COMMISSION
EUROPÉENNE

Bruxelles, le 13.3.2019
C(2019) 1789 final

ANNEX 3

ANNEXE

du

Règlement délégué de la Commission

complétant la directive 2010/40/UE du Parlement européen et du Conseil en ce qui concerne le déploiement et l'utilisation opérationnelle des systèmes de transport intelligents coopératifs

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

TABLE DES MATIÈRES

1. Introduction 8
1.1. Aperçu et champ d'application de la présente politique 8
1.2. Définitions et acronymes 10
1.3. Participants à la PKI 13
1.3.1. Introduction 13
1.3.2. Autorité de politique de certification des STI-C 17
1.3.3. Gestionnaire de la liste de confiance (TLM) 18
1.3.4. Auditeur agréé de la PKI 18
1.3.5. Point de contact des STI-C (CPOC) 18
1.3.6. Rôles opérationnels 19
1.4. Usage des certificats 20
1.4.1. Domaines d'utilisation applicables 20
1.4.2. Limites de responsabilité 20
1.5. Administration de la politique de certification 20
1.5.1. Mise à jour des CPS des CA énumérées dans l'ECTL 20
1.5.2. Procédure d'approbation des CPS 21
2. Responsabilités en matière de publication et de répertoires 22
2.1. Méthodes de publication des informations des certificats 22
2.2. Date ou fréquence de publication 22
2.3. Répertoires 23
2.4. Contrôles d'accès sur les répertoires 23
2.5. Publication des informations des certificats 24
2.5.1. Publication des informations des certificats par le TLM 24
2.5.2. Publication des informations des certificats par les CA 24
3. Identification et authentification 25
3.1. Nommage 25
3.1.1. Types de nom 25
3.1.1.1. Noms pour les TLM, les CA racine, les EA et les AA 25
3.1.1.2. Noms des entités finales 25
3.1.1.3. Identification des certificats 25
3.1.2. Nécessité d'utiliser des noms explicites 25
3.1.3. Anonymat et emploi de pseudonymes pour les entités finales 25
3.1.4. Règles d'interprétation des diverses formes de noms 25
3.1.5. Unicité des noms 26

3.2. Validation initiale de l'identité 26
3.2.1. Méthode visant à prouver la possession d'une clé privée 26
3.2.2. Authentification de l'identité d'une organisation 26
3.2.2.1. Authentification de l'identité d'une organisation de CA racine 26
3.2.2.2. Authentification de l'identité d'une organisation de TLM 27
3.2.2.3. Authentification de l'identité d'une organisation de sous-CA 27
3.2.2.4. Authentification de l'organisation du souscripteur des entités finales 28
3.2.3. Authentification de l'entité individuelle 28
3.2.3.1. Authentification de l'entité individuelle du TLM/de la CA 28
3.2.3.2. Authentification de l'identité du souscripteur des stations STI-C 29
3.2.3.3. Authentification de l'identité des stations STI-C 29
3.2.4. Renseignements non vérifiés sur le souscripteur 30
3.2.5. Validation de l'autorité 30
3.2.5.1. Validation du TLM, de la CA racine, de l'EA et de l'AA 30
3.2.5.2. Validation des souscripteurs de la station STI-C 30
3.2.5.3. Validation des stations STI-C 30
3.2.6. Critères d'interopérabilité 30
3.3. Identification et authentification des demandes de régénération de clés 31
3.3.1. Identification et authentification pour régénération de clé courante 31
3.3.1.1. Certificats du TLM 31
3.3.1.2. Certificats de la CA racine 31
3.3.1.3. Régénération de clé ou renouvellement du certificat d'EA /AA 31
3.3.1.4. Authentifiants d'inscription des entités finales 31
3.3.1.5. Tickets d'autorisation des entités finales 31
3.3.2. Identification et authentification pour régénération de clés après révocation 32
3.3.2.1. Certificats de CA 32
3.3.2.2. Authentifiants d'inscription des entités finales 32
3.3.2.3. Demandes d'autorisation des entités finales 32
3.4. Identification et authentification des demandes de révocation 32
3.4.1. Certificats de CA racine/EA /AA 32
3.4.2. Authentifiants d'inscription de la station STI-C 32
3.4.3. Tickets d'autorisation de la station STI-C 32
4. Exigences opérationnelles du cycle de vie des certificats 33
4.1. Demande de certificat 33
4.1.1. Qui peut présenter une demande de certificat 33

4.1.1.1. CA racine 33
4.1.1.2. TLM 33
4.1.1.3. EA et AA 33
4.1.1.4. Station STI-C 33
4.1.2. Processus d'inscription et responsabilités 33
4.1.2.1. CA racine 34
4.1.2.2. TLM 34
4.1.2.3. EA et AA 34
4.1.2.4. Station STI-C 35
4.2. Traitement des demandes de certificat 36
4.2.1. Exécution des fonctions d'identification et d'authentification 36
4.2.1.1. Identification et authentification des CA racine 36
4.2.1.2. Identification et authentification du TLM 36
4.2.1.3. Identification et authentification de l'EA et l'AA 36
4.2.1.4. Identification et authentification du souscripteur EE 36
4.2.1.5. Tickets d'autorisation 37
4.2.2. Approbation ou rejet des demandes de certificat 37
4.2.2.1. Approbation ou rejet des certificats de la CA racine 37
4.2.2.2. Approbation ou rejet du certificat du TLM 37
4.2.2.3. Approbation ou rejet des certificats de l'EA et de l'AA 37
4.2.2.4. Approbation ou rejet de l'EC 37
4.2.2.5. Approbation ou rejet de l'AT 37
4.2.3. Délai de traitement des demandes de certificat 38
4.2.3.1. Demande de certificat de CA racine 38
4.2.3.2. Demande de certificat du TLM 38
4.2.3.3. Demande de certificat de l'EA et de l'AA 38
4.2.3.4. Demande d'EC 38
4.2.3.5. Demande d'AT 38
4.3. Délivrance des certificats 38
4.3.1. Tâches de la CA lors de la délivrance des certificats 38
4.3.1.1. Délivrance de certificat par la CA racine 38
4.3.1.2. Délivrance de certificat du TLM 38
4.3.1.3. Délivrance de certificat d'EA et AA 38
4.3.1.4. Délivrance de l'EC 39
4.3.1.5. Délivrance d'AT 39

