SYSTEME CHRONOTACHYGRAPHE NUMERIQUE

POLITIQUE EUROPEENNE GENERIQUE DE CERTIFICATION (ERCA)

ABRÉVIATIONS

Cf. chapitre 11 du présent document

SYNTHESE

Ce document est la traduction en français non officielle du document émis par le JRC :

Digital Tachograph System
European Root Policy

Version 2.1

Administrative Agreement TREN-E1-08-M-ST-SI2.503224

European Commission
Joint Research Centre
Institute for the Protection and Security of the Citizen

Contact information	E-mail: erca@jrc.ec.europa.eu
Address: Head of Unit	Tel.: +39-0332-785754
JRC IPSC TRVA (TP.361)	Fax: +39-0332-786280
Via E. Fermi, 2749	http://ipsc.jrc.ec.europa.eu
I-21027 Ispra I(VA); ITALY	http://www.jrc.ec.europa.eu

Le but de ce document est de fournir les éléments de base pour l'élaboration d'un politique de sécurité nationale nécessaire à la mise en place du chronotachygraphe numérique dans un pays.

Ce document initialement rédigé à l'intention des Etats Membres de l'Union Européenne a été utilisé par le Parties Contractantes de l'AETR non membres de l'Union, puisque toutes les politiques de sécurité nationales sont approuvées par le JRC, au terme d'un accord entre la CEE-ONU et la Commission Européenne.

Le JRC, en approuvant les politiques nationales de sécurité vérifie et qu'elles sont à un même niveau pour assurer le même niveau de sécurité sur l'ensemble des territoires des pays ayant signé l'Accord AETR.

Lorsque le document cite les Etats Membres, il faut donc comprendre Etats Membres de l'Union Européenne ou Partie Contractante de l'AETR.

Dans le document, les mentions suivantes doivent être comprises comme suit pour les Parties Contractantes de l'AETR non membre de l'Union Européenne :

Etat Membre	:	Partie Contractante
Annexe 1(B)	:	Appendice 1(B)
Appendice n	:	Sous-appendice n

Avis légal
Ni la Commission Européenne, ni qui que ce soit agissant au nom de la Commission est responsable de l'utilisation qui pourrait être faite de cette documentation.

TABLE DES MATIERES

1. Introduction
2. Rôles et responsabilités
3. Gestion et champ d'application de la politique ERCA
4. Exigences de fonctionnement et de sécurité de l'ERCA
4.1. Exigences de sécurité
4.2. Exigences de fonctionnement
4.3. Approbation de la politique MSA
4.4. Classification des éléments constitutifs de l'ERCA
5. Obligation de MSA
5.1. Responsabilités
5.2. Soumission d'une politique MSA à l'ERCA
5.3. Exigences
6. Pratique de l'ERCA
6.1 Déclaration de pratiques de certification
6.2 Génération des clés ERCA
6.3 Stockage, sauvegarde récupération de clé ERCA
6.4 Distribution de clé ERCA
6.5 Clé factice
6.6 Clé ERCA en service
6.7 Cycle de fin de vie de clé ERCA
6.8 Demandes de MSCA
6.9 Validité de certificat
6.10 Certificat et distribution de clé de capteur de mouvement
6.11 Information de l'état d'un certificat
6.12 Révocation de certificat
7. Gestion et fonctionnement de l'ERCA
7.1 Gestion de la sécurité
7.2 Classification d'élément constitutif
7.3 Sécurité du personnel
7.4 Sécurité physique et environnementale
7.5 Enregistrements des demandes de MSCA
7.6 Récupération de catastrophe
7.7 Pérennité de l'ERCA
8. Procédures de changement de la politique ERCA
9. Conformité aux normes

10. Références

11. Abréviations

12. Définitions

Annexe A Demande de certificat de clé

Annexe B Format de distribution de clé publique

Annexe C Distribution de clé

Annexe D Distribution de clé maître de capteur de mouvement

LISTE DES TABLEAUX

Table 1: Classification des éléments constitutifs ERCA

LISTE DES FIGURES

Figure 1 Description De la gestion de clé de l'Annexe I(B)

1 INTRODUCTION

Le système chronotachygraphe numérique a été introduit par le Règlement du Conseil Européen n°3821/85 amendé par le règlement du Conseil n°2135/98 [1] et le règlement de la Commission n°1360/2002 [2].

Le règlement de la Commission n°1360/2002 inclue dans l'Annexe 1(B) – Exigences pour la construction, l'installation et le contrôle – la description technique du système chronotachygraphe numérique. Une information technique très détaillée est contenue dans une série de onze appendices à l'Annexe 1(B).

En ce qui concerne les questions de gestion de clé traitée par l'Annexe 1(B), l'existence de l'Appendice 11 CSM_007 [6] déclare :

> *Au niveau Européen, une unique paire de clés EUR.SK et EUR.PK doit être générée. Les clés privées Européennes doivent être utilisées pour certifier les clés publiques des Etats Membres. Les enregistrements de toutes les clés certifiées doivent être conservés. Ces tâches seront effectuées par une autorité Européenne de certification, sous l'autorité et la responsabilité de la Commission Européenne.*

L'exigence CSM_008 de l'Appendice 11 de l'annexe 1(B) déclare :

> *Au niveau d'un Etat Membre, une paire de clés d'Etat Membre (MS.SK et MS.PK) doit être générée. Les clés publiques des Etats Membres doivent être certifiées par l'Autorité de Certification Européenne. Les clés privées d'un Etat Membre doivent être utilisées pour certifier les clés publiques qui seront insérées dans les équipements (Unité Embarquée Véhicule –UEV- et Carte Tachygraphique). Les enregistrements de toutes les clés publiques certifiées devront être conservés avec l'identification de l'équipement auquel il est destiné. Ces tâches devront être réalisées par l'autorité de certification de l'Etat Membre. Un Etat Membre peut changer sa paire de clés régulièrement.*

L'exigence CSM_009 de l'Appendice 11 de l'annexe 1(B) déclare :

> *Au niveau de l'équipement, une seule paire de clés (EQT.SK et EQT.PK) devra être générée et insérée dans chaque équipement. Les clés publiques de l'équipement doivent être certifiées par l'autorité de certification de l'Etat Membre. Ces tâches peuvent être effectuées par le fabricant d'équipements, le personnalisateur d'équipement ou des autorités de l'Etat Membre. Cette paire de clés est utilisée pour les fonctions d'authentification, de signature numérique et de chiffrement.*

Un aperçu des mesures de sécurité exigées par le système chronotachygraphe numérique est contenu dans le *Guide de Sécurité Commun* [3].

L'information et le guide sur les processus à mettre en œuvre au niveau de l'Etat Membre sont fournis dans le *Guide et Référentiel National Politique CA pour le système chronotachygraphe numérique* [4].

Cette politique est développée selon les guides présentés dans la section 8 *Trame pour la définition des politiques d'autres certificats* de la norme ETSI TS 102 042 *Exigences de politique pour la certification des autorités émettant des certificats de clés publiques* [5].

La norme ETSI TS 102 042 a été choisie pour sa description concise et complète des meilleures pratiques courante pour la mise ne place de PKI. La norme ETSI ne fournit pas de solution à toutes les exigences du Règlement, et donc la conformité totale à l'ETSI TS 102 042 n'est pas exigée.

2 ROLES ET RESPONSABILITES

2.1 Le service responsable de la Commission Européenne pour la politique ERCA et dénommé ci-après *l'Autorité Européenne*.

2.2 L'adresse et le contact de l'Autorité Européenne sont :

Commission Européenne

Direction Générale du Transport et de l'Energie

Unité E1 – Politique du Transport Terrestre

Rue de Mot, 24

B-1040 Bruxelles

2.3 Le service responsable de la Commission Européenne pour la mise en œuvre de la politique ERCA et pour les dispositions des services de certification des Etats Membres est dénommé ci-après l'ERCA

2.4 l'adresse et le contact de l'ERCA est :

Digital Tachograph Root Certification Authority
Traceability and Vulnerability Assessment Unit
European Commission
Joint Research Centre, Ispra Establishment (TP.361)
Via E. Fermi, 2749

I-21027 Ispra (VA)

2.5 L'Autorité Européenne désigne l'organisation qui met en œuvre la politique ERCA et fournit les services de certification de clé aux Etats Membres.

2.6 L'Autorité Européenne doit s'assurer que l'ERCA dispose des ressources exigées pour opérer en conformité avec la politique.

2.7 Les réclamations des Autorités de Etats Membres pour les services fournis par l'ERCA doivent être adressées à l'Autorité Européenne pour traitement.

2.8 L'Autorité Européenne doit gérer la procédure de changement de la politique ERCA décrit au chapitre 8.

2.9 L'ERCA doit documenter la mise en œuvre de la politique ERCA dans un Etat des Pratiques de Certification.

2.10 L'ERCA doit établir les contenus de ses CPS disponibles pour les autorités des Etats Membres et/ou des Autorités de Certification des Etats Membres sur une base « à savoir ».

