Tachygraphe Numérique
Politique de Certification
CPA Andorre

Version 1.00

16 Mai 2022

Historique des versions du document

Version	Auteur	Commentaires
1.00	Roman ZAICH Pascal MERLIN	Création

Affaire suivie par

Sylvain TRIQUET

Date d'approbation :

Table des matières

I. Introduction

I.1. Présentation générale

Remarque préliminaire :
Pour la définition des termes et acronymes, se référer au chapitre 0

I.1.1. Objet du document

Ce document présente la Politique de Certification (PC) de l'Autorité Andorrane (notée AND-CPA) qui s'inscrit dans l'Infrastructure de Gestion de Clés (IGC ou PKI) du système Tachygraphe Numérique Européen et qui couvre également la gestion des clés secrètes symétriques. La gestion de l'Autorité Racine ainsi que des clés maîtresses symétriques est placée sous la responsabilité de l'ERCA (European Root Certification Authority).
La présente PC est basée sur la Politique de Certification de l'ERCA [6]. Elle décrit les exigences que l'Autorité de Certification de la Partie Contractante Andorran (notée AND-CPCA) s'engage à respecter dans le cadre de son service de certification et de distribution des clés maîtresses auprès des autres acteurs. Les parties impliquées dans la gestion du cycle de vie des certificats, cartes et applications du Système Tachygraphe Andorran doivent également respecter les exigences décrites dans cette PC.

I.1.2. Contexte règlementaire

La première génération (Génération 1) du système tachygraphe, appelée Tachygraphe Numérique, a été introduite par le règlement (EU) N° 3821/85 du 20/12/1985 [1] du Parlement européen et du Conseil.

L'accord européen relatif au travail des équipages des véhicules effectuant des transports internationaux par route (AETR) [2] a été signé par 51 pays d'Europe et d'Asie, avec comme objectif de réduire les obstacles au transport international par route de marchandises et de passagers en harmonisant les règles relatives aux temps de conduite et de repos, y compris les spécifications techniques du tachygraphe. Cet accord multilatéral a été élaboré sous l'égide de la Commission économique pour l'Europe des Nations unies (CEE-ONU).
En 2006, l'UE a instauré le tachygraphe numérique comme équipement obligatoire pour le contrôle des temps de conduite et des périodes de repos en remplacement du tachygraphe analogique utilisé depuis 1985. Par la suite, les parties contractantes à l'AETR ont convenu d'introduire à partir de 2011 le même tachygraphe numérique dans leurs véhicules utilisés en transport international. Elles ont convenu à cette occasion d'insérer dans l'accord AETR [2] un nouvel article 22 bis, qui prévoit que les spécifications du tachygraphe, bien que définies unilatéralement par l'UE sans consultation préalable des parties contractantes non membres de l'Union lors de la modification de l'annexe 1B du règlement (CEE) n° 3821/85 [1], sont automatiquement appliquées par extension à toutes les parties contractantes.

Afin qu'Andorre, contractant à l'Accord Européen (AETR), puisse bénéficier des services de certification et de distribution des clés maîtresses de l'ERCA, la présente Politique couvre les exigences définies par l'ERCA dans le cadre exclusif de la première génération du tachygraphe dit Tachygraphe Numérique. Cette Politique fait donc référence en particulier aux différentes exigences de l'Appendice 1B (adaptation à l'accord AETR de l'Annexe 1B du Règlement (CEE) 3821/85) de l'Accord Européen (AETR).

I.1.3. Infrastructure de Gestion Clés

Une infrastructure de Gestion de Clés (IGC ou PKI) a été conçue pour prendre en charge les systèmes cryptographiques à clé publique, tandis que les systèmes cryptographiques symétriques reposent sur des clés maîtresses qui doivent être remises aux acteurs concernés. Cette infrastructure est composée de trois niveaux hiérarchiques :

- Autorité de Certification Racine (niveau Européen)
- Autorité de Certification subordonnée (niveau Etat Membre et/ou Partie Contractante)
- Entités finales détentrices des certificats d'équipement (niveau Etat Membre et/ou Partie Contractante)

L'Autorité de Certification Racine européenne (ERCA) est chargée de la génération et de la gestion des bi-clés racine (clés publiques-privées) avec les certificats correspondants ainsi que des clés maîtresses symétriques. L'ERCA délivre des certificats et distribue des clés symétriques aux Autorités de Certification des Etats Membre et/ou des Parties Contractantes. Les MSCA/CPCA sont responsables de la délivrance des certificats d'équipement Tachygraphe Numérique, ainsi que de la distribution des clés principales symétriques et d'autres données dérivées des clés principales à installer dans les équipements Tachygraphe Numérique.

I.1.4. Structure du document

La structure du document respecte la structure décrite dans le document ETSI TS 319 411-1 [3] qui présente les exigences générales de la communauté internationale en matière de confiance dans les transactions électroniques.

Ce document suit le cadre pour les Politiques de Certification décrit dans la RFC 3647 [4]. La Politique relative à la gestion des clés secrètes symétriques a été ajoutée à ce document, en préservant toutefois le sommaire de la RFC 3647 [4].
Les mots clés "requis", "doit", "ne doit pas", "devrait", "ne devrait pas", "recommandé", "peut" et "facultatif" dans ce document doivent être interprétés de la manière décrite dans la RFC 2119 [5].

I.2. Nom et identification du document

Le nom du présent document est « Tachygraphe Numérique - Politique de Certification CPA Andorre - v_1_00.docx »
La version courante est 1.00.
Il n'y a pas d'Identifiant d'Objet (OID pour Object Identifier) attribué à ce document. Les certificats délivrés par la CPCA Andorre (AND-CPCA) ne contiennent, en effet, aucune référence à la présente politique.

I.3. Participants

L'architecture de l'IGC (PKI) « Tachygraphe Numérique » est composée d'une Autorité Racine européenne (ERCA) et de sous-autorités réparties sur les différents Etats Membres (MSCA) et/ou Parties Contractantes (CPCA). Cette hiérarchie permet de créer une chaîne de confiance pour les certificats émis par ces MSCA/CPCA ainsi que pour les clés maîtresses symétriques qui sont distribuées par l'ERCA.
Dans ce contexte, au niveau de l'Etat Membre et/ou de la Partie Contractante, différents rôles ont été définis qui peuvent être répartis sur une ou plusieurs entités distinctes :

- Autorité de l'Etat Membre et/ou de la Partie Contractante (MSA/CPA, Member State et/ou Contracting Party Authority)
- Autorité de Certification de l'Etat Membre et/ou de la Partie Contractante (MSCA/CPCA, Member State et/ou Contractring Party Certification Authority)
- Autorité de Délivrance de Cartes (CIA, Card Issuing Authority) ou Emetteur de Cartes.
- Personnalisateur de Cartes (CP, Card Personalizer).
- Les fabricants d'équipements (cartes, VU et MoS)
- Utilisateurs d'équipements (cartes tachygraphiques, VU et capteurs de mouvement)

NB : les fabricants d'équipements de type VU et MoS insèrent dans ces derniers des clés symétriques dérivées des clés maîtresses et utilisent, à ce titre, les services de la CPCA.

Dans le contexte spécifique Andorran, les Participants du système Tachygraphe Numérique (ERCA non inclus) sont les entités suivantes :

- L'Autorité de la Partie Contractante Andorrane (AND-CPA)
- La sous-Autorité de Certification Andorrane (AND-CPCA)
- L'Autorité de Délivrance de Cartes Andorranes (AND-CIA)
- Le Personnalisateur de Cartes pour l'état Andorran (AND-CP)
- Le fabricant de cartes pour l'état Andorran (AND-CM)
- Les Utilisateurs d'équipements

NB : seuls les équipements de type « cartes » sont concernés par la présente version de la PC. Les équipements de type VU et les éléments qui s'y rapportent n'entrent pas dans le périmètre de cette version. Aucun acteur (fabricant) n'étant enregistré sur le territoire Andorran.

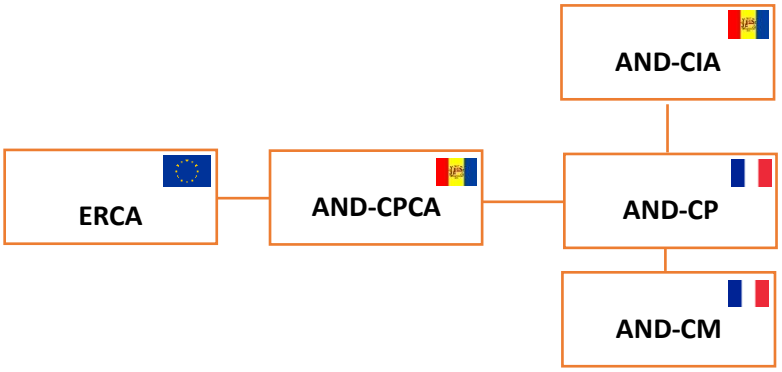

Schéma 1 : Relation entre les différentes entités intervenant dans le schéma Andorran

L'IGC (PKI) de la AND-CPCA est opérée par l'entité IN Groupe, elle-même désignée MSCA pour la France. IN Groupe assure donc le rôle d'Opérateur de Certification (OC) pour le compte de la AND-CPCA.

Remarque :

Dans la suite du document, sauf indication contraire, les opérations liées à l'exploitation de l'IGC AND-CPCA sont implicitement assurées par l'entité IN Groupe. Toutefois, lorsque la AND-CPCA est mentionnée et que l'OC est spécifiquement concerné, une indication est ajoutée entre parenthèses pour préciser l'implication ou la responsabilité de l'OC.

La AND-CPA s'appuie également sur les services de la F-CM et F-CP respectivement pour la fabrication et la personnalisation des cartes tachygraphiques. Le F-CM et F-CP sont le fabricant et le personnalisateur désignés par la CPA France (F-CPA) dans le contexte du système tachygraphe français. Toutefois, pour des questions de cohérence dans la notation, ce fabricant et ce personnalisateur sont désignés par les acronymes **AND**-CM et **AND**-CP pour spécifier le contexte **AND**orran du système tachygraphe.

Le schéma suivant fait apparaître les principaux participants (ERCA, AND-CPCA et AND-CP) dans le contexte spécifique Andorran ainsi que les différents échanges qui existent entre eux. Il s'agit du schéma original de l'ERCA qui a été adapté au contexte spécifique d'Andorre.

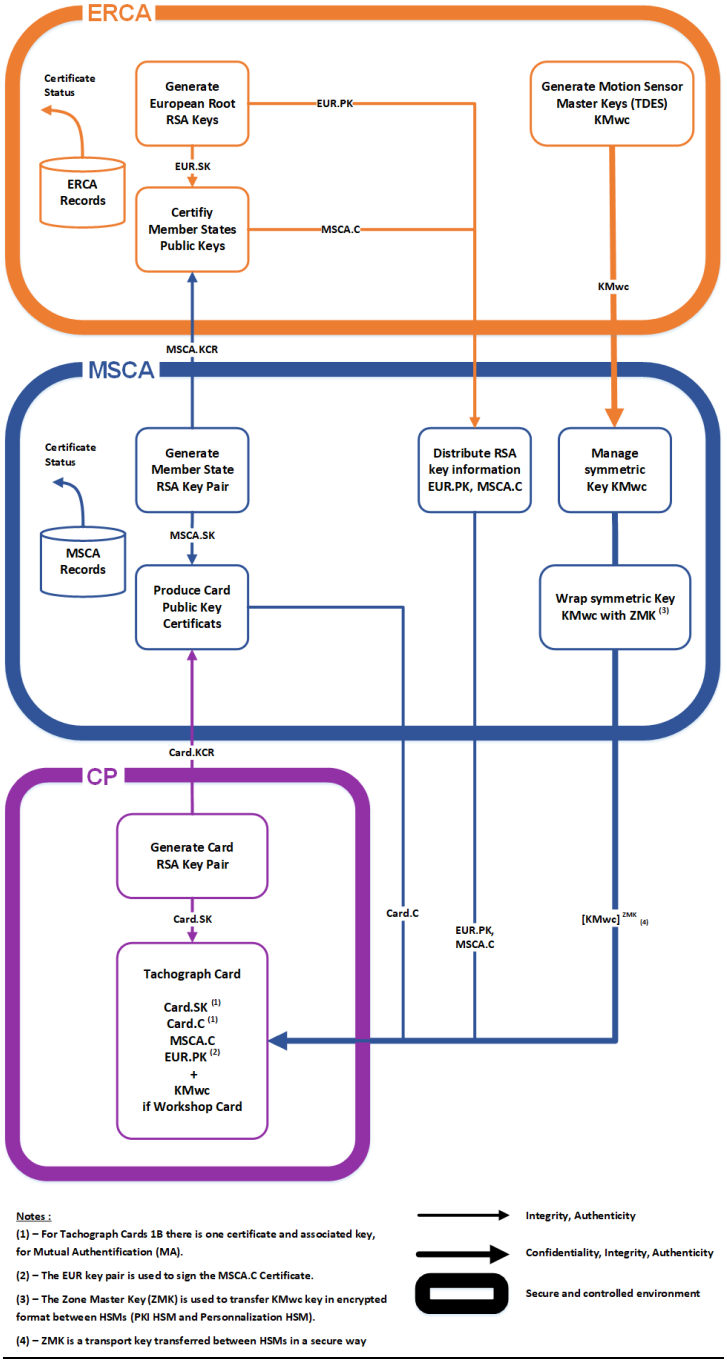

Schéma 2 : workflow au sein de l'IGC dans le contexte Andorran

I.3.1. Autorité de Certification

Autorité de Certification Racine Européenne (ERCA)

Contexte général

L'ERCA est l'Autorité Racine de l'IGC (PKI) des systèmes « Tachygraphe Numérique » (Génération 1) et « Tachygraphe Intelligent » (Génération 2).

L'ERCA génère les bi-clés racine et les certificats des clés publiques correspondantes, ainsi que les certificats de lien (pour la Génération 2 exclusivement) permettant de créer une chaîne de confiance entre les différents certificats racine générés.
Elle certifie les clés publiques des Autorités de Certification des différents Etats Membres (MSCA) et Parties Contractantes (CPCA).

Contexte Andorran (Tachygraphe Numérique)

L'ERCA assure les différents services suivants au sein de l'IGC (PKI) du système Tachygraphe Numérique :

- service d'enregistrement, service de génération et de remise des certificats.

L'ERCA assure également les différents services suivants au sein du système Tachygraphe Numérique :

- Génération, gestion et distribution des clés maîtresses symétriques.

Dans le contexte de la Génération 1 du système tachygraphe (Tachygraphe Numérique), il n'y a que deux clés maîtresses : la clé maîtresse de Capteur de Mouvement – partie VU ($K_{M\text{-}VU}$), la clé maîtresse capteur de Mouvement – partie Carte d'Atelier ($K_{M\text{-}WC}$).

NB : seuls les équipements de type « cartes » sont concernés par la présente version de la PC. Les équipements de type VU et les éléments qui s'y rapportent n'entrent pas dans le périmètre de cette version. Aucun acteur (fabricant de VU) n'étant enregistré sur le territoire Andorran. La AND-CPCA n'est donc concernée que par la partie « Carte ».

Autorité de Certification Andorrane (AND-CPCA)

La AND-CPCA est responsable de l'Autorité de Certification subordonnée à l'AC Racine (ERCA) pour le compte de l'Autorité Contractante Andorrane (AND-CPA).
La AND-CPCA certifie les clés publiques des équipements. Pour rappel, le périmètre des équipements concernés dans le contexte Andorran est restreint aux cartes tachygraphiques dans la version courante du document. De ce fait, seule la demande de certificat de type CPCA_Card est effectuée auprès de l'ERCA. La clé privée associée à ce certificat permet à la AND-CPCA de certifier les clés publiques des cartes tachygraphiques.

La AND-CPCA peut également effectuer auprès de l'ERCA une demande de clé maîtresse symétrique $K_{M\text{-}WC}$, clé qui est transmise sur demande au Personnalisateur de Cartes (AND-CP).

