Guide et structure de la politique nationale de l'autorité de certification

Gestion des Clés, Certificats et équipements

(Enregistrement, génération de clé, émission de certificat, personnalisation, distribution, utilisation et fin de vie)

pour le Système Chronotachygraphe

et les CIA, MSA, MSCA et CP

Version

Version préliminaire 0.4	**Février 2002**	**Présentée au projet Emission de cartes SWG3 à Paris**	**May-Lis Farnes, SNRA**
Version préliminaire 0.8		**Distribuée au Projet Emission de cartes SWG3**	**May-Lis Farnes, SNRA**
Version préliminaire 0.85	**Juin 2002**	**Distribuée au Projet Emission de cartes SWG3**	**May-Lis Farnes, SNRA**
Version préliminaire 0.9	**27 juin 2002**	**A utiliser et commenter par tous les Etats Membres**	**May-Lis Farnes, SNRA**
Version 1.0	**31 octobre 2002**	**Version finale soumise aux Etats Membres**	**May-Lis Farnes, SNRA**
Version 1.0-fr	**15 juin 2015**	**Traduction non officielle de la version 1.0**	**Gilles Baranger Road Transport Expert**

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

Table des matières

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

Guide de la Politique nationale de l'Autorité de Certification (CA)

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

0 Guide pour l'utilisation d'un modèle de la Politique nationale de CA

0.1 Origine et introduction

0.1.1 A propos de ce document

Ce document est un GUIDE et un MODELE pour les Etats Membres[1] permettant d'introduire une politique de CA[2] du système Chronotachygraphe. Une politique de CA est un document spécifiant les exigences pour la sécurité de la gestion des clés, des certificats et d'équipements. La Politique nationale de CA des Etats Membres introduisant le système chronotachygraphe est appelées la Politique Nationale de CA.

Le système chronotachygraphe est décrit dans le Règlement 2135/98 du Conseil[3], qui est référencé ci-après comme « le Règlement ». Le responsable du Règlement est la Commission Européenne, qui est référencée ci-après comme « la Commission ».

Ce document est basé sur les exigences de la réglementation, les exigences de politique de la norme [ETSI 102 042], et les analyses de risque partiellement effectuées pour le système chronotachygraphe.

0.1.2 Comment utiliser ce document

La vision des Etats Membres participant au travail de l'UE organisé par la Commission, le projet d'émission de cartes (SWG3), et celle de la Commission est qu'une Politique Nationale de CA est ***nécessaire pour chaque Etat Membre*** *pour satisfaire la réglementation, bien que ce ne soit pas expressément exigé par la réglementation.*

Chaque Etat Membre est responsable du développement de sa propre Politique Nationale de CA ; L'Autorité d'Etat Membre (MSA), est le propriétaire et le responsable de la Politique Nationale de CA.

La façon dont la responsabilité et la gestion du système chronotachygraphe sont différemment organisées dans différents Etats Membres si bien que la description de ce document est un **modèle générique** qui recouvre ces différences et doit être particulièrement détaillé dans chaque pays.

Le **chapitre 0** est un **guide** de développement de la politique nationale de CA et un modèle à utiliser. Les **chapitres 1 à 14** forment a structure de la politique nationale

[1] Les Etats Membres sont cités dans la réglementation, mais l'utilisation système chronotachygraphe n'est pas limité aux Etats Membres de l'UE mais aussi autres parties qui agréent avec l'UE pour l'utilisation du système, par exemple les pays de la zone économique Européenne.
(NdT : cette politique est applicable aux Parties Contractantes de l'Accord AETR de la CEE-ONU, il faut donc comprendre « Partie Contractante » dans ce document chaque fois qu'est utilisée la locution « Etat Membre »)

[2] La politique de CA est une terminologie commune pour une politique qui fixe les exigences de sécurité de la gestion des clés, des certificats et usuellement des cartes pour une certaine CA (Autorité de Certification).

[3] NdT : Conseil de l'Union Européenne

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

de CA à utiliser par les Etats Membres.

Pour davantage d'information à propos de la sécurité et de la terminologie utilisée dans ce document, veuillez vous référer au **Guide de Sécurité Commun** expliqué au chapitre 0.4

*Chaque politique nationale de CA doit être **approuvée par la Commission***

Origine de ce document
Ce document a été fourni par les Etats Membres représentatifs de l'UE dans le cadre d'un groupe de travail sur l'émission de cartes sponsorisé par la Commission.

Propriétaire du document
La **Commission** est le propriétaire du document

0.2 Champ d'application

Il est de la responsabilité de chaque Etat Membre de mettre en place les moyens garantissant la sécurité de ce nouveau système. Chaque Etat membre est alors prié de définir sa propre organisation pour le chronotachygraphe et établir sa propre politique de sécurité nationale de CA contenant les exigences de sécurité dévolues à chaque entité et impliquée dans son organisation. La conformité à ce document est considérée par les Etats membres et la Commission comme une preuve acceptable de conformité à la réglementation lors de demande de certification de clés d'Etat Membre à l'Autorité Européenne de Certification Générique. Cette conformité étaye la nécessité de cohérence parmi les Etats Membres alors que la confiance dans les systèmes chronotachygraphes doit s'en inspirer.

Le champ d'application de la politique nationale de CA est la gestion des clés, des certificats et des équipements (cartes, UEV, et capteurs de mouvement) à l'intérieur du système chronotachygraphe, au niveau de l'Etat Membre.

Le deux processus principaux sont :
- émission de cartes tachygraphiques incluant les clés et les certificats, y compris le renouvellement, etc…
- l'émission de clés et de certificat pour l'UEV et des clés pour le capteur de mouvement.

Ces processus incluent les fonctions suivantes au travers des processus :
- enregistrement (fonction RA) connecté au processus d'application
- gestion de clé
- génération de clé
- émission de certificat
- personnalisation
- distribution de cartes, de clés et de certificats.

De plus, les phases suivantes sont prévues :
- utilisation des équipements (partiellement)

- fin de vie des équipements (partiellement)
- fin de vie pour le MSCA

Les organisations désignées pour cette politique sont (comme défini dans ce document et le Guides Commun de Sécurité, CSG) :
- MSA – Member State Authority, Autorité de l'Etat Membre
- CIA – Card Issuing Authority, Autorité Emettrice de cartes
- *(NCA) – National CA, Autorité Nationale de Certification*
- MSCA – Member State Certification Authority, Autorité de Certification d'Etat Membre
- CP – Card personalization organisation, Organisme Personnalisateur de Cartes
- Fabricants d'équipements, c'est-à-dire fabricants d'UEV et de capteurs de mouvement
- ERCA – European Root Certification Authority, Autorité Européenne de Certification Générique

(Le nom NCA peut être utilisé communément pour deux fonctions :
- Autorité de Certification d'Etat Membre (MSCA)
- Organisme Personnalisateur de Cartes (CP))

En dehors du champ d'application de ce document se trouvent :
- L'approbation de type des équipements
- Les applications non tachygraphiques/les certificats sur les cartes de chronotachygraphe
- Les exigences détaillées de l'utilisation des équipements
- L'exigence pour la fin de vie des équipements
- Le support utilisateur

0.3 Définitions et interprétations

Les définitions utilisées dans ce document sont décrites dans ce chapitre et au chapitre 14 (Glossaire/définitions et abréviations) pour aider Etats membres guider les Etats Membres utilisant ce document.

0.3.1 Généralités sur l'organisation du système chronotachygraphe

Une vue schématique de l'organisation du système chronotachygraphe est représentée ci-dessous.

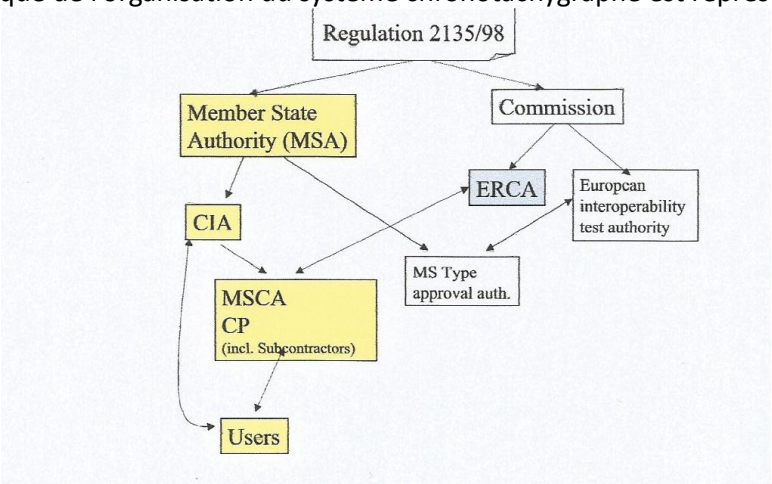

Figure 1. Organisation du système chronotachygraphe (les cadres en couleur sont couverts par ce document)

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

Le système chronotachygraphe est système hiérarchique où la racine se trouve au niveau de l'UE (ERCA) et est relié aux différents Etats Membres pour assurer un système cohérent et sûr. Le rôle de l'ERCA est de certifier avec sécurité les clés génériques des Etats Membres pour former une chaîne fiable de certification.

Dans ce texte, les différents rôles sont décrits. A noter que ces rôles n'ont pas besoin d'être dans des organismes distincts, ils peuvent être combinés en un ou plusieurs organismes.
Les rôles suivants sont couverts par ce document :
- Autorité d'Etat Membre (**MSA**)
- Autorité Emettrice de Cartes (**CIA**)
- Autorité de Certification d'Etat Membre (**MSCA**)
- Organisme Personnalisateur de Cartes (**CP**)
- Utilisateurs d'équipement (cartes tachygraphiques, UEV et capteurs de mouvement)

La communication avec l'**ERCA** est partiellement couverte, pour être cohérente avec la politique ERCA.

Le **MSA** a avant tout la responsabilité de créer les processus du système chronotachygraphe au niveau de l'Etat Membre.

Le **CIA** fait soit partie de l'organisme MSA, soit appartient à un autre organisme de l'Etat Membre ou d'un sous traitant **désigné par le MSA**. Le MSCA traite certaines parties des processus d'émission.

Le CP fait soit partie de l'organisme MSA, soit appartient à un autre organisme de l'Etat Membre ou d'un sous traitant **désigné par le MSA.** Le CP traite certaines parties des processus d'émission.

Dans ce document, **le NCA**, lorsque c'est applicable, est une autorité combinée assurant les rôles de **MSCA** et de **CP**. Si un Etat Membre choisit l'utilisation de ce modèle, le NCA est **désigné par le MSA**.

Les responsabilités des différents rôles sont définies ci-après.

0.3.1.1 Autorité d'Etat Membre

Chaque Etat Membre est responsable de la mise en place du système chronotachygraphe dans son périmètre. Chaque Etat Membre doit désigner une Autorité d'Etat Membre, MSA, pour mettre en place les processus d'émission.
Le MSA a avant tout la responsabilité des processus d'émission dans le système chronotachygraphe de son pays.
Le MSA doit coordonner les différentes tâches du système chronotachygraphe et, dans le champ de ce document, ces tâches sont une partie de deux processus principaux, l'un pour les cartes, et l'autre pour les UEV et les capteurs de mouvement :

- Emission de cartes tachygraphiques, incluant clés et certificats
- émission de clés des capteurs de mouvement, des certificats et des clés pour le UEV

Le MSA est responsable de l'établissement de l'organisation du chronotachygraphe dans son domaine :

- Le MSA est responsable de la désignation d'un CIA
- Le MSA est responsable de la désignation d'un MSCA

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

- Le MSA est responsable de la désignation d'un CP.

0.3.1.2 Autorité Emettrice de cartes

Le CIA est désigné par le MSA, et est l'autorité traitant de la gestion utilisateur, incluant les fonctions de demande de cartes et d'approbation, d'aide à l'support utilisateur et dans certains cas de la distribution de cartes.

0.3.1.3 L'organisme Personnalisateur de cartes

Le CP est désigné par le MSA, et est responsable de la génération de clé (optionnel), de la personnalisation et (optionnellement) de la distribution de certificats et de cartes du système chronotachygraphe.

Le CP désigné est responsable de :

- la génération des paires de clés pour équipement, c'est-à-dire les cartes et les UEV (la génération actuelle de clé ne nécessite pas l'action du CP, mais la responsabilité des opérations sécurisées repose sur le CP)
- personnalisation de cartes, c'est-à-dire l'insertion des données utilisateur, des clés RSA et du certificat sur la carte. Cela inclue la vérification croisée des données visuelles et des données numériques.
- distribution des cartes (cette fonction peut être partagée avec le CIA ou le MSCA)

0.3.1.4 Autorité de certification de l'Etat Membre

Le MSCA est désigné par le MSA, et est défini comme l'autorité responsable de l'émission des certificats de clés publiques pour l'équipement (cartes et UEV), et de la gestion des clés génériques de l'Etat Membre. Le MSCA peut également générer les clés asymétriques de carte.

Les différentes fonctions du MSCA peuvent être réalisées pa le MSCA même ou par des partenaires sous traitants, des Agences de Services, auquel cas le MSCA peut être une organisation virtuelle plutôt que physique.

La partie principale du MSCA est la fonction CA, responsable de :

- la gestion de clé
- la génération de clé (optionnel)
- l'émission de certificat

En plus détaillé, le MSCA désigné est responsable de :

- la génération sécurisée et la gestion de paire(s) de clés d'Etat Membre
- l'émission de certificats pour les clés publiques d'équipement (c'est-à-dire cartes et UEV)
- la conservation d'enregistrements de toutes les clés publiques avec l'identification d'équipement (c'est-à-dire conserver les enregistrements des certificats émis)
- la gestion et la distribution des clés symétriques des capteurs de Mouvement Km, Km_{VU} et Km_{WC} [4] aux fabricants de capteurs de mouvement, d'UEV et de cartes atelier, en incluant le chiffrage des données de capteur de mouvement avec Km. Les clés sont fournies de l'ERCA sur demande.
- **la distribution** de certificat MSCA et de clé publique ERCA pour les cartes et les UEV (cette fonction peut être partagée avec le CIA ou le CP).

0.3.1.5 Utilisateurs (porteurs de certificat)

Les utilisateurs sont définis comme les utilisateurs d'équipement du système chronotachygraphe.

[4] NdT : Km = clé du Capteur de mouvement, Km_{VU} = clé équivalente pour l'UEV et Km_{WC} = clé équivalente pour la carte Atelier

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

L'équipement (ou les parties d'équipement) du système chronotachygraphe est défini par :

- les cartes tachygraphiques
- l'Unité Embarquée Véhicule (UEV)
- les Capteurs de Mouvement

Quatre différents types d'utilisateurs des cartes tachygraphiques existent, d'où quatre différents types de cartes, l'utilisateur qui détient une carte est appelé utilisateur porteur de carte et est :

- Conducteur (D)
- Entreprise de Transport (HC)
- Atelier (WS)
- Corps de Contrôle (CB)

Les utilisateurs d'UEV et de Capteurs de Mouvement sont définis comme les fabricants d'équipement, et les fabricants sont respectivement :

- les fabricants d'UEV
- les fabricants de Capteurs de Mouvement

0.3.2 Interlocuteur de confiance du MSCA (MSA)

L'interlocuteur de confiance du MSCA (MSA) est le corps de contrôle de chaque Etat Membre.

Dans sa tâche de contrôle, les utilisateurs du corps de contrôle (porteur de carte) doivent faire confiance aux certificats émis dans tous les Etats Membres, ainsi qu'aux certificats correspondants des Etats Membres.