2.11 L'ERCA doit maintenir les enregistrements de ses opérations de façon appropriée pour démontrer la conformité de la politique ERCA, et

devra rendre ces enregistrements disponibles pour l'Autorité Européenne sur demande.

2.12 La politique ERCA a été approuvée par l' l'Autorité Européenne le 28 juillet 2009

2.13 L'information de la structure de la Commission Européenne est disponible pour le public sur l'internet (par exemple http://europa.eu.int/comm).

3 GESTION ET CHAMP D'APPLICATION DE LA POLITIQUE ERCA

3.1 La politique ERCA s'applique seulement aux clés de chiffrement et aux certificats de clé utilisés dans les authentification mutuelles, les messages sécurisés et les mécanismes de signature numérique du Système de Chronotachygraphe Numérique décrit à l'Annexe 1(B) [6] et l'ISO/CD 16844-3 [7].

3.2 Les certificats des clés publiques émis par l'ERCA sont faits dans ce seul but comme exigé par le Règlement.

3.3 Les signataires de l'ERCA ne peuvent être que les autorités des Etats Membres selon l'Annexe 1(B), Appendice 11, exigence CSM_008[6].

3.4 Les exigences de fonctionnement et de sécurité de l'ERCA sont décrites au chapitre 4 de ce document.

3.5 La politique ERCA est disponible en format électronique sur le site web http://dtc.jrc.ec.europa.eu

3.6 Les documents ERCA seront préparés en anglais. Des traductions peuvent être disponibles, mais seule la version anglaise fait foi.

3.7 Les communications officielles entre l'ERCA et les autorités des Etats Membres devront utiliser une correspondance recommandée.

4 EXIGENCES DE FONCTIONNEMENT ET DE SECURITE DE L'ERCA

La gestion de clé et de certificat du Système de Chronotachygraphe Numérique est décrite en figure 1. Quatre entités sont décrites : le fournisseur de service de certification ERCA (CSP) ; le MSCA CSP ; et deux types de composant de personnalisation (CP) : fabrication de carte tachygraphique et d'unité embarquée véhicule, ainsi que la fabrication du capteur de mouvement.

L'ERCA et les MSCA CSP de la figure 1 créent et maintiennent les clés de chiffrement appropriées et les utilisent pour valider les données de sécurité du chronotachygraphe numérique, seulement après avoir vérifié que les données à chiffrer sont complètes, correctes et dûment autorisées.

Les CPs des cartes, UEV ou capteurs de mouvement de la figure 1insèrent les données de sécurité dans l'équipement du chronotachygraphe numérique par des moyens sécurisés appropriés.

4.1 Exigences de sécurité

4.1.1 La mise en œuvre de l'ERCA doit être conforme aux meilleures pratiques décrites dans l'ISO 17799 - Technologie de l'Information – Codes de pratique pour la gestion de la sécurité de l'information [8].

4.1.2 L'ERCA doit maintenir la confidentialité de la racine RSA de la clé privée et des copies des clés maîtres des capteurs de mouvement qu'il conserve.

4.1.3 L'ERCA doit maintenir dans le but indiqué par le règlement l'intégrité et la disponibilité, des paires de clés générique RSA, et des clés maîtres des capteurs de mouvement.

4.1.4 L'ERCA doit vérifier l'authenticité, l'intégrité et l'unicité dans le cadre du règlement de chaque modulo de clé publique MSCA et de l'identification de clé soumise à la certification.

4.1.5 L'authenticité et l'intégrité de la clé publique ERCA et les certificats de clé publique MSCA RSA doivent être maintenus pendant toute la durée de vie des clés.

4.1.6 La confidentialité, l'intégrité et l'authenticité des clés maîtres du capteur de mouvement doivent être maintenus.

4.1.7 L'ERCA ne doit pas générer les clés RSA pour un MSCA

4.1.8 L'ERCA doit distribuer les clés maître du capteur de mouvement et les certificats des clés publiques sur une base « à savoir ».

4.1.9 L'ERCA doit maintenir l'intégrité et la disponibilité des enregistrements de certificat de clé publique MSCA.

4.1.10 L'ERCA doit rendre disponible la clé publique ERCA RSA, et doit publier le statut de révocation de certificat de clé publique.

4.1.11 *L'ERCA doit distribuer des clés de test et maintenir l'intégrité des clés de test ainsi que les certificats générés selon le règlement à des fins d'interopérabilité.*

4.2 Exigences de fonctionnement

4.2.1 *Les clés MSCA RSA peuvent être changées régulièrement. Il est supposé que chaque Etat Membre n'aura besoin que d'un nombre réduit de clés par an.*

4.2.2 *Le service de certification de l'ERCA dépendra de la réception à temps des rapports d'audit MSA démontrant que l' Etat Membre continue de remplir ses obligations comme écrit dans la politique MSA approuvée.*

4.2.3 *Le délai exigé pour l'ERCA pour la délivrance de certificat de clé publique MSCA doit être seulement déterminé par le temps exigé pour l'exécution correcte des procédures ERCA.*

4.2.4 *L'ERCA n'imposera aucune limite au nombre de clés MSCA à certifier. Cependant, si des clés MSCA se distinguent simplement par le champ keySerialNumber du CertificationAuthorityKID (Annexe 1(B), Appendice 1 – Dictionnaire de données Section2.36), le nombre de clés uniques dédié à un MSCA sera limité à un maximum de 256.*

4.2.5 *Le service ERCA (Certification de clé et distribution) exige une faible disponibilité. Leur intégrité et l'authenticité pendant le transport seront assurées par des moyens procéduraux (par exemple courrier recommandé). Une durée d'un cycle d'un mois est garantie.*

4.2.6 *La durée de vie exigée des clés ERCA n'est pas définie dans le règlement de la Commission 1360/2002 [2]. L'ERCA devra alors maintenir la paire de clés générique ERCA et les clés maître de capteur de mouvement pendant une période de trente ans. Leur maintenance signifiera : confidentialité, intégrité et disponibilité de clé privée RSA, des clés maître de capteur de mouvement et l'intégrité et la disponibilité de clé publique RSA.*

4.2.7 *L'ERCA fait l'hypothèse que le progrès technologique au cours des trente prochaines années rendra son système obsolète. Des mesures pour la gestion de l'obsolescence sont définies dans le CPS.*

4.3 Approbation de la politique MSA

4.3.1 *L'objectif du processus d'approbation est d'assurer des niveaux de sécurité comparables dans chaque Etat Membre.*

4.3.2 *L'ERCA révisera la politique MSA en fonction de la conformité avec les exigences définies dans la section 5.3.*

4.3.3 *L'ERCA fournira les services de certification de clé à un MSA seulement si la revue du résultat de la politique apporte suffisamment d'éléments pour juger que les exigences de la section 5.3 de ce document sont remplies.*

4.3.4 L'ERCA archivera la revue de la politique et la politique MSA afin de s'y référer.

4.4 Classification des élément constitutifs de l'ERCA

Au tableau 1, les colonnes titre C, I et A indiquent les exigences de sécurité pour la Confidentialité, l'Intégrité et la Disponibilité (Availability). Les niveaux de sécurité possibles sont : X (très haut), H (haut), M (bas à moyen) selon les définitions suivantes :

X (très haut) : briser cet élément constitutif de sécurité conduit à une rupture totale de l'ensemble sécurité et/ou de fonctionnalité du Système de chronotachygraphe numérique. Il est très difficile voire même impossible d'en réparer les dommages causés.

H (haut) : Briser cet élément constitutif de sécurité conduit à des problèmes de rupture sévère de sécurité ou de fonctionnalité du Système de chronotachygraphe numérique. Il sera difficile et/ou très long à réparer les dommages.

M (bas ou moyen) : briser cet élément constitutif de sécurité conduit (au plus) à des problèmes limités de sécurité ou de fonctionnalité du Système de chronotachygraphe numérique. Il est probable que ces problèmes seront rapidement identifiés et/ou pourront être résolus facilement.

La classification de la colonne Sécurité contient la classe de sécurité affectée à chaque élément constitutif et est définie comme suit :

Haut : L'élément constitutif ne doit jamais quitter un environnement sécurisé et contrôlé.

Moyen : L'élément constitutif ne doit pas être connu d'un tiers sans autorisation spéciale.

Bas : L'élément constitutif peut être publié.

Elément constitutif	C	I	A	Classification de sécurite	Remarques
ERCA.SK	X	H	M	High	
ERCA.SK sauvegarde	X	H	M	High	Deux sauvegardes, une hors site
ERCA.PK		H	M	Low	Récepteur (MSCA) exige les preuves d'origine (ERCA).
KmVU, KmWC, Km	X	H	M	High	Récepteur (MSCA) exige les preuves d'origine (ERCA).
Sauvegardes de KmVU, KmWC et Km	X	H	M	High	Deux sauvegardes, une hors site
Clés de test		H		Low	Les identifiants des clés Test doivent être inclues dans les enregistrements MS.C .
Générateur de clé ERCA		X	M	High	Utilisé une seule fois, Exigences appliquées au logiciel générateur de clé avant usage.

