple le déchiffrage de courriels). Les clefs arrivées à échéance doivent être soit détruites soit conservées d'une manière en empêchant l'utilisation ;

e) Communiquer à ~~l'autorité d'enregistrement~~ **l'instance de validation des demandes** l'identité des représentants habilités à demander la révocation des certificats délivrés à l'organisme (les demandes de révocation doivent inclure un mot de passe de demande de révocation et des informations détaillées sur les faits justifiant la révocation) ;

f) Empêcher une utilisation abusive des clefs privées en demandant la révocation du certificat de clef publique correspondant lorsque la clef privée ou les données d'activation de la clef privée sont fragilisées ;

g) Être responsables et assumer 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 ;

[1] Une ICP (infrastructure à clef 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 la rubrique Nom distinctif du sujet du certificat émis.

h) Informer sans délai ~~l'autorité d'enregistrement~~ **l'instance de validation des demandes** de la perte, du vol ou de la fragilisation potentielle de toute clef AETR utilisée dans le cadre du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~.

5. Responsabilité

Sans préjudice de la responsabilité de la Commission européenne lorsqu'il y a contradiction avec les dispositions des législations nationales applicables ou eu égard à sa responsabilité dans les cas qui ne peuvent être exclus en vertu de ces mêmes législations, la Commission européenne n'engage pas sa responsabilité en ce qui concerne :

a) Le contenu du certificat, qui relève exclusivement de la responsabilité de son détenteur, à qui il incombe de vérifier l'exactitude de son contenu ;

b) L'utilisation du certificat par son détenteur.

Sous-appendice 4.9

Description du service ICP mis en place pour le système d'échange électronique d'informations sur les cartes de conducteur ~~TACHOnet~~

1. Introduction

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

Le service ICP d'eDelivery s'appuie sur l'autorité de certification Trust Center Services TeleSec Shared Business à laquelle s'applique la politique de certification (PC)/déclaration d'activité de certification (CPS) de l'autorité de certification TeleSec Shared-Business-CA de **Deutsche Telekom Security** ~~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 « Organisme » ou « autorité nationale » demandant le certificat

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

2.1.1.2 L'autorité nationale doit :

a) Demander les certificats au service MIE ICP ;

b) Générer les clefs privées et les clefs publiques correspondantes à joindre aux certificats délivrés par l'autorité de certification ;

c) Télécharger le certificat une fois qu'il a été approuvé ;

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

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

d) Signer et renvoyer à **l'instance de validation des demandes** ~~l'autorité d'enregistrement~~ :

i) Le formulaire d'identification des contacts et des messagers certifiés ;

ii) La procuration individuelle signée[5].

2.1.2 Messager certifié

2.1.2.1 L'autorité nationale doit désigner un messager certifié **si cela n'a pas encore été fait pour l'ERCA, le messager certifié désigné devant être le même pour le système d'échange électronique d'informations sur les cartes de conducteur et l'ERCA**.

2.1.2.2 Le messager certifié doit :

a) **Authentifier la demande de certificat pour l'instance de validation des demandes durant un processus d'identification et d'enregistrement en face à face déjà établi et bien connu aux fins des sessions de signature de l'ERCA** ~~Remettre la clef publique à l'autorité d'enregistrement durant un processus d'identification et d'enregistrement en face à face~~ ;

b) ~~Obtenir~~ **Télécharger** le certificat correspondant **depuis le système d'ICP de l'autorité de certification une fois que le certificat a été émis et qu'il est disponible** ~~de l'autorité d'enregistrement~~.

2.1.3 Propriétaire de domaine

2.1.3.1 La DG MOVE sera le propriétaire de domaine.

2.1.3.2 Le propriétaire de domaine doit :

a) Valider et coordonner le réseau ~~TACHOnet~~ **du système d'échange électronique d'informations sur les cartes de conducteur** et l'architecture sécurisée ~~TACHOnet~~, notamment la validation des procédures de délivrance des certificats ;

b) Exploiter le système central ~~TACHOnet~~ et coordonner l'activité des parties concernant le fonctionnement du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~ ;

c) Réaliser, avec les autorités nationales, les essais de connexion au système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~.