0.3.3 Principaux processus et fonctions

Les processus principaux supportés par la politique nationale de CA sont :

- l'émission de cartes tachygraphiques, incluant les clés et les certificats (incluant le renouvellement de cartes, etc…)
- l'émission de clés et de certificats d'UEV et de Capteurs de Mouvement
- la gestion des clés et certificats génériques ERCA et MSCA
- l'usage de l'équipement, des clés et des certificats (partiellement)
- la fin de vie du MSCA

Ces cinq processus sont décrits de façon plus détaillée dans le sous-chapitre suivant.

0.3.3.1 Emission de cartes tachygraphiques

Le processus d'émission de carte est décrit par la figure 3, ci-dessous

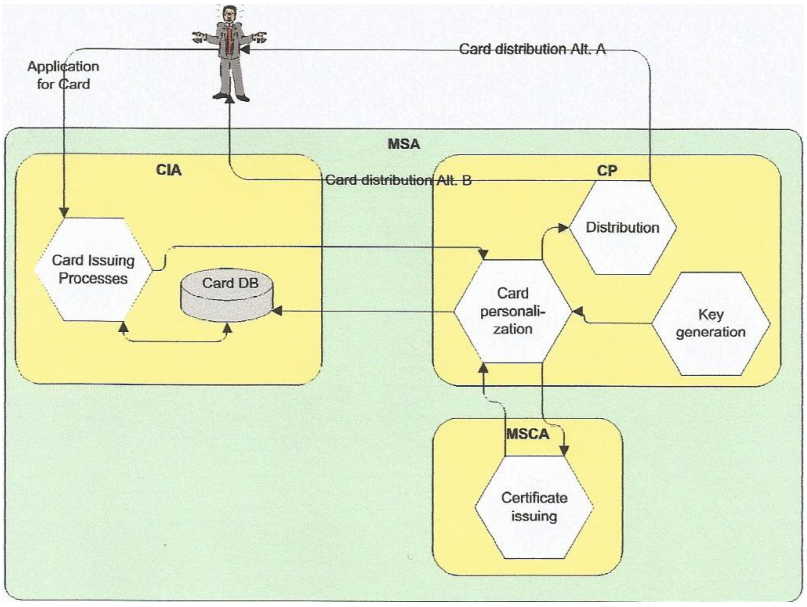

Figure 2. Processus : émission de cartes tachygraphiques

Le MSA a la responsabilité totale de l'intégralité du processus d'émission de cartes tachygraphiques, incluant la génération de clé et de certificat.

Le CIA a la responsabilité de :

- le processus de demande (incluant l'approbation, etc…)
- l'enregistrement de demande approuvée (information d'entrée pour MSCA et CP)
- la maintenance d'une base de données des cartes émises
- (optionnel) distribution des cartes (cette fonction peut être réalisée par le MSCA ou le CP)

Dans le processus de demande, les demandes sont reçues et approuvées ou rejetées. Dès qu'une demande est approuvée et enregistrée, l'information est passée au MSCA.
Le CIA peut être responsable de la distribution des cartes tachygraphiques aux utilisateurs, comme indiqué par l'alternative B de la figure 3 ci-dessus.

Le NCA (c'est-à-dire le MSCA ou le CP) a la responsabilité de ce qui suit :

- la génération de clé (bien que la génération de clé actuelle puisse être réalisée par un sous traitant ou par le fabricant d'équipement). En pratique, la génération de clé est plus proche de la personnalisation que de l'émission de certificat.

Le CP a la responsabilité de ce qui suit :

- personnalisation de carte (visuelle et électronique)
- (optionnel) distribution de cartes (cette fonction peut être réalisée par le MSA ou le CIA)

Le MSCA a la responsabilité de ce qui suit :

- émission de certificat
- conservation d'enregistrements de toutes les clés publiques avec l'identification de l'équipement (c'est-à-dire conservation des enregistrements de certificats émis)
- gestion des clés de Capteur de Mouvement Km_{VU}, Km_{WC} et Km (pour les cartes atelier)

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

0.3.3.2 Emission de clés et de certificats pour les UEV et les Capteurs de Mouvement

Le MSA a l'entière responsabilité de l'intégralité du processus d'émission de clés et de certificats pour les UEV, et de clés pour les capteurs de mouvement. Ce processus inclue à la fois la distribution de clé asymétrique et l'émission de certificat, ainsi que la distribution de clé symétrique.
Le processus est en grande partie semblable à celui d'émission de carte.

Le **CIA est responsable** de ce qui suit :

- processus de demande (incluant l'approbation, etc…)
- enregistrement de la demande approuvée (entrée pour le MSCA)
- maintenance d'une base de données d'équipement
- (optionnel) distribution de clés et de certificats (cette fonction devrait plutôt être réalisée par le MSCA)

Le NCA (c'est-à-dire le MSCA ou le CP) est responsable de ce qui suit :

- génération de clé (bien que la génération de clé actuelle puisse être réalisée par un tiers ou par le fabricant d'équipement)
- émission de certificats pour les UEV
- conservation des enregistrements de toutes les clés publiques avec l'identification l'équipement (c'est-à-dire conservation des enregistrements des certificats émis)
- gestion des clés des capteurs de mouvement Km_{VU}, Km_{WC} et Km
- (optionnel) distribution de clés et de certificats pour les fabricants d'équipement (cette fonction peut être réalisé par le CIA)

Les fabricants d'UEV sont responsables de la personnalisation des UEV, c'est-à-dire l'insertion de clés et de certificats dans les UEV.

Les fabricants de capteurs de mouvement sont responsables de l'insertion des données chiffrées de capteur de mouvement dans les capteurs de mouvement.

La division des tâches de MSA ou CIA, des tâches de MSCA et de fabricants d'équipement pour l'émission des clés et de certificats pour les UEV et les capteurs de mouvement est décrite par la figure 4 ci-dessous.

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

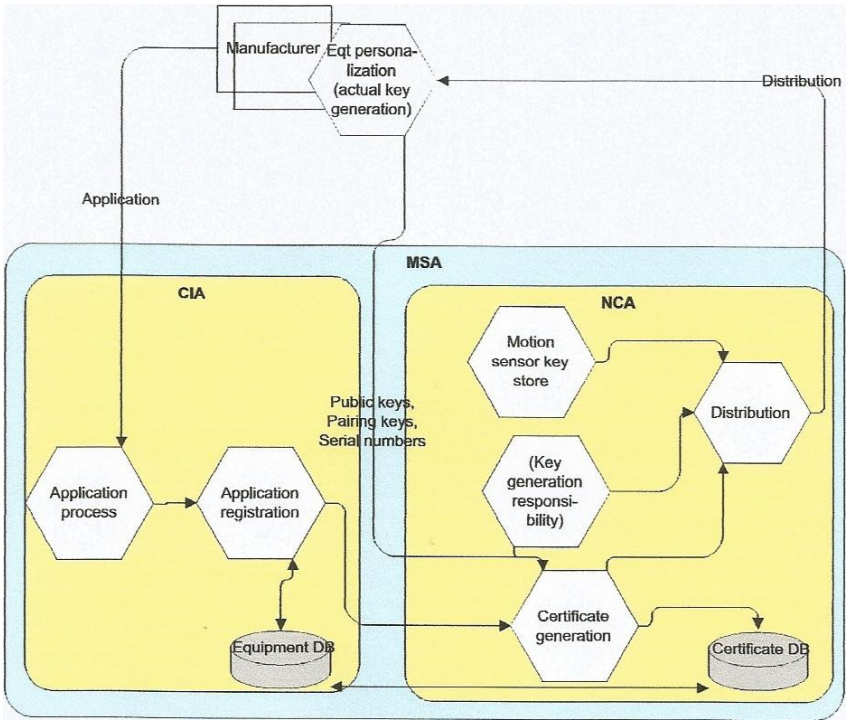

Figure 4. Processus : émission de clés et de certificats pour l'UEV et le capteur de mouvement

0.3.3.3 Gestion des clés génériques et des certificats

Le MSCA est responsable de la gestion de clés génériques Européennes et d'Etat Membre, des clés de capteurs de mouvement, pour avoir sa clé publique d'Etat Membre certifié par l'ERCA.
Le MSCA est responsable de :

- la génération et la gestion de paire(s) de clé d'Etat Membre
- la soumission de clé publique d'Etat Membre à l'ERCA pour la certification
- la gestion de certificat d'Etat Membre
- la gestion de la clé publique ERCA
- la gestion des clés de capteur de mouvement
- la distribution sécurisée de clés et de certificats entre MSCA et CP

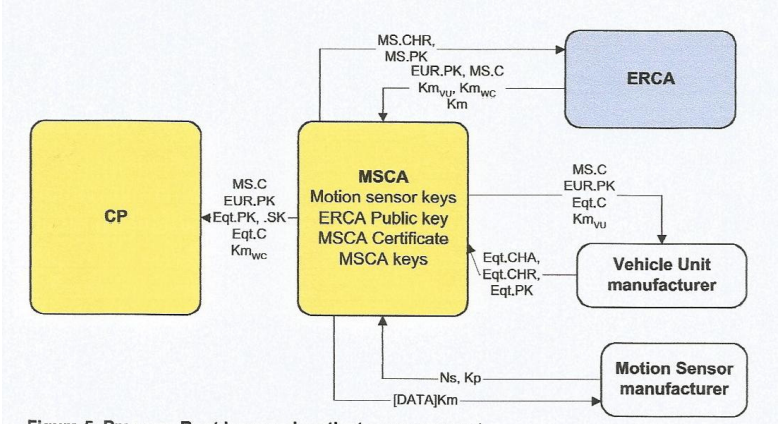

Figure 5. processus : gestion de clés génériques et de certificat

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

0.3.3.3.1 Processus d'utilisation – équipement

Pour assurer la fonction et la sécurité du système, l'équipement doit être utilisé à bon escient.

Le MSA/CIA est responsable de la fourniture aux utilisateurs de l'information/ des instructions/ des règles d'utilisation de l'équipement.

0.3.3.3.2 Fin de vie

Quelques aspects de la fin de vie d'équipement sont consignés dans la politique. D'autres aspects devraient pris en compte par les autorités respectives des Etats Membres.
La fin de vie (arrêt) du MSCA est pris en compte dans cette politique. Cela est nécessaire en cas de changement de MSCA ou la fin de l'utilisation du système chronotachygraphe.

0.4 Politique et structure du document de sécurité pour le système chronotachygraphe

Les documents descriptifs de la mise en place du système chronotachygraphe sont les suivants :

- Guide Commun de Sécurité (CSG)
- Manuel des meilleures pratiques d'émission de cartes (BPM)
- Guide de la politique nationale CA et format (ce document)

En plus, les documents suivants sont développés par l'ERCA :

- Politique Générique Européenne de CA (Politique ERCA)
- ERCA PS (Dispositions pratiques de l'ERCA)

Chaque MSA est responsable du développement du document suivant :

- Politique nationale CA (basée sur ce guide et ses formats)
- Politique de sécurité d'information nationale basée sur le CSG (optionnel)
- Description du processus national d'émission de cartes basé sur le BPM (optionnel)

Les MSCA et CP désignés sont responsables du développement des documents suivants, devraient être approuvés par le MSA :

- Dispositions pratiques (PS) (optionnel)
- Politique de sécurité de l'information (nationale) (optionnel)

La structure des différents documents est indiquée dans le schéma ci-dessous :

Vue générale des documents pour le système chronotachygraphe

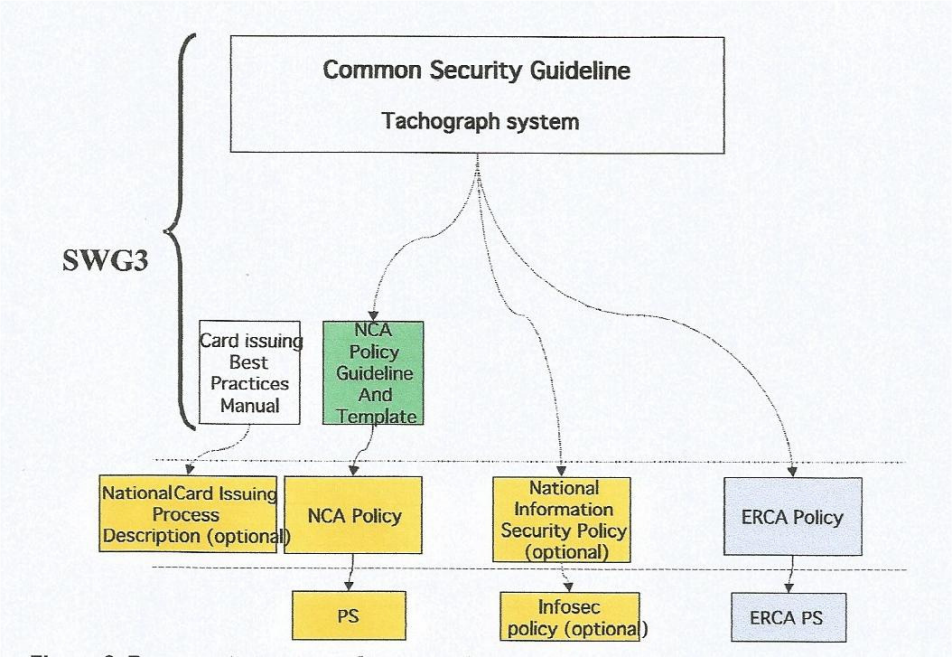

Figure 6. Documentation de gestion de la structure de clé, de certificat et de carte du système chronotachygraphe

Des descriptions plus détaillées des documents suivent ci-après.

0.4.1 Guide de sécurité commun

Le Guide de Sécurité Commun (CSG) existe en tant que trame globale pour toutes les organisations dépendantes du système. Il offre une vue générale des exigences de sécurité du Règlement.

C'est un document de recommandations, indiquant le niveau actuel des documents de politique des Etats Membres et de l'Europe.

La Commission est détenteur du CSG

0.4.2 Manuel des meilleures pratiques d'émission de cartes

Le Manuel des meilleures pratiques d'émission de cartes (BPM) est une introduction pour tous les Etats Membres et les MSA lors du développement du processus d'émission de cartes et principalement le processus d'application, ainsi que les autres processus de MSA.

C'est un document de recommandations mais aide les Etats Membres à mettre en place les processus d'émission de cartes et une politique nationale d'émission de cartes (optionnel).

La Commission est le détenteur du BPM pour l'émission de cartes.

0.4.3 Guide de la politique national de CA et format

Le Guide de la politique national de CA et format (ce document) est un guide et un format pour

chaque Etat Membre permettant le développement de sa politique nationale de CA.

Ce Guide de la politique national de CA et sa structure devraient être utilisés par tous les Etats Membres, pour assurer la compatibilité entre les politiques d'Etats Membres et la sécurité de l'ensemble du système.

La Commission est le détenteur du Guide de la politique national de CA et de sa structure

0.4.4 La Politique nationale de CA

Une politique nationale de CA devrait être développée [recommandé] par chaque Etat Membre pour spécifier un ensemble de règles requises pour la gestion des clés, des certificats et d'équipement dans le système chronotachygraphe.

Il est imposé au MSCA par le MSA. Cf section 0.3 pour plus de détails.

Dans le but d'assurer la conformité et l'interopérabilité entre tous les Etats Membres, la Commission doit approuver chaque politique Nationale de CA, de même que toutes ses révisions significatives.

La politique nationale de CA de chaque Etat Membre appartient au MSA qui en dépend.

0.4.5 Les Dispositions Pratique (PS)

Les PS sont les documents procéduraux des MSCA et des CP, qui détaillent la façon dont la politique nationale est contrôlée dans sa gestion au jour le jour. Il dispose d'une forte connotation de sécurité. Dans une structure standard de PKI et d'organisation, ce document est appelé un CPS (Certification Practice Statement = Dispositions Pratiques de Certification). Si des Agences de Service réalisent certaines fonctions, chaque agence doit avoir un PS pour mettre en pratique la Politique Nationale de CA. Cf plus de détails à la section 0.6.