MS.KR	M	X	M	Low	Récepteur (ERCA) exige les preuves d'originer (MSCA). ERCA exige les preuves de reconnaissance de clé privée correspondante. ERCA doit établir l'unicité dans le cadre du règlement de la clé de MSCA.
MS.C		M	M	Low	Récepteur (MSCA) exige les preuves d'origine (ERCA).
MS.C Status Information	M	H	H	Low	Information de certificat en ligne
MS.C Records	M	H	H	Medium	L'enregistrement de certificates émis par l'ERCA devient seulement une prevue de validité de MS.C en cas de compromission de ERCA.SK
ERCA CPS	L	M	M	Medium	
MSA policy		M	M	Low	
MSA Evaluation Report	H	M	M	Medium	

Table 1: Classification des éléments constitutifs ERCA

5 OBLIGATION DE MSA

5.1 Responsabilités

5.1.1 Le MSA doit produire et maintenir une politique MSA couvrant les processus suivants, s'ils sont applicables :

a) émission de cartes tachygraphiques, incluant les clés et les certificats ;

b) émission de clés et de certificats pour les UEV ;

c) gestion des clés de capteur de mouvement.

d) Gestion des clés d'un Etat Membre

5.1.2 L'opération et les pratiques de gestion de ce processus doivent être documentées en éléments pratiques approuvés par le MSA.

5.1.3 Le MSA doit être responsable des dispositions des versions anglaises de politiques MSA de l'ERCA.

5.1.4 La politique MSA peut consister en un recueil de documents, comme étant adaptés à l'organisation des services la composant.

5.1.5 Les exigences sur le contenu de la politique MSA sont écrites à la section 5.3 de ce document.

5.2 Soumission d'une politique MSA à l'ERCA

5.2.1 L'objectif de la soumission de chaque politique MSA est de démontrer des niveaux comparables de sécurité se chaque Etat Membre.

5.2.2 La MSA doit soumettre la politique MSA à l'ERCA par une communication formelle.

5.2.3 La politique MSA doit être accompagnée par une référence rationnelle à chaque exigence de la section 5.3.

5.3 Exigences

Exigences formelles

5.3.1 La politique MSA doit identifier les entités en charge des opérations.

5.3.2 la certification des paires de clés d'Etat Membre pour l'équipement et la distribution des clés maîtres pour capteur de vitesse doivent être générés et stockées dans un dispositif qui :

a) soit, est certifié comme satisfaisant aux exigences identifiées dans le FIPS 140-2 (ou FIPS 140-1) au niveau 3 ou supérieur [9] ;

b) soit, est certifié comme satisfaisant les exigences identifiées dans l'Atelier d'Agrément CEN 14167-2 [10] ;

c) soit, est un système digne de confiance qui assure le niveau EAL4 ou supérieur selon l(ISO 15408 [11], ou des critères de sécurité équivalents . Ces évaluations le seront pour un profil de protection ou un objectif de sécurité.

d) Soit, est démontré comme produisant un niveau équivalent de sécurité.

5.3.3 La génération d'une paire de clés d'Etat Membre doit être réalisée dans un environnement physiquement sécurisé par le personnel ayant des rôles de confiance sous au moins un double contrôle.

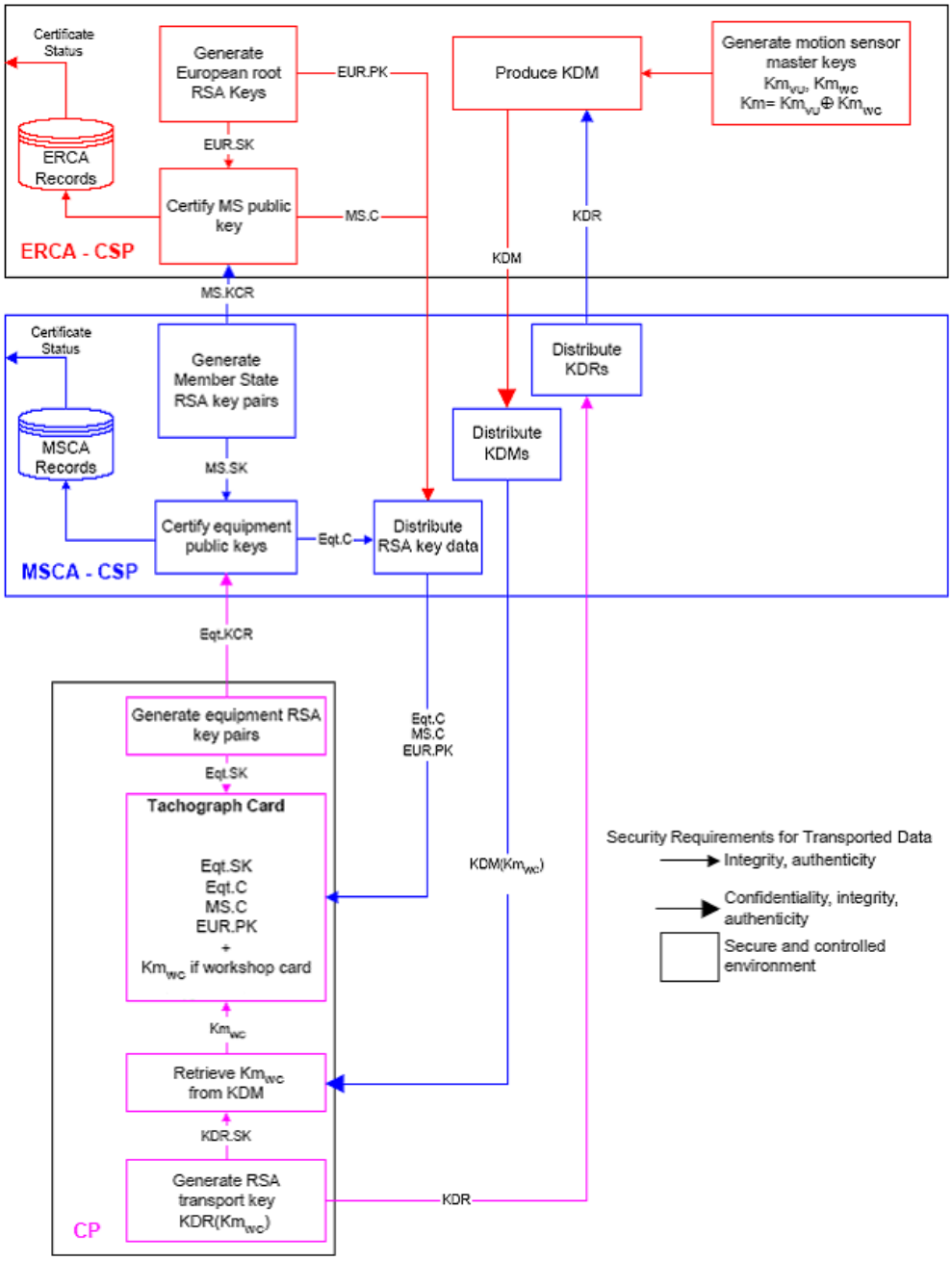

Figure 1 Description De la gestion de clé de l'Annexe I(B)

5.3.4 Les paires de clés d'Etat Membre doivent être utilisées pour une période maximum de deux ans débutant à partir le la certification de l'ERCA.

5.3.5 La génération de paires de clés d'un nouvel Etat Membre doit prendre en compte le cycle d'un mois exigé pour la certification par l'ERCA (Cf. section 4.2.5).

Demandes de certification de clé ERCA de demandes de distribution de clé de capteur de mouvement

5.3.6 Le MSA doit soumettre les clés publique MSCA à la certification par l'ERCA en utilisant le protocole de demande de certification (KCR) décrit à l'Annexe A.

5.3.7 Le MSA doit demander les clés maître de capteur de mouvement à l'ERCA en utilisant le protocole de demande de distribution de clé (KDR) décrit à l'Annexe D.

5.3.8 Le MSA doit reconnaître la clé publique ERCA dans le format de distribution décrit en Annexe B.

5.3.9 Le MSA doit utiliser des supports physiques pour le transport de clé et de certificat comme décrit en Annexe C.

5.3.10 Le MSA doit s'assurer que l'identificateur de clé (KID) et le modulo (n) des clés soumis à l'ERCA pour certification et pour la distribution de clé de capteur de mouvement sont uniques dans le domaine du MSCA.

Fin de vie d'une paire de clés d'Etat Membre

5.3.11 Le MSA doit s'assurer que les clés expirées ne sont pas utilisées d'aucune façon. La clé privée d'un Etat Membre doit être :

Soit détruite, de façon à ce que la clé privée ne puisse être retrouvée

Ou

Soit gelée de façon a en éviter son usage.