4.3.2. Notification au souscripteur de la délivrance des certificats par la CA 39
4.4. Acceptation des certificats 39
4.4.1. Acceptation des certificats 39
4.4.1.1. CA racine 39
4.4.1.2. TLM 39
4.4.1.3. EA et AA 40
4.4.1.4. Station STI-C 40
4.4.2. Publication du certificat 40
4.4.3. Notification de la délivrance des certificats 40
4.5. Utilisation des paires de clés et des certificats 40
4.5.1. Utilisation de la clé privée et du certificat 40
4.5.1.1. Utilisation de la clé privée et du certificat pour le TLM 40
4.5.1.2. Utilisation de la clé privée et du certificat pour les CA racine 40
4.5.1.3. Utilisation de la clé privée et du certificat pour les EA et les AA 40
4.5.1.4. Utilisation de la clé privée et du certificat pour l'entité finale 41
4.5.2. Utilisation du certificat et de la clé publique par une partie utilisatrice 41
4.6. Renouvellement de certificat 41
4.7. Régénération de clés de certificat 41
4.7.1. Circonstances de la régénération des clés de certificat 41
4.7.2. Qui peut demander la régénération 41
4.7.2.1. CA racine 41
4.7.2.2. TLM 41
4.7.2.3. EA et AA 41
4.7.2.4. station STI-C 42
4.7.3. Traitement des demandes de régénération des clés de certificat 42
4.7.3.1. Certificat du TLM 42
4.7.3.2. Certificat de CA racine 42
4.7.3.3. certificats d'EA et d'AA 42
4.7.3.4. Certificats de la station STI-C 43
4.8. Modification d'un certificat 43
4.9. Révocation et suspension de certificat 43
4.10. Services d'état des certificats 43
4.10.1. Caractéristiques opérationnelles 43
4.10.2. Disponibilité du service 43
4.10.3. Caractéristiques optionnelles 43

4.11. Fin de la souscription 43
4.12. Séquestre et récupération des clés 43
4.12.1. Souscripteur 43
4.12.1.1. Quelles paires de clés peuvent être mises sous séquestre 43
4.12.1.2. Qui peut présenter une demande de récupération 43
4.12.1.3. Processus de récupération et responsabilités 43
4.12.1.4. Identification et authentification 44
4.12.1.5. Approbation ou rejet des demandes de récupération 44
4.12.1.6. Actions KEA et KRA pendant la récupération de la paire de clés 44
4.12.1.7. Disponibilité de KEA et KRA 44
4.12.2. Politique et pratiques d'encapsulation et de récupération des clés de session 44
5. Installation, gestion et contrôles opérationnels 44
5.1. Contrôles physiques 44
5.1.1. Emplacement et construction des installations 44
5.1.1.1. CA racine, CPOC, TLM 44
5.1.1.2. EA/AA 45
5.1.2. Accès physique 45
5.1.2.1. CA racine, CPOC, TLM 45
5.1.2.2. EA/AA 46
5.1.3. Alimentation électrique et climatisation 46
5.1.4. Exposition à l'eau 47
5.1.5. Prévention et protection contre les incendies 47
5.1.6. Gestion des supports 47
5.1.7. Élimination des déchets 47
5.1.8. Sauvegarde hors site 48
5.1.8.1. CA racine, CPOC et TLM 48
5.1.8.2. EA/AA 48
5.2. Contrôles des procédures 48
5.2.1. Rôles de confiance 48
5.2.2. Nombre de personnes requises par tâche 49
5.2.3. Identification et authentification pour chaque rôle 49
5.2.4. Rôles nécessitant une séparation des tâches 50
5.3. Contrôles du personnel 51
5.3.1. Exigences en matière de qualifications, d'expérience et d'habilitation de sécurité 51
5.3.2. Procédures de vérification des antécédents 51

5.3.3. Exigences en matière de formation 52
5.3.4. Fréquence et exigences en matière de recyclage 52
5.3.5. Fréquence et séquence de rotation des postes 52
5.3.6. Sanctions pour des actions non autorisées 52
5.3.7. Exigences concernant les contractants indépendants 53
5.3.8. Documentation fournie au personnel 53
5.4. Procédures relatives aux journaux d'audit 53
5.4.1. Types d'événements à enregistrer et à signaler par chaque CA 53
5.4.2. Fréquence de traitement des journaux 55
5.4.3. Période de conservation des journaux d'audit 55
5.4.4. Protection des journaux d'audit 55
5.4.5. Procédures de sauvegarde des journaux d'audit 55
5.4.6. Système de collecte des audits (interne ou externe) 56
5.4.7. Notification du sujet ayant causé un événement 56
5.4.8. Évaluation des vulnérabilités 56
5.5. Archivage des enregistrements 57
5.5.1. Types d'enregistrements archivés 57
5.5.2. Période de conservation des archives 58
5.5.3. Protection des archives 59
5.5.4. Archives système et stockage 59
5.5.5. Exigences d'horodatage des enregistrements 59
5.5.6. Système de collecte des archives (interne ou externe) 59
5.5.7. Procédures d'obtention et de vérification des informations archivées 59
5.6. Changement de clés pour les éléments du modèle de confiance des STI-C 59
5.6.1. TLM 59
5.6.2. CA racine 60
5.6.3. Certificat d'EA/AA 60
5.6.4. Auditeur 60
5.7. Compromission et reprise après sinistre 60
5.7.1. Traitement des incidents et des compromissions 60
5.7.2. Corruption des ressources informatiques, des logiciels et/ou des données 61
5.7.3. Procédures en cas de compromission de la clé privée d'une entité 61
5.7.4. Capacités en matière de continuité des activités après un sinistre 62
5.8. Cessation et transfert 62
5.8.1. TLM 62

5.8.2. CA racine 63
5.8.3. EA/AA 63
6. Contrôles techniques de sécurité 64
6.1. Génération et installation des paires de clés 64
6.1.1. TLM, CA racine, EA et AA 64
6.1.2. EE — station STI-C mobile 64
6.1.3. EE — station STI-C fixe 64
6.1.4. Exigences cryptographiques 65
6.1.4.1. Algorithme et longueur de la clé - algorithmes de signature 65
6.1.4.2. Algorithme et longueur de la clé - algorithmes de chiffrement pour l'inscription et l'autorisation 66
6.1.4.3. Crypto-agilité 67
6.1.5. Stockage sécurisé de clés privées 67
6.1.5.1. Niveau CA racine, sous-CA et TLM 67
6.1.5.2. Entité finale 68
6.1.6. Sauvegarde de clés privées 69
6.1.7. Destruction de clés privées 69
6.2. Données d'activation 69
6.3. Contrôles de sécurité informatique 69
6.4. Contrôles techniques tout au long du cycle de vie 69
6.5. Contrôles de sécurité du réseau 70
7. Profils de certificats, CRL et ECTL 70
7.1. Profil de certificats 70
7.2. Validité des certificats 70
7.2.1. Certificats de pseudonymes 71
7.2.2. Tickets d'autorisation pour les stations STI-C fixes 72
7.3. Révocation de certificats 72
7.3.1. Révocation de certificats de la CA, l'EA et l'AA 72
7.3.2. Révocation de certificats d'inscription 72
7.3.3. Révocation de tickets d'autorisation 73
7.4. Liste de révocation de certificats 73
7.5. Liste de confiance européenne des certificats 73
8. Vérification de la conformité et autres évaluations 73
8.1. Sujets faisant l'objet d'audits et fondement des audits 73
8.2. Fréquence des audits 74
8.3. Identité/qualifications de l'auditeur 74