Le PS appartient au MSCA, CP et à chaque Agence de Service.

Les PS doivent être approuvés par le MSA.

0.4.6 La politique ERCA

La politique ERCA est un ensemble de règles qui régissent l'Autorité Européenne de Certification Générique.

La politique ERCA appartient à l'ERCA.

La politique ERCA doit être approuvée par la Commission.

0.4.7 Les Dispositions Pratiques de l'ERCA (ERCA PS)

L'ERCA PS est le document procédural de l'ERCA, qui détaille la façon dont la politique ERCA est contrôlée dans sa gestion au jour le jour.

Ce document est développé par l'ERCA.

L'ERCA PS appartient à l'ERCA.

0.5 Généralités de la politique nationale de CA

Une politique nationale de CA est requise, pour s'assurer que les clés, les certificats et l'équipement (cartes, UEV et capteurs de mouvement) sont gérés de façon sûre et digne de confiance par les organisations suivantes :

- ERCA
- MSA
- CIA
- MSCA
- CP
- Utilisateurs

La politique nationale de CA est un ensemble de règles qui décrivent la façon dont les clés, les certificats et l'équipement sont émis.

La politique nationale de CA décrit partiellement les règles d'utilisation des équipements

En outre, le processus de fin de vie est traité pour la MSCA.

La politique nationale de CA établit les exigences principalement pour les MSCA, les CP et leur sous traitants.

Pour les différentes parties impliquées, il est important d'avoir la possibilité d'évaluer le niveau de confiance lié aux cartes, aux certificats et à l'équipement du système chronotachygraphe. La confiance n'est pas simple à mettre en chiffres. La politique nationale de CA est une façon de prouver la confiance dans la sécurité de l'organisation des MSCA, leur stabilité et leur intégrité.

La politique nationale de CA devrait essentiellement répondre aux questions suivantes :

- Quelle est la finalité des clés, des certificats et de l'équipement ?
- Quelles règles et contrôles sont en place pour assurer la sécurité, la stabilité et la confiance ?

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

0.6 Généralités sur les Dispositions Pratiques (PS)

Pour documenter la mise en place de la politique nationale de CA, particulièrement en ce qui concerne les sujets de sécurité, des Dispositions Pratiques (PS) sont nécessaires. Et l'organisme de personnalisation de cartes (CP) et le MSCA ont besoin de PS. Combinés, elles sont plus ou moins équivalentes à des Dispositions Pratiques de Certification (CPS), qui forment un document standard dans un PKI.

Lorsque des sous traitants ou des Agences de Service (SA) réalisent certaines ou toutes les fonctions, chacune de telles SA doit avoir un PS, qui décrit les pratiques de sécurité qui sont utilisées dans le(s) processus.

Le PS contrôle les règles établies par la politique nationale spécifique de CA et est une description plutôt détaillée des termes et conditions ainsi que des pratiques opérationnelles et commerciales d'un MSCA et d'un CP pour l'émission et autres gestions de clés, de certificats et d'équipement. Un PS définit comment les organisations répondent aux exigences techniques, organisationnelles et procédurales identifiées par la politique nationale de CA.

Le PS devrait répondre à la question :

- De quelle façon les fonctions, les processus et les contrôles de sécurité renforcent la politique nationale de CA ?

Si des Agences de Service sont employées et possèdent des instructions, ces dernières doivent être compilées par le CP ou le MSCA et rendues disponibles aux utilisateurs par le **MSA ou le CIA**.

0.7 Généralités sur la politique de sécurité de l'information

Tous les organismes du système chronotachygraphe doivent gérer la sécurité de l'information à un niveau général et spécifique selon les exigences du Règlement.

Dans le but d'opérer la sécurité de l'information, il est considéré comme meilleure pratique à ce jour de développer une politique de sécurité de l'information pour chaque organisme et de la baser sur la norme ISO 17799 – Norme de gestion de la Sécurité de l'Information [ISO 17799]. Cette norme décrit ce que les organismes devraient prendre en compte lors du développement de sa politique de sécurité de l'information.

Une description détaillée de l'ISO 17799 va au-delà du champ d'application de ce document, c'est pourquoi nous nous référons à la seule norme.

Les organismes au niveau de l'Etat Membre nécessitant fortement une politique de sécurité de l'information sont :

- MSA et CIA [recommandé]
- MSCA [fortement recommandé]
- CP [fortement recommandé]

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

De plus, les organismes suivants nécessitant fortement une politique de sécurité de l'information sont :

- les fabricants d'équipement [fortement recommandé]
- les ateliers [recommandé]
- les corps de contrôle [optionnel]

Les documents de la politique de sécurité de l'information devront s'inspirer fortement du Guide de Sécurité Commun (CSG) et de ce document (Guide et structure de la politique nationale CA). Pour davantage d'information, voir le Guide de Sécurité Commun (CSG).

Il est* recommandé *aux MSA ou CIA et aux ateliers de mettre en place des politiques de sécurité de l'information.

Il est* fortement recommandé *aux MSCA, CP et fabricants d'équipement de mettre en place une politique de sécurité de l'information.

0.8 Comment utiliser le guide et les formats MSCA

Le chapitre 0 est une introduction et un guide de développement de la politique nationale de CA utilisant ce document comme modèle. Les chapitres 1 à 14 constituent le modèle pour une politique nationale de CA.

Ce guide et ce modèle sont suggérés pour être utilisé par tous les Etats Membres. En utilisant le modèle de façon appropriée, un Etat Membre remplira les exigences dépendant du règlement et nécessaires aux exigences de sécurité.

Politique nationale et structure de CA -> Politique nationale de CA *pour chaque Etat Membre*.

Les chapitres 1 à 14 devraient être vus comme un modèle pour la politique nationale de CA. Tous les Etats Membres sont autorisés, et encouragés, à copier les chapitres et utiliser le modèle comme départ pour réaliser la politique nationale de CA.

Les références exactes au Règlement dans ce document ne devraient pas être incluses dans la politique nationale de CA actuelle, ce sont de simples informations.

Il est* fortement recommandé *de suivre le plus possible le modèle, cela rendant plus facile la lecture de chaque autre politique MSCA (pour agrément et acceptation mutuel).

Si un Etat Membre n'utilise pas ce modèle, il doit entreprendre les mesures appropriées pour s'assurer que toutes les exigences de ce guide de politique nationale de CA soient satisfaites.

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

0.8.1 Interprétation du modèle

Les parties de texte formant les exigences pour les procédures et les responsabilités de MSCA sont appelées des règles et sont marquées avec le préfixe de référence « **[r*n*]** », où *n* est un numéro séquentiel du document.

Le modèle a trois niveaux de règles notées par le formatage suivant :

- Exigences obligatoires (exigé soit par le Règlement, soit par des normes reconnues. S'il s'agit du règlement, la référence est indiquée.)
- [Recommandé] Fortement recommandé par le groupe de travail sur l'émission de cartes pour chaque niveau de sécurité.
- [Pratique] Bonne pratique recommandée par le projet d'émission de cartes (SWG3) pour atteindre un niveau de sécurité recommandé.

Lorsque le format utilise les crochets <> le contenu devrait être spécifié par le MSCA spécifique (Etat Membre particulier).

Un Etat Membre peut également ajouter des exigences optionnelles à la politique, à condition que cela ne contredise pas le Règlement.

0.9 Procédure de révision de ce document

Les Etats Membres peuvent soumettre des propositions de modifications à la **Commission**. La **Commission** informera les autres Etats Membres des modifications proposées. Si nécessaire, la **Commission** organisera une réunion des représentants des Etats Membres pour étudier les révisions de ce document.

La révision actuelle de ce document doit être mise à disposition par la **Commission** sur demande.

La **Commission** doit notifier à tous les Etats Membres la publication des révisions.

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

Modèle de
Politique nationale de CA

1 Introduction

Ce document est la politique nationale de CA de <pays> pour le système chronotachygraphe.

Cette politique nationale de CA répond aux :

- Règlement du Conseil sur le système chronotachygraphe, 2135/98
- Règlement de la Commission 1360/2002
- [fortement recommandé] Guide et structure de la politique Nationale de CA
- [fortement recommandé] le « Guide Commun de Sécurité »

1.1 Organisme responsable

Le responsable pour cette politique nationale de CA est l'Autorité de l'Etat Membre, MSA <organisme>.

Le CIA désigné est <organisme>.

Le MSCA désigné est <organisme>.

Le CP désigné est <organisme>.

Les MSCA et CP peuvent sous traiter des parties de leurs processus à des sous traitants, des Agences de Service. L'utilisation d'Agences de Service ne diminue en rien l'entière responsabilité du MSCA ou du CP.

[Recommandé] Liste des agences de Service :
<SA 1>
<SA 2>
….

1.2 Approbation

Cette politique nationale de CA est approuvée par la Commission par <nom> le <date>.

1.3 Disponibilité et détails de contacts

[Recommandé] La politique nationale de CA est accessible au public sur <adresse Internet>.
Les questions concernant la politique nationale de CA doivent être adressées à :
<organisme>.
[Recommandé] <Détails des contacts pour cette politique nationale de CA>

2. Champ d'application et applicabilité

[r1] la politique nationale de CA est valable pour le système chronotachygraphe seulement.
[r2] Les clés et certificats émis par le MSCA sont exclusivement réservés à l'usage du système chronotachygraphe.
[r3] [Recommandé] Les cartes émises par le système sont exclusivement réservées au système chronotachygraphe.

Le champ d'application de la politique nationale de CA pour le système chronotachygraphe est décrit par la figure ci-dessous.

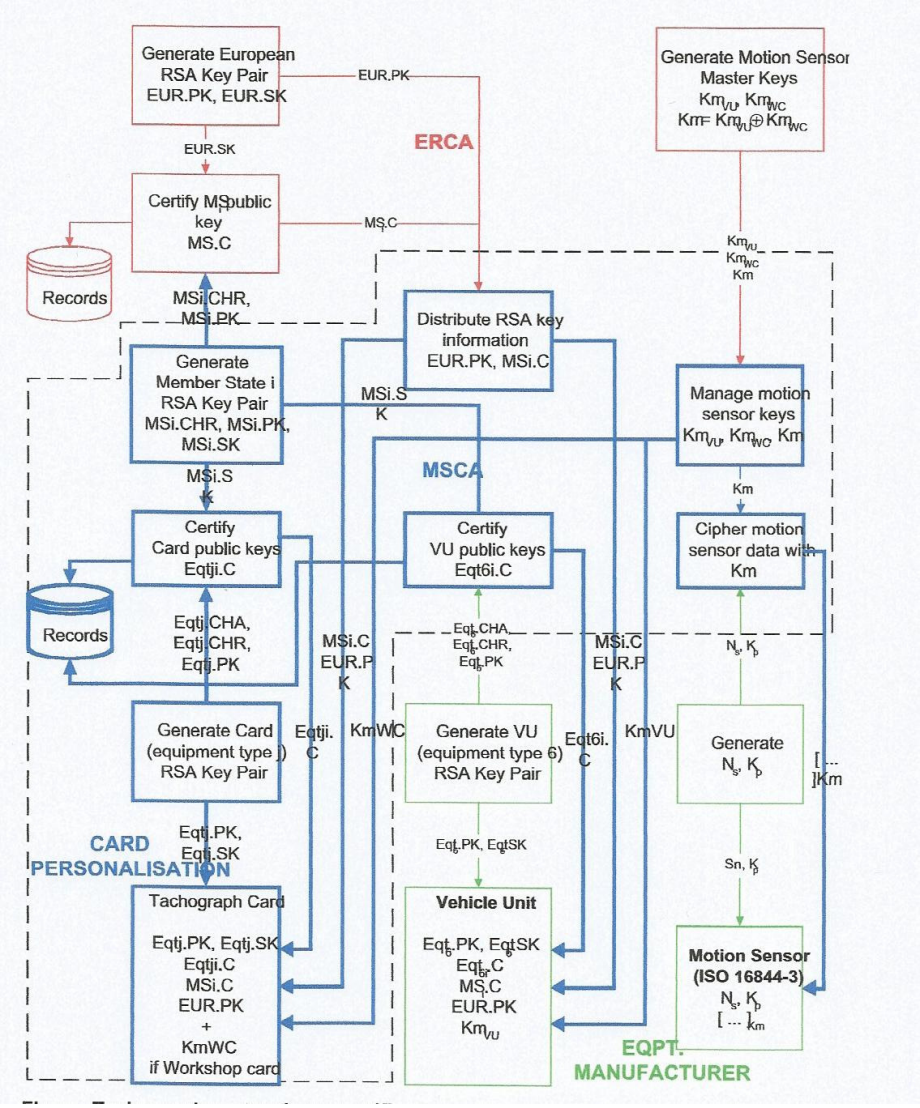

Figure. Clés du système chronotachygraphe, gestion des certificats et de l'équipement. (Champ d'application de la politique est indiqué en pointillé.)

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

3. Dispositions générales

Cette section contient des dispositions se rapportant aux obligations respectives de MSA, CIA, MSCA, CP, Agences de Services et utilisateurs, et d'autres questions relatives à la loi et la résolution de conflit.

3.1 Obligations

Cette section contient des dispositions se rapportant aux obligations respectives des :

- MSA et CIA
- MSCA et Agences de Service (le cas échéant)
- CP et Agences de Service (le cas échéant)
- Utilisateurs (porteurs de cartes, fabricants d'UEV et de capteurs de mouvement)

3.1.1 Obligations de MSA et CIA

En référence à la politique NCA, le MSA et le CIA ont les obligations suivantes :

[r4] Le MSA doit :

a) Maintenir la politique nationale de CA
b) Désigner un MSCA et un CP
c) Auditer les MSCA et CP désignés, en incluant les Agences de Service
d) Approuver le MSCA/CP PS
e) Informer les parties désignées de la présente politique
f) Informer les fabricants d'UEV et les fabricants de capteurs de mouvement de la présente politique
g) Laisser approuver la présente politique par la **Commission**

[r5] Le CIA doit :

a) s'assurer que les informations utilisateur correctes et adéquates du processus de demande sont fournies au MSCA et au CP
b) informer les utilisateurs des exigences de cette politique en relation avec l'utilisation du système, c'est-à-dire les porteurs de cartes, les fabricants d'UEV et les fabricants de capteurs de mouvement

3.1.2 Obligations de MSCA

[r6] Le MSCA désigné doit :

a) suivre cette politique nationale de CA
b) publier des dispositions pratiques de MSCA (MSCA PS) qui incluent la référence à cette politique nationale de CA, à approuver par le MSA
c) Maintenir des ressources d'organisation et financières suffisantes pour opérer en

conformité avec les exigences décrites dans cette politique nationale de CA, *en particulier pour assumer le risque des dommages dus à sa responsabilité*

[r7] Le MSCA doit s'assurer que toutes les exigences imputables au MSCA, comme détaillées dans cette politique, sont mises en place.

[r8] Le MSCA a la responsabilité de la conformité aux procédures prescrites dans cette politique, même lorsque la fonction de MSCA est reprise par un sous traitant, des Agences de Service. Le MSCA est responsable de s'assurer que toute Agence de Services fournit tous ses services en cohérence avec ses Dispositions Pratiques (PS) et la politique nationale de CA.

3.1.3 Obligations de CP

[r9] Le CP désigné (organisme de personnalisation de cartes) doit :

a) suivre la politique nationale de CA
b) publier des dispositions pratiques de CP (CP PS) qui incluent la référence à cette politique nationale de sécurité, à approuver par le MSA
c) Maintenir des ressources d'organisation et financières suffisantes pour opérer en conformité avec les exigences décrites dans la politique nationale de CA, en particulier pour assumer le risque des dommages dus à sa responsabilité.

[r10] Le CP doit s'assurer que toutes les exigences qui lui incombent, comme détaillé dans cette politique, sont mises en place.