Clés d'équipement RSA

5.3.12 Le MSA doit s'assurer qu'une clé RSA d'équipement est générée, transportée, et insérée dans l'équipement de façon à conserver sa confidentialité et son intégrité. Dans ce but, le MSA doit :

- s'assurer que toute prescription pertinente exigée pour la certification de sécurité de l'équipement est satisfaite
- s'assurer qu'à la fois la génération et l'insertion (si non embarqué) a lieu dans un environnement physiquement sécurisé.
- Sauf si la génération de clé était couverte par la certification de sécurité de l'équipement, s'assurer que les algorithmes de génération de clé de chiffrement spécifiés et appropriés soient utilisés ;

Ces deux dernières exigences de génération doivent être satisfaites en générant des clés d'équipement dans un dispositif qui :

a) soit est certifié pour satisfaire les exigences identifiées dans FIPS 140-2 (ou FIPS 140-1) au niveau 3 ou plus haut [9] ;

b) soit est certifié pour satisfaire les exigences identifiées dans l'Agrément d'Atelier CEN 14167-2 [10] ;

c) soit est un système digne de foi qui est confirmé par EAL4 ou plus haut selon l'ISO 15408 [11], au niveau E3 ou plus haut de l'ITSEC [12], ou des critères de sécurité équivalents. Ces évaluations doivent être pour un profil de protection ou un objectif de sécurité.

d) Soit est démontré apporter un niveau de sécurité équivalent.

Généralités sur la clé RSA

5.3.13 *Le MSA doit s'assurer de la confidentialité, de l'intégrité et de la disponibilité des clés privées générées, stockées et utilisées sous le contrôle de la politique MSA.*

5.3.14 *Le MSA doit prévenir l'utilisation non autorisée de clés privées générées, stockées et utilisées sous le contrôle de la politique MSA.*

5.3.15 *Les clés privées des Etats Membres doivent être sauvegardées en utilisant une procédure de récupération de clés exigeant au moins un double contrôle.*

5.3.16 *Les demandes de certification de clé qui reposent sur le transport de clés privées ne sont pas autorisées.*

5.3.17 *Les clés factices sont strictement interdites (cf. définition 12.1)*

Clés symétriques (TDES)

5.3.18 *Les MSA doivent éviter l'usage non autorisé de clés de ses capteurs de mouvement.*

5.3.19 *Le MSA doit s'assurer que la clé maître de capteur de vitesse (Km) ne quittera jamais l'environnement sécurisé et contrôlé du MSA.*

5.3.20 *La clé maître de capteur de mouvement (Km) ne doit jamais abandonner l'environnement sécurisé et contrôlé du MSA.*

5.3.21 *Le MSA devra envoyer la clé atelier de capteur de mouvement (Km_{WC}) au personnalisateur du composant (dans ce cas, le service de personnalisation de carte) par des moyens sécurisés appropriés, dans le seul but de leur insertion dans les cartes Atelier.*

5.3.22 *Le MSA doit envoyer la clé de capteur de mouvement d'UEV (Km_{VU}) au personnalisateur de composant (dans ce cas au fabricant d'UEV) par des moyens appropriés et sécurisés dans le seul but de les insérer dans les UEV.*

5.3.23 La MSA doit maintenir la confidentialité, l'intégrité et la disponibilité des copies des clés des capteurs de mouvement.

5.3.24 Le MSA doit s'assurer que les copies de clés de capteur de mouvement sont stockées dans un dispositif qui :

a) soit est certifié pour satisfaire les exigences identifiées dans FIPS 149-2 (ou FIPS 140-1) niveau 3 ou plus haut [9] ;

b) soit est un système digne de foi qui est confirmé par l'EAL4 ou supérieur selon l'ISO 15408 {11], au niveau E3 ou supérieur de l'ITSEC [12], ou des critères de sécurité équivalents. Ces évaluations doivent être pour un profile de protection ou un objectif de sécurité.

Génération de certificat

5.3.25 Le MSA doit posséder plusieurs paires de clés d'Etat Membre pour la production de certificats d'équipements UEV et cartes tachygraphiques.

5.3.26 Le MSA doit s'assurer de la disponibilité du service de certification de clés publiques d'équipement.

5.3.27 Le MSA doit utiliser les clés privées d'Etat Membre seulement pour :

a) la production de certificats de clé d'équipement de l'Annexe 1(B) en utilisant l'algorithme de signature numérique ISO 9796-2 comme décrit à l'Annexe 1(B) Appendice 11 « Mécanismes de Sécurité Communs »[6].

b) l'émission de listes de révocation des certificats comme décrit à l'annexe A.

c) L'émission de listes de révocation de certificat si cette méthode est utilisée pour fournir l'information de l'état de certificat (cf. 5.3.31)

5.3.28 Le MSA doit signer les certificats d'équipement avec le même dispositif utilisé pour stocker les clés privées de l'Etat Membre (cf.5.3.2)

5.3.29 Dans son périmètre, le MSA doit s'assurer que les clés publiques d'équipement sont identifiées par un identificateur unique de clé qui suit les prescriptions de l'Annexe 1(B)[6].

5.3.30 Sauf si la génération et la certification de clé sont effectuées dans le même environnement sécurisé, le protocole de demande de certification de clé doit fournir la preuve de l'origine et de l'intégrité des demandes de certification, sans révéler la clé privée.

Information d'état de certificat

5.3.31 Le MSA doit maintenir et rendre disponible l'information d'état de certificat.

Personnalisation de composant

5.3.32 La validité de certificat de carte tachygraphique doit être égal à la validité de la carte tachygraphique.

5.3.33 Le MSA doit éviter l'insertion de certificats de validité indéfinie dans des cartes tachygraphiques.

5.3.34 Le MSA peut autoriser l'insertion de certificats d'Etat Membre à validité indéfinie dans les UEV ;

Enregistrement utilisateur

5.3.35 Le MSA doit s'assurer que les utilisateurs des cartes sont identifiés à une étape du processus d'émission de cartes.

Récupération de catastrophe

5.3.36 Le MSA doit s'assurer que l'ERCA est informé sans délai de perte, vol ou compromission potentielle de clés MSA.

5.3.37 Le MSA doit mettre en œuvre des mécanismes appropriés de récupération de catastrophe qui ne dépend pas du temps de réponse de l'ERCA.

Exigences générales de sécurité

5.3.38 Le MSA doit établir un système de gestion de sécurité de l'information (ISMS) basé sur l'évaluation du risque pour toutes les opérations concernées.

5.3.39 Le MSA doit s'assurer que les politiques traitent de la formation du personnel, de leur mise à jour et de leurs rôles

5.3.40 Le MSA doit s'assurer que des enregistrements appropriés des opérations de certification sont maintenus.

5.3.41 Le MSA doit inclure des dispositions pour l'arrêt de sa politique MSA.

5.3.42 La politique MSA doit inclure des procédures de modification.

Audit

5.3.43 L'audit MSA doit établir que les exigences de cette section sont bien maintenues.

5.3.44 Le MSA doit effectuer le premier audit dans les 12 mois depuis le démarrage des opérations couvertes par la politique approuvée. Lorsqu'un audit ne trouve aucune preuve de non-conformité, le prochain audit peut être effectué dans les 24 mois. Lorsqu'un audit trouve une preuve de non-conformité, le prochain audit doit être effectué dans les 12 mois.

5.3.45 Le MSA doit faire un rapport des résultats de l'audit comme mentionné en 5.5.43 et fournir le rapport d'audit, en anglais, à l'ERCA.

5.3.46 *Le rapport d'audit doit définir toute action corrective, y compris un calendrier de mise en œuvre exigé pour remplir les obligations du MSA.*

6 PRATIQUE DE L'ERCA

L'ERCA doit fournir aux MSCA les services suivants :

a) Enregistrement

b) Génération de certificat

c) Distribution

d) Révocation

e) Etat de révocation

6.1 Déclaration de pratiques de Certification

6.1.1 L'ERCA CPS est le document de procédure de l'ERCA, qui détaille la façon dont la politique est imposée dans une gestion au jour le jour. Le document est développé par l'ERCA. L'ERCA CPS appartient à l'ERCA.

6.1.2 L'ERCA CPS doit avoir une divulgation restreinte.

6.1.3 L'ERCA doit fournir un CPS complet aux MSCA et fournir toute information nécessitée par les MSCA.

6.1.4 L'ERCA CPS doit être géré, revu, et modifié suivant les procédures de contrôle de documents.

6.2 Génération des Clés ERCA

6.2.1 Les clés RSA ERCA doivent être générées selon l'Annexe 1(B) Appendice 11 CSM_014 [6].

6.2.2 La génération des clés RSA ERCA, les clés maîtres de capteur de mouvement et leur copies de sauvegarde sont prises en charge dans un environnement physiquement sécurisé par un personnel de confiance sous au moins un double contrôle. La cérémonie de génération de clé est décrite dans l'ERCA CPS.

6.2.3 L'ERCA ne doit pas générer de paires de clés RSA pour ses abonnés (MSCA).

6.2.4 Une séquence de tests RSA et de clés de capteur de mouvement, y compris de clés MSCA, de clé d'équipement, de certificats de clé publique, et de code source est disponible sur demande à l'ERCA pour les tests d'interopérabilité.