8.4. Lien entre l'auditeur et l'entité soumise à audit 74
8.5. Mesures prises à la suite du constat de lacunes 74
8.6. Communication des résultats 75
9. Autres dispositions 75
9.1. Redevances 75
9.2. Responsabilité financière 75
9.3. Confidentialité des informations opérationnelles 76
9.4. Plan en matière de protection de la vie privée 76
10. Références 76

ANNEXE III

1. INTRODUCTION

1.1. Aperçu et champ d'application de la présente politique

La présente politique de certification définit le modèle de confiance européen des STI-C sur la base de l'infrastructure à clés publiques (PKI) dans le cadre du système de l'UE pour la gestion des authentifiants de sécurité des services STI-C (CCMS de l'UE). Elle définit les exigences de gestion des certificats de clé publique pour les applications STI-C par les entités qui les ont délivrés et leur usage par les entités finales en Europe. À son plus haut niveau, la PKI est composée d'un ensemble de CA racine «activées» à la suite de l'insertion par le gestionnaire de la liste de confiance (TLM) des certificats dans une liste de confiance européenne des certificats (ECTL), qui est établie et publiée par le TLM de l'entité centrale (voir sections 1.2 et 1.3).

La politique est contraignante pour l'ensemble des entités participant au système de confiance des STI-C en Europe. Elle est utile pour l'évaluation du niveau de confiance que tout récepteur d'un message authentifié par un certificat d'entité finale de la PKI peut accorder aux informations reçues. Pour permettre l'évaluation de la confiance dans les certificats fournis par le CCMS de l'UE, la politique énonce une série contraignante d'exigences pour le fonctionnement du TLM de l'entité centrale et l'établissement et la gestion de l'ECTL. Par conséquent, le présent document régit les aspects suivants liés à l'ECTL:

- identification et authentification des donneurs d'ordre obtenant les rôles de PKI pour le TLM, y compris des déclarations des privilèges octroyés à chaque rôle;
- exigences minimales relatives aux pratiques de sécurité locale pour le TLM, notamment les contrôles physiques, du personnel et des procédures;
- exigences minimales relatives aux pratiques de sécurité technique pour le TLM, y compris les contrôles techniques de sécurité informatique, de sécurité réseau et des modules cryptographiques;
- exigences minimales relatives aux pratiques opérationnelles pour le TLM, y compris l'enregistrement de nouveaux certificats de CA racine, la radiation temporaire ou permanente des CA racine existantes incluses, et la publication et la répartition des mises à jour de l'ECTL;
- un profil ECTL, y compris tous les champs de données obligatoires et optionnels dans l'ECTL, les algorithmes cryptographiques à utiliser, le format ECTL exact et les recommandations pour le traitement de l'ECTL;
- gestion du cycle de vie des certificats ECTL, y compris la répartition des certificats ECTL, leur activation, leur expiration et leur révocation;
- gestion de la révocation de la confiance des CA racine si nécessaire.

Étant donné que la fiabilité de l'ECTL ne dépend pas uniquement de l'ECTL en elle-même mais aussi, dans une large mesure, des CA racine qui composent la PKI et leurs sous-CA, la présente politique énonce également des exigences minimales, qui sont impératives pour toutes les CA participantes (CA racine et sous-CA). Les exigences sont les suivantes:

- identification et authentification des donneurs d'ordre obtenant les rôles de la PKI (par exemple, agent de sécurité, agent chargé de la protection de la vie privée, administrations chargées de la sécurité, administrateur de registre et utilisateur final), y compris une déclaration des tâches, des responsabilités, des engagements et des privilèges associés à chaque rôle;
- gestion des clés, y compris des algorithmes de signature de données et de signature de certificats acceptables et obligatoires, et des périodes de validité des certificats;
- exigences minimales relatives aux pratiques de sécurité locale, notamment des contrôles physiques, du personnel et des procédures;
- exigences minimales relatives aux pratiques de sécurité technique, telles que les contrôles techniques de sécurité informatique, de sécurité réseau et des modules cryptographiques;
- exigences minimales relatives aux pratiques opérationnelles de la CA, l'EA, l'AA et des entités finales, y compris les aspects liés à l'enregistrement, l'annulation de l'enregistrement (c'est-à-dire la radiation), la révocation, la compromission des clés, le licenciement motivé, la mise à jour du certificat, les pratiques de vérification et la non-divulgation des informations relatives à la vie privée;
- certificat et profil de la CRL, y compris les formats, les algorithmes acceptables, les champs de données obligatoires et optionnels et leur plage de valeurs valides, ainsi que la manière dont les vérificateurs doivent traiter les certificats;
- opérations régulières de suivi, notification, alerte et tâches de rétablissement des entités du modèle de confiance des STI-C afin d'établir un fonctionnement sécurisé, y compris en cas de comportement répréhensible.

Outre ces exigences minimales, les entités qui gèrent les CA racine et les sous-CA peuvent décider de leurs propres exigences supplémentaires et les établir dans les déclarations de pratiques de certification (CPS) concernées, à condition qu'elles ne contredisent pas les exigences établies dans la politique de certification (CP). Voir section 1.5 pour obtenir des précisions sur la manière dont les CPS sont vérifiées et publiées.

La CP énonce également les fins auxquelles les CA racine, les sous-CA et leurs certificats délivrés peuvent être utilisés. Elle présente les engagements assumés par:

- le TLM;
- chaque CA racine dont les certificats sont énumérés dans l'ECTL;
- les sous-CA de la CA racine (EA et AA);
- chaque membre ou organisation responsable ou gestionnaire de l'une des entités du modèle de confiance des STI-C.

La CP définit également les obligations impératives s'appliquant:

- au TLM;
- chaque CA racine dont les certificats sont énumérés dans l'ECTL;
- à chaque sous-CA certifié par une CA racine;

- à l'ensemble des entités finales;
- à chaque membre ou organisation responsable ou gestionnaire de l'une des entités du modèle de confiance des STI-C.

Enfin, la CP établit les exigences relatives à la documentation des limitations des responsabilités et obligations figurant dans la CPS de chaque CA racine dont les certificats sont énumérés dans l'ECTL.

La présente CP est conforme à la politique de certification et au cadre de pratiques de certification adoptés par l'Internet Engineering Task Force (IETF) [3].

1.2. Définitions et acronymes

Les définitions de [2], [3] et [4] sont applicables.