2.1.4 ~~Autorité d'enregistrement~~ **Instance de validation des demandes**

2.1.4.1 Le Centre commun de recherche (CCR) sera ~~l'autorité d'enregistrement~~ **l'instance de validation des demandes**.

2.1.4.2 **L'instance de validation des demandes sera chargé d'authentifier l'identité de l'organisme demandeur, de ses points de contact et de ses messagers certifiés. Il validera les demandes de certificat du système d'échange électronique d'informations sur les cartes de conducteur au cours de l'appel téléphonique de validation passé au point de contact de l'ERCA (officiellement désigné par l'Autorité des États membres) à l'occasion des sessions de l'ERCA** ~~L'autorité d'enregistrement sera chargée de vérifier l'identité du messager certifié, d'enregistrer et d'approuver les~~

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

~~demandes de délivrance, de révocation et de renouvellement des certificats numériques~~.

2.1.4.3 ~~L'autorité d'enregistrement~~ **L'instance de validation des demandes** doit :

a) Assigner l'identificateur unique à l'autorité nationale ;

b) Authentifier l'identité de l'autorité nationale, ses contacts et ses messagers certifiés ;

c) Communiquer avec l'équipe d'appui du MIE en ce qui concerne l'authenticité de l'autorité nationale, de ses contacts et de ses messagers certifiés ;

d) Informer l'autorité nationale de l'approbation ou du rejet du certificat.

2.1.5 Autorité de certification

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

2.1.5.2 L'autorité de certification doit :

a) Fournir l'infrastructure technique pour les demandes de certificat formulées par les autorités nationales ;

b) Valider ou rejeter la demande de certificat ;

c) Communiquer avec ~~l'autorité d'enregistrement~~ **l'instance de validation des demandes** pour la vérification de l'identité de l'organisme demandeur, le cas échéant.

2.2 Délivrance du certificat

2.2.1 Le certificat doit être délivré selon les étapes consécutives suivantes :

a) Étape 1 : Identification du messager certifié ;

b) Étape 2 : Création de la demande de certificat ;

c) Étape 3 : Enregistrement auprès de ~~l'autorité d'enregistrement~~ **l'instance de validation des demandes** ;

d) Étape 4 : Émission du certificat ;

e) Étape 5 : Publication du certificat ;

f) Étape 6 : Acceptation du certificat.

2.2.2 Étape 1 : Identification du messager certifié

La procédure d'identification du messager certifié doit être la suivante :

a) ~~L'autorité d'enregistrement~~ **L'instance de validation des demandes** doit envoyer à l'autorité nationale le formulaire d'identification des contacts et des messagers certifiés[6] **(identique au formulaire d'identification de l'ERCA)**. Ce formulaire ~~inclut également~~ **doit être accompagné d'**un pouvoir que l'organisme (autorité AETR) doit signer ;

b) L'autorité nationale doit renvoyer le formulaire rempli et la procuration signée à ~~l'autorité d'enregistrement~~ **l'instance de validation des demandes** ;

c) ~~L'autorité d'enregistrement~~ **L'instance de validation des demandes** doit confirmer qu'elle a bien reçu le formulaire et qu'il est complet ;

[6] Voir point 5.

d) ~~L'autorité d'enregistrement~~ **L'instance de validation des demandes** doit fournir au propriétaire de domaine un exemplaire de la liste à jour des contacts et des messagers certifiés.