6.3 Stockage, sauvegarde et récupération de clé ERCA

6.3.1 L'ERCA doit maintenir la confidentialité, l'intégrité et la disponibilité de la clé privée générique RSA et les clés maîtres de capteur de mouvement.

6.3.2 *L'ERCA doit seulement maintenir les paramètres suivants de la clé générique RSA : le modulo (n), l'exposant public (e), l'exposant privé (d).*

6.3.3 *La clé privée RSA de l'ERCA et les clés maître de capteur de mouvement doivent être sauvegardées, stockées et récupérées seulement par le personnel de confiance en utilisant au moins un double contrôle dans un environnement physique sécurisé.*

6.3.4 *Les copies de sauvegarde de la clé privée RSA de l'ERCA et les clés maître de capteur de mouvement doivent l'objet du même niveau de contrôles de sécurité que pour les clés en service. Une copie de sauvegarde de la clé privée RSA de l'ERCA et des clés maître de capteur de mouvement doit être maintenue hors site.*

6.4 Distribution de clé ERCA

6.4.1 *Les procédures assurant la confidentialité, l'intégrité et l'authenticité au cours de la distribution sont décrites dans l'ERCA CPS.*

6.4.2 *L'ERCA doit distribuer les clés maître de capteur de mouvement de façon sécurisée sur une base « à savoir » :*

a) Km aux MSCA dont dépendent les fabricants de capteur de mouvement

b) Km_{VU} aux MSCA dont dépendent les fabricants d'UEV

c) Km_{WC} aux MSCA dont dépendent les personnalisateurs de cartes atelier.

6.5 Clé factice

La clé factice est strictement interdite (cf. définition 12.1)

6.6 Clé ERCA en service

6.6.1 *La clé privée RSA de l'ERCA doit seulement être utilisée pour la production des certificats des clés publiques des MSCA comme décrit à l'Annexe 1(B), Appendice 11, CSM_018 [6].*

6.6.2 *La clé privée RSA de l'ERCA doit seulement être utilisée dans un environnement physique sécurisé par un personnel digne de foi avec un double contrôle.*

6.6.3 *Tous les événements d'usage de clé privée ERCA doivent être enregistrés.*

6.6.4 *L'ERCA ne doit pas utiliser les clés maître de capteur quelque soit la finalité.*

6.7 Cycle de fin de vie de clé ERCA

A la fin du cycle de vie, toutes les copies de clé privée RSA de l'ERCA doivent être détruites de telle façon que la clé privée ne puisse être retrouvée.

6.8 Demandes de MSCA

6.8.1 L'ERCA doit s'assurer que les demandes de certification de clé publique de MSCA et les demandes de distribution de clé maître de capteur de mouvement soient complètes, précises et dûment autorisées.

6.8.2 L'ERCA doit s'assurer que, dans le domaine des clés publiques des MSCA reçues de l'ERCA, chaque clé publique de MSCA a un identifiant unique (KID) et un modulo (n), et qu'il n'a pas été précédemment certifié par l'ERCA, ou utilisé pour la distribution de clé de capteur de mouvement.

6.8.3 L'ERCA doit s'assurer que le MSCA a en sa possession la clé privée associée à la clé publique présentée à la certification ou à la distribution de clé de capteur de mouvement.

6.8.4 Après la distribution réussie d'un nouveau certificat de MSCA, L'ERCA doit mettre à jour l'information du statut du certificat.

6.8.5 L'ERCA doit conserver les demandes de certification de clé d' Etat Membre, les demandes de distribution de clé de capteur de mouvement et les certificats des clés publiques.

6.9 Validité de certificat

6.9.1 L'ERCA établira, par défaut, la fin de validité des certificats des clés publique des MSCA pour les cartes tachygraphiques pour sept ans à partir de la date de la production de signature.

6.9.2 L'ERCA produira uniquement des certificats à validité indéfinie lorsque le MSCA spécifie que les clés RSA seront utilisées pour la production de certificats d'UEV (Cf. protocole KCR en Annexe A)

6.9.3 L'ERCA doit utiliser la fin de validité spécifiée par le KCR de MSCA si elle ne dépasse pas la limite définie dans la clause 6.9.1 ci-dessus.

6.10 Certificat et distribution de clé de capteur de mouvement

Les procédures par lesquelles des certificats et des messages de distribution de clé de capteur de mouvement sont rendus disponibles pour les MSCA sont décrites dans l'ERCA CPS et communiquées aux MSCA.

6.11 Information de l'état d'un certificat

6.11.1 Le statut des certificats de clé publique des MSCA peut être retrouvé en ligne par toute partie intéressée utilisant l'information de l'état de certificat public sur http:// dtc.jrc.ec.europa.eu

6.11.2 *L'information de certificat publiée doits consister en la Référence du Porteur de Certificat et un message de résumés du certificat en question.*

6.12 Révocation de certificat

6.12.1 *Les procédures de révocation de certificat sont décrites dans le CPS*

6.12.2 *Un MSA peut demander la révocation de ses propres certificats de MSCA*

6.12.3 *L'authenticité et l'intégrité de demande de révocation de certificat doivent être établies avant que le certificat soit révoqué.*

6.12.4 *Les certificats de MSCA doivent être révoqués en cas de doute fondé ou de compromission des clés secrètes de MSCA.*

6.12.5 *L'ERCA doit maintenir l'intégrité de l'information de l'état de révocation de certificat.*

7 GESTION ET FONCTIONNEMENT DE L'ERCA

7.1 Gestion de la sécurité

7.1.1 Les procédures administratives et de gestion de l'ERCA ainsi que le système de gestion de la sécurité de l'information font l'objet d'audits périodiques.

7.1.2 L'ERCA conserve la responsabilité pour tous les aspects de dispositions des services de certification. Aucune fonction de l'ERCA n'est sous-traitée à des tiers.

7.1.3 Tous les changements de l'infrastructure de la sécurité de l'information qui impactera le niveau de sécurité fourni devra faire l'objet d'une revue.

7.1.4 Les procédures opérationnelles de moyens de l'ERCA, les systèmes et les éléments constitutifs d'information fournissant les services de certification font l'objet de procédures de contrôle de révision définies dans l'ERCA CPS.

7.1.5 Les incidents de sécurité sont reportés à l'autorité Européenne sans délai déraisonnable et au moins dans les 8 heures après leur découverte.

7.2 Classification d'élément constitutif

7.2.1 Les éléments constitutifs d'information doivent être assignés à une classification de sécurité et assignés à un niveau de protection compatible avec les exigences de fonctionnement et de sécurité du chapitre 4.

7.2.2 Les éléments constitutifs d'information ERCA doivent être assignés à une classification de sécurité selon le besoin, les priorités et le degré de protection.

7.3 Sécurité du personnel

7.3.1 Le personnel doit être des employés de l'ERCA, possédant la connaissance d'expert, l'expérience et la qualification nécessaire pour les services offerts et appropriée pour la fonction du poste.

7.3.2 La formation du personnel est gérée selon le plan de formation décrit dans l'ERCA CPS.

7.3.3 La désignation du personnel pour des rôles de confiance doit être gérée selon un processus établi de dépistage.

7.3.4 Les rôles et responsabilités de sécurité sont documentés dans la description de poste dans l'ERCA CPS. Les rôles de confiance, pour lesquels la sécurité du fonctionnement de l'ERCA dépend, sont clairement identifiés.

7.3.5 Les descriptions de postes du personnel ERCA sont définies du point de vue de la séparation des charges et de privilège réduit.

7.3.6 Les rôles de confiance suivants sont définis :

a) officier : Responsable de l'authentification des demandes de certification de clés des MSCA. Autorisé à produire les certificats des clés publiques RSA pour les MSCA.

b) Administrateur : responsable de la génération de paire de clés RSA ERCA et des clés maître de capteur de mouvement.

c) Opérateur : autorisé à effectuer la sauvegarde et la récupération du système.

d) Auditeur : autorisé à voir et maintenir des archives et des enregistrements d'audit des systèmes fiabilisés de l'ERCA.

7.3.7 Aucune personne n'est autorisée d'effectuer plus d'un des rôles de confiance définis ci-dessus.

7.4 Sécurité physique et environnementale

Les services de génération de clé et de certificat doivent être hébergés dans une zone sécurisée, protégée par un périmètre de sécurité défini, avec des barrières de sécurité appropriées et des contrôles d'accès pour éviter des accès non autorisés, des dommages et des interférences.

7.5 Enregistrements des demandes de MSCA

7.5.1 Les enregistrements de certificat ERCA devront consister au minimum en :

a) référence de détenteur de certificat (CHR)

b) Certificat de fin de validité (EOV)

c) Le modulo (n) et l'exposant (e) de la clé publique MSCA

d) Demande de certification de clé MSCA (KCR)

e) Le certificat MSCA

7.5.2 Les enregistrements de distribution de clé de capteur de mouvement consistent au minimum en :

a) Identifiant de clé publique MSCA (KID)

b) Le modulo (n) et l'exposant (e) de la clé publique MSCA

c) La demande de distribution de clé MSCA (KDR)

d) Le message de distribution de la clé de capteur de mouvement (KDM)

7.5.3 L'intégrité des enregistrements de certificat de clé et des enregistrements de distribution de clé de capteur de mouvement doit être maintenue.