[r11] Le CP a la responsabilité de la conformité aux procédures prescrites dans cette politique, même lorsque la fonction de CP est reprise par des sous traitants, des Agences de Service.

3.1.4 Obligation des Agences de Service

[r12] les Agences de Service (lorsque c'est applicable) ont des obligations envers le MSCA ou le CP et les utilisateurs selon les agréments contractuels.

3.1.5 Obligations de porteurs de cartes

[r13] [Recommandé] Le CIA doit obliger, au travers d'un agrément (cf. 5.1.2), l'utilisateur (ou l'organisme utilisateur) à remplir les obligations suivantes :

a) une information précise et complète est soumise au CIA en accord avec les exigences de cette politique, en particulier en ce qui concerne l'enregistrement ;
b) les clés et le certificat sont utilisés exclusivement pour le système chronotachygraphe ;
c) [Recommandé] la carte est exclusivement utilisée pour le système chronotachygraphe ;
d) une attention raisonnable est exercée pour éviter une utilisation non autorisée de la clé privée de l'équipement et de la carte ;

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

e) l'utilisateur peut seulement utiliser ses propres clés, certificat et sa carte (Règlement 14.4a) ;
f) un utilisateur ne peut seulement utiliser qu'une carte conducteur valide (Règlement 14.4a) ;
g) un utilisateur peut seulement disposer dans des conditions très spécifiques, et dûment justifiées, à la fois d'une carte atelier et d'une carte entreprise (Annexe 1B, VI :1) ; [Recommandé] ou à la fois une carte atelier et une carte conducteur ; ou plusieurs cartes atelier
h) L'utilisateur ne doit utiliser une carte endommagée ou expirée (Règlement 14.4.a) ;
i) L'utilisateur doit notifier au CIA dans un délai raisonnable si l'un des cas suivants arrive avant la fin de validité de la période indiquée sur le certificat :
- La clé privée de l'équipement ou de la carte a été perdue, volée ou potentiellement compromise (Règlement 15.1) ; ou
- le contenu du certificat est ou devient inexact.

3.1.6 Obligations des fabricants d'UEV (rôle comme organisme de personnalisation)

[r14] Le MSA doit obliger, au travers d'un agrément (cf 5.1.2), les fabricants d'UEV de s'assurer que les obligations suivantes sont remplies :
a) une information précise et complète est soumise au MSA en accord avec les exigences de cette politique, en particulier en ce qui concerne l'enregistrement ;
b) les clés et certificat sont exclusivement utilisés pour le système chronotachygraphe ;
c) la clé privée d'équipement est exclusivement utilisée pour l'UEV ;
d) une attention raisonnable est exercée pour éviter une utilisation non autorisée de la clé privée de l'équipement ;
e) notifier le MSA dans un délai raisonnable si l'un des cas suivants arrive avant la fin de la période de validité indiquée sur le certificat :
- la clé privée de l'équipement a été perdue, volée, potentiellement compromise ; ou
- le contenu du certificat est ou devient inexact.

3.1.7 Obligations des fabricants de capteurs de mouvement (rôle comme organisme de personnalisation)

[r15] Le MSA doit obliger, au travers d'un agrément (cf 5.1.2), les fabricants de capteurs de mouvement de s'assurer que les obligations suivantes sont remplies :
a) une information précise et complète est soumise au MSA en accord avec les exigences de cette politique, en particulier en ce qui concerne l'enregistrement ;
b) les clés et certificat sont exclusivement utilisés pour le système chronotachygraphe ;
c) Notifier le MSA dans un délai raisonnable si la clé secrète a été perdue ou détruite

3.2 Responsabilité

Note : le Règlement ne traite pas de la question de la responsabilité.
Le MSCA et le CP ne sont pas responsables envers les utilisateurs finaux, seulement envers le MSA et le CIA.

Toutes les questions de responsabilité envers les utilisateurs finaux sont de la responsabilité du MSA/CIA.

[r16] [Recommandé] Les cartes tachygraphiques, les clés et les certificats sont exclusivement destinés au système chronotachygraphe, tout autre certificat présent sur les cartes tachygraphiques sont une violation de cette politique, et de là ni le MSA, le CIA, le MSCA ni le CP n'en porte la responsabilité.

3.2.1 Responsabilité du MSA et du CIA envers les utilisateurs et parties afférentes.

[r17] [Recommandé] Le MSA et le CIA sont responsables des dommages résultant des défections à remplir leur obligation seulement s'ils ont procédé avec négligence. Si le MSA ou le CIA a procédé selon cette politique nationale de CA, et tout autre document de gouvernance, il ne sera pas considéré comme avoir été négligent.

3.2.2 Responsabilité du MSCA et du CP envers le MSA et le CIA

[r18] [Recommandé] Le CP ou le MSCA est responsable des dommages résultant de défections à remplir ses obligations seulement s'il a procédé avec négligence. Si l'organisme a procédé selon cette politique nationale de CA et le PS correspondant, il ne sera pas considéré comme avoir été négligent.

3.3 Interprétation et contrôle

3.3.1 Loi de gouvernance

Le sujet de loi de gouvernance n'est pas résolu.

3.4 Confidentialité

La confidentialité est stricte selon la Directive 95/46/EC (ou loi nationale correspondante) pour la protection des individus en ce qui concerne le traitement de données personnelles et le mouvement de telles données.

3.4.1 Types d'information à garder confidentielle

[r19] Toute information personnelle ou d'entreprise détenue par le MSCA, le CP ou de Agences de Service qui n'apparaissent pas sur les cartes émises ou les certificats est considérée confidentielle, et ne doit pas être divulguée sans accord préalable de l'utilisateur, ni de l'accord préalable de l'employeur de l'utilisateur ou son représentant, à moins que cela soit légalement exigé par ailleurs.

[r20] Toutes les clés privées et secrètes utilisées et traitées par les opérations de MSCA/CP sous cette politique nationale de CA doivent être gardées confidentielles.

[r21] Toute clé privée et secrète utilisée et manipulée lors d'opération par des fabricants d'UEV sous cette politique nationale de CA doivent être gardées confidentielles

[r22] Toute clé privée et secrète utilisée et manipulée lors d'opération par des fabricants de capteur de mouvement sous cette politique nationale de CA doivent être gardées confidentielles

[r23] les enregistrements et archivages des audits ne doivent pas être rendus accessibles, sauf lorsque c'est exigé par la loi.

3.4.2 Types d'information considérés comme non confidentielles

[r24] Les certificats ne sont pas considérés comme confidentiels

[r25] Les informations d'identification ou autres informations personnelles ou d'entreprises qui sont visibles sur les cartes et les certificats ne sont pas considérées comme confidentielles, à moins que des statuts ou des agrément spéciaux l'imposent.

4. Dispositions Pratiques (PS)

[r26] Le MSCA et le CP doivent avoir des dispositions des pratiques et des procédures utilisées pour répondre à toutes les exigences identifiées dans la politique nationale de CA, Dispositions Pratiques (PS). Le MSA doit approuver le PS.
En particulier :

a) le PS doit identifier les obligations de tous les organismes externes en charge des services de MSCA et de CP incluant les politiques applicables et les pratiques.
b) Les Dispositions Pratiques doivent être rendus accessibles aux MSA, utilisateurs du système chronotachygraphe et aux parties s'y référant (par exemple les corps de contrôle).
Cependant, le MSCA/CP n'a pas généralement l'obligation de rendre publique et disponible pour les utilisateurs tous les détails de ses pratiques.
c) La gestion du MSCA/CP a la responsabilité de s'assurer que le PS est correctement mis en place.
d) Le MSCA/CP doit définir un processus de revue pour le PS.
e) Le MSCA/CP doit fournir la notice obligatoire des changements qu'il a l'intention de faire dans le PS et doit, suivant l'approbation, rendre immédiatement disponible le PS revu. Des révisions mineures peuvent être publiées sans approbation du MSA.

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

5 Gestion d'équipement

L'équipement du système chronotachygraphe est défini comme :
- les cartes tachygraphiques
- les Unités Embarquées Véhicule
- les capteurs de mouvement

L'équipement est traité et géré par différents rôles :
- CIA (enregistrement, renouvellement, etc.)
- MSCA (certificats, clés)
- CP (personnalisation visuelle et électronique, distribution, désactivation)
- Fabricants d'UEV et fabricants de capteurs de mouvement

Les fonctions suivantes sont réalisées par le MSA :
- contrôle qualité (approbation de type)

Les fonctions suivantes sont réalisées par le CIA :
- Demandes de cartes, certificats d'UEV et clés de capteurs de mouvement
- Demandes d'enregistrement d'approbation
- Enregistrement d'équipement et stockage de données (DB)

Les fonctions suivantes sont réalisées par le MSCA et le CP :
- contrôle qualité (tests d'échantillon)
- insertion de clé
- personnalisation des cartes
- distribution

Les fonctions suivantes sont réalisées par les fabricants d'UEV :
- personnalisation des UEV
- insertion de la clé de capteur de mouvement
- distribution

Les fonctions suivantes sont réalisées par les fabricants de capteur de mouvement :
- insertion de la clé de capteur de mouvement
- distribution

5.1 Cartes tachygraphiques

5.1.1 Contrôle qualité – fonction du MSCA/CP

[r27] Le MSCA/CP doit s'assurer que seul un type de cartes approuvé selon le Règlement sont personnalisées dans le système chronotachygraphe. Cf également 5.1.7.5

5.1.2 Demande de cartes – traitée par le CIA

[r28] Le CIA doit informer l'utilisateur des termes et conditions concernant l'usage de la carte. Cette information doit être rendue accessible et dans un langage facilement compréhensible.
[Pratique] Il est recommandé que les informations soient disponibles au moins à la fois dans la (les) langue(s) nationale (s) de l'Etat Membre et en anglais.

[r29] L'utilisateur doit, en demandant une carte et acceptant la livraison de la carte, en accepter les termes et les conditions.

5.1.2.1 Demande d'utilisateur

[r30] Les demandeurs de carte tachygraphique doivent fournir une demande selon un format à définir par le MSA ou le CIA. Au minimum, la demande doit inclure les données nécessaires à l'identification correcte de l'utilisateur. D'autres données pourraient par exemple être récupérées à partir du registre du permis de conduire.

Note : Selon le règlement, les certificats et cartes des ateliers, entreprises et contrôleurs peuvent être émis soit au nom du représentant des entreprises ou d'organismes (personne légale), soir à la personne légale. Il est recommandé d'appliquer le premier cas, pour plus de sécurité. S'il est décidé que ces cartes et certificats peuvent ne pas être individuelles, la politique devra être amendée en conséquence.

Les informations suivantes sont exigées pour émettre une carte. A moins qu'elles ne soient collectées d'autres sources, elles doivent être incluses dans la demande :

- Nom complet
- Date et lieu de naissance
- Lieu de résidence
- [Recommandé] numéro d'enregistrement national (si disponible)
- [Recommandé] adresse postale
- photo (sauf si un fichier valide de photo est utilisé) (optionnel sauf pour les cartes conducteur)
- Langage préféré

Pour les cartes conducteur :

- le numéro de permis de conduire

Pour les cartes atelier :

[r31] **[Recommandé]** les cartes atelier doivent être uniquement émises à des personnes physiques associées à une personne légale, et qui peuvent fournir les preuves suivantes :

- Nom complet (y compris le prénom et les surnoms) de l'utilisateur
- date et lieu de naissance, référence à un document d'identité nationalement reconnu, ou d'autres éléments de l'utilisateur qui peuvent servir,

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

autant que possible, à distinguer la personne d'autres personnes portant le même nom ;

- nom complet et statut légal associé à la personne légale, ou autre entité de l'organisme ;

Pour les cartes de contrôleur :

[r32] **[Recommandé]** les certificats de corps de contrôle doivent être émis seulement à des personnes physiques associées à des personnes légales, et qui peuvent fournir les preuves suivantes :

- Nom complet (y compris le prénom et les surnoms) de l'utilisateur
- date et lieu de naissance, référence à un document d'identité nationalement reconnu, ou d'autres éléments de l'utilisateur qui peuvent servir, autant que possible, à distinguer la personne d'autres personnes portant le même nom ;
- nom complet et statut légal associé à la personne légale, ou autre entité de l'organisme ;

Pour les cartes entreprise :

[R 33] **[Recommandé]** les certificats des entreprises doivent être émis aux personnes représentant les entreprises possédant ou détenteurs de véhicules équipés de chronotachygraphes numériques et qui peuvent apporter la preuve de :

- Nom complet (y compris le prénom et les surnoms) de l'utilisateur ;
- date et lieu de naissance, référence à un document d'identité nationalement reconnu, ou d'autres éléments de l'utilisateur qui peuvent servir, autant que possible, à distinguer la personne d'autres personnes portant le même nom ;
- nom complet et statut légal associé à la personne légale, ou autre entité de l'organisme ;
- toute information d'enregistrement significative existante (par ex. numéro d'enregistrement de l'entreprise) de la personne légale associée ou autre entité de l'organisme :
- relation de l'utilisateur avec la personne légale ou autre entité de l'organisme.

5.1.2.2 Agrément

[r34] le demandeur doit, en faisant la demande de carte et acceptant sa livraison, signer un agrément avec le MSA (ou CIA), établissant au minimum les points suivants :

- L'utilisateur accepte les termes et les conditions concernant l'utilisation et la manipulation de la carte tachygraphique
- l'utilisateur accepte, et certifie, qu'à partir du moment où la carte est acceptée, pendant la période opérationnelle de la carte et jusqu'à ce que le CIA soit notifiée par l'utilisateur :
  - aucune personne non autorisée n'a jamais accès à la carte utilisateur
  - toute information fournie par l'utilisateur au CIA concernant l'information dans la carte est véridique ;
  - la carte est utilisée consciencieusement et conformément aux restrictions d'usage de la carte.

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

5.1.2.3 Termes d'approbation du CIA – pour la carte conducteur

[r35] Une carte conducteur doit seulement être émise à des personnes dont la résidence permanente se trouve dans le pays de la demande.

[r36] Le CIA doit s'assurer que le demandeur n'a pas de carte conducteur valide émise par un autre Etat Membre.

[r37] Le CIA doit s'assurer que le demandeur de carte conducteur a un permis de conduire valide pour la classe (de véhicule) concernée.

5.1.3 Renouvellement de carte – traitement par le CIA

[r38] Les cartes Atelier ne doivent pas être valides plus d'un an à partir de son émission (Règlement 12.1)

[r39] les cartes conducteur ne doivent pas être valides plus de cinq ans à partir de son émission (Règlement 14.4.a)

[r40] les cartes entreprises ne doivent pas être valides plus de cinq ans à partir de son émission.

[r41] les cartes de contrôleur ne doivent pas être valides plus de deux ans à partir de son émission.

[r42] le CIA devra établir les programmes de rappel de l'utilisateur pour l'expiration à venir.

[r43] Une demande de renouvellement doit suivre la section 5.1.2

5.1.3.1 Cartes Conducteur

[r44] l'utilisateur doit faire une demande de renouvellement de carte au moins **15** jours avant l'expiration de la carte (Règlement article 15.1)

[r45] Si l'utilisateur satisfait aux règles ci-dessus, le CIA doit émettre une nouvelle carte conducteur avant l'expiration de la carte. (Règlement article 14.4.a)

5.1.3.2 Cartes Atelier

[r46] l'utilisateur doit faire une demande de renouvellement de carte au moins **15** jours avant la date d'expiration de la carte.

[r47] le CIA doit émettre une nouvelle carte dans les **5** jours ouvrés de la réception d'une demande complète. (Règlement article 12.1)

5.1.3.3 Carte Entreprise

[r48] l'utilisateur doit faire une demande de nouvelle carte au moins **15** jours avant

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

l'expiration de la carte.