2.2.3 Étape 2 : Création de la demande de certificat

2.2.3.1 La demande et la réception du certificat doivent se faire sur le même ordinateur et avec le même navigateur.

2.2.3.2 Le processus suivant doit être appliqué pour la création de la demande de certificat :

a) L'organisme demandeur doit aller sur l'interface utilisateur https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en. Il doit saisir ~~le nom d'utilisateur « sbca/CEF_eDelivery.europa.eu » et le mot de passe « digit.333 »~~**les identifiants (nom d'utilisateur et mot de passe) reçus du système d'ICP de l'autorité de certification pour le portail utilisateur** ;

b) L'organisme doit cliquer sur « request » dans le menu de gauche, et sélectionner « CEF_TACHOnet » dans la liste déroulante ;

c) L'organisme doit saisir dans le formulaire de demande de certificat les informations figurant au tableau 3 et cliquer ensuite sur « Next (soft-PSE) » pour terminer le processus.

Tableau 3
Explications détaillées sur les champs à renseigner

Champ à renseigner	*Description*
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)
Organisme/société (O)	**O = nom de l'organisme du détenteur du certificat**
Domaine central (OU1)	**OU = CEF_eDelivery.europa.eu**
Domaine de compétence (OU2)	**OU = CEF_TACHOnet**
Département (OU3)	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 : (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. Par exemple : AP_PROD-GTC_OID-1.3.130.0.2018.xxxxxx
Prénom (CN)	Ne pas remplir
Nom de famille (CN)	Doit commencer par « GRP », suivi par le nom Format : **CN = GRP :<AREA OF RESPONSIBILITY>_<TYPE>_<COUNTRY CODE>_<UNIQUE IDENTIFIER>** Par exemple : GRP : CEF_TACHOnet_AP_PROD_BE_001
Courriel	**E = CEF-EDELIVERY-SUPPORT@ec.europa.eu**
Adresse électronique 1 (SAN)	Ne pas remplir
Adresse électronique 2 (SAN)	Ne pas remplir
Adresse électronique 3 (SAN)	Ne pas remplir
Adresse	Ne pas remplir

Champ à renseigner	*Description*
Rue	Doit correspondre à l'adresse officielle de l'organisme du détenteur du certificat (utilisée pour la procuration).
Numéro	Doit correspondre à l'adresse officielle de l'organisme du détenteur du certificat (utilisée pour la procuration).
Code postal	Doit correspondre à l'adresse officielle de l'organisme du détenteur du certificat (utilisée pour la procuration). **Attention** : si le code postal n'est pas un code à 5 chiffres, laisser ce champ vide et inscrire le code postal dans le champ « City » (Ville).
Ville	Doit correspondre à l'adresse officielle de l'organisme du détenteur du certificat (utilisée pour la procuration). **Attention** : si le code postal n'est pas un code à 5 chiffres, laisser ce champ vide et inscrire le code postal dans le champ « City » (Ville).
Numéro de téléphone	Ne pas remplir
Données d'identification	L'adresse e-mail doit être celle qui est utilisée pour enregistrer l'identifiant unique. + Doit être le nom de la personne représentant l'organisme (utilisé pour la procuration). + **Numéro d'immatriculation au registre du commerce** (obligatoire uniquement pour les organismes privés) **Inscrit au tribunal local de** (obligatoire uniquement pour les organismes privés allemands et autrichiens)
Mot de passe de révocation	Champ obligatoire choisi par le demandeur
Répétition du mot de passe de révocation	Champ obligatoire choisi par le demandeur (répétition)

d) La longueur de clef doit être de 2 048 bits (haut niveau) ;

e) L'organisme doit enregistrer le numéro de référence afin d'obtenir le certificat ;

f) L'équipe d'appui du MIE doit vérifier les nouvelles demandes de certificats et s'assurer que les informations contenues dans la demande sont valides ;

g) L'équipe d'appui du MIE doit vérifier 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 d'appui du MIE doit envoyer un courriel à l'adresse électronique qui figure dans le champ « Données d'identification » du formulaire de demande (avec copie au propriétaire du domaine) dans lequel l'organisme est invité à suivre à nouveau la procédure. La demande de certificat rejetée sera annulée ;

i) L'équipe d'appui du MIE doit envoyer un courriel à ~~l'autorité d'enregistrement~~ **l'instance de validation des demandes** concernant la validité de la demande. Le courrier électronique doit comprendre :