AA	Autorité d'autorisation *(authorisation authority)*
AT	Ticket d'autorisation (*authorisation ticket*)
CA	Autorité de certification (*certification authority*)
CP	Politique de certification (*certificate policy*)
CPA	Autorité de politique de certification des STI-C (*C-ITS certificate policy authority*)
CPOC	Point de contact STI-C (*C-ITS point of contact*)
CPS	Déclaration de pratiques de certification (*certificate practice statement*)
CRL	Liste de révocation de certificats (*certificate revocation list*)
EA	Autorité d'inscription (*enrolment authority*)
EC	Authentifiant d'inscription (*enrolment credential*)
ECIES	Système de chiffrement intégré à base de courbes elliptiques (*Elliptic curve integrated encryption scheme*)
EE	Entité finale (station STI-C par exemple) (*end-entity*)
ECTL	Liste de confiance européenne des certificats (*European certificate trust list*)
CCMS de l'UE	Système de l'UE pour la gestion des authentifiants de sécurité des services STI-C (*EU C-ITS security credential management system)*
RGPD	Règlement général sur la protection des données
HSM	Module matériel de sécurité (*Hardware security module)*
PKI	Infrastructure à clés publiques (*public key infrastructure*)
RA	Autorité d'enregistrement (*registration authority*)

sous-CA	EA et AA
TLM	Gestionnaire de liste de confiance (*trust list manager*)

Glossaire

demandeur	La personne physique ou l'entité juridique qui demande un certificat ou le renouvellement de ce dernier. Lorsque le certificat initial est créé (initialisation), le demandeur est désigné comme étant le souscripteur. Pour les certificats délivrés aux entités finales, le souscripteur (demandeur du certificat) est l'entité chargée de contrôler ou de diriger/maintenir l'entité finale à laquelle le certificat est délivré, même si l'entité finale envoie la demande effective de certificat.
autorité d'autorisation	Dans le présent document, le terme «autorité d'autorisation» (AA) fait référence non seulement à la fonction spécifique de l'AA, mais également à l'entité juridique et/ou opérationnelle qui la gère.
autorité de certification	l'autorité de certification racine, l'autorité d'inscription et l'autorité d'autorisation sont conjointement désignées sous la dénomination «autorité de certification» (CA).
modèle de confiance des STI-C	Le modèle de confiance des STI-C est chargé d'établir une relation de confiance entre les stations STI-C. Il est mis en œuvre au moyen d'une PKI composée des CA racine, du CPOC, du TLM, des EA, des AA et d'un réseau sécurisé.
crypto-agilité	La capacité des entités du modèle de confiance des STI-C à adapter la CP aux environnements changeants ou à de nouvelles exigences futures, par exemple grâce à un changement des algorithmes cryptographiques et de la longueur de clé au fil du temps.
module cryptographique	Un élément sécurisé basé sur le matériel informatique au sein duquel des clés sont générées et/ou stockées, des nombres aléatoires sont générés et des données sont signées ou chiffrées.
autorité d'inscription	Dans le présent document, le terme «autorité d'inscription» (EA) fait référence non seulement à la fonction spécifique de l'EA, mais également à l'entité juridique et/ou opérationnelle qui la gère.
participants à la PKI	entités du modèle de confiance des STI-C, à savoir le TLM, les CA racine, les EA, les AA et les stations STI-C.
régénération de la clé	Ce sous-composant est utilisé pour décrire certains éléments liés à un souscripteur ou à un autre participant générant une nouvelle paire de clés et demandant la délivrance d'un nouveau certificat attestant la nouvelle clé publique, conformément à la description figurant à [3].
répertoire	Le répertoire utilisé pour le stockage des certificats et des informations figurant sur les certificats fournis par les entités du modèle de confiance des STI-C, tel que défini à la section 2.3.
autorité de certification racine	Dans le présent document, le terme «autorité de certification racine» (CA) fait référence non seulement à la fonction spécifique de la CA, mais également à l'entité juridique et/ou opérationnelle qui la gère.
sujet	La personne physique, le dispositif, le système, l'unité ou l'entité juridique indiquée dans un certificat comme étant le sujet, à savoir soit le souscripteur soit un dispositif contrôlé et exploité par le souscripteur.
souscripteur	Une personne physique ou une entité juridique à laquelle est délivré un certificat et qui est légalement liée par un accord de souscription ou sur les conditions d'utilisation.
Accord de souscription	Un accord entre la CA et le demandeur/le souscripteur qui spécifie les droits et responsabilités des parties.

1.3. Participants à la PKI

1.3.1. Introduction

Les participants à la PKI jouent un rôle dans la PKI définie par la présente politique. À moins que cela ne soit explicitement interdit, un participant peut jouer plusieurs rôles en même temps. Jouer plusieurs rôles en même temps peut être interdit afin d'éviter des conflits d'intérêts ou de garantir la séparation des tâches.

Les participants peuvent également déléguer une partie de leurs rôles à d'autres entités dans le cadre d'un contrat de service. Par exemple, lorsque des informations sur l'état de révocation sont fournies au moyen de CRL, la CA est également l'émetteur de la CRL, mais elle peut déléguer la responsabilité de délivrer les CRL à une autre entité.

Les rôles de la PKI consistent en:

- des rôles d'autorité (chaque rôle est instancié de façon unique);
- des rôles opérationnels (des rôles pouvant être instanciés dans une ou plusieurs entités).

Par exemple, une CA racine peut être mise en œuvre par une entité commerciale, un groupe d'intérêt commun, une organisation nationale et/ou une organisation européenne.

La figure 1 montre l'architecture du modèle de confiance des STI-C sur la base de [2]. L'architecture est brièvement décrite ici, mais les principaux éléments sont décrits de façon plus détaillée aux sections 1.3.2 à 1.3.6.

La CPA nomme le TLM, qui est donc une entité de confiance pour l'ensemble des participants à la PKI. La CPA approuve le fonctionnement de la CA racine et confirme que le TLM peut faire confiance à la/aux CA racine. Le TLM délivre l'ECTL qui permet à tous les participants à la PKI de faire confiance aux CA racine approuvées. La CA racine délivre des certificats aux EA et AA, ce qui permet de se fier à leur fonctionnement. L'EA délivre des certificats d'inscription aux stations STI-C émettrices et de relais (en tant qu'entités finales), ce qui permet de se fier à leur fonctionnement. L'AA délivre des AT aux stations STI-C sur la base de la confiance dans l'EA.

La station STI-C réceptrice et de relais (en tant que partie de relais) peut faire confiance à d'autres stations STI-C, étant donné que les AT sont délivrés par une AA à laquelle une CA racine fait confiance, cette CA racine bénéficiant également de la confiance du TLM et de la CPA.

Il convient de noter que la Figure 1 décrit uniquement le niveau de la CA racine du modèle de confiance des STI-C. Des détails relatifs aux couches inférieures sont fournis dans les sections suivantes de la présente CP ou dans les CPS des CA racine spécifiques.

La Figure 2 offre un aperçu des flux d'informations entre les participants à la PKI. Les points verts indiquent des flux nécessitant des communications entre machines. Les flux d'informations en rouge ont des exigences de sécurité particulières.

Le modèle de confiance des STI-C repose sur une architecture de CA racine multiple, où les certificats de CA racine sont transmis régulièrement (comme établi ci-après) au point de contact central (CPOC) au moyen d'un protocole sécurisé (par exemple des certificats de lien) défini par le CPOC.