[r49] si l'utilisateur satisfait aux règles ci-dessus, le CIA doit émettre une nouvelle carte Entreprise avant l'expiration de la carte courante.

5.1.3.4 Carte Contrôleur

[r50] l'utilisateur doit faire une demande de nouvelle carte au moins **15** jours avant l'expiration de la carte.

[r51] Le CIA doit émettre une nouvelle carte dans les **5** jours ouvrés de la réception d'une demande complète.

5.1.4 Mise à jour ou échange de carte – traitement par le CIA

[r52] Un utilisateur qui change de pays de résidence peut demander le changement de sa carte.
Si la carte courante est valide, l'utilisateur devra seulement apporter la preuve de résidence pour obtenir une demande confirmée.

[r53] le CIA doit, sous réserve de la livraison de la nouvelle carte, prendre possession de la carte précédente et l'envoyer au MSA d'origine (Règlement article 14.4.c)

[r54] L'échange de carte due à un changement de pays de résidence doit d'autre part suivre les règles d'émission de la nouvelle carte.

5.1.5 Remplacement de cartes perdues, volées, endommagées ou en dysfonctionnement – traitement par le CIA

[r55] Si une carte a été perdue ou volée, l'utilisateur doit le déclarer à la Police locale et recevoir une copie de sa déclaration. La perte de carte peut être déclarée par l'utilisateur, ou par la Police sous réserve de réception de la carte trouvée. La Police doit sans délai notifier le CIA émetteur de sa déclaration.

[r56] la carte volée ou perdue doit être mise dans une liste noire disponible aux autorités de tous les Etats Membres.

[57] les cartes endommagées ou en dysfonctionnement doivent être envoyées au CIA émetteur, annulées visuellement et électroniquement, et placées dans une liste noire.

[58] Si la carte est perdue, volée endommagée ou en dysfonctionnement, l'utilisateur doit faire une demande pour une carte de remplacement dans les **7** jours. (Règlement article 15.1)

[59] Si l'utilisateur suit les exigences ci-dessus, le CIA doit émettre une carte de

remplacement avec des nouvelles clés et certificat dans les 5 jours ouvrés à partir de la réception d'une demande complète. (Règlement article 15.1)

[r60] la carte de remplacement doit hériter de la durée de validité de la carte originale. (Règlement Annexe 1B : VII). Si la carte remplacée a moins de six mois de validité restante, le CIA peut émettre une carte de renouvellement à la place d'une carte de remplacement.

5.1.6 Enregistrement de demande approuvée – traitement par le CIA

[r61] Le CIA doit enregistrer les demandes approuvées dans une base de données. Cette donnée est rendue disponible pour le MSCA/CP, qui utilise l'information comme entrée pour la génération de certificat et la personnalisation de la carte.

5.1.7 Personnalisation de la carte – traitement par le CP

Les cartes sont personnalisées à la fois visuellement et électroniquement. Dans certains cas ce processus sera réalisé par une Agence de Services externe, ce qui ne diminue pas l'entière responsabilité du MSA.

5.1.7.1 Personnalisation visuelle

[r62] les cartes doivent être visuellement personnalisées selon le Règlement, Annexe 1B, section IV.

5.1.7.2 Entrée de données utilisateur

[r63] Les données doivent être insérées dans la carte selon la structure du Règlement, Annexe 1B, appendice 2, règles TCS_403, TCS_408, TCS_413 et TCS_418, selon le type de carte.

5.1.7.3 Entrée de clé

[r64] [Recommandé] La clé privée doit être insérée dans la carte sans avoir jamais quitté l'environnement de génération de clé. Cet environnement doit garantir qu'aucune personne, de quelque façon que ce soit, ne puisse obtenir le contrôle de génération de clé privée sans être détectée. Voir aussi la gestion de clé d'équipement en 7.2.

5.1.7.4 Entrée de certificat

[r65] le certificat utilisateur doit être inséré dans la carte avant sa distribution à l'utilisateur.

5.1.7.5 Contrôle Qualité

[r66] Des demandes documentées doivent exister pour assurer que les informations visuelles sur les cartes des utilisateurs et les informations électroniques dans les cartes émises et les certificats se correspondent mutuellement et aussi correspondent au propriétaire reconnu. Les demandes doivent être décrites dans le

PS de personnalisation.

5.1.7.6 Annulation (destruction) de cartes non distribuées

[r67] Toutes les cartes endommagées ou détruites (ou pour d'autres raisons n'ont pas été complétées ni distribuées) au cours de la personnalisation doivent être physiquement et électroniquement détruites (annulées).

[r68] Toutes les cartes détruites doivent être enregistrées dans une base de données d'annulation.

5.1.8 Enregistrement de carte et stockage de données (DB) – traité par le CP et le CIA

[r69] Le CP est responsable de la conservation des traces des cartes et des numéros de cartes qui ont été fournies et à quel utilisateur. Les données doivent être transférées du CP au registre du CIA.

5.1.9 Distribution de carte à l'utilisateur – traité par le CP ou le CIA

[r70]

a) la personnalisation doit être planifiée de façon à minimiser la durée de conservation sécurisée exigée de la carte personnalisée avant sa livraison à l'utilisateur. Un stockage de plus de d'un jour exige une conservation sûre et sécurisée. Des demandes documentées doivent exister pour les traitements exceptionnels, y compris les perturbations du processus de production, panne de distribution, et perte ou endommagement de cartes.

b) Les cartes personnalisées doivent être immédiatement transférées dans le lieu de livraison ou de distribution à l'utilisateur, c'est-à-dire un endroit contrôlé.

c) Les cartes personnalisées doivent toujours être conservées dans un lieu distinct des cartes non personnalisées.

d) Les cartes tachygraphiques doivent être distribuées de façon à minimiser les risques de perte.

e) Au point de livraison de la carte à l'utilisateur, la preuve de l'identité de l'utilisateur (par ex. son nom) doit être vérifiée auprès de la personne même.

f) [Recommandé] l'utilisateur doit présenter des moyens valides d'identification.

g) [Recommandé] la réception de la carte doit être sanctionnée par la signature de l'utilisateur.

5.1.10 Codes d'authentification (PIN)[5] – générés par le CP

Cette section ne s'applique qu'aux cartes Atelier uniquement.

[r71] les cartes Atelier doivent avoir un code PIN, utilisé pour l'authentification de la

[5] (NdT) PIN : Personal Identification Number, c'est un code secret qui doit rester strictement personnel.

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

carte par l'UEV (Règlement, Annexe 1B, Appendice 10 : UEV : 4.1.2).

[r72] le code PIN consiste en 4 digits au moins (Règlement, Annexe 1B, Appendice 10 : UEV : 4.1.2)

5.1.10.1 Génération de PIN

[r73] les codes PIN doivent être générées dans un système sécurisé, transférés en toute sécurité dans les cartes Atelier, et directement imprimés dans les enveloppes de PIN. Les codes PIN ne doivent jamais être stockés dans un système informatique de façon à permettre la connexion entre le PIN et l'utilisateur. Le système de génération de PIN doit satisfaire aux exigences de l'ITSEC E3, CC EAL4 ou des critères équivalents de sécurité.

5.1.10.2 Distribution de PIN

[r74] Les codes PIN peuvent être distribués par un courrier ordinaire.

[r75] les codes PIN ne doivent pas être distribués avec la carte correspondante.

5.1.10.3 Désactivation de carte – traité par les MSC/CIA et CP

[r76] [Recommandé] Il doit être possible de désactiver de façon permanente une carte et les clés qu'elle contient. La décision de désactivation doit être prise par le MSA ou le CIA, l'opération devrait alors être réalisée par le CP ou l'Agence de Service.

[r77] la désactivation de cartes doit avoir lieu dans l'équipement approprié pour l'opération et il doit être vérifié que les fonctions de la carte et les clés sont détruites. La carte doit également être visuellement annulée.

[r78] la désactivation de cartes doit être enregistrée dans la base de données des cartes et le numéro de la carte doit être placé dans la liste noire.

5.2 Unités Embarquée Véhicules et Capteurs de Mouvement

5.2.1 Contrôle qualité – fonction du CIA

[r79] le CIA doit s'assurer que des certificats (et les données chiffrées de capteur de mouvement) sont émises uniquement pour les UEV approuvées (et le Capteurs de mouvement).

5.2.2 Processus de demande et d'enregistrement d'UEV et de capteur de mouvement – traité par le CIA

Les fabricants d'UEV demandent des certificats, pas d'équipement, mais fonctionnellement le

processus de demande est équivalent à celui utilisé pour les cartes tachygraphiques, et à partir de là leur est distribué. Les fabricants de Capteurs de Mouvement demandent des clés de Capteur de Mouvement, et cette requête peut être traitée comme un enregistrement.

5.2.2.1 Unités Embarquées Véhicule

[r80] le CIA doit s'assurer de la preuve de l'indentification de l'UEV et la précision des noms du fabricant et les données associées doit être correctement examinée comme faisant partie du service d'enregistrement.

[r81] Les fabricants d'UEV peuvent demander des certificats pour des UEV non encore identifiées. Dans ce cas, la relation entre l'identité de l'UEV et du certificat doit être ajoutée à l'enregistrement le plus tôt possible. (Règlement, Annexe 1B, Appendice 11 : 3.3.1).

[r82] Le CIA doit informer le fabricant des termes et conditions d'usage du certificat. Cette information doit être disponible dans un langage facilement compréhensible. [Pratique] Il est recommandé que l'information soit disponible au moins à la fois dans le(s) langage(s) national(aux) de l'Etat Membre et en anglais.

[r83] [Recommandé] le fabricant doit, en faisant une demande de certificat et en acceptant la livraison du certificat, établir un agrément avec le MSA (ou le CIA), acceptant les termes et les conditions.

[r84] Le fabricant doit fournir une adresse postale, ou autres attributs, qui précisent comment il peut être contacté.

5.2.2.2 Capteurs de Mouvement

Les fabricants de capteur de mouvement demandent des clés au CIA. Sont inclus dans la demande les données du capteur de mouvement et du fabricant.. Fonctionnellement cela peut être vu comme une demande. Les données de capteur de mouvement telles que le numéro de série et le fabricant doivent être stockés dans la base de données.

5.2.3 Enregistrement de demande d'approbation – traité par le CIA

[r85] Le CIA doit enregistrer les demandes d'approbation dans une base de données. Ces données doivent être accessibles au CP, qui utilise l'information comme une donnée d'entrée de la génération de certificat.

5.2.4 Enregistrement et stockage de certificat d'UEV – traité par le CIA et le MSCA

[r86] Le CP est responsable de l'enregistrement du certificat émis pour chaque UEV ou pour chaque demande de certificat d'UEV. Le CIA est responsable de la maintenance de la base de donnée relatant les UEV et les certificats.

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

5.2.5 Personnalisation d'UEV – traitée par le fabricant d'UEV

Les UEV sont personnalisées par l'insertion du certificat d'UEV et des clés. Il est attendu que dans la plupart des cas cette tâche soit traitée par les fabricants d'UEV, mais le règlement autorise que la tâche soit traitée, grâce à des équipements spécifiques de personnalisation, même par le MSCA (Règlement, Annexe 1B, appendice 11 : 3.1.1).

[r87] Si personnalisation est une tâche du fabricant, le MSA du pays de l'approbation de type doit inspecter et approuver les moyens de personnalisation.

5.2.5.1 *Insertion de clé*

[r88] la clé privée RSA doit être insérée dans l'UEV sans quitter l'environnement de génération de clé. Cet environnement doit garantir que personne, de quelque façon que ce soit, ne puisse obtenir le contrôle de la génération de clé sans être détecté. La clé symétrique Km_{VU} doit être insérée doit être insérée dans l'UEV de façon sécurisée. Voir aussi la gestion de clé d'équipement en 7.2.

5.2.5.2 *Insertion de certificat*

[r89] Le certificat utilisateur doit être inséré dans l'UEV de façon à maintenir son intégrité.

5.2.6 Distribution de clés et de certificat d'UEV et de Capteur de Mouvement au fabricant d'équipement – traitée par le CP

[r90] Le CP est responsable de la distribution des clés et de certificats des UEV et de capteurs de mouvement aux fabricants respectifs de façon correcte !

5.2.7 Distribution d'UEV – traitée par le fabricant d'UEV

[R91] La distribution d'UEV est la responsabilité des fabricants d'UEV et doit être traité de façon correcte !

5.2.8 Renouvellement d'UEV

[r92] L'UEV ne nécessite pas un renouvellement sauf en cas de dysfonctionnement, d'endommagement, etc.

5.2.9 Remplacement d'UEV perdue, endommagée ou en dysfonctionnement

[r93] Le remplacement d'UEV revient au cas de distribution d'une nouvelle UEV.

[94] Si une UEV a été perdue ou volée, le conducteur ou l'utilisateur du véhicule doit le déclarer à la Police locale et recevoir une copie de sa déclaration. La perte d'UEV peur être déclarée par le conducteur ou l'utilisateur du véhicule, ou par la Police à réception de la carte trouvée.[6]

[r95] [Recommandé] Les UEV volées ou perdues doivent être enregistrées dans une liste noire à distribuer à tous les Etats Membres. C'est une tâche du CIA.

5.2.10 Fin de vie des UEV

La fin de vie des UEV devrait être traitée pour que :

[r96] [Recommandé] Les clés et les certificats soient détruits

[r97] La destruction d'une UEV soit enregistrée par le CIA dans le pays d'émission.

[6] (NdT) Il s'agit sans doute d'une erreur du texte original « upon receiving a found card », qui devrait dire « upon receiving a found VU » = à réception de l'UEV trouvée.

6 Gestion de clés génériques et des clés de transport : Clé Générique Européenne, Clés d'Etat Membre, clés de Capteur de Mouvement, clés de transport

Cette section contient des dispositions pour la gestion de :

- la clé Générique Européenne – la clé publique ERCA
- les clés d'Etat Membre, c'est-à-dire les paires de clé de signature d'Etat Membre
- Les clés de Capteur de Mouvement
- Les clés de transport (entre l'ERCA et le MSCA)

La **clé publique ERCA** est utilisée pour vérifier les certificats d'Etat Membre. La clé secrète ERCA n'est pas traitée ici, car elle ne quitte jamais l'ERCA.

Les **clés d'Etat Membre** sont les clés de signature d'Etat Membre et peuvent également être appelées clés génériques d'Etat Membre.

Les **clés de Capteur de Mouvement** sont des clés symétriques à placer dans les cartes Atelier, les UEV et les Capteurs de Mouvement pour une reconnaissance mutuelle. Le MSCA reçoit les clés de Capteur de Mouvement de l'ERCA, les stocke et les distribue aux fabricants.

Les **clés de transport** sont des clés symétriques utilisées pour l'échange sécurisé de l'information entre l'ERCA et le MSCA.

6.1 Clé publique ERCA

[r98] Le MSCA doit conserver la clé publique ERCA (EUR.PK) de façon à maintenir son intégrité et sa disponibilité à tout moment. Si l'EUR.PK est stockée par le CP, la même règle s'applique.

[r99] Le CP doit s'assurer que l'EUR.PK est insérée dans chaque carte tachygraphique et chaque UEV.

6.2 Clés d'Etat Membre

Les clés d'Etat Membre sont la(es) paire(s) de clés de signature du MSCA, utilisée(s) pour signer tous les certificats d'équipement.

La paire de clés consiste en une clé publique (MS.PK) et une clé privée, ou secrète, (MS.SK)

La clé publique MSCA est certifiée par l'ERCA, mais est toujours générée par le MSCA.