1) Le nom de l'organisme figurant dans le champ « Organisation (O) » de la demande de certificat ;

2) Les données relatives au certificat, notamment le nom du point d'accès pour lequel le certificat doit être délivré, disponible dans le champ « Nom de famille (CN) » de la demande de certificat ;

3) Le numéro de référence du certificat ;

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

2.2.4 Étape 3 : Enregistrement auprès de ~~l'autorité d'enregistrement~~ **l'instance de validation des demandes** (~~approbation du~~ **validation de la demande de** certificat)

2.2.4.1 Le messager certifié ou le point de contact doit prendre rendez-vous avec ~~l'autorité d'enregistrement~~ **l'instance de validation des demandes** par échange de courriels et identifier le messager certifié qui participera à la réunion en face à face.

2.2.4.2 L'organisme doit préparer les documents suivants :

a) La procuration remplie et signée ;

b) Une copie du passeport en cours de validité du messager certifié qui participera à la réunion en face à face~~. Cette copie doit être signée par l'un des contacts de l'organisme identifiés à l'étape 1~~ ;

c) Le formulaire de demande de certificat sur papier, signé par l'un des contacts de l'organisme.

2.2.4.3 ~~L'autorité d'enregistrement~~ **L'instance de validation des demandes** doit recevoir le messager certifié après un contrôle d'identité à l'accueil du bâtiment. ~~L'autorité d'enregistrement~~ **Elle** doit effectuer en face à face l'enregistrement de la demande de certificat en :

a) Identifiant et authentifiant le messager certifié ;

b) Comparant l'aspect physique du messager certifié avec la photo figurant sur le passeport présenté par le messager ;

c) Vérifiant la validité du passeport présenté par le messager certifié ;

d) Comparant le passeport valide présenté par le messager certifié avec la copie du passeport valide du messager certifié ~~qui a été signée par l'un des contacts de l'organisme identifiés. La signature est authentifiée par comparaison avec l'original du « formulaire d'identification du messager certifié et des contacts »~~ ;

e) Vérifiant la procuration remplie et signée ;

f) Vérifiant le formulaire de demande de certificat sur papier ~~et sa signature par comparaison avec l'original du « formulaire d'identification du messager certifié et des contacts »~~ ;

g) Invitant le point de contact signataire à vérifier une nouvelle fois l'identité du messager certifié et le contenu de la demande de certificat.

2.2.4.4 ~~L'autorité d'enregistrement~~ **L'instance de validation des demandes** doit confirmer à l'équipe d'appui du MIE que l'autorité nationale est effectivement autorisée à exploiter les éléments pour lesquels elle demande les certificats et que le processus d'enregistrement en face à face correspondant a été probant. La confirmation doit être envoyée par courriel sécurisé au moyen d'un certificat « CommiSign », accompagné d'une copie scannée des documents authentifiés en face à face et de la liste correspondant au contrôle des étapes du processus effectué par ~~l'autorité d'enregistrement~~ **l'instance de validation des demandes** dûment signée.

2.2.4.5 Si ~~l'autorité d'enregistrement~~ **l'instance de validation des demandes** confirme la validité de la demande, le processus doit se poursuivre conformément aux points 2.2.4.6 et 2.2.4.7. Dans le cas contraire, la délivrance du certificat doit être rejetée et l'organisme en être informé.

2.2.4.6 L'équipe d'appui du MIE doit approuver la demande de certificat et informer ~~l'autorité d'enregistrement~~ **l'instance de validation des demandes** de cette approbation.

2.2.4.7 L'**équipe d'appui du MIE** ~~autorité d'enregistrement~~ doit informer l'organisme que le certificat peut être obtenu depuis le **système d'ICP de l'autorité de certification (**portail utilisateur**)**.

2.2.5 Étape 4 : Émission du certificat

Dès l'approbation de la demande, le certificat doit être émis.