La AND-CPCA gère uniquement les certificats et les clés symétriques respectivement émis par et reçues de l'ERCA. Pour rappel, seule la Génération 1 du système de Tachygraphe Numérique est supportée par la AND-CPCA. Cela signifie que seuls les clés et les certificats conformes aux spécifications de la première génération

du système de tachygraphe numérique sont présents dans le système IGC (PKI) de la AND-CPCA. Ces certificats et clés sont référencés dans l'Appendice 1B [2].

Liste des clés et des certificats de la Génération 1 du système Tachygraphe Numérique stockés dans le système IGC (PKI) de la AND-CPCA :

- Certificat ERCA (ERCA.C) ;
- Bi-clé CPCA_Card (CPCA_Card.PK et CPCA_Card.SK) ;
- Certificat CPCA_Card (CPCA_Card.C) ;
- Clé maîtresse $K_{M\text{-}WC}$.

L'échange de clés symétriques entre l'ERCA et la AND-CPCA s'effectue de façon sécurisée (chiffrée avec la clé publique RSA de transport générée et transmise par la AND-CPCA).

I.3.2. Opérateur de Certification

L'Autorité de Certification est opérée par l'entité IN Groupe qui fournit donc un service d' « Opérateur de Certification » à la AND-CPCA.
Cette dernière met en œuvre pour le compte de la AND-CPCA une plate-forme opérationnelle, fonctionnelle, sécurisée, dans le respect des exigences énoncées dans la présente Politique de Certification (PC) et dont les modalités sont détaillées dans la Déclaration des Pratiques de Certification (DPC) dont la rédaction est sous sa responsabilité. Cette plateforme est mise en œuvre pour :

- La gestion des clés privées de signature de la AND-CPCA
- La gestion et la diffusion des certificats des équipements tachygraphes
- La gestion des clés maîtresses symétriques
- La distribution de ses clés aux équipements tachygraphiques

I.3.3. Autorités d'Enregistrement

Une chaîne est mise en place dans le cadre de l'enregistrement et de la validation des demandes de certificat et des demandes de distribution des clés maîtresses qui sont transmises à la AND-CPCA.

Enregistrement du AND-CP par la AND-CPCA
Le AND-CP est désigné par la AND-CPA. La AND-CPCA s'assure que le Personnaliseur de Cartes AND-CP est formellement enregistré avant de traiter les demandes qu'il émet.
Des informations sur le processus d'enregistrement sont fournies dans la Déclaration des Pratiques de Certification de la AND-CPCA.
Les exigences d'authentification sont décrites dans la section Identification et authentification (cf. chapitre III).

Enregistrement de la AND-CIA par le AND-CP
La AND-CIA est désignée par la AND-CPA.
Le Personnalisateur de Cartes (AND-CP) s'assure que l'Emetteur de Cartes (AND-CIA) est formellement enregistré avant de traiter les demandes de personnalisation de cartes.
Les exigences d'authentification sont décrites dans la section Identification et authentification (cf. chapitre III).

Enregistrement des demandeurs de cartes par la AND-CIA
Le traitement des demandes des certificats est délégué par la AND-CPCA à l'Emetteur de Cartes (AND-CIA). Ce dernier assure donc le rôle d'Autorité d'Enregistrement Déléguée (AED) auprès de la AND-CPCA dans le cadre du contrôle et du traitement des demandes de cartes qu'il reçoit des demandeurs. En particulier, l'Emetteur de Cartes (AND-CIA) est responsable de l'identification du demandeur.

I.3.4. Personnalisateur des Cartes Tachygraphiques (AND-CP)

Il s'agit de l'organisme qui personnalise les cartes tachygraphiques à partir des données d'identification des détenteurs de carte, des clés et des certificats.
Le AND-CP (système de personnalisation) transmet ses demandes de signature des clés publiques à la AND-CPCA. Le système de personnalisation de cartes est authentifié par la AND-CPCA afin de pouvoir demander un certificat. Les exigences d'authentification sont décrites dans la section Identification et authentification (cf. chapitre III).
La AND-CPCA transmet également la clé maîtresse symétrique au AND-CP qui l'intègre dans les cartes qu'il personnalise.

I.3.5. Emetteur de Cartes (AND-CIA)

Le rôle de la AND-CIA (Andorre) est de :

- Vérifier si tous les documents requis pour la délivrance d'une carte ont été produits par le demandeur et si ces documents sont valides ; En particulier, la AND-CIA est responsable lors du traitement des demandes de la vérification de :
    - L'identité du demandeur (contrôle de la carte d'identité, du passeport, etc.)
    - L'habilitation du demandeur pour commander une carte (par exemple contrôle de la validité du permis de conduire dans le cas d'une demande de carte de conducteur)
- Vérifier que toutes les conditions préalables à la délivrance d'une carte tachygraphique soumise à l'Accord AETR [2] (en particulier à l'Appendice 1B), toutes les autres dispositions juridiques applicables, la Politique de Certification de l'ERCA [6] et la présente Politique de Certification de la AND-CPA sont remplies ;
- Vérifier si une carte tachygraphique en cours de validité, n'a pas déjà été délivrée au demandeur dans un autre État Membre de l'UE ou dans une autre Partie Contractante (non membre de l'UE) ; (via réseau TACHOnet)
- Veiller à ce que les données des demandes soient correctement transmises au Personnalisateur de Cartes AND-CP), conformément aux documents produits et aux exigences de la présente Politique de Certification ;
- Informer tous les utilisateurs des exigences de cette Politique de manière appropriée en veillant à ce que l'atelier commande les cartes de ses techniciens, et que seul le technicien reçoive le code PIN associé à la carte commandée par l'atelier en son nom ;
- Informer immédiatement la AND-CPA et la AND-CPCA ou l'un de ses organismes autorisés de tous les incidents liés à la sécurité.

I.3.6. Demandeurs de certificats et de clés maîtresses

Demandeurs auprès de l'ERCA
La AND-CPCA agit en tant que demandeur auprès de l'ERCA. Elle peut demander la signature de ses clés publiques ainsi que la distribution des clés maîtresses du système Tachygraphe.

Demandeurs auprès de la AND-CPCA
Le seul demandeur de certificats et de clés maîtresses auprès de la AND-CPCA est le Personnalisateur de Cartes (AND-CP). Ses demandes sont subséquentes aux demandes de personnalisation qu'il reçoit de l'Emetteur de Cartes (AND-CIA). Les certificats et les clés maîtresses transmis par la AND-CPCA sont insérés dans les cartes que le AND-CP personnalise pour le compte de l'Emetteur de Cartes.

Le Personnalisateur de Cartes (AND-CP) est responsable de la personnalisation des cartes de conducteur, des cartes d'atelier, des cartes d'entreprise et des cartes de contrôleur.

Pour la personnalisation des cartes de conducteur et des cartes d'atelier, il assure :
- la génération d'une bi-clé carte pour l'authentification mutuelle ;
- le traitement de la demande de certification des clés publiques auprès de la AND-CPCA (avec le certificat CPCA_Card) ;
- le traitement de la demande de la clé maîtresse $K_{M\text{-}WC}$ (pour les cartes d'atelier uniquement) ;
- la disponibilité dans les cartes des clés et des certificats pour l'authentification mutuelle et la signature, l'appariement MoS-VU .

Pour la personnalisation des cartes d'entreprise et des cartes de contrôleur, il assure :
- la génération de la bi-clé pour l'authentification mutuelle :
- le traitement de la demande de certification des clés publiques auprès de la AND-CPCA (avec le certificat CPCA_Card) ;
- la disponibilité dans les cartes des clés et des certificats pour l'authentification mutuelle et la signature.

I.3.7. Autres participants

Outre le Personnalisateur de Cartes (AND-CP) et l'Emetteur de Cartes (AND-CIA), les autres participants qui s'appuient sur le service de la AND-CPCA sont les conducteurs, les entreprises, les ateliers et les contrôleurs qui utilisent indirectement les certificats de la AND-CPCA pour vérifier la validité des certificats des équipements (la AND-CPCA fournit l'ensemble des certificats permettant de vérifier la chaîne de certification : certificats de l'ERCA et certificat de la AND-CPCA), lesquels servent à leur tour à valider l'authenticité des données téléchargées à partir des unités embarquées sur le véhicule et des cartes de conducteur.

I.4. Usage des clés et des certificats

Les certificats racine de l'ERCA servent à vérifier les certificats que cette dernière émet pour la AND-CPCA

(certificats CPCA_Card.C). Le certificat de l'ERCA constitue le dernier maillon de la chaîne de certification. Il est inclus avec les certificats CPCA_Card.C de la AND-CPCA dans les cartes émises par le Personnalisateur de Cartes (AND-CP).

La AND-CPA ainsi que tous les participants à l'IGC (PKI) (cf. chapitre I.3) reconnaissent les certificats de l'ERCA à condition qu'ils soient publiés par l'ERCA selon les exigences décrites au chapitre II du présent document.
La AND-CPCA utilise la clé privée de l'Autorité de la Partie Contractante (AND-CPA) uniquement pour :

- Signer les certificats des équipements « carte » conformément à l'Appendice 1B [2]
- Signer les demandes de certificats (KCR)

La clé maîtresse (K_{M-WC}) est communiquée par la AND-CPCA au Personnalisateur de Cartes (AND-CP) par des moyens dûment sécurisés aux seules fins pour lesquelles la clé est destinée.

La clé maîtresse K_{M-WC} est fournie au Personnalisateur de Cartes pour son installation dans les cartes d'atelier. K_{M-WC} est utilisée par la VU avec la clé K_{M-VU} pour générer la clé K_M pendant l'appariement de la VU avec le Capteur de mouvement.

Le certificat *CPCA_Card.C* est utilisé pour vérifier les certificats des cartes signés avec la clé privée *CPCA_Card.SK* associée au certificat *CPCA_Card.C*.
Les certificats *Card_MA.C* sont utilisés pour l'authentification mutuelle et l'échange de clé de session entre la VU et la carte.

I.5. Gestion de la Politique de Certification

Les principaux processus supportés par cette Politique de Certification sont :

- La Génération et la Gestion des clés *CPCA_Card* (*CPCA_Card.PK* et *CPCA_Card.SK*) et des certificats (*CPCA_Card.C*) de la AND-CPCA,
- La Gestion et la Diffusion des clés et des certificats des cartes,
- La Gestion et la Diffusion des clés K_{M-WC}.

I.5.1. ERCA

Le service de la Commission Européenne responsable de la mise en œuvre de la Politique de Certification au niveau Européen, de la fourniture des services de certification et de distribution des clés maîtresses auprès des Etats membres et des Parties Contractantes est désigné comme Autorité de Certification Racine Européenne (European Root Certificate Authority ou ERCA).

L'adresse du contact à l'ERCA est :

Head of the Cyber and Digital Citizens' Security Unit E3
Directorate E - Space, Security and Migration
Joint Research Center (TP 580)
European Commission
Via Enrico Fermi, 2749
I-21027 Ispra (VA)

La présente Politique de Certification est traduite en anglais et a été mise à disposition de l'ERCA. L'ERCA a

examiné cette Politique pour s'assurer de sa conformité par rapport aux exigences exprimées dans sa propre Politique de Certification. L'ERCA a archivé le rapport d'examen ainsi que la Politique de Certification de la AND-CPA à titre de référence.
La AND-CPA s'engage à répondre à tout commentaire émis par l'ERCA et à effectuer toute mise à jour de sa PC à la demande de l'ERCA et ce, afin d'offrir un niveau de sécurité équivalent à celui des autres Parties Contractantes.
Sur la base de la garantie de conformité du présent document par rapport à la PC de l'ERCA [6], cette dernière fournit à la AND-CPCA le service de certification et le service de distribution des clés maîtresses symétriques. La fourniture de ces services dans le temps est conditionnée par la transmission périodique des rapports d'audits (cf. chapitre VIII.1) démontrant que la AND-CPCA continue de remplir ses obligations telles que définies dans la présente PC approuvée par l'ERCA.

I.5.2. Autorité de la Partie Contractante Andorrane (AND-CPA)

L'Autorité de la Partie Contractante pour Andorre (AND-CPA), est responsable de l'établissement et de la documentation de la Politique de Certification, objet du présent document. Cette Politique de Certification est conforme aux exigences applicables aux CPCA et exprimées dans la Politique de Certification de l'ERCA [6].

Après son approbation par l'ERCA, la Politique de Certification de la AND-CPA est mise à disposition de :

- toutes les parties utilisatrices, incluant en particulier la AND-CPCA, le Personnalisateur de Cartes (AND-CP) et l'Emetteur de Cartes (AND-CIA).
- L'Opérateur de Certification (OC).

L'adresse du contact de la AND-CPA est :

Àrea de Transport Terrestre, Aeri i per Cable
Departament d'Empresa, Comerç, Desenvolupament, Seguretat i Qualitat Industrial, i Transport
Ministeri de Presidència, Economia i Empresa
Govern d'Andorra
Carrer Prat del Rull, 7, 3a planta
Edifici Prat del Rull
AD500 Andorra la Vella
Principat d'Andorra
Tel.: + 376 875 700

I.5.3. Autorité de Certification de la Partie Contractante Andorrane (AND-CPA)

La AND-CPA a désigné l'entité qui mettra en œuvre la Politique de Certification nationale et qui sera responsable de la fourniture du service de certification et du service de distribution des clés maîtresses auprès du Personnalisateur de Cartes (AND-CP). Il s'agit de la AND-CPCA qui a elle-même désigné l'entité qui fournira les services d'Opérateur de Certification (OC).
L'Opérateur de Certification (OC) décrit sa mise en œuvre de la Politique de Certification de la AND-CPA dans le document « Déclaration des Pratiques de Certification » (DPC) ou « Certification Practice Statement » (CPS). Ce document identifie les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'Opérateur de Certification (OC) applique dans le cadre de la fourniture de ses services de certification électronique et de distribution des clés maîtresses au Personnalisateur de Cartes (AND-CP) pour

le compte de la AND-CPCA et en conformité avec la ou les politiques de certification qu'il s'est engagé à respecter. Cette Déclaration des Pratiques de Certification (DPC) est par conséquent rédigée par l'Opérateur de Certification (OC). Sa diffusion est restreinte car ce document contient des informations techniques et organisationnelles confidentielles. L'OC diffuse le contenu de sa Déclaration des Pratiques de Certification uniquement sur le principe du besoin d'en connaître (cf. II.2.2).

La Déclaration des Pratiques de Certification de l'OC est gérée, examinée et modifiée conformément aux procédures de contrôle des documents.
La Déclaration des Pratiques de Certification est fournie à la AND-CPA. Il est de la responsabilité de la AND-CPA de s'assurer de la conformité de la Déclaration des Pratiques de Certification par rapport à la Politique de Certification qu'elle s'est elle-même fixée.
La AND-CPCA tient à jour un registre de ses opérations, le cas échéant, pour démontrer la conformité avec la Politique de Certification de la AND-CPA. Ce registre doit être mis à disposition de la AND-CPA ou à l'ERCA sur demande.
Sur demande, la AND-CPCA peut fournir à l'ERCA une version de la Déclaration des Pratiques de Certification de l'Opérateur de Certification (OC). Les documents référencés dans la Déclaration des Pratiques de Certification, fournissant des informations classées « confidentiel » sur les procédures, les moyens techniques, etc. mis en œuvre, ne sont pas fournis avec la Déclaration des Pratiques de Certification.

L'adresse du contact de la AND-CPCA

Àrea de Transport Terrestre, Aeri i per Cable
Departament d'Empresa, Comerç, Desenvolupament, Seguretat i Qualitat Industrial, i Transport
Ministeri de Presidència, Economia i Empresa
Govern d'Andorra
Carrer Prat del Rull, 7, 3a planta
Edifici Prat del Rull
AD500 Andorra la Vella
Principat d'Andorra
Tel.: + 376 875 700

L'adresse du contact de l'Opérateur de Certification (OC) est :

IN Groupe
Direction des Programmes Tachygraphe
Rue des Frères Beaumont
59128 Flers-en-Escrebieux
FRANCE
Tél : +33 327937070

I.5.4. Personnalisateur de Cartes (AND-CP)

La AND-CPA a également désigné le Personnalisateur de Cartes (AND-CP), qui est l'entité qui personnalisera les cartes sur demande de l'Emetteur de Cartes (AND-CIA). Le AND-CP est responsable de la génération des bi-clés et de la demande de certification des clés publiques auprès de la AND-CPCA. Il est également responsable de la sécurisation des clés maîtresses transmises par la AND-CPCA pour écriture dans les cartes qu'il émet.