[r100] Les clés d'Etat Membre ne doivent pas être utilisées pour d'autres buts que la signature d'équipement de chronotachygraphe

6.2.1 Génération de clés d'Etat Membre

[r101] la paire de clés d'Etat Membre doit être produite par un appareil qui :

- soit répond aux exigences identifiée par FIPS 140-2 (ou 140-1) niveau 3 ou supérieur [FIPS]
- soit répond aux exigences identifiées par le CEN Workshop Agreement 14167-2 [CEN]
- soit est un système digne de confiance qui respecte EAL 4 ou supérieur en accord avec la norme ISO 15408, [CC], E3 ou supérieur de l'ITSEC, ou des critères de sécurité équivalents. Il doit y avoir un objectif de sécurité ou un profile de protection qui répond aux exigences du présent document, basé sur une analyse de risque et prenant en compte les mesures de sécurité physiques et non techniques.

[r102] Le dispositif de génération de clé doit être autonome.

[r103] Le dispositif utilisé et le niveau d'exigences atteint doivent être décrits dans le MSCA PS.

[r104] La génération de paire de clés de MSCA doit exiger la participation active de trois personnes différentes. Au moins une de ces personnes doit avoir le rôle de CAA/PA (certification authority/personnalization administrator = autorité de certification/ administrateur de personnalisation), les autres peuvent avoir d'autres rôles de confiance (voir section 9.3.19.3.1 pour la description des rôles).

[r105] Les clés doivent être générées en utilisant l'algorithme RSA avec une longueur de clé modulo *n* = 1024 bits (Règlement, Annexe 1B, app. 11 : 2.1/3.2).

[r106] [Fortement recommandé] Le MSCA doit avoir plus d'une paire de clés d'Etat Membre avec des certificats de signature pour assurer la continuité, alors que l'ERCA ne peut pas émettre des certificats d'Etat Membre rapidement.
ou
[Recommandé] le MSCA doit avoir au moins deux (2) et au maximum cinq (5) paires de clés d'Etat Membre avec les certificats de signature associés pour assurer la continuité, alors que l'ERCA ne peut pas émettre des certificats d'Etat Membre rapidement.

6.2.2 Durée de validité des clés d'Etat Membre

[r107] [Recommandé] La clé privée d'Etat Membre ne doit pas être valide plus de 2 ans à partir de la certification de la clé publique correspondante, et ne doit pas être

utilisée après son expiration pour quelque motif que ce soit.

[r108] la clé publique correspondante n'a pas de fin de validité.

6.2.3 Stockage de la clé privée d'Etat Membre

[r109] les clés privées doivent être contenues et utilisées à partir d'un dispositif spécifique résistant au sabotage qui :
- répond aux exigences identifiées par FIPS 140-2 (ou 140-1) niveau 3 ou supérieur ; ou
- est un système digne de foi qui est assuré par EAL 4 ou supérieur en concordance avec l'ISO 15408 [CC], au niveau E3 de l'ITSEC ou à des critères de sécurité équivalents. Cela doit être un objectif de sécurité ou de profile de protection qui répond aux exigences du présent document, basé sur une analyse de risques et prenant en compte les mesures de sécurité physiques et non techniques.

[r110] pour accéder aux clés privées de signature de MSCA, un double contrôle est exigé. Cela signifie qu'une personne seule ne doit pas posséder les moyens exigés pour accéder à l'environnement où les clés privées sont stockées. Cela ne signifie pas que la signature de certificats d'équipement doive être exécutée sous un double contrôle.

6.2.4 Sauvegarde de clé privée d'Etat Membre

[r111] les clés privées de signature d'Etat Membre peuvent être sauvegardées, en utilisant une procédure de recouvrement de clé exigeant au moins un double contrôle. La procédure utilisée doit être établie dans le MSCA PS. Cependant, si des paires de clés selon [r106] sont utilisées, aucune sauvegarde n'est nécessaire.

6.2.5 Falsification de clé privée d'Etat Membre

[r112] Les clés privées de signature d'Etat Membre ne doivent pas être falsifiées.

6.2.6 Compromission de clés d'Etat Membre

[r113] Une disposition écrite doit exister, y compris dans le MSCA PS, qui établit les mesures à prendre par les utilisateurs et les personnes responsables de la sécurité du MSCA et/ou des Agences de Services si les clés privées de l'Etat Membre sont divulguées, ou apparaissant par un autre moyen, ou soupçonnées d'être compromises.

[r114] Dans un tel cas, le MSCA doit au minimum :
- informer le MSA, l'ERCA et les autres MSCA

6.2.7 Fin de vie des clés d'Etat Membre

[r115] Le MSCA doit avoir une application pour s'assurer qu'il dispose toujours d'une paire de clés de signature d'Etat Membre valide et certifiée.

[r116] A la fin de l'utilisation d'une paire de clés de signature d'Etat Membre, la clé publique doit être archivée, et la clé privée doit être:
- détruite de telle façon que la clé privée ne puisse être retrouvée ; ou
- retenue de telle façon qu'elle est protégée contre une utilisation ultérieure.

6.3 Clés de Capteur de Mouvement

[r117] le MSCA doit, comme de besoin, demander des clés de capteur de mouvement Km, Km_{VU} et Km_{WC} à l'ERCA (Règlement, Annexe 1B, app. 11 :3.1.3).

[r118] Le MSCA doit, sur demande de fabricant, chiffrer des données de capteur de mouvement (appairage avec K_P et le numéro de série étendu N_S) avec Km (Règlement, Annexe 1B, app 11 : 3.1.3).

[r119] le MSCA doit envoyer la clé d'UEV Km_{VU} aux fabricants d'UEV pour son insertion dans l'UEV (Règlement, Annexe 1B, app 11 : 3.1.3).

[r120] le MSCA doit envoyer la clé d'atelier au CP pour son insertion dans les cartes Atelier.

[r121] Le CP doit reprendre la tâche du MSCA pour s'assurer que la clé d'atelier Km_{WC} est insérée dans toutes les cartes Atelier (Règlement, Annexe 1B, app. 11 :3.1.3).

[r122] Le MSCA et ou le CP doit, au cours du stockage, de l'utilisation et de la distribution protéger les clés de capteur de mouvement avec une assurance physique de haut niveau et des contrôles de sécurité. Les clés devraient être contenues et transférées à partir d'un dispositif spécifique résistant contre le sabotage qui :
- répond aux exigences identifiées par FIPS 140-2 (ou 140-1) niveau 3 ou supérieur ; ou
- est un système digne de foi qui est assuré par EAL 4 ou supérieur en concordance avec l'ISO 15408 [CC], au niveau E3 de l'ITSEC ou à des critères de sécurité équivalents. Cela doit être un objectif de sécurité ou de profile de protection qui répond aux exigences du présent document, basé sur une analyse de risques et prenant en compte les mesures de sécurité physiques et non techniques.

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

6.4 Clés de transport

[r123] pour sécuriser la communication des données, l'ERCA émet des clés de transport spéciales et symétriques. Le MSCA doit, au cours du stockage, de la l'utilisation et de la distribution protéger les clés de capteur de mouvement avec une assurance physique de haut niveau et des contrôles de sécurité. Les clés devraient être contenues et transférées à partir d'un dispositif spécifique résistant contre le sabotage qui :

- répond aux exigences identifiées par FIPS 140-2 (ou 140-1) niveau 3 ou supérieur ; ou
- est un système digne de foi qui est assuré par EAL 4 ou supérieur en concordance avec l'ISO 15408 [CC], au niveau E3 de l'ITSEC ou à des critères de sécurité équivalents. Cela doit être un objectif de sécurité ou de profile de protection qui répond aux exigences du présent document, basé sur une analyse de risques et prenant en compte les mesures de sécurité physiques et non techniques.

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

7 Clés d'équipement (asymétriques)

Les clés d'équipement sont des clés asymétriques générées quelque part dans le processus d'émission / fabrication, et certifiées par le MSCA pour l'équipement du système chronotachygraphe :

- cartes tachygraphiques
- UEV

Les clés symétriques de capteur de mouvement ne sont pas traitées ici.

7.1 Aspects généraux concernant les CP/MSCA y compris les Agences de Service et les fabricants d'UEV

[r124] l'initialisation d'équipement (UEV et cartes), le chargement de clé et la personnalisation doivent être réalisés dans un environnement physique sécurisé et contrôlé. L'accès à ce lieu doit être strictement réglementé, contrôlable au niveau individuel, et exigeant au minimum la présence de deux personnes pour faire fonctionner le système. Un archivage doit être conservé des accès et des actions réalisées dans ce système.

[r125] Aucune information sensible contenue dans les systèmes de génération de clés ne peut sortir du système pour ne pas de violer cette politique.

[r126] Cartes tachygraphiques : aucune information sensible du système de personnalisation des cartes ne peut sortir du système pour ne pas de violer cette politique.

[r127] UEV/Capteur de Mouvement : aucune information sensible du système de personnalisation d'UEV ne peut sortir du système pour ne pas de violer cette politique.

[r128] **Les organismes (sous traitants, Agences de Services)** qui effectuent la génération de clé et la personnalisation de carte au nom de plus d'un Etat Membre doivent le faire par des processus clairement séparés pour chacun d'entre eux. Un archivage doit être gardé pour chaque processus individuel et le MSA correspondant doit y avoir accès sur demande.

[r129] [Recommandé] **Les fabricants d'UEV** qui effectuent la personnalisation d'UEV doivent le faire par un processus clairement séparé de la production d'UEV. Un archivage doit être gardé de la personnalisation et le MSA correspondant doit pouvoir y avoir accès sur demande.

[r130] MSCA/CP/Agences de Services/fabricants d'UEV : l'archivage du système de personnalisation doit contenir la référence de la commande, et lister les numéros d'équipement correspondants ainsi que les certificats. Le MSA correspondant doit

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

avoir accès à l'archivage sur demande.

7.2 Génération de clé d'équipement

[r131] Les clés peuvent être générées soit par le fabricant d'équipement, par le CP ou par le MSCA. (Annexe 1B, Appendice 11 : 3.1.1).

[r132] L'entité qui effectue la génération de clé doit s'assurer que les clés d'équipement sont générées de façon sûre et que la clé privée d'équipement reste secrète.

[r133] La génération de clé doit être réalisée par un dispositif qui soit :

- répond aux exigences identifiées par FIPS 140-2 (ou 140-1) niveau 3 ou supérieur ; soit
- répond aux exigences identifiées par le CEN Workshop Agreement 14167-2 [CEN] ; soit
- est un système digne de foi qui est assuré par EAL 4 ou supérieur en concordance avec l'ISO 15408 [CC], au niveau E3 de l'ITSEC ou à des critères de sécurité équivalents. Cela doit être un objectif de sécurité ou de profile de protection qui répond aux exigences du présent document, basé sur une analyse de risques et prenant en compte les mesures de sécurité physiques et non techniques.

[r134] le clés doivent être générées en utilisant l'algorithme RSA ayant une longueur de clé modulo *n* = 1024 bits. (Annexe 1B Appendice 11 : 2.1/3.2).

[r135] la procédure de génération et le stockage de clé privée doit éviter d'être divulguée en dehors du système qui la crée. De plus, elle doit être effacée du système immédiatement après voir été insérée dans un dispositif.

[r136] c'est la responsabilité de l'entité de génération de clé d'entreprendre les mesures adéquates pour s'assurer que la clé publique est unique dans son domaine avant que le certificat associé soit mis en place. (Ceci est présumé être fait en s'assurant que le système de génération de clé est aléatoire par nature, et de là, la probabilité de générer des clés non univoques est insignifiante.)

7.2.1.1 Génération de lot de clés

[r137] La génération de clé de chiffrement peut être réalisée par traitement de lot préalablement à la demande de certificat, ou en connexion directe avec la demande de certificat.

[r138] le traitement par lot doit être effectué sur un équipement autonome répondant aux exigences de sécurité établies plus haut. L'intégrité de la clé doit être protégée jusqu'à la réalisation de l'émission du certificat.

7.2.2 Validité de clé d'équipement

7.2.2.1 *Clés sur les cartes*

[r139] l'utilisation de clé privée d'équipement en relation avec les certificats émis selon cette politique ne doit jamais excéder la fin de validité du certificat.

7.2.2.2 *Unité Embarquée Véhicules*

[r140] [Recommandé] La clé privée de l'UEV ne doit avoir une validité supérieure à **30** ans.
ou
La clé privée de l'UEV ne doit pas être valide au-delà de la durée de vie de l'UEV.

7.2.3 Protection et stockage de clé privée d'équipement – Cartes

[r141] Le CP doit s'assurer que la clé privée de la carte est protégée par, et limitée à, une carte qui a été livrée à l'utilisateur selon les procédures établies dans cette politique.

[r142] des copies de clé privée ne doivent pas être conservées où que ce soit sauf dans la carte tachygraphique, à moins que ce soit exigé au cours de la génération de clé et la personnalisation du dispositif.

[r143] En aucun cas la clé privée de la carte ne peut être divulguée ou stockée en dehors de la carte.

7.2.4 Protection et stockage de clé privée d'équipement – UEV

[r144] Le fabricant d'UEV doit s'assurer que la clé privée d'UEV, et les moyens correspondants de son utilisation, sont protégés par, et limités à, une UEV.

[r145] des copies des clés privées ne sont pas conservées dans quelqu'endroit que ce soit sauf dans l'UEV à moins que ce soit exigé au cours de la génération de clé et de la personnalisation du dispositif.

[r146] en aucun cas la clé privée d'UEV ne doit être divulguée ou stockée en dehors de l'UEV.

7.2.5 Falsification et archivage de clé privée d'équipement

[r147] les clés privées d'équipement ne doivent ni être falsifiées ni archivées.

7.2.6 Archivage de clé publique d'équipement

[r148] Toutes les clés publiques certifiées doivent être archivées par le MSCA certifiant, ou par le CIA.

7.2.7 Fin de vie des clés d'équipement

[149] A la fin de l'utilisation d'une carte tachygraphique, la clé publique doit être archivée et la clé privée doit être :
- détruite de façon à ce qu'elle ne puisse être retrouvée ; ou
- conservée de telle façon qu'elle soit protégée contre toute réutilisation ultérieure.

[r150] A la fin de l'utilisation d'une UEV, la clé publique doit être archivée et la clé privée doit être :
- détruite de façon à ce qu'elle ne puisse être retrouvée ; ou
- conservée de telle façon qu'elle soit protégée contre toute réutilisation ultérieure.

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

8 Gestion de certificat d'équipement

Cette section décrit le cycle de vie du certificat, contenant la fonction d'enregistrement, l'émission de certificat, la distribution, l'utilisation, le renouvellement, la révocation (si applicable) et la fin de vie.

8.1 Données d'entrée

8.1.1 Cartes tachygraphiques

Les utilisateurs porteurs de cartes ne font pas de demande de certificat, leurs certificats sont émis à partir des informations fournies pour leur demande de carte tachygraphique (section5.1.2) et saisies à partir du registre du CIA. La clé publique à certifier est extraite du processus de génération de clé.

[r151] Le CP doit s'assurer que les données d'entrée contiennent les informations qui confèrent l'unicité du « Certificate Holder Reference » (CHR = référence du porteur du certificat). Le MSCA doit vérifier l'unicité du CHR dans son domaine.

8.1.2 Unités embarquées véhicule

Les fabricants (ou des représentants équivalents) de unités embarquées véhicule doivent faire la demande de certificats selon la section [r79] : demande/enregistrement pour UEV et Capteur de Mouvement.

[r152] Le CP doit s'assurer que les données d'enregistrement contiennent l'information qui confère l'unicité du CHR. Le MSCA doit vérifier l'unicité du CHR dans son domaine.

[r153] si la paire de clés d'équipement n'est pas générée par le MSCA, le processus de demande de certificat doit assurer que le fabricant a en sa possession la clé privée associée à la clé publique présentée à la certification.

8.2 Certificats de cartes tachygraphiques

8.2.1 Certificats de conducteurs

[r154] les certificats de conducteur sont émis seulement aux demandes satisfaisantes de carte conducteur.