2.2.6 Étape 5 : Publication et obtention du certificat

2.2.6.1 Dès l'approbation de la demande de certificat, **l'équipe d'appui du MIE informe l'instance de validation des demandes que le certificat est approuvé et informe l'organisme qu'il peut être téléchargé**~~l'autorité d'enregistrement doit obtenir le certificat et en remettre une copie au messager certifié~~.

2.2.6.2 L'organisme doit être informé par l'autorité d'enregistrement que les certificats peuvent être obtenus.

2.2.6.**2**3 L'organisme doit se rendre sur le portail utilisateur, à l'adresse https://sbca.telesec.de/sbca/ee/login/displayLogin.html?locale=en, et se connecter avec **les identifiants (nom d'utilisateur et mot de passe) reçus du système d'ICP de l'autorité de certification pour le portail utilisateur** ~~le nom d'utilisateur « sbca/CEF_eDelivery.europa.eu » et le mot de passe « digit.333 ».~~

2.2.6.**3**4 L'organisme doit cliquer sur le bouton « fetch » du menu de gauche et saisir le numéro de référence enregistré durant le processus de demande de certificat.

2.2.6.**4**5 L'organisme doit installer les certificats en cliquant sur le bouton « install ».

2.2.6.**5**6 Le certificat doit être installé au point d'accès. Comme l'installation est propre à la mise en œuvre, l'organisme doit se référer à son fournisseur de point d'accès pour obtenir la description de ce processus.

2.2.6.**6**7 Les étapes suivantes sont nécessaires pour installer le certificat au point d'accès :

a) Exporter la clef privée et le certificat ;

b) Créer le keystore et le truststore ;

c) Installer le keystore et le truststore au point d'accès.

3. Processus de révocation du certificat

3.1 L'organisme doit faire une demande de révocation via le **système d'ICP de l'autorité de certification (**portail utilisateur**)** ;

3.2 L'équipe d'appui du MIE doit procéder à la révocation du certificat.

4. Conditions générales d'utilisation 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 finals ») qui font partie du **système d'échange électronique d'informations sur les cartes de conducteur** ~~réseau TACHOnet~~.

La DIGIT est un utilisateur de la solution TeleSec Shared-Business-CA (« SBCA ») exploitée au sein du Trust Center de **Deutsche Telekom Security GmbH** ~~T-Systems International GmbH (« T-Systems »[8])~~. La DIGIT joue le rôle de registraire principal 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 conditions d'utilisation du sous-domaine **du système d'échange électronique d'informations sur les cartes de conducteur** ~~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 de son détenteur, à qui il incombe de vérifier l'exactitude du contenu.

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.

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 de ces législations.

4.3 Usages permis et interdits des certificats

4.3.1 Usage permis des certificats

Une fois le certificat délivré, son détenteur[9] devra l'utiliser uniquement dans le cadre du système **d'échange électronique d'informations sur les cartes de conducteur** ~~TACHOnet~~. Dans ce cadre, 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 mentionnée parmi les cas d'usage permis est interdite.

[7] Une ICP (infrastructure à clef 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] La fonction certificatrice de l'opérateur du Trust Center, situé dans le Trust Center de **Deutsche Telekom Security GmbH** ~~T-Systems~~, fait également office **d'instance de validation des demandes**~~d'autorité d'enregistrement~~ interne.

[9] Identifié par la valeur d'attribut « O = » dans la rubrique Nom distingué du sujet du certificat émis.

4.4 Autres obligations du détenteur de certificat

Les modalités et les conditions détaillées de la SBCA sont définies par **Deutsche Telekom Security GmbH**~~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'instance de validation des demandes** ~~d'autorité d'enregistrement (AE)~~ ainsi que de tiers délégué par **l'instance de validation des demandes** ~~l'autorité d'enregistrement (AE)~~.

Seules les entités autorisées à participer au **système d'échange électronique d'informations sur les cartes de conducteur** ~~réseau TACHOnet~~ peuvent demander un certificat.