Une CA racine peut être exploitée par une organisation publique ou privée. L'architecture du modèle de confiance des STI-C contient au moins une CA racine (la CA racine de l'UE avec le même niveau que les autres CA racine). La CA racine de l'UE est déléguée par l'ensemble des entités qui participent au modèle de confiance des STI-C et ne souhaitent pas mettre en place leur propre CA racine. Le CPOP transmet les certificats de CA racine reçus au TLM, qui est chargé de les recueillir et de signer la liste des certificats de CA racine ainsi que de les renvoyer au CPOC, qui les rend universellement accessibles (voir ci-après).

Les relations de confiance entre les entités dans le modèle de confiance des STI-C sont décrites aux figures, tableaux et sections ci-après.

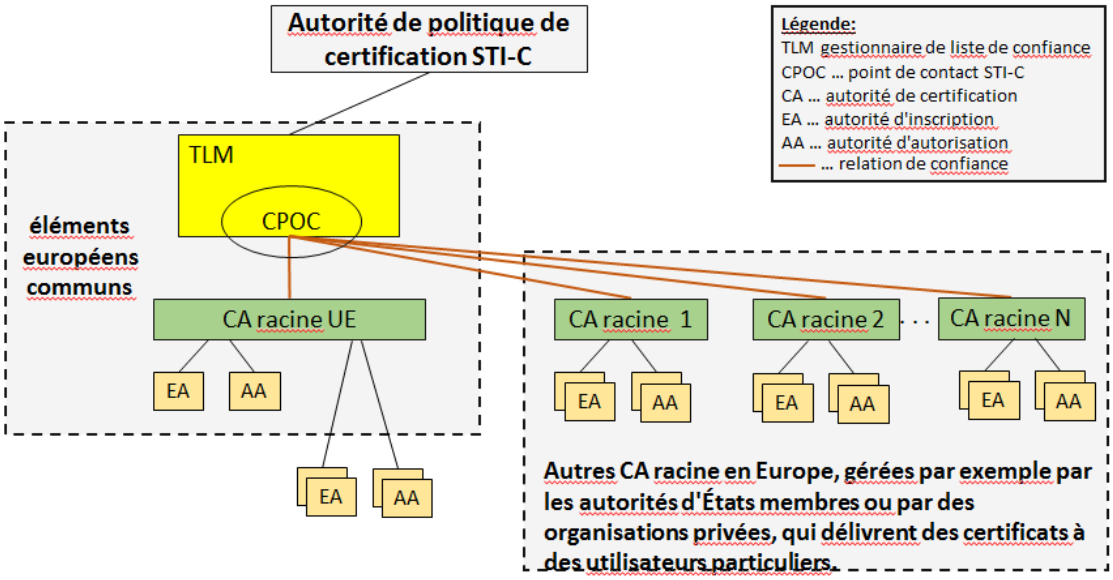

Figure 1: Architecture du modèle de confiance des STI-C

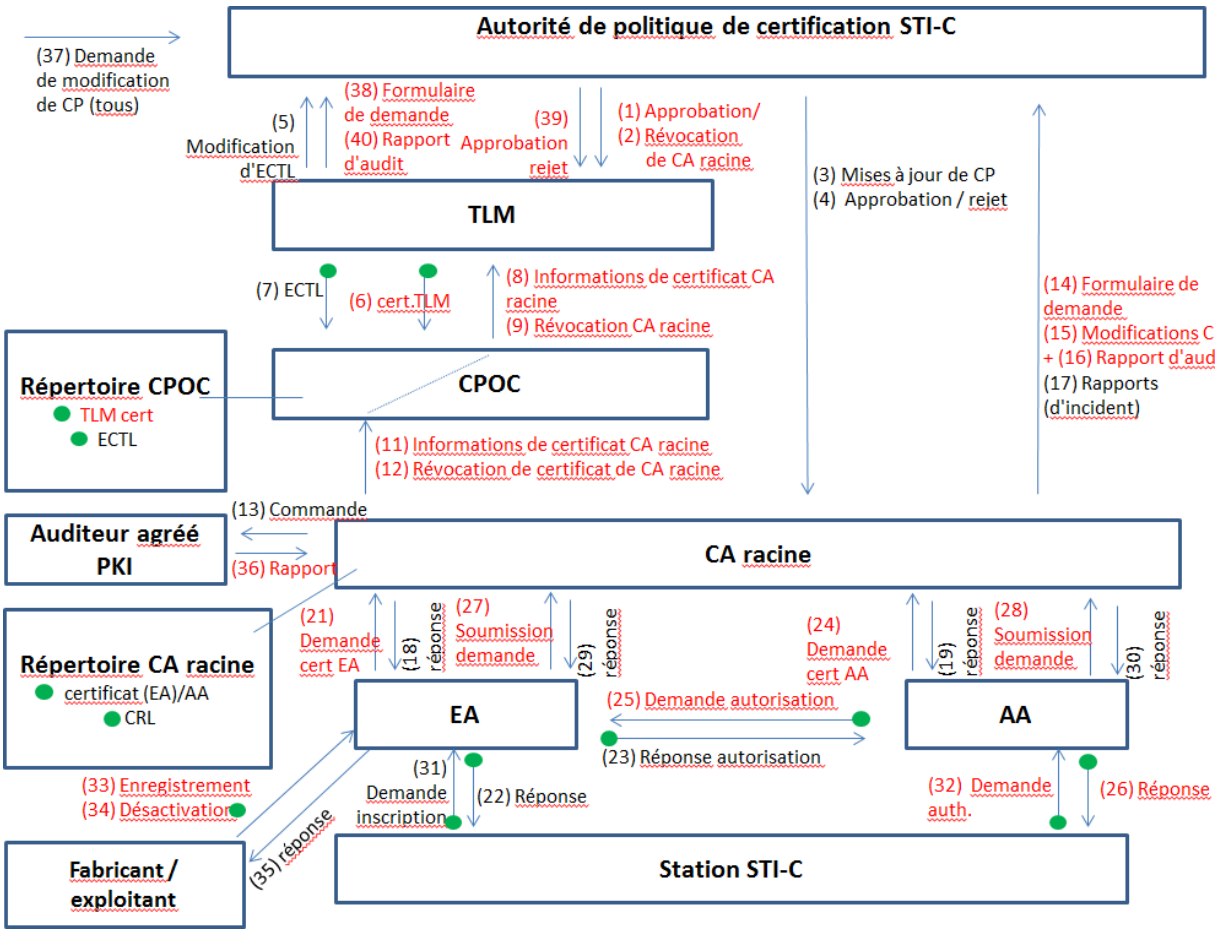

Figure 2: Flux d'informations du modèle de confiance des STI-C

Numéro d'identification du flux	De	À	Contenu	Référence
(1).	CPA	TLM	approbation de la demande de CA racine	8
(2).	CPA	TLM	informations relatives à la révocation de la CA racine	8.5
(3).	CPA	CA racine	mises à jour de la CP	1.5
(4).	CPA	CA racine	Approbation/rejet du formulaire de demande de CA racine ou des changements de la demande de CPS ou du processus de vérification.	8.5, 8.6
(5).	TLM	CPA	notification de changement de l'ECTL	4, 5.8.1
(6).	TLM	CPOC	Certificat du TLM	4.4.2
(7).	TLM	CPOC	ECTL	4.4.2
(8).	CPOC	TLM	informations du certificat de CA racine	4.3.1.1
(9).	CPOC	TLM	révocation du certificat de CA racine	7.3
(10).	CPOC	toutes les entités finales	Certificat du TLM	4.4.2
(11).	CA racine	CPOC	informations du certificat de CA racine	4.3.1.1
(12).	CA racine	CPOC	révocation du certificat de CA racine	7.3
(13).	CA racine	Auditeur	Commande d'audit	8
(14).	CA racine	CPA	formulaire de demande de CA racine — demande initiale	4.1.2.1
(15).	CA racine	CPA	formulaire de demande de CA racine — changements de CPS	1.5.1
(16).	CA racine	CPA	formulaire de demande de CA racine — rapport d'audit	8.6
(17).	CA racine	CPA	rapports d'incidents de la CA racine, y compris la révocation d'une sous-CA (EA, AA)	Annexe III, 7.3.1
(18).	CA racine	EA	réponse de certificat d'EA	4.2.2.3
(19).	CA racine	AA	réponse de certificat d'AA	4.2.2.3
(20).	CA racine	Tous	certificat d'EA/AA, CRL	4.4.2
(21).	EA	CA racine	demande de certificat d'EA	4.2.2.3
(22).	EA	station STI-C	réponse d'authentifiant d'inscription	4.3.1.4
(23).	EA	AA	réponse d'autorisation	4.2.2.5
(24).	AA	CA racine	demande de certificat d'AA	4.2.2.3
(25).	AA	EA	demande d'autorisation	4.2.2.5

(26).	AA	station STI-C	réponse de ticket d'autorisation	4.3.1.5
(27).	EA	CA racine	présentation de demande	4.1.2.3
(28).	AA	CA racine	présentation de demande	4.1.2.3
(29).	CA racine	EA	réponse	4.12 et 4.2.1
(30).	CA racine	AA	réponse	4.12 et 4.2.1
(31).	station STI-C	EA	demande d'authentifiant d'inscription	4.2.2.4
(32).	station STI-C	AA	demande de ticket d'autorisation	4.2.2.5
(33).	fabricant/exploitant	EA	enregistrement	4.2.1.4
(34).	fabricant/exploitant	EA	désactivation	7.3
(35).	EA	fabricant/exploitant	réponse	4.2.1.4
(36).	auditeur	CA racine	rapport	8.1
(37).	tous	CPA	demandes de changement de la CP	1.5
(38).	TLM	CPA	formulaire de demande	4.1.2.2
(39).	CPA	TLM	approbation/rejet	4.1.2.2
(40).	TLM	CPA	rapport d'audit	4.1.2.2

Tableau 1: Description détaillée des flux d'informations dans le modèle de confiance des STI-C

1.3.2. Autorité de politique de certification des STI-C