L’adresse du contact du AND-CP est :

IN Groupe
Direction des Programmes Tachygraphe
Rue des Frères Beaumont
59128 Flers-en-Escrebieux
FRANCE
Tél : +33 327937070

I.6. Définitions et acronymes

Acronyme	Définition
AC	Autorité de Certification
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
AES	Algorithm Encryption Standard
CIA	Card Issuing Authority (Autorité Emettrice de Cartes)
CM	Card Manufacturer (Fabricant de Cartes)
CP	Card Personalizer (Personnalisateur de Cartes)
CRL	Certificate Revocation List (Liste de révocation des certificats)
DPC	Déclaration des Pratiques de Certification (CPS, Certification Practice Statement en anglais)
EA	European Authority (Autorité Européenne)
EC	European Commission (Commission Européenne)
EA	European Authority (Autorité Européenne)
EAL	Evaluation Assurance Level (Niveau d'Assurance d'Evaluation)
AND-CIA	Andorran Card Issuing Authority (Autorité Emettrice de Cartes d'Andorre)
AND-CM	Andorran Card Manufacturer (Fabricant de Cartes d'Andorre)
AND-CP	Andorran Card Personalizer (Personnalisateur de Cartes d'Andorre)
AND-CPA	Andorran Contracting Party Authority (Autorité de la Partie Contractante Andorrane)
AND-CPCA	Andorran Contracting Party Certification Authority (Autorité de Certification de la Partie Contractante Andorrane)
GNSS	Global Navigation Satellite System (Système Mondial de Navigation par Satellite)
HSM	Hardware Security Module (Module de Sécurité Matérielle)
IGC	Infrastructure de Gestion de Clés
JRC	Joint Research Centre (Centre Commun de Recherche)
KCR	Key Certification Request (Demande de Certification de Clé = Demande de signature de certificat)
KDR	Key Distribution Request (Demande de Distribution de Clé)
KDM	Key Distribution Message (Message de Distribution de Clé)
KM	Motion Sensor Master Key (Clé Maitresse Capteur de Mouvement)
K_{M-VU}	Motion Sensor Master Key – VU part (Partie VU de KM) : Clé TDES
K_{M-WC}	Motion Sensor Master Key – Workshop part (Partie WC de KM) : Clé TDES
KID	Key Identifier (Identifiant de Clé du Capteur de Mouvement)
KP	Key Pairing (Clé d'Appariement du Capteur de Mouvement)
MA	Mutual Authentication (Authentification Mutuelle)
MSCA	Member State Certifiaton Policy (Autorité de Certification de l'Etat Membre)
MoS	Motion Sensor (Capteur de Mouvement)
CPA	Contracting Party Authority (Autorité de la Partie Contractante)
CPCA	Contracting Party Certification Authority (Autorité de Certification de la Partie Contractante)
OC	Opérateur de Certification

OCSP	On-line Certificate Status Protocol (protocole de statut de certificat en-ligne)
PC	Politique de Certification (CP, Certificate Policy en anglais)
PKI	Public Key Infrastructure (Infrastructure de Clé publique)
RFC	Request For Comment (Demande De Commentaire)
RSA	Rivest-Shamir-Adleman (algorithme à clé publique du nom de leurs inventeurs)
SMSI	Système de Management de la Sécurité de l'Information
TDES	Algorithme symétrique Triple DES (Data Encryption Standard) [15]
VU	Vehicle Unit (Unité de Véhicule)
WC	Workshop Card (Carte d'Atelier)
ZMK	Zone Master Key (Clé pour transport sécurisé entre HSMs)
ENT.PK	Clé publique de l'entité « *ENT* » Ex : Card_MA.PK est la clé publique de la carte utilisée pour l'authentification mutuelle
ENT.SK	Clé privée de l'entité « *ENT* » Ex : CPCA_Card.SK est la clé privée de la AND-CPCA utilisée pour signer les certificats des cartes
ENT.C	Certificat de l'entité « *ENT* » Ex : EUR.C est le certificat de l'ERCA

Tableau 1 – Définitions Acronymes

II. Responsabilités concernant la publication des informations

II.1. Dépôt

Les certificats des équipements émis par la AND-CPCA sont enregistrés dans sa base de données.
Aucun dépôt de certificats n'est rendu public par la AND-CPCA.

II.2. Publication des informations de certification

II.2.1. Publication de la Politique de Certification

La présente Politique de Certification est publiée par la AND-MSA sur le site du Transport Andorran à l'adresse suivante :
https://www.transports.ad/ca/targetes-de-tacograf,

Les certificats de la AND-CPCA (*CPCA_Card.C*) peuvent être publiés par l'ERCA (après émission) et sont accessibles depuis un serveur public.

II.2.2. Publication de la Déclaration des Pratiques de Certification (DPC)

La Déclaration des Pratiques de Certification est rédigée par l'Opérateur de Certification. Cette DPC doit être approuvée par la AND-CPA.
La DPC n'est pas un document public mais elle peut être communiquée sur demande aux parties utilisatrices (uniquement sur le principe du besoin d'en connaître). En particulier, la AND-CPA doit demander à la AND-CPCA de lui fournir la DPC de l'OC afin de s'assurer de sa conformité par rapport à la PC qu'elle a elle-même rédigée.
Périodicité de publication
Les informations relatives aux modifications de cette Politique de Certification doivent être publiées conformément au calendrier défini par les procédures de modification (amendement) décrites au chapitre IX.12IX.12 du présent document.
De même, les informations relatives aux modifications apportées à la Déclaration des Pratiques de Certification de l'OC seront publiées selon les calendriers définis par les procédures de modification (amendements) spécifiées dans la Déclaration des Pratiques de Certification.

III. Identification et Authentification

Ce chapitre décrit les procédures en place pour contrôler l'identité et/ou les attributs des demandeurs avant l'émission ou le renouvellement des certificats ou pour la distribution des clés maîtresses symétriques. Dans le contexte de la AND-CPCA, ces procédures couvrent l'identification et l'authentification du système de personnalisation de carte.
Le Personnalisateur de Cartes (AND-CP) doit, de son côté, identifier et authentifier tous les ordres de production de cartes avant de demander à la AND-CPCA l'émission d'un certificat carte.

III.1. Nommage

III.1.1. Types de nom

Emetteur et Sujet du certificat

La Référence de l'Autorité de Certification (Certification Authority Reference) et la Référence du Titulaire du Certificat (Certificate Holder Reference) identifient respectivement l'émetteur et le sujet d'un certificat. Elles doivent respecter le format décrit dans le sous-appendice 11 de l'Appendice 1B [2] (CSM_017).
Demande de Distribution de Clé et Message de Distribution de Clé

Les Demandes de Distribution de Clé (Key Distribution Requests) et les Messages de Distribution de Clés (Key Distribution Messages) contiennent un identifiant de clé (Key Identifier) constitué en partie par le numéro et le nom de la Partie Contractante ainsi que du type de clé maîtresse respectivement demandé par l'AND-CPCA dans la KDR et transmis par l'ERCA dans le KDM.

III.1.2. Nécessité d'utilisation de noms explicites

N/A

III.1.3. Anonymisation et pseudonymisation

Les certificats émis dans le périmètre de la AND-CPCA ne contiennent aucune identité anonyme ou pseudonyme.

III.1.4. Règles d'interprétation des différentes formes de nom

Aucune interprétation n'est faite sur le nom des certificats.

III.1.5. Unicité des noms

Tous les noms de certificat et toutes les demandes de signature de certificat (KCR) doivent être uniques.

III.1.6. Identification, authentification et rôle des marques déposées

N/A

III.2. Validation initiale de l'identité

III.2.1. Méthode pour prouver la possession de la clé privée

Demande de Certificat effectuée par la AND-CPCA auprès de l'ERCA

Lors de la soumission de demandes de signature de certificat (Key Certification Request), la AND-CPCA prouve la possession de la clé privée correspondante grâce à une signature interne générée avec cette clé privée (comme décrit dans l'Annexe A de la PC de l'ERCA [6]). Cette signature est vérifiée par l'ERCA.
Une preuve supplémentaire d'intégrité, d'authenticité et de confiance doit être fournie en vérifiant le hash calculé sur la KCR transmise par la AND-CPA, lors de la réception par l'ERCA (tel que décrit dans la PC de l'ERCA [6]).

Demande de Certificat effectuée par le Personnalisateur de Cartes auprès du AND-CPCA

Lors de la soumission de demandes de signature de certificat de clé publique (KCR), le Personnalisateur de Cartes (AND-CP) prouve la possession de la clé privée correspondante grâce à une signature interne avec cette clé privée. La AND-CPCA vérifie la signature avant la délivrance du certificat.

III.2.2. Validation de l'identité d'un organisme

Toutes les demandes de délivrance de certificat ne doivent être traitées que lorsqu'elles ont été reçues d'une entité formellement authentifiée. La AND-CPCA effectue par conséquent l'authentification du Personnalisateur de cartes (AND-CP). Le Système de Personnalisation de Cartes peut ensuite envoyer les demandes d'émission de certificats carte.
Une authentification mutuelle doit être effectuée lors du traitement des demandes émises par le système de personnalisation de cartes par l'IGC (PKI) de la AND-CPCA. L'IGC (PKI) de la AND-CPCA rejette toutes les demandes si l'authentification mutuelle a échoué.

III.2.3. Validation de l'autorité d'un demandeur

Dans le contexte de la AND-CPA, il est attendu que le Système de Personnalisation de Cartes identifie et authentifie les autres parties utilisatrices de la AND-CPSA. Le Personnalisateur de Cartes vérifie l'authenticité de leur identité et applique toutes les conditions préalables requises pour pouvoir être reconnue comme entité de confiance par la AND-CPCA.

III.2.4. Informations non vérifiées d'un demandeur

Les informations non vérifiées d'un demandeur sont rejetées par l'Autorité de Certification (AND-CPCA) et ne peuvent pas, par conséquent, être incluses dans les certificats.

III.2.5. Validation de l'autorité du demandeur

La CPCA doit définir une procédure pour la validation de l'autorité du demandeur. Dans le contexte de la AND-CPCA, cette procédure est référencée dans sa Déclaration des Pratiques de Certification.

III.2.6. Critère pour l'interopérabilité

La AND-CPCA ne doit s'appuyer sur aucune autorité de certification externe, à l'exception de l'ERCA pour les services de signature de certificats et de distribution de clés qu'elle fournit au système de Tachygraphe Numérique.
Si la AND-CPCA doit s'appuyer sur une IGC (PKI) externe pour tout autre service ou fonction, elle doit examiner et approuver la Politique de Certification et/ou la Déclaration des Pratiques de Certification de ce fournisseur de services de certification externe avant de s'appuyer sur ses services.

III.3. Identification et authentification d'une demande de renouvellement de clés

III.3.1. I&A d'une demande de renouvellement de clés, AND-CPCA

L'identification et l'authentification d'une demande de renouvellement de clé pour la AND-CPCA doivent suivre la Politique de Certification de l'ERCA [6].

III.3.2. I&A d'une demande de renouvellement de clés, Personnalisateur de Cartes

Le renouvellement de la clé des équipements (cartes) n'est pas envisagé dans le cadre du système du Tachygraphe Numérique. Cela signifie que, pour une carte donnée, il n'est pas possible de remplacer la bi-clé et le certificat associé.

III.4. Identification et validation d'une demande de révocation

Les listes de révocation de certificat ne sont pas gérées par la AND-CPCA.

IV. Exigences opérationnelles pour la gestion du cycle de vie des certificats et des clés maîtresses

Ce chapitre décrit les formats de message, les mécanismes et procédures cryptographiques pour le traitement et la distribution des certificats et des clés symétriques pour les cartes ainsi que les services de cryptage des données d'équipement entre la AND-CPCA et le Personnalisateur de Cartes (AND-CP), ainsi que pour le traitement et la distribution des certificats AND-CPCA (*CPCA_Card.C*) et des clés maîtresses entre l'ERCA et la AND-CPCA.

IV.1. Traitement et émission des certificats

IV.1.1. Demande de certificat (Key Certificate Request)

Demande de Signature de Certificat émise par la AND-CPCA à l'ERCA

Les demandes de signature de certificat (KCR) ne peuvent être soumises par la AND-CPCA que si cette dernière a été déclarée comme CPCA auprès de l'ERCA par la AND-CPA. L'Autorité européenne est quant à elle responsable de la reconnaissance de la AND-CPA.

La KCR émise par la AND-CPCA doit respecter le format suivant :

Champ	Octets	Explication
Certificate Content	164	Voir ci-après
Signature of Certificate Content	128	Voir ci-après

Tableau 2 – Format de la KCR émise par la AND-CPCA

Champ	Format	Octets	Explication
CPI	Integer	1	Certificate Profile Identifier '01'
CAR	Octet String	8	Certification Authority Reference
nationNumeric	Integer	1	Numeric code for issuing nation (See JRC website) 'FD' (253) = European Community
nationAlpha	IA5String	3	Alpha-3 code for issuing nation (See JRC website) '45 43 20' = "EC "
keySerialNumber	Integer	1	'00'
additionalInfo	Octet String	2	'FF FF' Production Certificate '54 4B' Test Certificate
caIdentifier	Octet String	1	'01'
CHA	Octet String	7	Certificate Holder Authorization
tachographApplicationID	Octet String	6	'FF 54 41 43 48 4F'
equipmentType	Integer	1	'00'
EOV	TimeReal	4	Certificate End Of Validity 'FF' padded if not used.
CHR	Octet String	8	Certificate Holder Reference
nationNumeric	Integer	1	Numeric code for issuing nation (See JRC website) '03' = Andorra
nationAlpha	IA5String	3	Alpha-3 code for issuing nation (See JRC website) '41 4E 44'= "AND"
keySerialNumber	Integer	1	Unique serial number
additionalInfo	Octet String	2	'FF FF' Production Certificate '54 4B' Test Certificate
caIdentifier	Octet String	1	'01'
Public Key			
n	Octet String	128	Public Key modulus
e	Octet String	8	Public Key public exponent

Tableau 2.a – Format de *Certificate Content*

Le modulus de la clé publique soumise à l'ERCA (via une KCR) doit être unique dans le domaine de la AND-CPCA.
La KCR est signée avec la clé privée (*CPCA_Card.SK*) associée à la clé publique (*CPCA_Card.PK*) soumise par la AND-CPCA à l'ERCA. La signature du Contenu du Certificat est la primitive de signature RSASP1 (PKCS#1) [14] avec la clé privée de la carte (*Card.SK*).

Champ	Octets	Explication
Fixed value	1	'4B'
Fixed value	58	58 x 'BB'
Fixed value	1	'BA'
Hash	20	SHA-1(CC)
Hash	20	SHA-1(SHA-1(CC))
Fixed value	1	'BC'

Tableau 2.b – Format de *Signature of Certificate Content*

Demande de Signature de Certificat émise à la AND-CPCA par le Personnalisateur de Cartes

La AND-CPCA ne délivre les certificats que si une demande appropriée est présentée à l'autorité responsable et si toutes les exigences de l'Accord AETR [2] et de toutes les autres dispositions légales et accords associés ont été respectés au moment de la demande.