7.5.4 Les événements de gestion de clé et de certificat doivent être horodatés et enregistrés.

7.5.5 L'intégrité des enregistrements du système d'événement ERCA doit être maintenu.

7.6 Récupération de catastrophe

7.6.1 Les incidents suivants sont considérés comme des catastrophes :

a) compromission ou vol de clé générique ERCA et/ ou des clés maître de capteur de mouvement

b) perte de la clé générique ERCA et ou des clés maître de capteur de mouvement

c) Panne matérielle de l'informatique

7.6.2 Dans le cas de compromission ou de vol de la clé générique ERCA et ou des clés maître de capteur de mouvement, l'ERCA doit informer immédiatement la Commission et les MSCA et la Commission doit prendre des mesures appropriées dans un délai raisonnable.

7.6.3 Dans le cas de perte de la clé générique ERCA, les mécanismes d'authentification mutuelle cesseront de fonctionner dès que la validité des certificats de clé publique de l'Etat Membre expire. Cet incident, pour lequel il n'y effectivement aucune récupération, est évité par l'utilisation de multiples copies de sauvegarde des clés générique, sur un éventail de supports d'enregistrements objets de contrôles périodiques.

7.6.4 Dans le cas de perte des clés maître de capteur de mouvement, la récupération peut être effectuée grâce au transfert de responsabilité pour les clés maître de capteur de mouvement à un MSCA qui détient deux clés parmi Km, Km_{VU} et Km_{WC}. Toute clé peut être récupérée connaissant les deux autres. Les mesures de prévention de cet incident sont l'utilisation de copies de multiples sauvegardes des clés maîtres de capteur de mouvement, sur un éventail de supports de stockage objet de contrôles périodiques. La façon de transférer la responsabilité est en dehors du champ de ce document.

7.6.5 La protection contre les pannes matérielles est assurée par la redondance, c'est-à-dire la duplication du système informatique. Pour se protéger de l'obsolescence matérielle, le système ERCA sera réimplanté sur de nouveaux types de matériels, de façon à ce que , à tout moment, deux systèmes au moins soient capables d'effectuer les opérations de certification en étant disponibles.

7.7 Pérennité de l'ERCA

7.7.1 En cas d'arrêt de l'activité de l'ERCA par l'organisation désignée, l'autorité Européenne doit désigner une nouvelle organisation responsable de la mise en œuvre de cette politique et des dispositions des services de certification de clé pour l'Etat Membre.

7.7.2 L'ERCA doit transférer ses élément constitutifs (cf. section 4.4) à l'autorité Européenne en s'assurant que la confidentialité et l'intégrité sont maintenues.

8 PROCEDURES DE CHANGEMENT DE LA POLITIQUE ERCA

8.1 Les seuls changements qui peuvent être apportés à cette politique sans notification sont des corrections éditoriales ou typographiques.

8.2 Les changements que l'ERCA peut apporter à cette politique avec notification aux MSA mais sans commentaire des MSA sont des changements de détails de contact.

8.3 Tous les autres changements de la politique ERCA seront apportés seulement après notification et réception des commentaires de l'ERCA et des MSA selon la procédure suivante :

a) Les MSA ou l'ERCA doit soumettre des propositions de changement de la politique ERCA à l'Autorité Européenne

b) L'Autorité Européenne doit distribuer les propositions de changement de la politique ERCA aux MSA et à l'ERCA.

c) L'Autorité Européenne doit fixer une période appropriée pour les commentaires.

d) Les MSA et l'ERCA peuvent commenter les changements proposés dans la période définie pour cela.

e) L'autorité Européenne doit prendre en considération les commentaires et doit décider lequel, s'ils sont multiples, des changements notifiés mettre en œuvre.

f) L'autorité Européenne doit notifier les MSA et l'ERCA de sa décision, et doit fixer une période appropriée pour que les changements soient mis en œuvre.

9 CONFORMITE AUX NORMES

9.1 ETSI TS 102 042 ne contient pas de disposition pour la gestion des clés de chiffrement symétriques telles que celles utilisées dans le capteur de mouvement (cf ISO / IEC 16844-3 *interface de capteur de mouvement* [7]).

9.2 ETSI TS 102 042 fait explicitement référence à l'ISO/IEC 9794-8 | ITU-T, *Recommandation X.509, Technologie de l'information – Interconnexion des systèmes ouverts –répertoire : clé publique et trames de certificat d'attribut* [13].

9.3 Les certificats X.509 n'ont pas été adoptés par le concepteur du système chronotachygraphe numérique.

9.4 Une structure de certificat de clé publique propriétaire basée sur l'ISO/IEC 9796-2, *Technologie de l'information – Techniques de sécurité – principes de signature numérique avec récupération de message* [14], et incompatible avec X.509 a été développée pour le Règlement (cf Annexe 1(B) Appendice 11 [6]).

9.5 L'étape de minimisation de signature – décrite à l'Annexe A.4 de la norme ISO/IEC 9796-2 : 1997 – ne doit pas être effectuée pendant la production des certificats de clé publique de l'Annexe 1(B).

10 REFERENCES

[1] Règlement du Conseil (EC) No 2135/98 du 24 Septembre 1998; Journal Officiel des Communautés Européennes L274, 09.10.98.

[2] Règlement de la Commission (EC) No 1360/2002 du 13 Juin 2002 Journal Officiel des Communautés Européennes L207, 05.08.2002.

[3] Guide de Sécurité Commun, v1.0; Card Issuing Group SWG3; disponible sur: http://www.urba2000.com/chrono/public/public.htm

[4] Guide et Format Politique Nationale d'Autorité de Certification pour le système de chronotachygraphe Numérique, v1.0; Card Issuing Group SWG3; disponible sur :http://www.urba2000.com/chrono/public/public.htm

[5] ETSI TS 102 042 V1.1.1 (2002-04) *Policy requirements for certification authorities issuing public key certificates*

[6] Règlement de la Commission (EC) No 1360/2002, Annex I(B) Appendix 11 – *Mécanismes communs de sécurité*

[7] ISO / IEC 16844-3 *Road vehicles – Tachograph systems – Part 3: Motion sensor interface*

[8] ISO / IEC 17799:2000 *Information technology – Code of practice for information security management*

[9] FIPS PUB 140-2 *Security Requirements for Cryptographic Modules* NIST, 2001

[10] CEN Workshop Agreement 14167-2: *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2 Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP)*

[11] ISO / IEC 15408 (Parts 1 to 3) *Information technology – Security techniques – Evaluation criteria for IT security*.

[12] ITSEC *Information Technology Security Evaluation Criteria* 1991 v1.2

[13] ISO / IEC 9794-8 | ITU-T Recommendation X.509 *Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks*

[14] ISO / IEC 9796-2 (1997-09-01) *Information Technology – Security Techniques – Digital signature schemes giving message recovery*

[15] PKCS#1 v2.0: *RSA Cryptography Standard*, RSA Laboratories, October 1, 1998.

11 ABREVIATIONS

CA Certification Authority

CP Component Personaliser

CPS Certification Practice Statement

CRL Certificate Revocation List
CSP Certification Services Provider
EA European Authority
ERCA European Root Certification Authority
ETSI European Telecommunications Standards Institute
KCR Key Certification Request
KDR Key Distribution Request (for motion sensor master keys)
KDM Key Distribution Message (encrypted motion sensor master key)
Km Motion sensor master key
Km_{VU} Motion sensor master key inserted in vehicle unit
Km_{WC} Motion sensor master key inserted in workshop card
MSA Member State Authority *(Etat Membre ou Partie Contractante à l'AETR)*
MSCA Member State Certification Authority *(Etat Membre ou Partie Contractante à l'AETR)*
PK RSA public key
PKI Public Key Infrastructure
RSA Rivest, Shamir, Adleman (asymmetric encryption scheme)

SK RSA secret key

UEV Unité Embarquée Véhicule

12 DEFINITIONS

12.1 Clé factice : la soumission d'une copie d'une clé à une entité autorisée à utiliser cette copie pour un motif autre que de la retourner à son entité d'origine**.**

ANNEXE A : DEMANDES DE CERTIFICAT DE CLE

A.1 Demande de certification de clé d'un MSCA

A.1.1 Le format et le protocole de demande de certificat de clé publique suivant doivent être utilisés par l'ERCA. Ce format est seulement basé sur les mécanismes de sécurité déjà définis dans le règlement. Le protocole démontre que l'entité (E) soumettant une demande de certificat possède la clé privée RSA (E.SK) associée à la clé publique RSA (E.PK) dont la certification par l'ERCA est exigée.

A.1.2 L'entité (E) soumettant la demande de certification de clé est identifiée par des moyens procéduraux définis dans l'ERCA CPS.