(1) L'autorité de politique de certification (CPA) des STI-C est composée des représentants des parties prenantes publiques et privées (par exemple, les États membres, les constructeurs de véhicules, etc.) participant au modèle de confiance des STI-C. Elle est responsable de deux sous-rôles:

(1) la gestion de la politique de certification, notamment:

- l'approbation des demandes de modification des CP actuelle et future;
- la décision d'examiner les demandes de modification de la CP et les recommandations soumises par d'autres entités ou participants à la PKI;
- la décision de publier de nouvelles versions de la CP;

(2) la gestion de l'autorisation de la PKI, notamment:

- la définition, la décision et la publication des procédures d'approbation des CPS et d'audit des CA (désignées collectivement sous la dénomination «procédures d'approbation des CA»);
- l'autorisation du CPOC à agir et à présenter des rapports de façon régulière;

- l'autorisation du TLM à agir et à présenter des rapports de façon régulière;
- l'approbation de la CPS des CA racine, si elle est conforme à la CP commune et valide;
- l'examen des rapports de l'auditeur agréé d'une PKI pour l'ensemble des CA racine;
- la notification au TLM de la liste de CA racine approuvées ou non et de leurs certificats sur la base des rapports d'approbation reçus des CA racine et des rapports réguliers sur le fonctionnement.

(2) Le mandataire de la CPA est chargé de l'authentification du mandataire du TLM et de l'approbation du formulaire de demande de processus d'inscription du TLM. La CPA est chargée d'autoriser le TLM à agir comme mentionné dans la présente section.

1.3.3. Gestionnaire de la liste de confiance (TLM)

(3) Le TLM est une entité unique nommée par la CPA.

(4) Le TLM est chargé:

- du fonctionnement de l'ECTL conformément à la CP commune valide et de rapports réguliers à la CPA pour le fonctionnement global sécurisé du modèle de confiance des STI-C;
- De la réception de certificats de CA racine émanant du CPOC;
- de l'inclusion dans l'ECTL/l'exclusion de l'ECTL de certificats de CA racine dès la notification de la CPA;
- de la signature de l'ECTL;
- de la transmission régulière et en temps utile de l'ECTL au CPOC.

1.3.4. Auditeur agréé de la PKI

(5) L'auditeur agréé de la PKI est chargé de:

- réaliser ou organiser les audits des CA racine, du TLM et des sous-CA;
- transmettre le rapport d'audit à la CPA (à partir d'un audit initial ou périodique) conformément aux exigences établies à la section 8 ci-après. Le rapport d'audit doit inclure les recommandations de l'auditeur agréé de la PKI;
- notifier à l'entité qui gère la CA racine de l'exécution réussie ou non d'un audit initial ou périodique des sous-CA;
- évaluer la conformité des CPS à la présente CP.

1.3.5. Point de contact des STI-C (CPOC)

(6) Le CPOC est une entité unique nommée par la CPA. Le mandataire de la CPA est chargé de l'authentification du mandataire du CPOC et de l'approbation du formulaire de demande de processus d'inscription du CPOC. La CPA est chargée d'autoriser le CPOC à agir comme établi dans la présente section.

(7) Le CPOC est chargé:

- d'établir l'échange de communication sécurisé entre l'ensemble des entités du modèle de confiance des STI-C et d'y contribuer de manière rapide et efficace;
- d'examiner les demandes de changement de procédure et les recommandations soumises par d'autres participants au modèle de confiance (par exemple les CA racine);
- de transmettre les certificats de CA racine au TLM;
- de publier le certificat approuvé commun («*trust anchor*») (clé publique actuelle et certificat de lien du TLM);
- de publier l'ECTL.

Tous les détails concernant l'ECTL figurent à la section 7.