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'organisme auquel 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) Protéger leurs clefs privées contre toute utilisation non autorisée ;

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

3) S'abstenir de poursuivre l'utilisation de la clef 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 (par exemple déchiffrage de courriels) ;

4) Se charger de la copie ou du transfert de la clef à l'entité finale ou aux entités finales ;

5) Obliger l'entité finale/toutes les entités finales à respecter les présentes conditions d'utilisation, y compris la PC/CPS de la SBCA, en ce qui concerne la clef privée ;

6) Fournir les données d'identification des représentants habilités à demander la révocation des certificats délivrés à l'organisme ainsi que les précisions relatives aux faits qui ont conduit à la révocation et le mot de passe de révocation ;

7) En ce qui concerne 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), empêcher toute utilisation abusive de la clef privée en révoquant le certificat ;

8) Faire 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 clef pour des certificats, la clause 4.6 ou 4.7 de la PC/CPS de la SBCA s'applique.

[10] La dernière version de la PC et de la CPS du service SBCA de **Deutsche Telekom Security GmbH** ~~T-Systems~~ est disponible à l'adresse https://www.telesec.de/en/sbca-en/support/download-area/.

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 contacts et des messagers certifiés (exemple)

~~Je soussigné~~, *~~[nom et adresse du représentant de l'organisme]~~*, **~~certifie que les informations ci-après seront utilisées dans le cadre de la demande, de l'émission et de l'envoi de certificats numériques de clefs publiques pour les points d'accès TACHOnet assurant la confidentialité, l'intégrité et la non-révocation des messages TACHOnet :~~**

~~Coordonnées du contact :~~

~~— Contact n° 1~~	**~~— Contact n° 2~~**
~~— Nom :~~	**~~— Nom :~~**
~~— Prénom(s) :~~	**~~— Prénom(s) :~~**
~~— Téléphone mobile :~~	**~~— Téléphone mobile :~~**
~~— Téléphone fixe :~~	**~~— Téléphone fixe :~~**
~~— Adresse électronique :~~	**~~— Adresse électronique :~~**
~~— Signature manuscrite :~~	**~~— Signature manuscrite :~~**

~~Coordonnées du messager certifié :~~

~~— Messager certifié n° 1~~	**~~— Messager certifié n° 2~~**
~~— Nom :~~	**~~— Nom :~~**
~~— Prénom(s) :~~	**~~— Prénom(s) :~~**
~~— Téléphone mobile :~~	**~~— Téléphone mobile :~~**
~~— Adresse électronique :~~	**~~— Adresse électronique :~~**
~~— 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 :~~**

Le ministère compétent de la Partie contractante à l'AETR :

En la personne de :

*** certifie que le présent formulaire de soumission de la politique de l'autorité de la Partie contractante par son autorité nationale compétente est authentique et que les pièces qui y sont jointes sont dûment valides ;**

*** précise par la présente que l'autorité nationale nommée et approuvée exercera ses activités dans le cadre du ou des textes suivants :**

Appendice 1B de l'AETR et *« Digital Tachograph System European Root Policy » (ci-après la politique de l'ERCA),*

ou

Appendice 1C de l'AETR et « Smart Tachograph − European Root Certificate Policy and Symmetric Key Infrastructure Policy » (ci-après la politique de l'ERCA de deuxième génération),

ou

Appendice 4 de l'AETR et « TeleSec Shared-Business-CA Certificate Policy (CP) and Certification Practice Statement (CPS) » (ci-après la politique ICP ~~du système TACHOnet~~* du système d'échange électronique d'informations sur les cartes de conducteur*).