Champ	Octets	Explication
Certificate Content	164	Voir ci-après
Signature of Certificate Content	128	Voir ci-après

Tableau 3 – Format de la KCR émise par le Personnalisateur de cartes

Champ	Format	Octet	Explication
CPI	Integer	1	Identifiant du Profile de certificat (Certificate Profile Identifier) '01'
CAR	Octet String	8	Référence de l'Autorité de Certification (Certification Authority Reference)
nationNumeric	Integer	1	Code numérique pour la nation émettrice (voir site web du JRC) '03' = Andorra
nationAlpha	IA5String	3	Code Alpha-3 code pour la nation émettrice (voir site web du JRC) '41 4E 44' = "AND"
keySerialNumber	Integer	1	Numéro de série pour distinguer les différentes clés de l'Autorité de Certification en cas de changement de clés.
additionalInfo	Octet String	2	'FF FF' Certificat de production '54 4B' Certificat réel
caIdentifier	Octet String	1	'01'
CHA	Octet String	7	Autorisation du titulaire du certificat (Certificate Holder Autorisation)
tachographApplicationID	Octet String	6	'FF 54 41 43 48 4F'
equipmentType	Integer	1	1 = Carte conducteur 2 = Carte atelier 3 = Carte contrôleur 4 = Carte entreprise
EOV	TimeReal	4	Fin de validité du certificat (Certificate End Of Validity) Rempli avec 'FF' si non utilisé.
CHR	Octet String	8	Référence du titulaire du certificat (Certificate Holder Reference)
serialNumber	Integer	4	Numéro de série de l'équipement, unique pour le fabricant, le type d'équipement et le mois et l'année ci-dessous.
monthYear	BCDString	2	Identification du mois et de l'année de fabrication (ou d'attribution du numéro de série).
type	Integer	1	1 = Carte conducteur 2 = Carte atelier 3 = Carte contrôleur 4 = Carte entreprise
manufacturerCode	Integer	1	'50' (80) = IN Groupe
Public Key			
n	Octet String	128	Modulus de la clé publique
e	Octet String	8	Exposant de la clé publique

Tableau 3.a – Format de *Certificate Content*

La signature du contenu du certificat est la primitive de signature RSASP1 (PKCS#1) [14] avec la clé privée de la carte (*Card.SK*).

Champ	Octets	Explication
Fixed value	1	'4B'
Fixed value	85	85 x 'BB'
Fixed value	1	'BA'
Hash	20	SHA-1(CC)
Hash	20	SHA-1(SHA-1(CC))
Fixed value	1	'BC'

Tableau 3.b – Format de *Signature of Certificate Content*

IV.1.2. Traitement d'une demande de certificat

La AND-CPCA doit s'assurer que la demande de signature de certificat émanant du système du Personnalisateur de Cartes (AND-CP) est complète, exacte et dûment autorisée pour pouvoir la traiter.
La AND-CPCA ne doit accepter que les demandes valides de certificat pour cartes tachygraphiques, telle que décrite dans l'Appendice 1B [2].

Pour chaque carte tachygraphique, une bi-clé unique (Card_MA.PK et Card_MA.SK) utilisée pour l'authentification mutuelle, doit être générée.
Cette tâche de génération des bi-clés des cartes tachygraphiques est confiée au Personnalisateur de Cartes (AND-CP). Chaque fois qu'une bi-clé de carte est générée, la partie générant cette bi-clé doit envoyer la partie publique (clé publique) à la AND-CPCA afin d'obtenir le certificat correspondant. La clé privée ne doit être utilisée que par la carte tachygraphique. Les demandes de certification de clés s'appuyant sur le transfert des clés privées ne sont pas autorisées.

Approbation ou rejet des demandes

Toutes les requêtes de signature de certificats reçues du Personnalisateur de Cartes (AND-CP) après authentification sont approuvées. Les requêtes qui ne présentent pas la structure ad hoc et qui ne peuvent pas, par conséquent, être traitées sont rejetées.

Délai pour traiter les demandes

Les demandes de certificats émises par le système du Personnalisateur de cartes sont traitées par la AND-CPCA de manière synchrone sans délai, sous réserve que le système du Personnalisateur ait été dûment authentifié.

IV.1.3. Emission du certificat

Si tous les contrôles sont effectués avec succès, la AND-CPCA signe le certificat et l'émet.

Les opérations cryptographiques (signature du certificat avec la clé privée *CPCA_Card.SK*) sont effectuées au sein d'un module cryptographique sécurisé (HSM). Une fois le certificat généré pour l'équipement (carte), il peut être transféré de manière synchrone au Personnalisateur de Cartes (AND-CP).

L'Autorité de Certification doit s'assurer, dans le cadre de ses compétences, que l'Autorité responsable est dûment enregistrée avant de délivrer un certificat au Personnalisateur de Cartes (AND-CP).
La génération de la bi-clé n'étant pas effectuée par l'Autorité de Certification, cette dernière ne délivre un certificat au Personnalisateur de Cartes que si elle a la preuve que le Personnalisateur est en possession de la clé privée correspondante. La clé privée ne doit pas quitter l'environnement sécurisé du Personnalisateur de Cartes pendant le traitement de la demande de certificat.
Les contrôles de cohérence et d'exactitude, les contrôles de signature de la demande sont effectués de manière automatisée par l'Autorité de Certification.

Période de validité du certificat

La période de validité d'un certificat d'authentification mutuelle (*Card_MA.C*) doit être la suivante :

- pour les cartes de conducteur : 5 ans
- pour les cartes d'entreprise : 5 ans
- pour les cartes de contrôleur : 5 ans
- pour les cartes d'atelier : 1 an

La période de validité des clés privées *Card_MA.SK* doit être la même que celle des certificats correspondants (*Card_MA.C*).

IV.1.4. Echange des requêtes et réponses

Echange des requêtes et réponses avec l'ERCA

Pour le transport des demandes de certificat et des certificats générés, un support de stockage amovible doit être utilisé. Ce support peut être uniquement un medium de type CD-ROM de 12 cm en mode « écriture unique » (formaté ISO 9660:1988 [11])
D'autres moyens de transport peuvent être utilisés avec accord préalable de l'ERCA. À des fins de test, l'ERCA accepte et distribue des KCR et des certificats par le biais de courriers électroniques.
La AND-CPCA doit écrire trois copies de chaque demande de signature de certificat sur le support de transport pour l'ERCA. Ces copies doivent être respectivement au format ASCII hexadécimal (fichier.txt), Base64 (fichier.pem) et binaire (fichier.bin).
D'autres moyens de transport peuvent être utilisés avec l'accord préalable de l'ERCA. A des fins de test, l'ERCA accepte et distribue les KCR et les certificats par e-mail.
L'ERCA écrit trois copies de chaque certificat sur le support de transport pour remise à la AND-CPCA. Ces copies sont respectivement au format ASCII hexadécimal (fichier.txt), Base64 (fichier.pem) et binaire (fichier.bin).
Chaque demande de signature de certificat et chaque certificat doivent être accompagnés d'une copie papier des données, formatée conformément à un modèle défini dans la Déclaration des Pratiques de Certification de l'ERCA. Une autre copie papier des données doit être conservée par l'ERCA ou la AND-CPCA, respectivement.
Pour les KCR et également les certificats, le support de transport et les impressions sont échangés entre un employé de l'ERCA et le porteur de la AND-CPCA dans un espace contrôlé par l'ERCA.

Echange des requêtes et réponses avec la AND-CPCA

La connexion au système IGC (PKI) de la AND-CPCA doit être sécurisée : authentification mutuelle et garantie de confidentialité des échanges.
Les requêtes et les réponses échangées entre le système IGC (PKI) de la AND-CPCA et le système de personnalisation de cartes du Personnalisateur de Cartes (AND-CP) dans le cadre du service de certification contiennent respectivement les informations suivantes :

- Demande de certification de clé (KCR) :
  - Données descriptives de la carte (valeurs conformes à l'Appendice 1B) :
    - Type d'équipement
    - Code Pays
    - Numéro de carte
    - Numéro de série étendu
    - Date de fin de validité

- Réponse :
  - Certificats
    - Certificat Génération 1 Carte

IV.1.5. Acceptation du certificat

Acceptation du certificat, AND-CPCA

Le porteur du media signe le reçu du certificat de la AND-CPCA dans les locaux de l'ERCA.
Dès réception du certificat dans les locaux de la AND-CPCA, cette dernière vérifie que :

- le media de transport est lisible, c'est-à-dire non endommagé ou corrompu ;
- le format du certificat est conforme au tableau 7 du chapitre VII.1 ;
- toutes les valeurs de champ de certificat correspondent aux valeurs demandées dans la KCR ;
- la signature du certificat peut être vérifiée à l'aide de la clé racine publique de l'ERCA indiquée dans le champ CAR (Certification Authority Reference).

Si l'une de ces vérifications échoue, la AND-CPCA doit abandonner le processus et contacter l'ERCA. Le rejet de certificat est géré conformément à la procédure de révocation de certificat.

Acceptation du certificat, Personnalisateur de Cartes

L'acceptation du certificat par le Personnalisateur de Cartes (AND-CP) peut être implicite à la condition qu'il ait la garantie d'origine de ce certificat (il provient de la AND-CPCA).
Toutefois, en cas de problème de personnalisation de la carte (personnalisation graphique et/ou électrique), le Personnalisateur de Cartes doit informer la AND-CPCA.
La liste noire contient la liste des certificats réputés non valides et par conséquent ne pouvant plus être utilisés dans le système du Tachygraphe Numérique.

IV.1.6. Usage de la bi-clé et du certificat

Usage de la bi-clé et du Certificat de la AND-CPCA

La AND-CPCA doit utiliser les bi-clés et les certificats correspondants conformément au chapitre VI.2.

Usage de la bi-clé et du Certificat du Personnalisateur de Cartes

Le Personnalisateur de Cartes (AND-CP) doit utiliser les bi-clés et les certificats correspondant conformément au chapitre VI.2.

La taille de la clé de la carte est fixée à 128 octets (soit 1024 bits).
Une carte tachygraphique doit utiliser sa bi-clé (*Card_MA.SK* et *Card_MA.PK*), exclusivement pour effectuer une authentification mutuelle et un échange de clé de session avec les unités embarquées, comme spécifié dans l'Appendice 1B – Sous-appendice 11 [2].
Les bi-clés, les clés symétriques et les codes PIN doivent être générés et conservés dans un dispositif dédié sécurisé qui :

- est certifié au niveau EAL 4 ou supérieure conformément à la norme ISO / IEC 15408 [8] ; ou au niveau E3 ou supérieur de ITSEC ; ou à des critères de sécurité équivalents. Les évaluations doivent être effectuées selon un profil de protection ou une cible de sécurité approprié ; ou
- répond aux exigences identifiées dans le CEN Workshop Agreement 14167-2 [9] ; ou
- répond aux exigences identifiées dans FIPS PUB 140-2 (ou FIPS 140-1) niveau 3 ou supérieur [10] ; ou
- démontre offrir un niveau de sécurité équivalent.

Le dispositif sécurisé le plus courant, destiné à être utilisé au sein d'une IGC (PKI), est le HSM (Hardware Security Module ou Module de Sécurité Matérielle).

Les opérations sur les clés privées doivent être exécutées dans le HSM qui stocke ces clés.
Les clés privées ne doivent être utilisées que dans un environnement physiquement sécurisé par du personnel occupant des rôles de confiance. Les clés privées ne doivent pas être exploitées en dehors du HSM sans application d'un cryptage ad-hoc. Tous les événements d'utilisation des clés privées doivent être enregistrés dans les journaux d'événements.
La bi-clé et le certificat correspondant d'une carte tachygraphique donnée ne doivent pas être ni remplacés, ni renouvelés une fois la carte émise.

Lorsqu'elles sont émises, les cartes tachygraphiques doivent contenir les clés et certificats suivants :

- La clé privée *Card_MA.SK* et le certificat correspondant *Card_MA.C* ;
- Le certificat *CPCA_Card.C* de clé publique (*CPCA_Card.PK*) de la AND-CPCA utilisé pour la vérification du certificat *Card*_MA.C ;
- Le certificat *EUR.C* de clé publique (*EUR.PK*) de l'ERCA utilisé pour la vérification du certificat *CPCA_Card.C* de la AND-CPCA ;
- La Clé maîtresse symétrique $K_{M\text{-}WC}$ pour les cartes d'atelier.

IV.1.7. Renouvellement d'un certificat

NOTE : Dans le cadre de la présente Politique de Certification, le terme « renouvellement » d'un certificat traduit l'action de régénérer le certificat en ne modifiant que la période de validité (conservation des identifiants et de la valeur de la clé publique).

Renouvellement d'un certificat, AND-CPCA

Le renouvellement d'un certificat de la AND-CPCA existant (c'est-à-dire l'extension de la période de validité, en conservant la bi-clé) n'est pas autorisé par la Politique de Certification de l'ERCA [6].

Renouvellement d'un certificat, Personnalisateur de Cartes (AND-CP)

Le renouvellement d'un certificat existant (c'est-à-dire l'extension de la période de validité, en conservant la bi-clé) n'est pas autorisé par la présente Politique de Certification.

IV.1.8. Renouvellement de la bi-clé

Renouvellement de la bi-clé, AND-CPCA

Le renouvellement de la bi-clé signifie la signature d'un nouveau certificat AND-CPCA, en remplacement d'un certificat existant. Le renouvellement d'une bi-clé est effectué dans l'un des deux cas suivants :

- à l'approche de la fin de la période d'utilisation de la clé privée. Dans ce cas, la bi-clé doit être renouvelée en temps utile afin que la AND-CPCA puisse poursuivre ses activités de certification après la fin de cette période.
- suite à la révocation du certificat.

La demande, le traitement, l'émission, l'acceptation et la publication du certificat sont effectués de manière identique au certificat initial.
Les bi-clés AND-CPCA peuvent être changées régulièrement. L'ERCA n'impose aucune limite au nombre de certificats de la AND-CPCA qu'elle signera. La AND-CPCA est autorisée à demander plusieurs certificats de même type, si son activité le justifie, avec des périodes de validité qui se chevauchent.
La génération de nouvelles paires de clés de Partie Contractante prend en compte le délai d'exécution d'un mois requis pour certification par l'ERCA.

Renouvellement de la bi-clé, Personnalisateur de Cartes (AND-CP)

Le renouvellement de la bi-clé d'un certificat carte tachygraphique (*Card_MA.C*) n'est pas autorisé. A la fin de validité du certificat et à la fin de la période d'utilisation de la bi-clé correspondante, une nouvelle carte tachygraphique doit être créée.

IV.1.9. Modification du certificat

Modification du certificat, AND-CPCA

La modification d'un certificat de la AND-CPCA n'est pas autorisée par la Politique de Certification de l'ERCA [6].

Modification du certificat, Personnalisateur de Cartes (AND-CP)

La modification d'un certificat carte tachygraphique n'est pas autorisée par la présente Politique de Certification. Toute éventuelle demande de modification de certificat reçue par la AND-CPCA sera rejetée et non traitée.

IV.1.10. Révocation et suspension du certificat

Circonstances de la révocation d'un certificat

Révocation et suspension d'un certificat, AND-CPCA

Les certificats de la AND-CPCA doivent être révoqués dans les cas suivants :

- rejet de la AND-CPCA d'un certificat nouvellement délivré par l'ERCA ;
- compromission ou suspicion de compromission de la clé privée associée au certificat de la AND-CPCA ;
- perte de la clé privée associée au certificat de la AND-CPCA ;
- cessation d'activité de la AND-CPCA ;
- non-respect par la AND-CPA , la AND-CPCA ou l'OC des obligations imposées par le Règlement et la Politique de Certification de l'ERCA [6].

Le cas échéant, sur appréciation de la AND-CPCA, dans le cas de cessation d'activité de l'OC avec impossibilité de réversibilité, les certificats de la AND-CPCA pourront être révoqués.

Révocation et suspension d'un certificat, Personnalisateur de Cartes (AND-CP)

La révocation des certificats carte tachygraphique n'est pas prévue dans la présente Politique de Certification. En cas de réception de demande de révocation, celle-ci ne sera ni acceptée, ni traitée par la AND-CPCA.

Qui peut demander la révocation d'un certificat

Révocation d'un certificat, AND-CPCA

L'ERCA n'accepte les demandes de révocation d'un certificat de la AND-CPCA que si elle émane de l'une des entités suivantes :

- l'Autorité Européenne (EA)
- la AND-CPA
- la AND-CPCA

L'Autorité Européenne est en effet autorisée à demander la révocation des certificats des CPCA ainsi que ceux des MSCA.
La AND-CPA est autorisée à demander la révocation des certificats émis pour la AND-CPCA qui est désignée par la présente Politique de Certification.
La AND-CPCA est autorisée à demander la révocation d'un certificat qui lui a été délivré par l'ERCA.
L'ERCA rejette toute demande émanant de toute autre entité.