1.3.6. Rôles opérationnels

(8) Les entités suivantes définies à [2] jouent un rôle opérationnel, tel que défini dans le RFC 3647:

Élément fonctionnel	**Rôle dans la PKI ([3] et [4])**	**Rôle détaillé ([2])**
autorité de certification racine	CA/RA (autorité d'enregistrement)	Apporte à l'EA et à l'AA la preuve qu'elles peuvent délivrer des EC ou des AT
Autorité d'inscription	Souscripteur à la CA racine/sujet du certificat de l'EA CA/RA	Authentifie une station STI-C et lui donne accès aux communications STI
Autorité d'autorisation	Souscripteur à la CA racine/sujet du certificat de l'AA CA/RA	Fournit à une station STI-C la preuve faisant autorité qu'elle peut utiliser des services STI spécifiques
Station STI-C émettrice	Sujet d'un certificat (EC) d'entité finale (EE)	Acquiert des droits auprès de l'EA pour avoir accès aux communications STI Négocie des droits auprès de l'AA pour invoquer les services STI Envoie des messages de diffusion relayés et à un seul bond
station STI-C de relais (transfert)	Partie relais/ sujet du certificat d'EE	Reçoit des messages de diffusion provenant de la station STI-C émettrice et les transfère à la station STI-C réceptrice si nécessaire
Station STI-C réceptrice	Partie relais	Reçoit des messages de diffusion provenant de la station STI-C émettrice ou de relais
Fabricant	Souscripteur de l'EA	Établit les informations nécessaires pour la gestion de la sécurité dans la station STI-C lors de la production
Exploitant	Souscripteur de l'EA/AA	Organise et met à jour les informations nécessaires pour la gestion de la sécurité dans la station STI-C lors du fonctionnement.

Tableau 2: Rôles opérationnels

Remarque: conformément à [4], différents termes sont utilisés dans la présente CP pour désigner le «souscripteur» qui signe un contrat avec la CA pour la délivrance de

certificats et le «sujet» auquel le certificat s'applique. Les souscripteurs sont toutes les entités ayant une relation contractuelle avec une CA. Les sujets sont les entités auxquelles le certificat s'applique. Les EA/AA sont les souscripteurs et les sujets de la CA racine et elles peuvent demander des certificats d'EA/AA. Les stations STI-C sont des sujets et peuvent demander des certificats d'entité finale.

(9) Autorités d'enregistrement:

L'EA doit jouer le rôle d'une autorité d'enregistrement pour les entités finales. Seul un souscripteur authentifié et autorisé peut enregistrer de nouvelles entités finales (stations STI-C) au sein d'une EA. Les CA racine pertinentes doivent jouer le rôle d'autorités d'enregistrement pour les EA et les AA.

1.4. Usage des certificats

1.4.1. Domaines d'utilisation applicables

(10) Les certificats délivrés dans le cadre de la présente CP sont destinés à être utilisés pour valider les signatures numériques dans le cadre de la communication coopérative STI conformément à l'architecture de référence de [2].

(11) Les profils de certificats dans [5] déterminent les utilisations des certificats pour le TLM, les CA racine, les EA, les AA et les entités finales.

1.4.2. Limites de responsabilité

(12) Les certificats ne sont pas destinés, ni autorisés, à être utilisés dans:

- des circonstances qui sont contraires ou contreviennent à tout règlement (par exemple, le RGPD), décret, arrêté ou loi applicable ou les enfreignent.
- des circonstances qui portent atteinte, contreviennent aux droits d'autrui ou les enfreignent;
- des circonstances qui portent atteinte à la présente CP ou à l'accord de souscription pertinent;
- toute circonstance dans laquelle leur utilisation pourrait directement entraîner un décès, des dommages corporels ou des dommages graves à l'environnement (par exemple, en cas de défaillance dans le fonctionnement d'installations nucléaires, de la communication ou de la navigation aérienne ou de systèmes de contrôle d'armement);
- des circonstances contraires aux objectifs généraux de renforcement de la sécurité routière et de plus grande efficacité du transport routier en Europe.

1.5. Administration de la politique de certification

1.5.1. Mise à jour des CPS des CA énumérées dans l'ECTL

(13) Chaque CA racine énumérée dans l'ECTL publie sa propre CPS, qui doit être conforme à la présente politique. Une CA racine peut ajouter des exigences supplémentaires, mais veille à ce que toutes les exigences de la présente CP soient satisfaites à tout moment.

(14) Chaque CA racine énumérée dans l'ECTL met en œuvre un processus de modification approprié pour son document CPS. Les caractéristiques

principales du processus de modification sont documentées dans la partie publique de la CPS.

(15) Dans le cadre du processus de modification, on veille à ce que toutes les modifications apportées à la présente CP soient attentivement analysées et, à ce que la CPS soit mise à jour, si c'est nécessaire pour assurer la conformité avec la CP modifiée, dans les délais prévus lors de l'étape de mise en œuvre du processus de modification de la CP. Ce processus comprend, en particulier, les procédures de modification d'urgence permettant d'assurer que les modifications apportées à la CP ayant une influence sur la sécurité sont mises en œuvre en temps utile.

(16) Le processus de modification inclut des mesures appropriées permettant de vérifier que toutes les modifications apportées à la CPS sont conformes à la CP. Toute modification apportée à la CPS est clairement documentée. Avant la mise en œuvre d'une nouvelle version d'une CPS, un auditeur agréé de la PKI doit vérifier sa conformité à la CP.

(17) La CA racine notifie à la CPA toute modification apportée à la CPS en précisant au moins les informations suivantes:

- une description précise de la modification;
- la justification de la modification;
- un rapport d'un auditeur agréé de la PKI confirmant la conformité à la CP;
- les coordonnées de la personne responsable de la CPS;
- le délai prévu pour la mise en œuvre.

1.5.2. Procédure d'approbation des CPS

(18) Avant le début de ses activités, une CA racine éventuelle présente sa CPS à un auditeur agréé de la PKI dans le cadre d'une commande d'audit de la conformité (flux 13) ainsi qu'à la CPA pour approbation (flux 15).

(19) Une CA racine présente les modifications apportées à sa CPS à un auditeur agréé de la PKI dans le cadre d'une commande d'audit de la conformité (flux 13) et à la CPA pour approbation (flux 15) avant que ces modifications ne prennent effet.

(20) Une EA/AA présente sa CPS ou les modifications apportées à celle-ci à la CA racine. Cette dernière peut demander un certificat de conformité auprès de l'organisme national ou de l'entité privée chargé de l'approbation de l'EA/AA, tel que défini aux sections 4.1.2 et 8.

(21) L'auditeur agréé de la PKI évalue la CPS conformément aux dispositions de la section 8.

(22) L'auditeur agréé de la PKI communique les résultats de l'évaluation de la CPS dans le cadre du rapport d'audit, conformément aux dispositions de la section 8.1. La CPS est acceptée ou rejetée dans le cadre de l'acceptation du rapport d'audit visée aux sections 8.5 et 8.6.

2. RESPONSABILITES EN MATIERE DE PUBLICATION ET DE REPERTOIRES

2.1. Méthodes de publication des informations des certificats

(23) Les informations des certificats peuvent être publiées conformément à la section 2.5:

- de manière régulière ou périodique; ou
- en réponse à une demande émise par l'une des entités participantes.