8.2.2 Certificats d'atelier

[r155] les certificats d'atelier sont émis seulement aux demandes satisfaisantes de carte atelier.

8.2.3 Certificats de corps de contrôle

[r156] les certificats de corps de contrôle sont émis seulement aux demandes satisfaisantes de carte contrôleur.

8.2.4 Certificats d'entreprises

[r157] les certificats d'entreprises sont émis seulement aux demandes satisfaisantes de carte entreprise.

8.3 Certificats d'unité embarquée véhicule (UEV)

[r158] les certificats des unités embarquées véhicule sont émis au fabricant d'UEV par le MSCA du pays de l'approbation de type, et seulement pour le type d'UEV approuvées.

[r159] les certificats d'unité embarquée véhicule doivent être émis uniquement aux fabricants, et la preuve doit être apportée de :
- l'identifiant du dispositif par lequel il doit être référencé (par ex. l'approbation de type et le numéro de série), ou un identificateur de demande de certificat, si le dispositif n'est pas identifié.
- nom complet du fabricant
- un numéro d'identité nationalement reconnu, ou autres attributs qui peuvent être utilisés pour, autant que possible, distinguer le fabricant d'autres qui auraient le même nom.
- le numéro d'enregistrement du fabricant (entreprise)

8 .4 Validité et durée du certificat d'équipement

[r160] les certificats ne doivent être valides plus longtemps que l'équipement correspondant (section 5) :
- les certificats de conducteur ne doivent pas être valides plus de **5** ans (Règlement 14.4.a).
- les certificats d'atelier ne doivent pas être valides plus de **1** ans (Règlement 12.1).
- [Recommandé] les certificats de contrôleur ne doivent pas être valides plus de **2** ans.
- [Recommandé] les certificats d'entreprise ne doivent pas être valides plus de **5** ans.
- [Recommandé] les certificats d'unité embarquée véhicule ne doivent pas être valides plus de **30** ans.

ou

Les certificats d'unité embarquée véhicule **n'ont pas** de fin de validité.

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

8.5 Emission de certificat d'équipement

[r161] Le MSCA doit s'assurer qu'il émet des certificats tels que leur authenticité et leur intégrité soit maintenue. Les contenus de certificats sont définis par le Règlement, Annexe 1B, appendice 11.

8.6 Renouvellement et mise à jour de certificat d'équipement

Voir la gestion d'équipement (section 5). Alors que les certificats et les cartes ont la même durée de validité, ils sont distribués ensemble. Les certificats d'UEV ont soit pas de fin de validité, soit une très longue durée de validité, on considère alors que la durée de vie de l'équipement est plus courte que celle du certificat.

8.7 Dissémination des certificats et des informations d'équipement

[r162] Le MSCA doit exporter toute donnée de certificat au registre du CIA de façon à relier les certificats, l'équipement et les utilisateurs.

[r163] Le CIA doit s'assurer que les certificats sont rendus accessibles comme nécessaire à tous les utilisateurs et les parties concernées.

[r164] le CIA doit s'assurer que tous les termes et conditions, de même que les parties correspondantes du MSCA PS et les autres informations afférentes, sont rendues disponibles pour tous les utilisateurs, les parties concernées et autres groupes en dépendant.

8.8 Utilisation du certificat d'équipement

[r165] Les certificats de chronotachygraphe sont uniquement utilisables pour le système chronotachygraphe.

8.9 Révocation de certificat d'équipement

[r166] Les certificats ne sont pas révoqués

Note : il est prévu que plutôt que de révoquer des certificats, des équipements tachygraphiques non valides sont placés dans une liste noire qui peut être vérifiée lors de contrôles sur route.

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

9 Gestion de la sécurité de l'information de MSCA et CP

Cette section décrit les mesures de sécurité de l'information imposées par cette politique.

Note : Cette section peut, au moins en partie, être substituée par les politiques de sécurité de l'information des entités concernées.

9.1 Gestion de la sécurité de l'information des MSCA et CP

[r167] Le MSCA/CP doivent s'assurer que les procédures administratives et de gestion appliquées sont adéquates et correspondent aux normes reconnues.

[r168] Le MSCA/CP doit garder la responsabilité de tous les aspects des dispositions des services de certification de clé, même si certaines fonctions sont confiées à des sous traitants. Les responsabilités des tiers devront être clairement définies par le MSCA/CP et des accords appropriés devront garantir que les tiers sont liés pour la mise en œuvre de tous les contrôles exigés par le MSCA CP. Le MSCA/CP doit garder la responsabilité de la divulgation des pratiques qui en dépendent à toutes les parties.

[r169] L'infrastructure de sécurité de l'information nécessaire à la gestion de la sécurité du MSCA/CP doit être maintenue en permanence. Tout changement qui impactera le niveau de sécurité existant devra être approuvé par le MSA.

[r170] Le MSCA/CP doit adopter un système de gestion de sécurité équivalent à l'ISO 17799 [ISO 17799]. Une certification formelle n'est pas exigée.

9.2 Classification d'éléments et gestion du MSCA/CP

[r171] le MSCA/CP doit s'assurer que ses éléments et informations ont un niveau de protection approprié.

En particulier :

a) Le MSCA/CP doit effectuer une évaluation du risque pour estimer les risques commerciaux et déterminer les exigences de sécurité nécessaires et les procédures opérationnelles.
b) Le MSCA/CP doit maintenir un inventaire de tous les éléments d'information et doit assigner une classification des exigences de protection à ces éléments en conformité avec l'analyse du risque.

9.3 Contrôle de sécurité du personnel des MSCA/CP

9.3.1 Rôles de confiance

[r172] [Recommandé] Un MSCA/CP, assumant cette politique nationale de CA, devrait distinguer au moins trois rôles différents, comme décrit ci-dessous. Différentes organisations de séparation des tâches peuvent être acceptables, à condition que la résistance aux attaques internes soit au moins aussi forte que le modèle recommandé et à condition que les rôles soient décrits dans le MSCA/CP PS.

[r173] Pour s'assurer qu'une personne agissant seule ne puisse outrepasser les mesures de sécurité, les responsabilités au sein du système MSCA/CP nécessitent d'être tenues par plusieurs rôles et personnes. Chaque fonction du système doit avoir des possibilités limitées en rapport avec le rôle du détenteur de la fonction.

[r174] Les rôles recommandés sont :
a) Administrateur de l'Autorité de Certification ou Administrateur de Personnalisation (CAA/PA) ;
b) Administrateur Système (SA) ;
c) Officier de Sécurité du Système d'Information (ISSO).

[r175] le rôle du CAA/PA inclue :
a) génération de clé ;
b) génération de certificat ; (Générant les demandes de certificats signés, à traiter et exécuter par l'équipement du MSCA/CP selon des règles définies) ;
c) personnalisation et distribution sécurisée de l'équipement ;
d) fonctions administratives associées à la maintenance de la base de données et assistant les recherches de compromission.

[r176] Le rôle du SA inclue :
a) réalisation de la configuration initiale du système y compris le démarrage sécurisé et son arrêt ;
b) initialisation de tous les nouveaux comptes ;
c) établissement de la configuration initiale de réseau ;
d) réalisant les moyens de redémarrage d'urgence du système pour éviter les pertes catastrophiques du système ;
e) réalisation des sauvegardes du système, récupération et mises à jour du système, y compris le stockage sécurisé et la distribution de sauvegarde et des mises à jour en un lieu hors site. Le sauvegardes doivent être réalisées au moins une fois par semaine, et le système doit être redémarré après la réalisation de la sauvegarde ;
f) Changement du nom de l'hôte et/ou de l'adresse réseau.

[r177] Le rôle de l'ISSO inclue :

a) assignation des privilèges de sécurité et des contrôles d'accès des CAA/PA ;
b) assignation de mots de passe à tous les nouveaux comptes ;
c) réalisation de l'archivage des enregistrements système exigés ;
d) revue de l'enregistrement d'audit pour détecter la conformité du CAA/PA avec la politique de sécurité du système ;
e) conduite personnelle ou supervision d'un inventaire annuel des enregistrements de MSCA/CP ;
f) Participation à la génération de clé d'Etat Membre.

Noter que l'ISSO qui n'est pas directement impliqué dans l'émission de certificats, réalise une fonction de superviseur par l'examen des enregistrements du système ou des enregistrements des audits pour assurer que les autres personnes agissent dans le cadre de leurs responsabilités avec la politique de sécurité établie.

9.3.2 Séparation des rôles

[r178] Pour un MSCA/CP, différentes personnes doivent remplir chacun des trois rôles décrits ci-dessus et **au moins une personne** doit être désignée pour chaque tâche.

9.3.3 Identification et authentification de chaque rôle

[r179] l'identification et l'authentification du CAA/PA, du SA et de l'ISSO doit être appropriée et cohérente avec les pratiques, les procédures et les conditions établies dans cette politique.

9.3.4 Formation, qualification, expérience et exigence d'indépendance

[r180] le CAA/PA qui s'implique dans la création et la gestion de certificat et dans les informations de clé, est un poste critique. La personne assumant le rôle de CAA/PA devrait être d'une loyauté indubitable, digne de confiance et intègre, et devrait avoir démontré sa conscience de la sécurité dans ses activités quotidiennes.

[r181] Tout le personnel de MSCA/CP dans des postes sensibles y compris, au moins, tous les postes de CAA/PA et ISSO, doivent :

a) ne pas être affectés à d'autres tâches qui peuvent entrer en conflit avec leurs devoirs et responsabilités en tant que CAA/PA et ISSO ;
b) ne pas être reconnus comme avoir préalablement relevé d'assignation passée pour des raisons de négligence ou de non performance dans leurs tâches ;
c) avoir reçu la formation nécessaire à la performance de leurs tâches.

[r182] les organismes MSCA/CP peuvent également spécifier des exigences

spécifiques telles que des exigences de citoyenneté, de rang, de qualification, de contrôle de probité satisfaisant et d'absence de casier judiciaire. De telles exigences doivent être établies dans le PS applicable.

9.3.5 Exigences de formation

[r183] Le personnel doit avoir la formation adaptée au rôle et à la fonction.

9.4 Contrôles de sécurité du système du CA systèmes de personnalisation

[r184] Le MSCA/CP doit s'assurer que les systèmes sont sécurisés et correctement opérés, avec un risque minimum de panne.
En particulier :

a) l'intégrité des systèmes et de l'information doit être protégée contre les virus, les logiciels frauduleux et non autorisés ;
b) les dommages provenant des incidents de sécurité et les dysfonctionnements doivent être minimisés grâce à l'utilisation du rapport d'incidents et les procédures en réponse ;

[r185] Le Système de l'Autorité de Certification (CAS) et le système de Personnalisation doivent fournir assez de contrôles de sécurité du système pour renforcer la séparation des rôles décrits dans cette politique ou relevant du PS.

[r186] Les contrôles de sécurité doivent fournir un contrôle d'accès et une traçabilité jusqu'au niveau individuel pour toutes les transactions et fonctions affectant l'utilisation de l'émission de clés privées du MSCA.

[r187] [Recommandé] les contrôles de sécurité du système imposés aux systèmes informatiques utilisés par les Agences de Service dépend du rôle assigné à l'Agence. Les Agences qui doivent prendre en charge les rôles de CAA/PA, charger les certificats sur les cartes, ou initialiser de telles cartes, doivent satisfaire aux exigences imposées par les MSCA/CP.

9.4.1 Exigences techniques spécifiques pour la sécurité des ordinateurs

[r188] L'initialisation du système réalisant les clés privées de certification de MSCA doit exiger la coopération d'au moins deux opérateurs, tous les deux sont authentifiés de façon sécuritaire par le système.

9.4.2 Performance de sécurité de l'ordinateur

[r189] le CA et les systèmes de personnalisation n'exigent pas de performance formelle tant qu'ils remplissent toutes les exigences de cette section.

9.4.3 Contrôles de développement du système

[r190] Le MSCA/CP doit utiliser des systèmes dignes de foi et des produits protégés contre des modifications.

[r191] Une analyse des exigences de sécurité doit être réalisée à la phase de conception et de spécification des exigences de tout projet de développement entrepris par le MSCA/CP ou au nom du MSCA/CP pour garantir que la sécurité fait partie intégrante des systèmes.

9.4.4 Contrôles de gestion de la sécurité

[r193] les rôles du système (section 9.3.1) doivent être mis en place et contrôlés.

9.4.5 Contrôles de sécurité du réseau

[r194] Des contrôles (par ex. des murs coupe-feu) doivent être mis en place pour protéger les domaines du réseau interne du MSCA/CP des domaines extérieurs du réseau accessibles aux tiers.

[r195] Les données sensibles doivent être protégées lors d'échanges sur le réseau qui ne sont pas sécurisés.

9.5 Procédures d'audit de sécurité

Les procédures d'audit de sécurité de cette section sont valables pour tous les ordinateurs et composants du système qui affectent la production de clés, de certificats et des processus d'émission d'équipement selon cette politique.

9.5.1 Types d'événement enregistré

[r196] les fonctions d'audit de sécurité relatives au système informatique doit archiver, dans le but d'audit :

a) la création de comptes (avec ou sans privilège)
b) les requêtes de transaction avec l'enregistrement du compte demandeur, le type de demande, l'indication de la réalisation complète de la transaction et la cause éventuelle de son non aboutissement
c) l'installation de nouveau logiciel ou de mises à jour de logiciel
d) l'heure et la date et autres informations descriptives de toute les sauvegardes

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

e) l'arrêt et le redémarrage du système
f) l'heure et la date de toutes les mises à jour du matériel
g) l'heure et la date des vidages de l'archivage d'audit
h) l'heure et la date des vidages de l'archivage des transactions

9.5.2 Fréquence de traitement d'archivage d'audit

[r197] L'archivage doit être traité régulièrement et examiné pour détecter des comportements malveillants. Les procédures d'archivage doivent être décrites dans le PS.

9.5.3 Durée de conservation de l'archivage d'audit

[r198] L'archivage d'audit doit être conservé au moins **7** ans.

9.5.4 Protection de l'archivage d'audit

[r199] l'intégrité des archivages d'audit doit être protégée de façon appropriée. Tous les accès doivent être horodatés (l'heure du système est suffisante)

[r200] les archivages d'audit doivent être vérifiés et consolidés au moins une fois par mois. Au moins deux personnes ayant le rôle de SA ou d'ISSO (voir section 9.3.1) doivent être présentes pour une telle vérification et consolidation.

9.5.5 Procédures de sauvegarde de l'archivage d'audit

[r201] Deux copies de l'archivage consolidé doivent être faites et réalisées et stockées dans des endroits distincts et physiquement sécurisés.

[r202] L'archivage d'audit doit être stocké de façon à rendre possible son examen au cours de sa période de conservation.

[r203] l'archivage d'audit doit être protégé contre des accès non autorisés

9.5.6 Système de groupement d'audits (internes par rapport à externes)

[r204] Seul un système de groupement interne d'audit est exigé.

9.6 Archivage d'enregistrement

9.6.1 Types d'événement enregistrés par le CIA

[r205] Les enregistrements doivent comprendre toute preuve associée en

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se

possession du CIA y compris, mais non limité à :

a) demandes de certificats et tous les messages relatifs échangés avec le MSCA/CP, les utilisateurs et le répertoire.
b) Les agréments d'enregistrement signés des demandes d'utilisateurs pour des certificats et des cartes, y compris l'identité de la personne responsable de l'acceptation de la demande
c) L'acceptation signée de la livraison de la carte
d) Les agréments contractuels concernant les certificats et les cartes associées
e) Les renouvellements de certificats et tous les messages échangés avec l'utilisateur.
f) Les demandes de révocation et tous les messages enregistrés échangés avec l'initiateur de la demande et ou de l'utilisateur
g) Documents de la politique mise en place actuellement et précédemment.