Révocation d'un certificat, Personnalisateur de Cartes (AND-CP)

N/A

Délai pour formuler la demande de révocation

Délai pour formuler la demande de révocation, AND-CPCA

Le délai pour formuler la demande de révocation est de 5 jours ouvrés à compter de la connaissance d'une des causes effectives de révocation.

Délai pour formuler la demande de révocation, Personnalisateur de Carte
N/A

Délai pour le traitement de la demande de révocation

Délai pour le traitement de la demande de révocation, AND-CPCA

L'ERCA traite toute demande de révocation correcte, complète et autorisée sous un délai de 3 jours ouvrés à compter de sa réception.

Délai pour le traitement de la demande de révocation, Personnalisateur de Cartes (AND-CP)

N/A

Exigence de vérification de la révocation par les utilisateurs des certificats

Exigence de vérification de la révocation par les utilisateurs des certificats, AND-CPCA

La AND-CPCA est responsable de la vérification du statut des certificats publiés sur le site de l'ERCA.

Exigence de vérification de la révocation par les utilisateurs des certificats, Personnalisateur de Cartes (AND-CP)

N/A

Fréquence de publication des informations de révocation

Fréquence de publication des informations de révocation, AND-CPCA

Les informations sur le statut des certificats de l'ERCA et de la AND-CPCA sont accessibles en ligne à l'adresse : https://dtc.jrc.europa.eu
L'ERCA maintient l'intégrité des informations de révocation qu'elle publie.

Fréquence de publication des informations de révocation, Personnalisateur de Cartes

N/A

Délai maximum de publication de la CRL

N/A

Exigences sur la vérification en ligne de la révocation et du statut des certificats

Aucune stipulation

Exigences particulières concernant la compromission de clé

Exigences particulières concernant la compromission de clé, AND-CPCA

La compromission d'une clé est un incident de sécurité qui doit être pris en compte et traité.
En cas de compromission ou de suspicion de compromission d'une clé de la AND-CPCA, cette dernière doit signaler l'incident à l'ERCA et à la AND-CPA. L'enquête de suivi et les actions potentielles doivent être conduites par la AND-CPA. Les conclusions de l'enquête de la AND-CPCA doivent être rapportées à l'ERCA.
Si une compromission est confirmée ou ne peut être écartée, la clé concernée doit être détruite. De même, toutes les copies de la clé compromise devront être détruites.

Exigences particulières concernant la compromission de clé, Personnalisateur de cartes (AND-CP)

La compromission d'une clé privée ou d'une clé maîtresse symétrique est un incident de sécurité qui doit être pris en compte et traité.
En cas de compromission ou de suspicion de compromission d'une clé privée ou d'une clé maîtresse symétrique, le Personnalisateur de Cartes (AND-CP) doit notifier l'incident à la AND-CPCA sans délai. Dans sa notification à la AND-CPCA, le Personnalisateur de Cartes indiquera les circonstances dans lesquelles la compromission est survenue.

Suspension de certificat

Suspension de certificat, AND-CPCA

Les certificats de la AND-CPCA émis par l'ERCA ne peuvent être suspendus.

Suspension de certificat, Personnalisateur de Cartes (AND-CP)

Les certificats du Personnalisateur de Cartes émis par la AND-CPCA ne peuvent être suspendus.

IV.1.11. Services d'information sur l'état des certificats

Les informations sur l'état des certificats des cartes tachygraphiques émises sont gérées par la AND-CPCA. Ces informations ne sont pas publiées mais sont mises à la disposition des parties qui en feraient la demande. Cette demande est toutefois soumise à l'appréciation de AND-CPCA qui en étudiera la légitimité.

IV.1.12. Fin d'abonnement

Fin d'abonnement, AND-CPCA

L'abonnement de la AND-CPCA aux services de certification de l'ERCA prend fin lorsque la AND-CPA décide de mettre fin à son rôle de CPA. Un tel changement est notifié à l'ERCA par la AND-CPA en tant que modification de la politique de certification de la AND-CPA.
En cas de fin d'abonnement, la décision de soumettre une demande de révocation de tous les certificats valides de la AND-CPCA ou d'autoriser leur usage jusqu'à leur expiration relève de la responsabilité de la AND-CPA.

Fin d'abonnement, Personnalisateur de Cartes (AND-CP)

L'abonnement au service de certification de la AND-CPCA prend fin lorsque le Personnaliseur de Cartes ou la

AND-CPA décide de mettre fin au service. Dans ce cas, tous les certificats des cartes tachygraphiques émises restent valides jusqu'à leur expiration (atteinte de la date de fin validité).
Le Personnaliseur de Cartes (AND-CP) doit notifier la fin du service à la AND-CPA et à la AND-CPCA.

IV.1.13. Séquestre des clés et recouvrement

Le séquestre des clés privées des cartes (*Card_MA.SK*) est formellement interdit. Cela signifie qu'après personnalisation des cartes ces clés ne peuvent être conservées et/ou stockées ailleurs que dans la carte concernée.

IV.2. Demande et distribution des Clés Maîtresses

IV.2.1. Requête de Distribution de Clés (KDR)

Requête de Distribution de Clés, ERCA

Les demandes de distribution de clés (KDR) peuvent être soumises par la AND-CPCA sous réserve de sa reconnaissance par la AND-CPA via sa déclaration auprès de l'ERCA.

Le format de la demande de distribution de la clé M-WC est le suivant :

Field	Octets	Explication
Key request Content	164	Voir ci-dessous
Signature of Key request Content	128	Voir ci-dessous

Tableau 4 – Format d'une Demande de Distribution de Clé

Champ	Format	Octets	Explication
CPI	Integer	1	Certificate Profile Identifier '01'
CAR	Octet String	8	Certification Authority Reference
nationNumeric	Integer	1	Code numérique pour la nation émettrice (voir site web du JRC) 'FD' (253) = Communauté Européenne
nationAlpha	IA5String	3	Code Alpha-3 pour la nation émettrice (voir site web du JRC) '45 43 20' = "EC "
keySerialNumber	Integer	1	'00'
additionaInfo	Octet String	2	'FF FF' Production '54 4B' Test
caIdentifier	Octet String	1	'01'
MRA	Octet String	7	Message Recipient Authorisation
tachographApplicationID	Octet String	6	'FF 54 41 43 48 4F'
type	Integer	1	'27' (correspond au type de clé $K_{M\text{-}WC}$. cf. valeurs de EquipmentType définies dans l'Appendice 1B)
EOV	TimeReal	4	End Of Validity 'FF FF FF FF'
KID	Octet String	8	Key Identifier
nationNumeric	Integer	1	Numeric code for issuing nation (See JRC website)
nationAlpha	IA5String	3	Alpha-3 code for issuing nation (See JRC website)
keySerialNumber	Integer	1	Serial number to identify the KDR
additionaInfo	Octet String	2	'FF FF' pour Production '54 4B' pour Test
type	Integer	1	'27' (correspond au type de clé $K_{M\text{-}WC}$)
Public Key			Clé publique éphémère utilisée pour le chiffrement de la clé maîtresse.
n	Octet String	128	Modulus de la clé publique
e	Octet String	8	Exposant de la clé publique

Tableau 4.a – Format de *Key request Content*

La signature de la KDR est la primitive de signature RSAP1 (PKCS#1) [14] avec la clé privée éphémère de la AND-CPCA.

Champ	Octets	Explanation
Fixed value	1	'4B'
Fixed value	58	58 x 'BB'
Fixed value	1	'BA'
Hash	20	SHA-1(Key request)
Hash	20	SHA-1(SHA-1(Key request))
Fixed value	1	'BC'

Tableau 4.b – Format de *Signature of Key request Content*

Requête de Distribution de Clés, AND-CPCA

Les demandes de distribution de clés peuvent être soumises par le Personnalisateur de Cartes (AND-CP) à la AND-CPCA.

IV.2.2. Traitement des demandes de clés maîtresses

Traitement des demandes de clés maîtresses, ERCA

L'ERCA s'assure que la KDR émanant de la AND-CPCA est complète, exacte et dûment autorisée.
L'ERCA ne créera le Message de Distribution de Clé (KDM) que si ces conditions sont remplies. Les contrôles sont effectués manuellement par les officiers de l'ERCA et/ou de façon automatisée par le service d'enregistrement de l'ERCA. Si le message est complet et correct, les officiers peuvent autoriser la génération du Message de Distribution de Clé (KDM) par le service de distribution de clé.

Traitement des demandes de clés maîtresses, AND-CPCA

La demande de distribution de clé effectuée par le AND-CP auprès de la AND-CPCA suit un autre workflow que celui présenté dans le schéma de l'ERCA (cf. chapitre I.3). Toutefois, son niveau de sécurité doit être à minima équivalent à celui du processus décrit dans la Politique de Certification de l'ERCA [6].

IV.2.3. Protection des clés maîtresses en confidentialité et intégrité

Transfert de l'ERCA vers la AND-CPCA

La confidentialité et l'authenticité des clés symétriques distribuées par l'ERCA à la AND-CPCA doivent être assurées par chiffrement RSA utilisant une bi-clé de transport générée par la AND-CPCA. Ce chiffrement ainsi qu'un calcul de hash permettent de protéger la clé maîtresse symétrique durant le processus de distribution. Ce process est détaillé dans l'Appendice 1B – Sous-appendice 11 [2].

Transfert de la AND-CPCA vers le Personnalisateur de Cartes (AND-CP)

La confidentialité et l'authenticité des clés symétriques distribuées par la AND-CPCA au Personnalisateur de Cartes (AND-CP) sont assurées par un processus de transfert sécurisé entre les deux entités : transfert direct entre le matériel cryptographique de la AND-CPCA et le matériel cryptographique du AND-CP, grâce à une clé de transport ZMK partagée par les deux HSM. Le niveau de sécurité de ce processus doit répondre aux exigences de l'ERCA.

IV.2.4. Message de Distribution de Clé (KDM)

Message de Distribution de Clé, ERCA

Après avoir traité la KDR, l'ERCA doit construire un message de distribution de la clé maîtresse.
Le tableau suivant montre le format attendu de la KDM.

Champ	Octets	Explication
KID	8	Voir ci-dessous
Encrypted Labeled Master Key	128	Schéma de chiffrement RSA-PKCS1-v2_0-ENCRYPT avec la clé publique éphémère de la CPCA

Tableau 5 – Format du Message de Distribution de Clé

Champ	Format	Octets	Explication
KID	Octet String	8	
nationNumeric	Integer	1	Code numérique pour la nation émettrice (voir le site web du JRC)
nationAlpha	IA5String	3	Code Alpha-3 code pour la nation émettrice (voir le site web du JRC)
keySerialNumber	Integer	1	Numéro de série identifiant la KDR
additionalInfo	Octet String	2	'44 4B' pour Production (='DK' pour DES Key) '54 4B' pour Test (='TK' pour Test Key)
type	Integer	1	'27' (correspond au type de clé K_{M-WC})
KM	Octet String	16	Certification Authority Reference

Tableau 5.a – Format de *Labeled Master Key*

Message de Distribution des Clés, AND-CPCA

Les clés sont exportées côté AND-CPCA sous forme chiffrée puis importées côté Personnalisateur de Cartes (AND-CP). Le message est constitué d'un fichier contenant la clé maîtresse K_{M-WC} chiffrée par une clé de transport ZMK (clé AES 256 bits) partagée par les deux entités. La confidentialité et l'intégrité de cette clé doivent être garanties par les deux entités (AND-CPCA et Personnalisateur de Cartes).

IV.2.5. Echange des Requêtes (KDR) et Réponses (KDM)

Echange des KDR et KDM entre l'ERCA et la AND-CPCA

Le transport de la KDR et de la KDM est effectué sur un support de stockage amovible (seul le CD-R est accepté).

La KDR est fournie par la AND-CPCA sous forme de 3 copies (3 formats distincts) sur support de stockage amovible en mains propres aux officiers de l'ERCA. L'ERCA doit contacter la AND-CPCA afin de s'assurer que le hash calculé sur la KDR reçue correspond à celui calculé et enregistré par la AND-CPCA.

Après traitement de la KDR, la KDM est fournie par l'ERCA sous forme de 3 copies (3 formats distincts) sur support de stockage amovible à la AND-CPCA.

Chaque KDR et KDM doit être accompagnée d'une copie papier des données, formatée selon un modèle défini dans la PC de l'ERCA [6]. Une autre copie papier des données doit être conservée par l'ERCA ou la AND-CPCA, respectivement.

Lors de la génération de la KDR par la AND-CPCA, la génération d'une bi-clé temporaire est effectuée. L'ERCA

s'assure qu'elle n'a pas certifié la clé publique transmise dans la demande ou que cette clé n'a pas été utilisée dans une précédente KDR.

IV.2.6. Acceptation de la Clé Maîtresse

Acceptation par le AND-CPCA

Le responsable du transport (représentant de la AND-CPA) signe la remise de la KDM dans les locaux de l'ERCA. Dès réception de la KDR par la AND-CPCA dans les locaux de l'OC, la AND-CPCA vérifie que :

- le support de stockage amovible est lisible, c'est-à-dire non endommagé ou corrompu ;
- le format du message est conforme au tableau 4 ;
- le message est authentique. Pour ce faire, la AND-CPCA contacte l'ERCA comme décrit dans la PC de l'ERCA et vérifie que le hash du KDM reçu correspond au hash du KDM envoyé par l'ERCA ;
- le type et la version de la clé principale dans le message correspondent au type et à la version demandés ;
- le point public spécifié dans le message se trouve sur la courbe spécifiée par la KDR envoyée par la AND-CPCA à l'ERCA.

Si l'une de ces vérifications échoue, la AND-CPCA doit abandonner le processus et contacter l'ERCA.

Acceptation par le Personnalisateur de Cartes (AND-CP)

Le système du Personnalisateur de Cartes (AND-CP) doit vérifier la cohérence et l'intégrité des clés symétriques qui lui sont transmises. L'acceptation d'une clé par le Personnalisateur de Cartes doit être explicite.

IV.2.7. Usage de la Clé Maîtresse

Usage de la Clé Maîtresse, AND-CPCA

La AND-CPCA doit utiliser les clés maîtresses reçues conformément au chapitre VI.2

Usage de la Clé Maîtresse, Personnalisateur de Cartes (AND-CP)

Le Personnalisateur de Cartes (AND-CP) doit utiliser les clés maîtresses reçues conformément au chapitre VI.2

IV.2.8. Renouvellement de la KDM

Renouvellement KDM, AND-CPCA

Le renouvellement de la KDM signifie l'émission d'une copie d'une KDM existante sans modifier la clé publique RSA de transport ou toute autre information contenue dans la KDM.
Le renouvellement de la KDM ne peut avoir lieu que si le support de stockage amovible d'origine reçu par la AND-CPCA est endommagé ou corrompu. Le dommage ou la corruption du support de transport constitue un incident de sécurité qui doit être rapporté à la AND-CPA et à l'ERCA. A la suite de ce rapport, la AND-CPCA

peut envoyer une demande de renouvellement de la KDM à l'ERCA, en faisant référence à la KDR d'origine. L'ERCA n'accepte que les demandes de renouvellement de KDM approuvées par la AND-CPA.

Remarque:
Si la AND-CPCA a besoin d'envoyer une demande pour redistribuer une clé maîtresse qui lui a été précédemment distribuée avec succès, elle générera une nouvelle KDR en utilisant une nouvelle bi-clé RSA de transport. Une telle demande peut amener l'ERCA à ouvrir une enquête sur la possibilité de compromission de la clé maîtresse.

Renouvellement KDM, Personnalisateur de Cartes (AND-CP)

Le renouvellement de la demande d'une clé maîtresse par le Personnalisateur de Cartes (AND-CP) ne peut avoir lieu qu'en cas exceptionnel de :

- perte du contenu (ou de la compromission de son intégrité) du matériel cryptographique (dysfonctionnement, panne, etc.) ;
- effacement involontaire d'un objet cryptographique.