1. **Identification de l'autorité de la Partie contractante**[11]

a. **Nom officiel de l'entité organisationnelle :**

b. **Adresse de l'entité organisationnelle :**

c. **Nom du représentant dûment désigné de l'entité organisationnelle :**

d. **Personne à contacter (si différente de c.**[12]**) :**

e. **Adresse électronique :**

f. **Adresse postale :**

g. **Numéro(s) de téléphone ou de télécopie :**

2. **Identification du messager certifié (personne qui communique les demandes de certificats/clefs de sécurité de l'ERCA ou les demandes de certificats ~~TACHOnet~~ pour le système d'échange électronique d'informations sur les cartes de conducteur et qui obtient les clefs de sécurité auprès de l'ERCA)**[13] **:**

a. **Nom :**

b. **Adresse postale :**

c. **Numéro(s) de téléphone ou de télécopie :**

3. **Accord et signature**

Je confirme par la présente mon acceptation en signant ce formulaire de demande, après avoir pris connaissance

de l'appendice 1B de l'AETR et de la politique de l'ERCA,

ou

de l'appendice 1C de l'AETR et de la politique de l'ERCA de deuxième génération,

[11] Veuillez NOTER que toute modifications de ces données doit être communiquée directement à l'ERCA.

[12] JOINDRE la lettre de mandat par laquelle la personne visée au point 1.c. mandate la personne visée au point 1.d., y compris une copie du laissez-passer de la personne visée au point d. lui donnant accès aux locaux de l'organisation identifiée comme étant l'autorité de la Partie contractante.

[13] JOINDRE la lettre de mission établie par la personne visée au point 1.d. à l'intention de la personne visée au point 2, ainsi qu'une copie de la pièce d'identité de cette dernière; ces renseignements seront intégrés dans les fichiers conservés par l'ERCA.

ou

***de l'appendice 4 de l'AETR et de la politique ICP ~~du système TACHOnet~~* du système d'échange électronique d'informations sur les cartes de conducteur.**

Je reconnais également que toute demande peut être invalidée par l'ERCA, s'il y a lieu de penser que :

- **les formulaires ou les pièces qui y sont jointes ont été établis sur la base d'informations fausses ou inexactes ;**
- **les informations qui y figurent sont périmées ;**

Je confirme par la présente que les informations fournies à l'ERCA au moyen du présent formulaire de demande et des pièces qui y sont jointes sont exactes, précises et complètes.

Le traitement des renseignements qui figurent dans le présent formulaire est couvert par une déclaration de confidentialité relative à la protection des données personnelles. Cette déclaration peut être consultée sur le site Web de l'Union européenne à l'adresse suivante : https://ec.europa.eu/dpo-register/detail/DPR-EC-00406. Veuillez consulter cette déclaration avant de remplir et d'envoyer le formulaire.

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

Signature du représentant habilité :

6. Documents

6.1 Procuration individuelle (modèle)

On trouvera ci-après un modèle de procuration individuelle qui doit être signée et présentée par le messager certifié lors de l'enregistrement en face à face chez **l'instance de validation des demandes** ~~l'ordonnateur régional~~ :

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 de demande de certificat sur papier (modèle)

On trouvera ci-après un modèle du formulaire de demande de certificat sur papier qui doit être signé et présenté par le messager certifié lors de l'enregistrement en face à face chez **l'instance de validation des demandes** ~~l'ordonnateur régional~~ :

Please print the text of this document on your letterhead, add your organisation stamp and have it signed by an authorised representative of your organisation.

TACHOnet certificate request paper form

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

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

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

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

Trusted courier #1

Name:

First names:

Mobile phone:

Email:

Passport issuing country:

Passport number:

Passport validity end date:

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

Signature of the authorised representative:

7. Glossaire

Les principaux termes utilisés dans le présent sous-appendice sont définis dans la section « CEF Definitions » sur le portail Web unique CEF Digital, à l'adresse suivante :

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

Les principaux sigles et acronymes utilisés dans la présente description sont définis dans le glossaire CEF sur le portail Web unique CEF Digital, à l'adresse suivante :

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

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 confier à des sous-traitants tout service dont la responsabilité leur incombe en vertu des dispositions du présent appendice.

8.2 Une telle sous-traitance ne dégage pas la partie des responsabilités qui lui incombent en vertu du présent appendice, y compris de la responsabilité relative aux niveaux de service requis conformément aux dispositions du sous-appendice 4.6.