9.6.2 Types d'événement enregistré par le MSCA/CP

[r206] Les enregistrements doivent inclure toutes les preuves associées en possession du MSCA/CP, mais non limité à :

a) Contenus des certificats émis
b) Journaux d'audit y compris les enregistrements de l'audit annuel du MSCA/CP de conformité avec le PS.
c) Les documents de la politique de certificat implémentée actuellement et précédemment et leur PS correspondants.

[r207] Les enregistrements des toutes les requêtes électroniques numériquement signées faites par le MSCA/CP ou le personnel de l'Agence de Service (CAA/PA) doit comprendre l'identité de l'administrateur responsable pour chaque requête avec toutes les informations exigées pour le contrôle de non répudiation de la requête tant que l'enregistrement est conservé.

9.6.3 Période de conservation d'archive

[r208] Les archives doivent être conservées et protégées des modification et de destruction pour une durée spécifiée dans le PS.

9.6.4 Procédure d'obtention et de vérification des informations archivées

[r209] Le MSCA/CP doit agir en conformité avec les exigences concernant la confidentialité comme établi en section 3.4.

[r210] Les enregistrements des transactions individuelles peuvent être libérées sur demande par toute entité impliquée dans la transaction, ou leurs représentants reconnus.

[r211] Le MSCA/CP doit rendre accessible sur demande la documentation produite de la conformité du MSCA/CP avec le PS applicable selon la section 11.5.

[r212] A décider : un coût raisonnable de traitement peut être facturé pour couvrir les frais de récupération d'enregistrement.

[r213] Le MSCA/CP doit s'assurer de la disponibilité de l'archivage et du stockage de l'information dans un format lisible pendant la durée de sa conservation, même si les activités du MSCA/CP sont interrompues, suspendues ou terminées.

[r214] Au cas où les services du MSCA/CP sont interrompus, suspendus ou terminés, le MSCA /CP doit envoyer une notification à tous les organismes client pour leur assurer la disponibilité ininterrompue de l'archivage. Toutes les requêtes d'accès aux informations archivées doivent être envoyées au MSCA/CP ou à l'entité identifiée par le MSCA/CP préalablement à la fin de ses services.

9.7 Planification de la continuité du MSCA/CP

[r215] MSCA/CP doit avoir un plan de continuité d'activité (Business Continuity Plan = BCP). Il devra comprendre (de façon non limitative) des événements tels que :
- Compromission de clé
- Perte de données catastrophique due par exemple à un vol, une panne de matériel ou de logiciel
- Panne système ou de toutes sortes

9.7.1 Compromission des clés d'Etat Membre

La compromission des clés d'Etat Membre est traitée à la section 6.

9.7.2 Recouvrement d'autres désastres

[r216] MSCA/CP et les sous traitants doivent avoir des applications destinées à éviter et minimiser les effets des catastrophes système. Ces applications comprennent le stockage de données sécurisé et indépendant, des procédures de restauration des données opérationnelles, etc…, à détailler dans le BCP.

9.8 Contrôle de sécurité physique du CA et des systèmes de personnalisation.

[r217] Les contrôles de sécurité physique doivent être mis en place pour contrôler l'accès au matériel et au logiciel du MSCA ou du CP. Cela comprend les postes de travail et les autres éléments matériels de personnalisation du CA et tout module ou carte matériel externe de chiffrement. Un enregistrement doit être conservé de

toutes les entrées physiques de cette zone (ou de ces zones).

[r218] Les clés de l'Etat Membre pour signer les certificats doivent être conservées physiquement et protégées logiquement comme décrit dans le PS.

[r219] Les services du MSCA/CP doivent également avoir un endroit pour stocker la sauvegarde et les moyens de distribution de façon satisfaisante pour éviter la perte, la falsification, ou l'utilisation non autorisée de l'information stockée. Les sauvegardes doivent être conservées à la fois pour le recouvrement de données et pour l'archivage des informations importantes. Le moyen de sauvegarde doit aussi être stocké sur un site différent de celui où réside le système MSCA/CP, pour permettre la restauration dans le cas d'une catastrophe naturelle survenant au service primaire.

[r220] Une vérification de la sécurité de l'hébergement des services de l'équipement central du MSCP/CA doit être réalisée au moins une fois par **24** heures. C'est un service de maintenance continue, cela peut être un contrôle visuel une fois par session pour assurer que les systèmes et les dispositifs/cartes de chiffrement associés sont stockés de façon sûre lorsqu'ils ne sont pas utilisés, que les systèmes de sécurité physiques (par ex. les verrous des portes et les alarmes) fonctionnent correctement, et que il n'y a eu aucune tentative de forçage de l'entrée ou d'accès non autorisé.

9.8.1 Accès physique

[r221] l'accès physique à la zone d'hébergement des clés d'Etat Membre et les moyens de leur utilisation, doivent exiger la présence simultanée d'au moins 2 personnes qui ont été individuellement désignées pour avoir le droit d'accéder à cette zone.

[r222] L'accès aux autres services de MSCA/CP doit être limité aux personnes en charge de l'un des rôles décrits en 9.3. L'accès peut être contrôlé par le truchement d'une liste de contrôle d'accès à la salle d'hébergement des systèmes. Toute personne qui n'est pas sur la liste de contrôle d'accès doit être escortée par une personne de la liste. Si une liste de contrôle d'accès n'est pas réalisable pour un site particulier, il peut être accepté de s'assurer que le CA et le matériel destiné à la personnalisation est verrouillé dans une pièce sûre ou une zone de stockage lorsqu'il n'est pas utilisé.

10 Arrêt du MSCA ou du CP

10.1 Arrêt final – responsabilité du MSA

L'arrêt final d'un MSCA ou d'un CP est considéré comme une situation où tous les services associés à une entité logique est arrêtée de façon définitive. Ce n'est pas le cas lorsque le service est transféré d'un organisme à un autre ou lorsque le service MSCA passe d'une ancienne paire de clés d'Etat Membre à une nouvelle paire de clés d'Etat Membre ou de clé ERCA.

[r223] Le MSA doit s'assurer que les tâches soulignées ci-dessous sont réalisées.

Note : L'arrêt de MSCA/CP implique soit que l'Etat Membre se retire du système chronotachygraphe, soit que la globalité du système chronotachygraphe est arrêté, alors qu'il ne peut fonctionner sans les MSCA ou des autorités équivalentes.

[r224] Avant que le MSCA/CP ne termine ses services, les procédures suivantes doivent être effectuées au minimum :

a) Informer tous les utilisateurs et partenaires avec lesquels le MSCA /CP a des agréments ou d'autres formes de relations formelles.
b) Faire une information publique disponible de l'arrêt au moins **3** mois avant l'arrêt.
c) Le MSCA/CP doit mettre fin à toutes les autorisations aux sous traitants d'agir au nom du MSCA/CP dans le processus d'émission de certificats
d) Le MSCA/CP doit réaliser les actions nécessaires pour maintenir et fournir un accès continue aux archives d'enregistrement en les transférant à l'ERCA.

10.2 Transfert de responsabilité de MSCA ou de CP

Le transfert de responsabilité de MSCA ou de CP arrive lorsque le MSA choisit de désigner un nouveau MSCA ou CP à la place de l'entité précédente.

[r225] Le MSA doit assurer que le transfert ordonné de responsabilité et ses éléments soit réalisé.

[r226] L'ancien MSCA doit transférer toutes les clés génériques au nouveau MSCA de manière décidée par le MSA.

[r227] L'ancien MSCA doit détruire toutes les copies de clés qui ne sont pas transférées.

May-Lis Farnes, SNRA, Suède, +46-70-622- 73 57, may-lis.farnes@vv.se
Traduction non officielle non encore approuvée par le JRC – G.Baranger – gilles.baranger@free.fr

11 Audit

[r228] Le MSA est responsable d'assurer que les audits de MSCA et de CP sont réalisés.

11.1 Fréquence d'audit de conformité d'entité

[r229] Un MSCA/CP agissant sous cette politique nationale de CA doit être audité au moins une fois par an pour la conformité avec cette politique.

11.2 Sujets à couvrir par l'audit

[r230] L'audit doit couvrir les pratiques du MSCA/CP.

[r231] L'audit doit couvrir la conformité du MSCA/CP avec cette politique nationale de CA.

[r232] l'audit doit aussi examiner les opérations des Agences de Service.

11.3 Que devrait faire l'audit

[r233] Le MSA peut consulter un organisme externe de certification et d'accréditation pour l'approbation du MSCA/CP PS dans le but d'améliorer le fait de compter sur la confiance des partenaires dans l'organisation.

11.4 Action prise comme résultat de déficience

[r234] Si des irrégularités sont trouvées au cours de l'audit, le MSA doit prendre les mesures appropriées en fonction de leur gravité.

11.5 Communication des résultats

[r235] Les résultats d'audit sur le niveau de sécurité doivent être disponibles sur demande. Les rapports d'audit actuels ne doivent pas être disponibles sauf sur une base « à savoir ».

12 Procédures de changement de la politique nationale de CA

12.1 Eléments qui peuvent changer sans notification

[r236] Les seuls changements qui peuvent être faits à ces spécifications sans notification sont :

a) corrections éditoriales ou typographiques
b) changements dans les détails des contacts

12.2 Changements avec notification

12.2.1 Avertissement

[r237] Tout élément dans cette politique de certificat peut être changé avec un avertissement préalable de **90** jours.

[r238] Les changements d'éléments qui, selon l'avis de l'organisme responsable de la politique (le MSA), n'auront pas d'impact matériel sur une majorité substantielle d'utilisateurs ou sur les partenaires comptants qui utilisent cette politique peuvent être réalisés avec un avertissement préalable de **30** jours.

12.2.2 Période pour les commentaires

[r239] Les utilisateurs impactés peuvent documenter des commentaires pour l'organisme d'administration de la politique dans les 15 jours suivant l'avertissement.

12.2.3 Qui informer

[r240] L'information des changements de cette politique doit être envoyée à
- La Commission Européenne
- l'ERCA
- le MSCA et le CP y compris les Agences de Service
- les fabricants d'UEV et de capteurs de mouvement concernés

12.2.4 Avertissement préalable au changement final

[r241] Si un changement proposé est modifié en conséquence d'un commentaire, l'avertissement du changement modifié proposé devra être fourni au moins 30 jours avant sa prise d'effet.

12.3 Changements exigeant une nouvelle approbation de la politique nationale de CA

[r242] Si le changement de la politique est déterminé par l'organisme MSA pour avoir un impact matériel sur un nombre significatif d'utilisateurs de la politique, le MSA doit soumettre la politique nationale de CA révisée à la **Commission** pour approbation.

13 Références

[BPM] Digital tachograph card Issuing Best Practice Manual. Card Issuing group, 16 Novembre 2001, appartenant à la Commission

[CC] Common Criteria. ISO/IEC 15408 (1999) : « Information technology – Security techniques – Evaluation criteria for IT security (parties 1 à 3) ».

[CEN] CEN workshop agreement 14167-2 : Cryptographic module for CSP signing operations – protection profile (MCSO-PP)

[ETSI 102 042] ETSI TS 102 042. Policy requirements for certification authorities issuing public key certificates.

[FIPS] FIPS PUB 140-2 (May 25, 2001): "Security Requirements for Cryptographic Modules". Information Technology Laboratory, National Institute of Standards and Technology (NIST)

[ISO 17799] BS ISO/IEC 17799: 2000. Information technology -- Code of practice for information security management.

[CSG] Common Security Guideline, Card Issuing Project. (under construction), appartenant à la Commission

14 Glossaire/ Définitions et abréviations

14.1 Glossaire/Définitions

Politique CA : Un ensemble dénommé de règles qui précise les demandes de clés, de certificats et d'équipement à une communauté particulière et /ou une classe de demande avec des exigences de sécurité communes.

Cartes. Cartes tachygraphiques : cartes équipées de circuits intégrés, dans cette politique c'est équivalent à l'utilisation de « **cartes à puce** » ou « **cartes intelligentes** ».

Porteur de carte : une personne ou un organisme qui est porteur et utilisateur de carte tachygraphique. Sont inclus les conducteurs, les représentants d'entreprises, les techniciens d'ateliers et le personnel des corps de contrôle.

Certificat : dans un contexte général un certificat est une structure de message impliquant une signature liée à l'utilisateur, vérifiant que l'information contenue dans le certificat est correcte et que le porteur de clé publique certifiée peut prouver la possession d'une clé privée associée.

Système d'autorité de certification (CAS) : un système informatique dans lequel les certificats dont émis par les données (utilisateur) signées de certificat avec la clé de signature privée du CA.

Dispositions pratiques de certification (CPS) : Un ensemble d'instructions de pratiques utilisé par une autorité de certification pour émettre des certificats et relié à la politique actuelle de CA. Le CPS est dans la politique nationale de CA remplacée par le PS, car il a une vue plus large et relie les clés, les certificats et l'équipement.

Equipement : Dans le système chronotachygraphe les équipements existant sont : les cartes tachygraphiques, les UEV (unité Embarquée Véhicule) et les Capteurs de Mouvement.

Fabricant/Fabricant d'équipement : fabricants de chronotachygraphes. Dans cette politique, le plus souvent utilisé pour fabricants d'UEV et de capteurs de mouvement puisqu'ils ont des rôles différents dans le système.

Clé de capteur de mouvement : clé symétrique utilisée par les capteurs de mouvements et les UEV pour une reconnaissance mutuelle.

Dispositions Pratiques (PS) : un ensemble de pratiques de sécurité employées dans les processus du chronotachygraphe. Un PS est comparable au document standard de PKI, le CPS.

Clé privée : la partie privée d'une paire de clés asymétriques utilisée dans les techniques de chiffrement de clé publique. La clé privée est typiquement utilisée pour signer les signatures numériques ou déchiffrer des messages. Egalement appelée clé secrète.

Clé publique : la partie publique d'une paire de clés asymétrique utilisée dans les techniques de chiffrement de clé publique. La clé publique est typiquement utilisée pour vérifier les signatures numériques ou chiffrer des messages aux détenteurs de clé privée.

Clés RSA : RSA est un algorithme de chiffrement utilisé pour les clés asymétriques (PKI) dans le système chronotachygraphe.

Agence de Service : une entité qui réalise les tâches au nom d'un MSA, comme sous traitant.

Cartes tachygraphiques/ cartes : Quatre différents types de cartes intelligentes pour l'utilisation du système chronotachygraphe : carte conducteur, carte entreprise, carte atelier, carte contrôleur.

Utilisateur : les utilisateurs sont les équipements utilisateurs et sont soit les porteurs de cartes pour les cartes, soit les fabricants d'UEV/Capteurs de mouvement. Tous les utilisateurs doivent être des entités identifiables de façon univoque.

Dans ce document :
Signé : lorsque la politique exige une signature, l'exigence est satisfaite par une signature numérique sécurisée et vérifiable.
Ecrit : lorsque la politique exige des informations écrites, cette exigence est satisfaite par un message de données si les informations qui y sont contenues est accessible de façon à être utilisable par les partenaires concernés.

14.2 Liste des abréviations

CA	Certification Authority
CAA/PA	Certification Authority Administrator/Personalization Administrator
CAS	Certification Authority System
CIA	Card Issuing Authority
CC	Common Criteria
CP	Card Personalization organization
CPS	Certification Practice Statement
ERCA	European Root CA
ISSO	Information System Security Officer
ITSEC	Information Technology Security Evaluation Criteria

KG	Key Generation
MS	Member State
MSA	Member State Authority
MSCA	Member State CA
PIN	Personal Identification Number
PKI	Public Key Infrastructure
RSA	Un algorithme à clé publique spécifique
SA	System Administrator
PS	Practice Statement
UEV	Unité Embarquée Véhicule
P-UEV	organisme de personnalisation d'UEV