La AND-CPCA pourra transférer de nouveau la clé maîtresse du matériel cryptographique (celui de l'OC) vers celui du Personnalisateur de Cartes (suivant le processus initial) en vérifiant que l'origine de l'incident n'est pas de nature à compromettre la clé maîtresse. La AND-CPCA informera néanmoins la AND-CPA de cet incident.
La demande du AND-CP doit être transmise à la AND-CPCA.
Si l'OC est destinataire de la demande, ce dernier doit la transférer obligatoirement à la AND-CPCA. C'est uniquement cette dernière qui peut prendre la décision de transférer à nouveau la clé maîtresse au AND-CP.

IV.2.9. Renouvellement de la Clé Maîtresse

Renouvellement de la Clé Maîtresse, AND-CPCA

En cas de génération d'une nouvelle version de clé maîtresse par l'ERCA, la disponibilité de cette nouvelle version est publiée sur le site Web de l'ERCA, en spécifiant son numéro de version et sa longueur.
Pour obtenir cette nouvelle version, la AND-CPCA doit soumettre une nouvelle KDR. La demande d'une nouvelle clé maîtresse doit s'effectuer en temps utile afin que la clé puisse être prise en compte rapidement dans les nouvelles cartes émises par le Personnalisateurs de Cartes (AND-CP).
Les processus de demande, de traitement, de distribution et d'acceptation de la clé sont les mêmes que pour la clé maîtresse initiale.

Renouvellement de la Clé Maîtresse, Personnalisateur de Cartes (AND-CP)

La AND-CPCA doit informer le Personnalisateur de Cartes (AND-CP) de la disponibilité d'une nouvelle version de clé maîtresse, sans délai, dès qu'elle l'a obtenue.
Le transfert de cette nouvelle version de clé maîtresse entre le matériel cryptographique de la AND-CPCA (plus exactement celui de l'OC) et celui du AND-CP s'effectue selon le processus initial (cf. IV.2.4 paragraphe *KDM, AND-CPCA*).

IV.2.10. Révocation de la Clé Maîtresse

Notification de compromission d'une clé maîtresse, AND-CPCA

Si la AND-CPCA détecte ou est informée de la compromission ou de la suspicion de compromission d'une clé maîtresse, elle en informera l'ERCA et la AND-CPA sans délai et au moins dans les 5 jours suivant cette détection. La AND-CPCA indiquera dans sa notification les circonstances dans lesquelles la compromission est survenue.
L'ERCA traite l'incident selon une procédure de traitement des incidents de sécurité définie et en informe immédiatement l'Autorité Européenne (EA).
Toute investigation et toute action potentielle de la part de la AND-CPA et/ou de la AND-CPCA doivent être effectuées conformément à la politique de la AND-CPA. Les conclusions des investigations de la AND-CPA doivent être transmises à l'ERCA.

Notification de compromission d'une clé maîtresse, Personnalisateur de Cartes (AND-CP)

Si le Personnalisateur de Cartes (AND-CP) détecte ou est averti de la compromission ou de la suspicion de compromission d'une clé maîtresse, il doit informer la AND-CPCA et la AND-CPA sans délai. Dans sa notification, le Personnalisateur de Cartes indiquera les circonstances dans lesquelles la compromission est survenue.

IV.2.11. Service d'information sur l'état d'une Clé Maîtresse

Le statut des clés maîtresses est exclusivement géré l'ERCA. Il doit être récupéré en ligne à l'adresse suivante : https://dtc.jrc.ec.europa.eu/
Les informations sur l'état des clés maîtresses publiées par l'ERCA sont mises à jour le premier jour ouvrable de chaque semaine. La disponibilité du site Web mentionné ci-dessus est assurée pendant les heures ouvrées.

IV.2.12. Fin d'abonnement

Fin de l'abonnement, AND-CPCA

L'abonnement aux services de distribution des clés maîtresses de l'ERCA prend fin lorsque la AND-CPA décide de mettre fin à son rôle de CPA. Ce changement est notifié à l'ERCA par la AND-CPA comme une modification de la politique nationale.
En cas de fin d'abonnement, la AND-CPCA doit détruire de manière sécurisée toutes les copies de clé maîtresse symétrique en sa possession et conserver une preuve de cette destruction qui peut être mise à disposition de la AND-CPA ou de l'ERCA. De ce fait, il doit notifier l'OC et participer avec lui à cette destruction.

Fin d'abonnement, Personnalisateur de Cartes (AND-CP)

Le Personnalisateur de Cartes (AND-CP) peut décider de mettre fin à son abonnement au service de distribution des clés maîtresses. Sa décision doit être notifiée à la AND-CPCA.
En cas de fin d'abonnement, le Personnalisateur de Cartes doit détruire de manière sécurisée toutes les copies de clé maîtresse en sa possession.

IV.2.13. Séquestre des clés maîtresses et recouvrement

Séquestre des clés maîtresses, AND-CPCA

Le séquestre des clés maîtresses est expressément interdit, ce qui signifie qu'elles ne doivent être ni exportées ni stockées dans un système autre que les systèmes de production et de secours de la AND-CPCA (matériels cryptographiques de l'OC).

Séquestre des clés maîtresses, Personnalisateur de Cartes (AND-CP)

Le séquestre des clés maîtresses est expressément interdit, ce qui signifie qu'elles ne doivent être ni exportées ni stockées dans un système autre que les systèmes de production et de secours du Personnalisateur de Cartes (AND-CP) (matériels cryptographiques).

V. Contrôles de la gestion et de l'exploitation des installations

V.1. Mesures de sécurité physique

V.1.1. AND-CPCA

Les services de génération des clés et des certificats doivent être hébergés dans une zone sécurisée, protégée par un périmètre de sécurité défini, avec des barrières de sécurité et des contrôles d'accès appropriés pour empêcher les accès non autorisés, les dommages et les interférences.
Les supports de stockage des informations confidentielles, tels que les disques durs, les cartes à puce et les HSM, doivent être protégés contre toute utilisation non autorisée ou non intentionnelle, l'accès, la divulgation ou les dommages causés par des personnes ou d'autres menaces (par exemple incendie, inondation).
Les procédures de destruction des supports de stockage doivent être mises en œuvre afin d'éviter toute utilisation, accès ou divulgation non autorisé des données confidentielles.
Des procédures d'élimination des déchets doivent être mises en place afin d'empêcher l'utilisation, l'accès à ou la divulgation non autorisés de données confidentielles.
Une sauvegarde hors site pour les données critiques de la AND-CPCA, en particulier pour ses clés privées, doit être mise en œuvre.

V.1.2. Personnalisateur de Cartes (AND-CP)

Le service de génération des clés doit être hébergés dans une zone sécurisée, protégée par un périmètre de sécurité défini, avec des barrières de sécurité et des contrôles d'accès appropriés pour empêcher les accès non autorisés, les dommages et les interférences.
Les supports de stockage des informations confidentielles, tels que les disques durs, les cartes à puce et les HSM, doivent être protégés contre toute utilisation non autorisée ou non intentionnelle, l'accès, la divulgation ou les dommages causés par des personnes ou d'autres menaces (par exemple incendie, inondation).
Les procédures de destruction des supports de stockage doivent être mises en œuvre afin d'éviter toute utilisation, accès ou divulgation non autorisé des données confidentielles.

V.2. Mesures de sécurité procédurales

Des contrôles procéduraux doivent être mis en place pour garantir la sécurité des opérations. En particulier, la séparation des tâches doit être imposée par la mise en œuvre d'un contrôle par plusieurs personnes pour les tâches critiques.
L'accès aux systèmes de la AND-CPCA (propriétés de l'OC) et du Personnalisateur de Cartes (AND-CP) doit

être limité aux personnes dûment autorisées et ayant besoin d'en connaître. En particulier, les mesures de contrôle d'accès suivantes doivent être mises en place :

- Les données confidentielles doivent être protégées afin de préserver leur intégrité et leur confidentialité lors de leur stockage.
- Les données confidentielles doivent être protégées afin de préserver leur intégrité et leur confidentialité lors de leur échange sur des réseaux non sécurisés.
- Les données confidentielles supprimées doivent être définitivement détruites, par exemple en réécrivant plusieurs fois le support de stockage avec des données aléatoires.
- les systèmes de la AND-CPCA et du Personnalisateurs de Cartes (AND-CP) doivent garantir une administration des utilisateurs et une gestion des accès efficaces ;
- Les systèmes de la AND-CPCA et du Personnalisateur de Cartes (AND-CP) doivent garantir que l'accès aux informations et aux fonctions du système d'application est réservé au personnel autorisé et prévoir des contrôles de sécurité informatiques suffisants pour séparer les rôles de confiance. En particulier, l'utilisation de programmes utilitaires du système doit être restreinte et rigoureusement contrôlée. L'accès doit être restreint, permettant uniquement l'accès aux ressources nécessaires à l'exécution du rôle attribué à un utilisateur ;
- Le personnel intervenant pour le compte de la AND-CPCA (dont le personnel de l'OC) et le personnel du Personnalisateur de Cartes (AND-CP) doivent être identifiés et authentifiés avant d'utiliser leur système respectif.
- Le personnel intervenant pour le compte de la AND-CPCA (dont le personnel de l'OC) et le personnel du Personnalisateur de Cartes (AND-CP) doivent rendre compte de leurs activités qui doivent être consignées dans les journaux d'événements, comme décrit à la section V.4.

La AND-CPCA (plus exactement l'OC) et le Personnalisateur de Cartes (AND-CP) doivent mettre en place un Système de Management de la Sécurité de l'Information (SMSI) basé sur une évaluation des risques pour toutes les opérations concernées. La AND-CPCA (plus exactement l'OC) et le Personnalisateur de Cartes (AND-CP) doivent s'assurer que la politique de leur SMSI traite de la formation du personnel, des rôles et des autorisations. L'implémentation du SMSI par la AND-CPCA (plus exactement l'OC) et le Personnalisateur de Cartes (AND-CP) devrait être conforme aux bonnes pratiques décrites dans l'ISO/IEC 27001 [12] et l'ISO/IEC 27005 [13].

V.3. Mesure de sécurité vis-à-vis du personnel

V.3.1. Mesures de sécurité vis-à-vis du personnel de la AND-CPCA

Les responsabilités de la AND-CPCA peuvent être sous-traitées à une entreprise spécialisée, ou du personnel d'un contractant peut être employé pour les exécuter. En particulier, la responsabilité de l'émission des certificats et de la distribution des clés maîtresses est sous-traitée à l'Opérateur de Certification retenu par la AND-CPCA.

Tout le personnel concerné par les activités de la AND-CPCA doit être correctement formé et posséder les connaissances, l'expérience et les qualifications requises pour les services offerts et en adéquation avec la fonction exercée. Cela concerne le personnel employé directement par la AND-CPCA, le personnel d'une société spécialisée pour laquelle des tâches ont été sous-traitées ou le personnel d'un contractant. En particulier, le personnel de l'OC est concerné.

La formation du personnel doit être gérée selon un plan de formation. En particulier, un plan de formation doit être décrit dans la Déclaration des Pratiques de Certification (DPC) de l'OC.

La nomination du personnel à des rôles de confiance doit être gérée conformément à une procédure de

sélection décrite dans la DPC de l'OC.
Les rôles de confiance, dont dépend la sécurité de l'opération, doivent être clairement identifiés dans la DPC de l'OC. Ces rôles et les responsabilités associées doivent être documentés dans des descriptions de poste. Ces descriptions de poste doivent être effectuées du point de vue de la séparation des tâches et du moindre privilège. Aucune personne ne doit être autorisée à exécuter simultanément plusieurs rôles de confiance.

V.3.2. Mesures de sécurité vis-à-vis du personnel du Personnalisateur de Cartes (AND-CP)

Tout le personnel concerné par les activités du Personnalisateur de Cartes (AND-CP) doit être correctement formé et posséder les connaissances, l'expérience et les qualifications requises pour les services offerts et adaptées à la fonction exercée. Cela concerne le personnel employé directement par le Personnalisateur de Cartes (AND-CP), le personnel d'une société spécialisée pour laquelle des tâches ont été sous-traitées ou le personnel des contractants.

V.4. Procédures de constitution des données d'audit

V.4.1. Procédures de constitution des données d'audit, AND-CPCA

Tous les événements de sécurité significatifs générés par les logiciels de la AND-CPCA (plus exactement de l'OC) doivent être automatiquement horodatés et enregistrés dans les journaux du système. Ceux-ci incluent au moins les éléments suivants :

- Les tentatives, réussies et en échec, de création, de mise à jour, de suppression ou de récupération d'informations sur les comptes du personnel, et de création ou de révocation des privilèges d'un compte ;
- Les tentatives, réussies et en échec, de la définition ou de la modification de la méthode d'authentification (mot de passe, certificat biométrique ou cryptographique, par exemple) d'un compte utilisateur ;
- Les tentatives, réussies et en échec, de connexion et de déconnexion à un compte ;
- Les tentatives, réussies et en échec, de modification de la configuration logicielle ;
- Le démarrage et l'arrêt des logiciels ;
- Les mises à jour de logiciel ;
- Le démarrage et l'arrêt du système ;
- Les tentatives, réussies et en échec, d'ajouter ou de supprimer une entité du registre des abonnés pour lesquels la AND-CPCA fournit (via l'OC) des services de certification de clé, ou de modifier les informations de l'un des abonnés ou d'extraire des informations de ce registre ;
- Les tentatives, réussies et en échec, de traitement d'une demande de signature de certificat (KCR) ou d'une demande de distribution de clé (KDR) ;
- Les tentatives, réussies et en échec, de signature d'un certificat (*ENT*.C) ou de génération d'un message de distribution de clé (KDM) ;
- Les interactions, réussies et en échec, avec la ou les bases de données contenant des informations sur les (statuts des) certificats émis, y compris les tentatives de connexion et les opérations de lecture, d'écriture, de mise à jour ou de suppression ;
- Les tentatives, réussies ou en échec, de connexion ou de déconnexion à un HSM ;
- Les tentatives, réussies ou en échec, d'authentification d'un utilisateur sur un HSM ;

- Les tentatives, réussies et en échec, de génération ou de destruction d'une bi-clé ou d'une clé symétrique à l'intérieur d'un HSM ;
- Tentatives, réussies et en échec, d'importer ou d'exporter une clé vers ou depuis un HSM ;
- Tentatives, réussies et en échec, de modifier l'état du cycle de vie de toute bi-clé ou de toute clé symétrique ;
- Tentatives, réussies et en échec, d'utilisation d'une clé privée ou symétrique à l'intérieur d'un HSM à quelque fin que ce soit.

Afin de pouvoir investiguer sur les incidents de sécurité, le journal système doit inclure, si possible, des informations permettant d'identifier la personne ou le compte ayant effectué les tâches système.
L'intégrité des journaux d'événements du système doit être assurée et les journaux d'événements doivent être protégés contre tout examen, modification, suppression ou destruction non autorisé. Les journaux des événements système doivent être sauvegardés et stockés en interne.

V.4.2. Procédures de constitution des données d'audit, Personnalisateur de Cartes (AND-CP)

Tous les événements de sécurité significatifs générés par le logiciel du Personnalisateur de Cartes (AND-CP) doivent être automatiquement horodatés et enregistrés dans les journaux d'événements du système.
Afin de pouvoir investiguer sur les incidents de sécurité, le journal système doit inclure, si possible, des informations permettant d'identifier la personne ou le compte ayant effectué les tâches système.
L'intégrité des journaux d'événements du système doit être conservée et les journaux d'événements doivent être protégés contre tout examen, modification, suppression ou destruction non autorisé. Les journaux d'événements du système doivent être sauvegardés et stockés en interne.

V.5. Archivage des données

Un résumé des événements à archiver doit être décrit dans les procédures internes et doit être conforme aux règles et réglementations en vigueur. La AND-CPCA (plus exactement l'OC) et le Personnalisateur de Cartes (AND-CP) mettent en œuvre les procédures d'archivage appropriées des enregistrements. Des mesures doivent être prises pour assurer l'intégrité, l'authenticité et la confidentialité des enregistrements.
Pour toutes les informations archivées, les périodes d'archivage sont indéterminées.
Des mesures doivent être prises pour garantir que les archives sont conservées sans risque raisonnable de perte.
Les événements mentionnés à la section V.4 doivent être contrôlé périodiquement en intégrité. Ces inspections ont lieu annuellement dans le cadre des audits périodiques de sécurité.