A.1.3 Le MSCA doit créer le CertificateContent (164 octets) selon les règles suivantes :

CPI	Certificate Profile Identifier. La valeur de ce champ est 01h (1 octet)
CAR	Certification Authority Reference. 8 octets champ identifiant l'ERCA, comme défini dans l'Annexe I(B), Appendice 1, Section 2.36. Ce champ doit être la chaine d'octets: 'FDh' NationNumeric: Communauté Européenne '45h' '43h' '20h' NationAlpha: 'EC ' '00h' keySerialNumber 'FFh' 'FFh' additionalInfo '01h' caIdentifier Les demandes de clés de Test doivent contenir les valeurs '54h', '4Bh' ('TK') dans le champ additionalInfo.
CHA	Certificate Holder Authorization. 7 octets comme défini dans l'Annexe I(B), Appendice 1, Section 2.34 having the value: 'FFh', '54h', '41h', '43h', '48h', '4Fh' EquipmentType: 1 octet comme défini dans l'Annex I(B), Appendix 1, Section 2.52 The MSCA doit specifier EquipmentType 6 (UEV) lors de demande d'un certificat à validité indéfinie. NB: L'ERCA doit fixer l' EquipmentType à 0 (utilisé pour identifier des certificats de clé CA) pendant la production de signature.
EOV	End Of Validity. 4 octets entier représentant le nombre de secondes depuis minuit le 1°Janvier 1970 GMT, comme retourné par la fonction time() d'Unix. Si indéfini, c-à-d illimité, la validité doit être 'FFh', 'FFh', 'FFh', 'FFh'
CHR	Certificate Holder Reference. Champ unique de octets identifiant le MSCA, comme défini dans l'Annexe I(B), Appendice 1, Section 2.36.
n	Le modulo de la clé publique du détenteur de certificat; dimension 128 octets (1024 bits)
e	L'exposant de la clé publique du détenteur de certificat, dimension 8 octets (64 bits)

A.1.4 Avec le CertificateContent comme défini ci-dessus, la demande de certification de clé de MSCA est préparée comme suit :

1 calcul du SHA-1 hash du CertificateContent (164 octets), produisant le *HASH(Cc)* (20 octets).
2 Format *HASH(Cc)* comme un message complètement récupérable à l'intérieur d'un message représentatif selon l'ISO/IEC 9796-2:1997 le SHA-1 hash implicitement identifié comme suit: '4Bh' | quatre vingt cinq fois 'BBh' | 'BAh' | *Hash(Cc)* | *Hash(Hash(Cc))* | 'BCh'
3 Signe le message représentatif ci-dessus utilisant E.SK, en appliquant la signature primitive définie dans PKCS#1, produisant la signature SKR 128 octets).
4 Concatène *Cc* et *SCc* pour donner la demande de certification de clé (292 octets)

A.1.5 La demande de certification de clé est traitée par l'ERCA comme suit :

1 Extraction E.PK du champ *Cc* de la demande de certification de clé .
2 Ouverture du champ *SCc* de la demande de certification de clé utilisant E.PK.
3 Vérification des contenus de la signature ISO 9796-2 signature, produisant le message récupéré *Mr'* (20 octets)
4 Calcul du SHA-1 hash du champ *Cc* de la demande de certification de clé, produisant HASH(Cc) (20 octets)
5 Rejet la demande de certification de clé si *Mr'* n'est pas égal à *HASH(Cc)*

A.1.6 Si la demande de certification de clé est acceptée, l'ERCA doit procéder à des vérifications additionnelles du contenu de certificat. Ces vérifications sont décrites dans les sections suivantes.

A.1.7 L'ERCA devra communiquer avec le MSA via un canal alternatif établissant que la demande de certification de clé est dûment autorisée.

A.1.8 Au cours de cette communication, l'ERCA devra vérifier que le SHA-1 hash de la demande de certification de clé est connue du MSA.

A.2 Vérifications de la valeur et de l'identité des clés RSA

A.2.1 L'ERCA doit appliquer les vérifications suivantes à chaque clé publique RSA, en incluant les clés de test, soumises à certification.

A.2.2 Le modulo (n) doit être un entier impair, compris dans les valeurs :

$$2^{1023}+1 \leq n \leq 2^{1024}-1$$

A.2.3 Le modulo (n) doit être vérifié pour son unicité parmi les enregistrements des clés signés par l'ERCA.

A.2.4 L'exposant public (e) doit être un entier impair compris dans les valeurs :

$$3 \leq e \leq 2^{64}-1$$

A.2.5 Le Certificate Holder Reference (CHR) doit être vérifié pour son unicité parmi les enregistrements de clés signés par l'ERCA.

A.2.6 L'ERCA doit rejeter les demandes de certification de clé de MSCA si une des exigences ci-dessus n'est pas satisfaite.

A.3 Vérification de la fin de validité et du type d'équipement

A.3.1 Le règlement identifie sept types d'équipements (cf. Règlement 1360/2002 Annexe 1(B), Appendice 1, Section 2.52 [2]).

A.3.2 les certificats des clés publiques des Etats Membres insérées dans quatre types d'équipement (cartes de conducteur, atelier, contrôleur et entreprise) doivent avoir une validité limitée.

A.3.3 Les certificats des clés publiques de MS insérés dans un type d'équipement (UEV) doivent avoir une fin de validité indéfinie.

A.3.4 Les certificats des clés publiques ne sont pas applicables aux fabricants de cartes et de capteurs de mouvement.

A.3.5 L'ERCA doit vérifier que le type d'équipement spécifié au 7° octet du champ CHA du CertificateContent, et doit fixer une fin de vie indéfinie seulement si cet octet a la valeur 6, identifiant un type d'UEV.

A.3.6 Au cours de la production de signature, l'ERCA doit fixer la valeur de l'EquipmentType à 0 (comme exigé pour identifier un certificat CA).

ANNEXE B : FORMAT DE DISTRIBUTION DE CLE PUBLIQUE

B.1 La clé publique ERCA doit être distribuée à l'abonné dans le format suivant :

CHR	Certificate Holder Reference. 8 octets identifiant l'ERCA, comme défini dans le Règlement 1360/2002 Annexe I(B), Appendice 1, Section 2.36 [2]. Ce champ doit être la suite d'octets : 'FDh' NationNumeric: Communauté Européenne '45h' '43h' '20h' NationAlpha: 'EC ' '00h' keySerialNumber 'FFh' 'FFh' additionalInfo '01h' caIdentifier Les clés de Test doivent contenir les valeurs '54h', '4Bh' ('TK') dans le champ additionalInfo.
n	Le modulo de la clé publique du détenteur de certificat; dimension 128 octets (1024 bits)
e	L'exposant du certifiact du détenteur de la clé publique, dimension 8 octets (64 bits)

B.2 La clé publique ERCA doit être fournie directement à l'abonné par un courrier recommandé. L'utilisation d'un courrier recommandé établit l'authenticité et l'intégrité de la clé publique.

ANNEXE C : DISTRIBUTION DE CLE

Le support physique utilisé au transport des demandes de certification de clé MSCA, de certificats MSCA, de la clé publique ERCA, et clés maître de capteur de mouvement son décrits ci-après.

C.1 Support de transport

C.1.1 Pour des raisons officielles et de test, l'ERCA doit accepter des demandes de certification de clé et des demandes de distribution de clé de capteur de mouvement et distribuer la clé publique ERCA, les certificats MSCA et les messages de distribution de clé maître de capteur de mouvement sur un CD-R.

C.1.2 le CD-R doit être un support de 12 cm en mode de session unique (format ISO 9660 :1988).

C.1.3 Les noms de fichiers doivent être en format 8.3. Les extensions de nom de fichier doivent être :

txt pour des fichiers contenant des données hexadécimales ASCII :

pem pour les fichiers contenant des données encodées en base 64.

bin pour les fichier contenant des données binaires.

C.1.4 Les demandes officielles de certification de clé, de certificats de clés et de demandes de distribution de clé de capteur de mouvement doivent être accompagnées d'une copie papier de données formatées selon un modèle défini par l'ERCA.

C.1.5 Dans le seul but de test, l'ERCA doit accepter et distribuer les demandes de certification de clé, des exemples de certificats, et des exemples de clés sur des floppy disks DOS de 3.5 pouces , ou comme pièces jointes à un email .

C.2 Procédures de transport

C.2.1 Les demandes officielles de certification de clé MSCA la clé publique ERCA, les demandes de distribution de clé maître de capteur de mouvement, et les messages de distribution de clé maître de capteur de mouvement doivent être exportées par un courrier recommandé désigné par le MSA.

C.2.2 La personne de contact du MSA doit communiquer des données d'identification du courrier recommandé à l'ERCA en temps utile (normalement 5 jours ouvrés) pour la préparation des permis exigés pour accéder aux locaux de la Commission Européenne.

ANNEXE D : DISTRIBUTION DE CLE MAITRE DE CAPTEUR DE MOUVEMENT

D.1 Demande de clé maître de capteur de mouvement

D.1.1 Le format et le protocole de demande de clé suivant doivent être utilisés pour transférer une des clés maître du capteur de mouvement (Km, KmWC et KmVU) de l'ERCA au MSCA. Le protocole est basé sur le protocole de demande de certification de clé.

D.1.2 Le protocole utilise une paire de clés RSA générée par le MSCA dans le seul but d'assurer la confidentialité de l'une des clés maître de capteur de mouvement Km, KmVU ou KmWC au cours du transport entre l'ERCA et le MSCA.

D.1.3 la procédure de distribution de clé de capteur de mouvement utilises le protocole ERCA KCR pour démontrer que l'entité (E) soumettant la demande possède la clé privée RAS (E.SK) associée à la clé publique RSA (E.PK) fournie pour le chiffrement de la clé maître de capteur de mouvement.

D.1.4 L'entité (E) soumettant la demande de certification de clé est identifiée par des moyens procéduraux définis par l'ERCA CPS.

D.1.5 Le MSCA doit créer la demande de clé maître de capteur de mouvement (KDR – 164 octets) selon les règles suivantes :

CPI	Certificate Profile Identifier. La valeur de ce champ est 01h (1 octet)
CAR	Certification Authority Reference. 8 octets identifiant l'ERCA, comme défini à l'Annexe I(B), Appendice 1, Section 2.36. Ce champ est constitué des octets: 'FDh' NationNumeric: Communauté Européenne '45h' '43h' '20h' NationAlpha: 'EC ' '00h' keySerialNumber 'FFh' 'FFh' additionalInfo '01h' caIdentifier Les demandes de clé Test doivent contenir les valeurs '54h', '4Bh' ('TK') dans le champ additionalInfo.
MRA	Message Recipient Authorization. 7 octets dont la valeur est la concaténation de : 'FFh', '54h', '41h', '43h', '48h', '4Fh' avec le type de clé maitre de capteur de mouvement : 1 octet défini comme suit: '07h': Km, clé maitre de capteur de mouvement; '27h': KmWC, clé maitre de capteur de mouvement insérée dans les cartes atelier; '67h': KmVU, clé maitre de capteur de mouvement insérée dans l'UEV; NB: Ces codes sont basés sur les codes EquipmentType définis à l'Annexe I(B), Appendice 1, Section 2.52.
KID	Key Identifier: unique octet identifiant une clé publique de MSCA, comme défini à l'Annexe I(B), Appendice 1, Section 2.36, avec les modifications suivantes : NationNumeric: approprié pour le MSCA NationAlpha: approprié pour le MSCA keySerialNumber: '00h' .. 'FFh' compteur incrémental de KDR à partir du CA national additionalInfo:'4Bh' '52h' ('KR' pour Key Request)

	type de clé maître: 1 octet comme defini après : '07h': Km, clé maitre de capteur de mouvement; '27h': KmWC, clé maitre de capteur de mouvement insérée dans les cartes atelier; '67h': KmVU, clé maitre de capteur de mouvement insérées dans les UEV
n	Le modulo de E.PK utilisé pour le chiffrement de la clé maitre de capteur de mouvement; dimension 128 octets (1024 bits)
e	L'exposant de E.PK utilisé pour le chiffrement de la clé maitre de capteur de mouvement, dimension 8 octets (64 bits)

D.1.6 Le MSCA construit la demande de distribution de clé comme suit :

1 Calculer le SHA-1 hash de la demande (164 octets), produisant *HASH(KR)* (20 octets).
2 Format *HASH(KR*) comme un message complètement récupérable encapsulé dans un message de 1024-bits représentatif comme indiqué dans ISO/IEC 9796-2:1997 avec SHA-1 hash implicitement identifié comme suit : '4Bh' | quatre vingt cinq fois 'BBh' | 'BAh' | *Hash(KR)* | *Hash(Hash(KR))* | 'BCh''
3 Signe le message représentatif ci-dessus utilisant E.SK, en appliquant la signature RSASP1 primitive definie dans PKCS#1, produisant la signature *SKR* (128 octets).
4 Concatène *KR* et *SKR* pour donner la demande de clé maître de capteur de mouvement (292 octets)

D.1.7 La demande de distribution de clé maître de capteur de mouvement est construite par l'ERCA comme suit :

1 Extraire E.PK du champ *KR* de la demande de clé maître.
2 Certification de clé ouvrir le champ *SKR* de la demande *de* certification de clé utilisant E.PK.
3 Vérifier les contenus de la signature ISO 9796-2 , produisant le message récupéré *Mr'* (20 octets)
4 Calcule le SHA-1 hash du champ *KR* de la demande de clé maître de capteur de mouvement, produisant *HASH(KR)* (20 octets)
5 Rejet de la demande de clé maître si *Mr'* n'est pas égal à *HASH(KR)*

D.1.8 Si la demande de clé maître de capteur de mouvement est acceptée, l'ERCA doit procéder aux vérifications complémentaires sur le contenu de la demande. Ces vérifications sont décrites dans la section suivante.

D.1.9 L'ERCA doit communiquer au MSA via un canal alternatif établissant que la demande de clé maître de capteur de mouvement est dûment autorisée.

D.1.10 Au cours de cette communication, l'ERCA doit vérifier que le SHA-1 hash de la demande de clé maître de capteur de mouvement est connue du MSA.

D.2 Vérifications sur le contenu de la demande

D.2.1 Le modulo (*n*) RSA doit être un entier impair, compris dans les valeurs :

$$2^{1023}+1 \leq n \leq 2^{1024}-1$$

D.2.2 L'exposant public RSA (e) doit être un entier impair, compris dans les valeurs :

$$3 \leq e \leq 2^{64}-1$$

D.2.4 La politique du MSCA identifiée par l'identifiant clé (KID) doit être vérifiée pour justifier le type de clé maître de capteur de mouvement demandé.

D.2.5 L'ERCA doit rejeter les demandes de clé maître de capteur de mouvement si une des exigences ci-dessus n'est pas satisfaite.

D.3 Chiffrement de la clé de capteur de mouvement

D.3.1 L'ERCA doit construire la clé étiquette de capteur de mouvement (LKM) selon les règles suivantes :

KID	Key Identifier. Champ unique de 8 octets identifiant le MSCA comme défini à l'Annexe I(B), Appendice 1, Section 2.36, avec les modifications suivantes pour identifier la clé maitre de capteur de mouvement demandée : NationNumeric: appropriée pour le MSCA NationAlpha: appropriée pour le MSCA keySerialNumber: '00h' .. 'FFh' compteur incremental de KDR provenant du CA national additionalInfo '44h', '4Bh' ('DK' pour clé DES) type de clé maître: 1 octet défini ci-dessous: '07h': Km, Clé maître de capteur de mouvement; '27h': KmWC, Clé maître de capteur de mouvement insérée dans les cartes atelier; '67h': KmVU, Clé maître de capteur de mouvement insérée dans les UEV.
KM	Clé maître de capteur de mouvement (16 octets).

D.3.2 L'ERCA doit chiffrer le LKM de 24 octets avec la clé publique fournie par le MSCA selon le modèle de chiffrement RSA RSAES-PKCS1-v1_5-ENCRYPT [15] pour produire la clé chiffrée DES de 128 octets (EDK).

D.3.3 L'ERCA doit distribuer la clé maître chiffrée de capteur de mouvement au MSCA demandeur dans un format de message de distribution clé (KDM) de 136 octets.

KID	Key Identifier: même valeur que définie en D.3.1.
EDK	Encrypted DES key. La clé maître chiffrée de capteur de mouvement selon le modèle de chiffrement RSA RSAES-PKCS1-v1_5-ENCRYPT [15]; dimension de 128 octets (1024 bits).

D.4 Déchiffrement de la clé de capteur de mouvement

D.4.1 Le MSCA doit déchiffrer un EDK avec la clé privée pour produire la demande de distribution de clé maître de capteur de mouvement, selon le modèles de déchiffrement RSA RSAES-PKCS1-V1_5-DECRYPT.

D.4.2 Seulement si le déchiffrement réussit et produit un message de dimension de 24 octets, dans lequel les 8 premiers octets sont égaux aux premiers octets de KDM, alors les 16 derniers octets du message doivent être utilisés comme clé maître de capteur de mouvement du type défini par le champ KID de KDM.

European Commission
Joint Research Centre – Institute for the Protection and Security of the Citizen
Title: Digital Tachograph System, European Root Policy, Version 2.1
Author(s): J.W.Bishop, J-P Nordvik
Luxembourg: Office for Official Publications of the European Communities

2009 – 29 pp. – (A4) 21 x 29.7 cm

Résumé

Ce document est la Politique de Certification Version 2.1 de l'Autorité de Certification Générique Européenne approuvée par la Politique du Transport Terrestre de la DG-TREN/E1 le 28 juillet 2009. Cette politique de certification définit l'ensemble des obligations pour les autorités nationales des Etats participant au système de chronotachygraphe numérique.

Cette révision englobe un changement de la périodicité du système d'audits nationaux (extension conditionnelle de la périodicité de 12 à 24 mois), suivant la demande des Pays-Bas approuvée par les autres autorités nationales.