V.6. Renouvellement d'une clé

La AND-CPCA doit générer une nouvelle bi-clé (CPCA_Card.PK et *CPCA_Card.SK*) selon ses besoins. Une fois que la AND-CPCA a généré une nouvelle bi-clé, elle doit soumettre une demande de signature de certificat (KCR).
La AND-CPCA doit s'assurer que les clés de remplacement sont générées de manière contrôlé et conformément aux procédures définies dans la présente Politique de Certification.

V.7. Reprise suite à une compromission ou à un sinistre

V.7.1. Reprise suite à une compromission ou à un sinistre, AND-CPCA

La AND-CPCA doit définir (conjointement avec l'OC) les incidents de sécurité et les procédures de traitement des cas de compromission à travers une Procédure de Traitement des Incidents de Sécurité, qui doit être publiée à l'intention des administrateurs et des auditeurs.
La AND-CPCA doit mettre à jour (conjointement avec l'OC) un plan de continuité des activités détaillant la manière dont elle maintiendra ses services en cas d'incident affectant les opérations normales. Lors de la détection d'un incident, les opérations doivent être suspendues jusqu'à ce que le niveau de compromission soit établi. L'OC présume en outre que les progrès technologiques rendront ses systèmes informatiques obsolètes au fil du temps et définira en conséquence les mesures pour gérer l'obsolescence.
Les procédures de sauvegarde et de restauration de toutes les données pertinentes doivent être décrites dans un plan de sauvegarde et de restauration.
Les incidents suivants sont considérés comme des sinistres :

- compromission ou vol d'une clé privée (de la AND-CPCA) et/ou d'une clé maîtresse ;
- perte d'une clé privée (de la AND-CPCA) ;
- défaillance du matériel informatique.

La perte d'une clé maîtresse par la AND-CPCA (donc par l'OC) ne constitue pas un sinistre, l'ERCA assurant la conservation des clés maîtresses qu'elle génère (existence de plusieurs copies soumises à des contrôles périodiques).
La protection contre les pannes de matériel informatique est assurée par la redondance des équipements.

V.7.2. Reprise suite à une compromission ou à un sinistre, Personnalisateur de Cartes (AND-CP)

Le Personnalisateur de Cartes (AND-CP) doit rédiger un plan de traitement des incidents de sécurité et des compromissions des clés privées et/ou des clés maîtresses.

V.8. Cessation d'activité

V.8.1. Cessation d'activité, AND-CPCA

En cas de cessation de l'activité de AND-CPCA par l'entité désignée par la AND-CPA, cette dernière en informera l'EA et l'ERCA en indiquant le cas échéant la nouvelle AND-CPCA désignée. La AND-CPA doit s'assurer qu'au moins une AND-CPCA est opérationnelle à tout moment.
Le cas échéant, le contrat avec l'OC pourra être transféré entre l'entité cessant l'activité de AND-CPCA et la nouvelle entité désignée.

V.8.2. Cessation d'activité, OC

En cas de cessation de l'activité de l'OC pour opérer l'IGC (PKI) de la AND-CPCA, l'OC informera la AND-CPCA. La AND-CPCA recherchera un nouvel OC pouvant opérer son IGC (PKI). La AND-CPA est responsable devant

l'ERCA de la bonne gestion du transfert/cessation des activités.

V.8.3. Cessation d'activité, Personnalisateur de Cartes (AND-CP)

Si le Personnalisateur de Cartes (AND-CP) met fin à ses activités, la AND-CPCA ainsi que la AND-CPA doivent en être informées.
La AND-CPA informera l'Autorité Européenne (EA) et l'ERCA de cette cessation d'activité. Elle indiquera également à la AND-CPCA, l'EA et l'ERCA le nouveau Personnalisateur de Cartes qu'elle aura désigné.
La AND-CPA doit s'assurer qu'au moins un Personnalisateur de Cartes est opérationnel à tout moment dans le périmètre d'Andorre.

VI. Contrôles de sécurité techniques

VI.1. Génération et installation des bi-clés

VI.1.1. Bi-clés de la AND-CPCA

La AND-CPCA doit générer ses clés privées conformément à l'Appendice 1B [2]. La génération des bi-clés doit être effectuée dans un environnement physiquement sécurisé, par du personnel occupant des rôles de confiance et en « dual control ». La cérémonie de clé doit être documentée.
Le système de la AND-CPCA (plus exactement de l'OC) doit pouvoir effectuer des demandes de signature de certificats (KCR) et des demandes de distribution de clés maîtresses (KDR) auprès de l'ERCA selon les processus décrits aux chapitres IV.1 et IV.2.
L'OC devrait disposer d'un environnement de test AND-CPCA à des fins de test d'interopérabilité, conformément au Règlement (cf. Spécifications des Tests d'Interopérabilité des Equipements [7]). S'il est présent, l'environnement de test AND-CPCA doit être un environnement séparé et il doit posséder ses propres clés privées AND-CPCA et ses propres clés maîtresses.
L'environnement de test AND-CPCA doit pouvoir demander la signature de certificats de test et la distribution de clé maîtresse de test auprès de l'ERCA suivant les processus décrits aux chapitres IV.1 et IV.2IV.2.

L'environnement de test AND-CPCA doit également être en mesure de signer des certificats d'équipement (certificat cartes) de test à la demande du Personnalisateur de Cartes (AND-CP) et de distribuer la clé maîtresse de test à ce dernier.

VI.2. Protection des clés privées/symétriques et contrôles techniques des modules cryptographiques

La AND-CPCA (via l'OC) et le Personnalisateur de Cartes (AND-CP) doivent préserver la confidentialité, l'intégrité et la disponibilité des clés privées et des clés maîtresses, comme décrit ci-après.
Les clés privées et les clés maîtresses doivent être générées et utilisées dans un dispositif sécurisé qui :

- est certifié au niveau EAL 4 ou supérieure conformément à la norme ISO / IEC 15408 [8] ; ou au niveau E3 ou supérieur de ITSEC ; ou à des critères de sécurité équivalents. Les évaluations doivent être effectuées selon un profil de protection ou une cible de sécurité approprié ; ou
- répond aux exigences identifiées dans le CEN Workshop Agreement 14167-2 [9] ; ou
- répond aux exigences identifiées dans FIPS PUB 140-2 (ou FIPS 140-1) niveau 3 ou supérieur [10] ; ou
- démontre offrir un niveau de sécurité équivalent.

Le dispositif sécurisé le plus courant, destiné à être utilisé au sein d'une IGC (PKI), est le HSM (Hardware Security Module ou Module de Sécurité Matérielle). D'autres implémentations utilisant différents périphériques sont également possibles, à condition que les périphériques mis en œuvre répondent à l'une des exigences de sécurité énumérées ci-dessus. Outre ces exigences de sécurité, la présente Politique de Certification de la AND-CPA contient d'autres exigences fonctionnelles pour le module de sécurité matériel utilisé dans le système de l'OC dédié à la AND-CPCA. Il est à noter que si un périphérique différent est utilisé à la place d'un HSM, toutes ces exigences fonctionnelles doivent également être satisfaites. Le terme «HSM»

est utilisé de façon générique dans le document comme abréviation pour les exigences mentionnées ci-dessus.

Les opérations sur les clés privées et les opérations sur les clés maîtresses doivent être exécutées dans le HSM qui stocke ces clés.
Les clés privées et les clés maîtresses de la AND-CPCA et du Personnalisateur de Cartes (AND-CP) ne doivent être utilisées que dans un environnement physiquement sécurisé par du personnel occupant des rôles de confiance et en « dual control ». Tous les événements liés à l'utilisation des clés privées et à l'utilisation des clés maîtresses symétriques doivent être consignés.
Les clés privées de la AND-CPCA et du Personnalisateur de Cartes (AND-CP) ainsi que les clés maîtresses ne doivent être sauvegardées, stockées et recouvrées que par du personnel occupant des rôles de confiance et en « dual control » dans un environnement physiquement sécurisé.
Les copies de sauvegarde des clés privées de la AND-CPCA et du Personnalisateur de Cartes (AND-CP) ainsi que des clés maîtresses doivent être soumises au même niveau de contrôle de sécurité que les clés utilisées.
Une copie de sauvegarde de la clé privée de la AND-CPCA (*CPCA_Card.SK*) et une copie de chaque clé maîtresse doivent être conservées hors site.
L'importation et l'exportation de clés privées ne doivent avoir lieu qu'à des fins de sauvegarde et de restauration.
L'importation et l'exportation de clé maîtresse sont autorisées pour la sauvegarde et la restauration.
L'exportation de la clé maîtresse $K_{M\text{-}WC}$ sous forme cryptée est autorisée pour répondre à une demande valide de distribution de clé émanant du Personnalisateur de Cartes (AND-CP) par du personnel occupant des rôles de confiance et en « dual control ».
À la fin de la période d'utilisation d'une clé privée de la AND-CPCA ou des Personnalisateurs de Cartes (AND-CP), toutes les copies de la clé concernée doivent être détruites de manière à ce qu'elles ne puissent pas être récupérées. A défaut, si cette clé privée est conservée, son détenteur doit empêcher toute utilisation de cette dernière.
De même, à la fin du cycle de vie d'une clé maîtresse symétrique (comme spécifié à l'Appendice 1B [2]), la AND-CPCA et le Personnalisateur de Cartes (AND-CP) doivent détruire toutes les copies de la clé en leur possession, de telle sorte que cette clé ne puisse pas être recouvrée.

Les clés privées et les clés maîtresses doivent être désactivées et détruites en cas de compromission ou de suspicion de compromission. Les clés doivent être détruites après étude de cette compromission et prise de décision de désactiver cette clé.
La destruction des clés privées et des clés maîtresses doit être effectuée en utilisant la fonction de destruction du HSM. De même, les copies de sauvegarde des clés compromises doivent être détruites.

VI.3. Autres aspects de la gestion des bi-clés

Les certificats de clé publique de la AND-CPCA et par conséquent les clés publiques doivent être archivés indéfiniment.
Les périodes de validité de tous les certificats de la AND-CPCA doivent être conformes à l'Appendice 1B [2].
L'ERCA, par défaut, fixe la fin de validité des certificats de clé publique de la AND-CPCA pour les cartes tachygraphiques à 7 ans à compter de la date d'émission.
L'ERCA utilisera l'information End-of-validity spécifiée par la AND-CPCA dans la KCR si elle ne dépasse la limite de 7 ans.
Conformément à la Politique de l'ERCA, la période d'utilisation des clés privées de la AND-CPCA doit être de

deux ans maximum. Les périodes d'utilisation des clés privées doivent commencer à la date d'effet indiquée dans le certificat correspondant.
La AND-CPCA ne doit pas exploiter une clé privée après la fin de sa période d'utilisation.

VI.4. Données d'activation

Les clés privées de la AND-CPCA et/ou les clés maîtresses symétriques stockées dans le HSM doivent être activées que si toutes les personnes contrôlant les clés se sont authentifiées sur le HSM. L'authentification doit être effectuée en utilisant des moyens appropriés (par exemple, passphrases, jetons d'authentification). La durée d'une session d'authentification ne doit pas être illimitée. Une nouvelle authentification des utilisateurs doit être effectuées dans le cas où une réactivation de la ou des clés est nécessaire.
Pour l'activation du logiciel de la AND-CPCA (plus exactement de l'OC), l'authentification de l'utilisateur doit s'effectuer à l'aide de moyens appropriés (par exemple par une passphrase).

VI.5. Mesures de sécurité des systèmes informatiques

La AND-CPCA (plus exactement l'OC) et le Personnalisateur de Cartes (AND-CP) doivent spécifier et approuver des procédures et des mesures de sécurité techniques spécifiques pour la gestion de leurs systèmes informatiques. Ces procédures doivent garantir que le niveau de sécurité requis est toujours atteint. Les procédures et les mesures de sécurité techniques doivent être décrites dans des documentations internes et/ou des concepts de sécurité. Les systèmes informatiques doivent être conçus et gérés conformément à ces procédures, aux procédures spécifiées dans les concepts de sécurité et dans les bonnes pratiques pour la fiabilité et la confiance informatique.

VI.6. Mesures de sécurité des systèmes pendant leur cycle de vie

La AND-CPCA (plus exactement l'OC) et le Personnalisateur de Cartes (AND-CP) doivent effectuer une analyse des exigences de sécurité lors de la phase de conception et de spécifications afin de s'assurer de la prise en compte de la sécurité dans leurs systèmes.
Une séparation entre les systèmes de recette (ou de pré-production) et de production doit être maintenue. Les procédures de changement et les procédures de gestion de la sécurité doivent garantir que le niveau de sécurité requis est maintenu dans le système de Production.
Les procédures de contrôle des modifications doivent être documentées et utilisées pour les versions, les modifications et les correctifs logiciels (urgents) de tous les logiciels opérationnels.

VI.7. Mesures de sécurité réseau

La AND-CPCA (plus exactement l'OC) doit concevoir et mettre en œuvre une architecture réseau de manière à permettre que l'accès depuis Internet à son réseau interne et depuis le réseau interne vers les systèmes de l'OC puisse être contrôlé efficacement.
En particulier, la mise hors ligne complète du système de signature de l'Autorité de Certification (isoler du

réseau) doit être envisagée.

VI.8. Horodatage et système de datation

La date et l'heure d'un événement doivent être incluses dans chaque enregistrement de la piste d'audit. La Déclaration des Pratiques de Certification (DPC) de l'OC et la Politique relative au Personnalisateur de Cartes (AND-CP) doivent décrire comment le temps est synchronisé et vérifié.

VII.Profils des certificats, des CRL et OCSP

VII.1. Profil du certificat AND-CPCA

Le certificat de la AND-CPCA (*CPCA_Card.C*) doit avoir le profil suivant, tel que spécifié dans l'Appendice 1B [2] :

Champ	Octets	Explication
Signature	128	Primitive de signature RSAP1 (PKCS#1) [14] avec la clé privée RSA de l'ERCA (*EUR.SK*)
Fixed value	1	'6A'
C_r	106	106 premiers octets du Contenu du Certificat fourni dans la KCR
Hash	20	SHA-1(CC)
Fixed value	1	'BC'
C_n	58	58 derniers octets du Contenu du Certificat fourni dans la KCR
CAR	8	Voir Request

Tableau 6 - Profil du certificat de la AND-CPCA

VII.2. Format des Certificats Cartes

Les certificats Carte (*Card.C*) émis par la AND-CPCA doivent avoir le profil suivant, tel que spécifié dans l'Appendice 1B [2] :

Champ	Octets	Explication
Signature	128	Primitive de signature RSAP1 (PKCS#1) [14] avec la clé privée RSA de la AND-CPCA (*CPCA_Card.SK*)
Fixed value	1	'6A'
C_r	106	106 premiers octets du Contenu du Certificat fourni dans la KCR
Hash	20	SHA-1(CC)
Fixed value	1	'BC'
C_n	58	58 derniers octets du Contenu du Certificat fourni dans la KCR
CAR	8	Voir Request

Table 7 – Profil des certificats cartes

VII.3. Profil des CRL

Le statut des certificats émis par l'ERCA (c'est-à-dire les certificats des CPCA) peut être consulté sur le site web : https://dtc.jrc.ec.europa.eu/

Aucune CRL (Liste de Révocation des Certificats) n'est émise par la AND-CPCA.

VII.4. Profil OCSP

Aucun service OCSP ne doit être mis en œuvre.

VIII. Audit de conformité et autres évaluations

VIII.1. Fréquence et/ou circonstances des évaluations

VIII.1.1. Audit de la AND-CPCA

Un audit complet et formel de l'activité de la AND-CPCA et de l'OC doit être effectué sur ordre de la AND-CPA. L'audit de la AND-CPCA et respectivement de l'OC doit établir si les exigences portant sur la AND-CPCA et respectivement de l'OC et décrites dans le présent document sont respectées. La AND-CPA doit effectuer le premier audit dans les 12 mois suivant le début des opérations couvertes par la présente Politique de Certification.
Si aucune preuve de non-conformité n'est trouvée lors de l'audit, le prochain doit être effectué dans un délai de 24 mois. Dans le cas contraire, le prochain audit devra être effectué dans un délai de 12 mois afin de s'assurer que les non-conformités ont été levées.
La AND-CPA doit rendre compte des résultats de l'audit et fournir le rapport d'audit, en anglais, à l'ERCA. Ce rapport doit définir toutes les actions correctives requises pour remplir les obligations de la AND-CPA. Il inclut également un calendrier de mise en œuvre de ces actions correctives.

VIII.1.2. Audit du Personnalisateur de Cartes (AND-CP)

Un audit de l'activité du Personnalisateur de Cartes (AND-CP) doit être également être effectué sur ordre de la AND-CPA. Cet audit doit établir que les pratiques du Personnalisateur de Cartes (AND-CP) répondent aux exigences de la présente Politique de Certification. Le Personnalisateur de Cartes (AND-CP) doit, a minima, suivre le même schéma d'audit que la AND-CPCA et l'OC car il est responsable des clés privées (*Card.SK*) et de la clé maîtresse symétrique qu'il inscrit dans les cartes.
Avant le début des opérations couvertes par la présente politique de certification, la AND-CPA doit effectuer une évaluation pré-opérationnelle pour obtenir la preuve que l'organisation est en mesure de fonctionner conformément aux exigences de la présente politique de certification.
Pour que le AND-CP puisse accéder au service AND-CPCA, le fabricant de la carte (AND-CM) doit démontrer que l'équipement (carte) qu'il fournit au AND-CP a reçu les certifications ad hoc.

VIII.1.3. Audit de l'Emetteur de Cartes (AND-CIA)

La AND-CPCA peut, si elle le souhaite, auditer ou faire auditer l'Emetteur de Cartes (AND-CIA) pour s'assurer que les pratiques de ce dernier répondent aux exigences de la présente Politique de Certification, en particulier sur son rôle d'Autorité d'Enregistrement Déléguée.
La fréquence et le nombre de ces audits ne sont pas fixés par la présente PC.

VIII.2. Identité et qualification des évaluateurs

L'audit doit être effectué par un auditeur indépendant spécialiste dans les Technologies de l'Information.

Toute personne sélectionnée ou proposée pour effectuer un audit de conformité de la AND-CPCA et de l'OC doit d'abord être agréée par la AND-CPA.
Les noms des auditeurs agréés qui effectueront les audits doivent être enregistrés par la AND-CPA.
Ces auditeurs doivent respecter les exigences suivantes :

- Comportement éthique : loyauté, régularité et confidentialité dans ses relations avec l'Autorité de Certification à auditer et lors du traitement des informations et des données de cette dernière ;
- Exactitude des présentations : les constatations, conclusions ainsi que les rapports d'audit sont exacts et décrivent avec précision toutes les activités réalisées au cours de l'audit ;
- Approche professionnelle : l'auditeur possède un niveau élevé d'expertise et de compétences professionnelles et exploite de manière efficace son expérience acquise grâce à de bonnes pratiques dans les technologies de l'information, les IGC (PKI) et les normes et standards techniques connexes.

L'auditeur doit posséder une expérience significative dans, et de préférence être accrédité pour :

- les audits de sécurité des systèmes d'information ;
- les technologies IGC (PKI) et cryptographiques ;
- L'exploitation des logiciels IGC (PKI) ;
- Les Politiques et Réglementations de la Commission Européenne.

VIII.3. Relations entre évaluateurs et entités évaluées

L'auditeur doit être indépendant et ne pas être en lien avec l'entité faisant l'objet de l'audit, c'est-à-dire la AND-CPCA ou l'OC. Il ne doit souffrir d'aucun conflit d'intérêt avec ces dernières.

VIII.4. Sujets couverts par les évaluations

L'audit de la AND-CPCA, de l'OC et du Personnalisateur de Cartes (AND-CP) doit couvrir la conformité à la présente Politique de Certification, à la Déclaration des Pratiques de Certification de l'OC ainsi qu'aux procédures et techniques associées rédigées par la AND-CPCA et/ou l'OC.
L'objet de l'audit de conformité doit être la mise en œuvre des pratiques techniques, procédurales et organisationnelles décrites dans ces documents.
Les domaines d'intervention des audits sont entre autres les suivants :

- identification et authentification ;
- fonctions/services opérationnels ;
- contrôles de sécurité physiques, procéduraux et de sécurité du personnel ;
- contrôles de sécurité techniques .

L'analyse des journaux d'audit permet de déterminer si la sécurité des systèmes de la AND-CPCA (plus exactement de l'OC) présente des faiblesses. Ces éventuelles faiblesses doivent être réduites par des mesures appropriées. L'analyse ainsi que les faiblesses éventuelles doivent être enregistrées.

En cas d'audit exceptionnel déclenché par un incident de sécurité grave, l'audit doit se concentrer sur les processus et les mesures techniques en rapport avec l'incident de sécurité.

VIII.5. Actions prises suite aux conclusions d'une évaluation

VIII.5.1. Audit de la AND-CPCA et de l'OC

Si des non-conformités sont découvertes par l'auditeur, des actions correctives doivent être entreprises immédiatement par l'entité concernée (AND-CPCA ou OC). Une fois les mesures correctives appliquées, un audit de suivi doit être effectué dans un délai de 12 mois.

VIII.5.2. Audit du Personnalisateur de Cartes (AND-CP)

Si des non-conformités sont découvertes par l'auditeur, des actions correctives doivent être entreprises immédiatement par le AND-CP. Une fois les mesures correctives appliquées, un audit de suivi doit être effectué dans un délai de 12 mois.

VIII.5.3. Audit de l'Emetteur de Cartes (AND-CIA)

Si des non-conformités sont découvertes par l'auditeur, des actions correctives doivent être entreprises immédiatement par l'Emetteur de Cartes (AND-CIA). La AND-CPCA pourra, si elle le souhaite, effectuer un audit de suivi. La présente PC ne fixe aucun délai pour cet audit.

VIII.6. Communication des résultats

VIII.6.1. Audit de la AND-CPCA et de l'OC

L'auditeur indépendant doit communiquer les résultats complets de l'audit de conformité de la AND-CPCA et de l'OC (en français) à la AND-CPA, le commanditaire de l'audit. Le AND-CPA doit envoyer à l'ERCA le rapport d'audit (en anglais) de l'activité de la AND-CPCA et indirectement de l'OC intégrant les conclusions de cet audit. Ce rapport doit comprendre a minima le nombre d'écarts trouvés et la nature de chaque écart. La date de réception du rapport d'audit doit être publiée sur le site web de l'ERCA.
Sur demande de l'ERCA, la AND-CPA doit envoyer à cette dernière l'intégralité des résultats de l'audit de conformité.

VIII.6.2. Audit du AND-CP

Les résultats et le rapport d'audit de conformité du Personnalisateur de Cartes doivent être communiqués à la AND-CPA, le commanditaire de l'audit. Ce rapport doit comprendre a minima le nombre d'écarts trouvés et la nature de chaque écart.

VIII.6.3. Audit de l'Emetteur de Cartes (AND-CIA)

Les résultats et le rapport d'audit de conformité de l'Emetteur de Cartes (AND-CIA) doivent être communiqués à la AND-CPCA, le commanditaire de l'audit. Ce rapport doit comprendre a minima le nombre d'écarts trouvés et la nature de chaque écart.

IX. Autres problématiques métier et légales

IX.1. Tarifs

La AND-CPCA a souscrit un contrat de services auprès de l'entité « IN Groupe ». Ces services couvrent :

- Les services de l'OC
- Les services du AND-CP
- Les services du AND-CM

Ces services sont facturés à la AND-CPCA selon les termes du contrat signé entre les parties.

IX.2. Responsabilité financière

Aucune stipulation

IX.3. Confidentialité des informations professionnelles

Les données confidentielles doivent comprendre a minima :

- Les données personnelles (par exemple, données des employés de la AND-CPCA, de l'OC, du Personnalisateur de Cartes ou des représentants de l'ERCA) ;
- Les clés privées ;
- Les clés maîtresses symétriques ;
- Les raisons de la révocation des certificats ;
- Les journaux d'audit (sauf si l'accès est requis par une décision de justice, par les réglementations ou par les dispositions de la PC ou de la DPC) ;
- La documentation détaillée concernant la gestion de l'IGC (PKI) ;
- Les rapports d'audit des auditeurs internes ou externes.

Les données confidentielles ne doivent pas être divulguées, sauf en cas d'obligation légale.

IX.4. Protection des informations personnelles

Les seules données personnelles traitées ou stockées dans le système de la AND-CPCA et/ou de l'OC sont celles des représentants de l'ERCA, de la AND-CPCA ainsi que celles des Personnalisateurs de Cartes.
Ces données doivent être traitées conformément au Règlement Général de la Protection des Données 2016/679 (RGPD).

IX.5. Droits sur la propriété intellectuelle et industrielle

La AND-CPCA n'est pas propriétaire du logiciel que l'OC met en œuvre dans le cadre de l'exploitation de l'IGC (PKI) du système Tachygraphe Numérique.

IX.6. Interprétations contractuelles et garanties

La AND-CPCA et l'OC doivent agir en vertu de la Politique de Certification de l'ERCA [6], de la présente Politique de Certification et, également pour l'OC, en vertu de la Déclaration des Pratiques de Certification (DPC) qu'il a rédigée.

IX.7. Exclusions de garantie

La AND-CPA et la AND-CPCA déclinent toute garantie commerciale et obligation de quelque type que ce soit. Elles déclinent également toute responsabilité pour négligence et manque de diligence raisonnable de la part des abonnés et des parties utilisatrices.

IX.8. Limites de responsabilité

Il est expressément entendu que, ni la AND-CPA, ni la AND-CPCA ne saurait être tenue pour responsable, ni d'un dommage résultant d'une faute ou négligence d'un abonné, ni d'un dommage causé par un fait extérieur, notamment en cas de :

- Utilisation d'un certificat pour une autre application que les applications définies au chapitre I.4 de la présente PC ;
- Utilisation frauduleuse ou négligente d'un certificat ou des informations de statut d'un certificat émis par la AND-CPCA via l'OC ;
- Utilisation d'un certificat pour garantir un autre objet que l'identité de l'équipement (carte) pour lequel le certificat a été émis ;
- Utilisation d'un certificat au-delà de sa limite de validité ;
- Non-respect par les entités concernées de leurs obligations définies dans la présente PC ;
- Faits extérieurs à l'émission du certificat tels qu'une défaillance de l'application ou de l'équipement (carte) pour lequel il a été émis ;
- Force majeure comme définie par les tribunaux français.

Les abonnés et les parties utilisatrices des services de la AND-CPCA ne peuvent prétendre à aucune indemnisation pour les pertes résultant d'une utilisation inappropriée ou frauduleuse du système de gestion de clés de la AND-CPCA.
La responsabilité de la AND-CPCA ou de l'OC ne peut être engagée que si il est démontré qu'elles ont agi de manière non conforme à la présente Politique de Certification et, uniquement pour l'OC, à la Déclaration des Pratiques de Certification qu'il a rédigée.

IX.9. Indemnités

Aucune stipulation

IX.10. Durée et fin anticipée de validité de la PC

Cette politique de certification est valide dès son approbation par la AND-CPA et le JRC. Elle reste valable jusqu'à nouvel ordre.
La validité de cette politique de certification prend fin lorsque la AND-CPA cesse son activité ou dès lors qu'elle annonce que cette politique n'est plus valide (par exemple une nouvelle version de politique a pris effet).

IX.11. Notifications individuelles et communications entre les Participants

Les avis officiels et les communications avec les participants au système de gestion de clés du Tachygraphe Numérique doivent être écrits et soumis aux procédures d'enregistrement de la correspondance en vigueur au sein du Transport Andorran.
La scission ou la fusion peuvent entraîner des modifications du champ d'application, de la gestion et/ou du fonctionnement de la AND-CPCA. Dans ce cas, la présente Politique de Certification ainsi que la Déclaration des Pratiques de certification de l'OC pourront également nécessiter des modifications. Les changements apportés à ces documents doivent être effectuées conformément aux exigences administratives stipulées au chapitre IX.12 ci-après.

IX.12. Amendements à la PC

Cette Politique de Certification est publiée sous la responsabilité de la AND-CPA. La AND-CPA peut réviser cette PC si elle le juge nécessaire.
La procédure à suivre pour les propositions de modification et l'approbation de la présente PC est la suivante:

1. Les commentaires ou les demandes de modification de la PC peuvent être adressés par la AND-CPCA ou le Personnalisateur de Cartes à la AND-CPA. Cette communication doit inclure une description des commentaires ou des modifications demandées, une justification ainsi que les informations de contact de la personne qui les a soumises.
2. La AND-CPA doit soit accepter, soit accepter avec modifications, soit rejeter les commentaires/modifications proposées après l'expiration de la période de commentaire (fixée de façon appropriée par la AND-CPA). Les modifications proposées par la AND-CPCA ou le Personnalisateur de Cartes (AND-CP) sont examinées par la AND-CPA. Les décisions concernant les propositions de modification sont laissées au libre arbitre de la AND-CPA.
3. Une nouvelle version de cette Politique de Certification sera publiée sur le site Web de la AND-CPA et transmise à l'ERCA, la AND-CPCA, l'OC, le Personnalisateur de Cartes (AND-CP) ainsi qu'à l'Emetteur de Cartes (AND-CIA).

Toute modification de la présente PC doit s'accompagner d'une augmentation du numéro de version du document. Les seules modifications pouvant être apportées à la PC et à la DPC sans modification du numéro de version du document ne concernent que les corrections rédactionnelles ou typographiques.
La AND-CPCA peut modifier les informations de contact du chapitre I.5 en informant la AND-CPA et l'ERCA, mais sans modifier le numéro de version du document. Toutes les autres modifications apportées à la PC

doivent être effectuées conformément à la procédure de modification décrite dans cette section.

IX.13. Dispositions concernant la résolution de conflits

Tout différend relatif à la gestion des clés maîtresses et des certificats du système Tachygraphe Numérique entre la AND-CPCA et une organisation ou une personne extérieure à la AND-CPCA et à l'OC doit être résolu à l'aide de la procédure ad-hoc de règlement des différends. Le différend doit être résolu si possible à l'amiable. En cas d'échec de règlement à l'amiable, il faudra recourir à l'arbitrage de la AND-CPA.

IX.14. Conformité aux législations et réglementations

Cette Politique de Certification est conforme à l'Accord AETR [2]. En cas de divergence entre le présent document et le Règlement, ce dernier prévaut.

IX.15. Dispositions diverses

Aucune stipulation

IX.16. Autres dispositions

Aucune stipulation

X. Annexe A : Liste des schémas

Schéma 1 : Relation entre les différentes entités intervenant dans le schéma Andorran
Schéma 2 : workflow au sein de l'IGC dans le contexte Andorran

XI. Annexe B : Liste des tableaux

XII. Annexe C : Références

1. Règlement (UE) N° 3821/85 du Parlement européen et du Conseil du 4 Février 2014, Journal Officiel de l'Union Européenne L60
2. Accord européen relatif au travail des équipages des véhicules effectuant des transports internationaux par route (AETR), en date du 1er juillet 1970
3. ETSI EN 319 411–1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements, version 1.1.1, 2016-02
4. RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003
5. RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997
6. Tachygraphe Numérique – Politique de Certification de l'ERCA, JRC, version 2.1
7. Tachygraphe Intelligent – Spécifications des Tests d'Interopérabilité des Equipements, JRC, version 1.0
8. ISO/IEC 15408-1:2009 Information technology — Security techniques — Evaluation criteria for IT security
9. CEN Workshop Agreement 14167-2 : Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 2 Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)
10. National Institute of Standards and Technology (NIST), FIPS PUB 140-2, Security requirements for cryptographic modules, May 25, 2001
11. ISO/IEC 9660:1988, Information processing – Volume and file structure of CD-ROM for information interchange
12. ISO/IEC 27001:2018, Information technology – Security techniques – Information security risk management systems -- Requirements
13. ISO/IEC 27005:2018, Information technology – Security techniques – Information security risk management
14. PKCS#1 v2.0 : RSA Cryptography Standard, RSA Laboratories, 1er Octobre 1998
15. TDES : National Institute of Standards and Technology (NIST). FIPS Publication 46-3: Data Encryption Standard. Projet de norme 1999