Selon les cas, les degrés d'urgence pour la publication et, par conséquent, les calendriers applicables varient, mais les entités doivent être préparées aux deux types de situations.

(24) La publication régulière des informations des certificats permet de déterminer un délai maximal au cours duquel les informations des certificats sont mises à jour pour l'ensemble des nœuds du réseau STI-C. La fréquence de publication de l'ensemble des informations des certificats est établie à la section 2.2.

(25) À la demande des entités participant au réseau STI-C, tout participant peut commencer à publier des informations des certificats à tout moment et, en fonction de son statut, demander un jeu d'informations de certificats en cours afin de devenir un nœud totalement digne de confiance du réseau STI-C. Cette publication vise principalement à informer les entités du statut global actuel des informations des certificats dans leur réseau et à leur permettre de communiquer en toute confiance jusqu'à la prochaine publication régulière des informations.

(26) Une CA racine unique peut également lancer la publication des informations des certificats à tout moment en envoyant un jeu actualisé de certificats à l'ensemble des «membres souscripteurs» du réseau STI-C qui reçoivent régulièrement ces informations. Cela permet aux CA, tout en soutenant leur action, de s'adresser aux membres entre les dates régulières et programmées pour la publication des certificats.

(27) La section 2.5 établit le mécanisme et l'ensemble des procédures relatifs à la publication des certificats de CA racine et de l'ECTL.

(28) Le CPOC publie les certificats de CA racine (tels qu'ils figurent dans l'ECTL et destinés au public), le certificat du TLM et l'ECTL qu'il délivre.

(29) Les CA racine publient leurs certificats d'EA/AA et les CRL, et sont capables de prendre en charge les trois mécanismes visés dans le présent document en ce qui concerne leur publication à l'intention de leurs membres souscripteurs et des parties utilisatrices, en prenant toutes les mesures nécessaires pour veiller à la transmission sécurisée, comme établi à la section 4.

2.2. Date ou fréquence de publication

(30) Les exigences relatives au calendrier de publication pour les certificats et les CRL doivent être déterminées en fonction des différents facteurs limitatifs des nœuds STI-C uniques, et l'objectif global consiste à exploiter un «réseau de confiance» et à publier des mises à jour le plus vite possible ainsi qu'à les communiquer à l'ensemble des stations STI-C concernées.

- Aux fins de la publication régulière des informations des certificats mises à jour (par exemple, les modifications relatives à la composition de la

CRL ou de l'ECTL), une période maximale de trois mois est nécessaire pour l'exploitation en toute sécurité du réseau STI-C.

- Les CA racine publient leurs certificats de CA et leurs CRL le plus rapidement possible après la délivrance.
- Pour la publication de la CRL, il convient d'utiliser le répertoire de CA racine.

En outre, la CPS relative à chaque CA précise le délai dans lequel un certificat sera publié après la délivrance du certificat par la CA.

Cette section précise uniquement la date ou la fréquence de la publication régulière. Les moyens de connectivité pour mettre à jour les stations STI-C avec l'ECTL et les CRL dans un délai d'une semaine suivant leur publication (dans des conditions normales de fonctionnement, par exemple avec une couverture cellulaire, un véhicule en fonctionnement effectif, etc.) sont mis en œuvre conformément aux exigences établies dans le présent document.

2.3. Répertoires

(31) Les exigences relatives à la structure du répertoire utilisé pour stocker les certificats et aux informations fournies par les entités du réseau STI-C sont les suivantes pour les entités uniques:

- en général, chaque CA racine devrait utiliser un répertoire de ses propres informations de certificats d'EA/AA en cours et une CRL pour publier des certificats à l'intention d'autres participants à la PKI (par exemple, un service d'annuaire LDAP). Le répertoire de chaque CA racine autorise tous les contrôles d'accès (section 2.4) et délais de transmission nécessaires (section 2.2) pour chaque méthode de diffusion des informations liées aux STI-C.
- Le répertoire du TLM (qui stocke l'ECTL et les certificats du TLM publiés par le CPOC, par exemple) devrait être fondé sur un mécanisme de publication en mesure d'assurer le respect des délais de transmission fixés à la section 2.2 pour chaque méthode de diffusion.

Les exigences des AA ne sont pas définies, mais elles doivent prendre en charge les mêmes niveaux de sécurité que les autres entités et ces niveaux doivent figurer dans leur CPS.

2.4. Contrôles d'accès sur les répertoires

(32) Les exigences relatives au contrôle d'accès des répertoires d'informations des certificats sont au moins conformes aux normes générales de traitement sécurisé des informations définies dans la norme ISO/IEC 27001 et aux exigences établies à la section 4. En outre, elles reflètent les besoins du processus en matière de sécurité à déterminer pour les différentes étapes du processus relatives à la publication des informations des certificats.

- Ces besoins comprennent la mise en œuvre du répertoire pour les certificats du TLM et l'ECTL dans le TLM/CPOC. Chaque CA ou chaque exploitant de répertoire met en œuvre des contrôles d'accès en ce qui concerne l'ensemble des entités STI-C et des parties externes pour au moins trois niveaux différents (par exemple, niveau public, niveau limité

aux entités STI-C ou niveau CA racine) afin d'empêcher les entités d'ajouter, de modifier ou de supprimer des entrées du répertoire.

- Les mécanismes exacts de contrôle d'accès de l'entité unique devraient faire partie de la CPS respective.
- Pour chaque CA racine, les répertoires d'EA et d'AA respectent les mêmes exigences en matière de procédures de contrôle d'accès quel que soit le lieu où le lien contractuel avec le fournisseur de service exploitant le répertoire.

Chaque CA racine ou chaque exploitant de répertoire devrait fournir au moins trois niveaux différents (par exemple, niveau public, niveau limité aux entités STI-C ou niveau CA racine) qui serviront de points de départ pour les niveaux de contrôle d'accès.

2.5. Publication des informations des certificats

2.5.1. Publication des informations des certificats par le TLM

(33) Le TLM dans le domaine de confiance européen commun des STI-C publie les informations suivantes via le CPOC:

- l'ensemble des certificats du TLM actuellement valides pour la prochaine période d'exploitation (certificat de lien et certificat en vigueur si disponible);
- les informations relatives aux points d'accès pour le répertoire du CPOC afin de fournir la liste signée des CA racine (ECTL);
- point d'informations général pour le déploiement de l'ECTL et des STI-C.

2.5.2. Publication des informations des certificats par les CA

(34) Les CA racine dans le domaine de confiance des STI-C européen commun publient les informations suivantes:

- les certificats de CA racine (actuellement valides) (certificats en vigueur et correctement régénérés, y compris un certificat de lien) dans le répertoire visé à la section 2.3;
- l'ensemble des entités EA et AA valides, ainsi que le code d'identification de l'exploitant et la période d'exploitation prévue;
- les certificats de CA délivrés dans les répertoires visés à la section 2.3;
- les CRL pour l'ensemble des certificats de CA révoqués couvrant leurs EA et AA subalternes;
- les informations relatives au point d'accès de la CA racine aux informations de la CA et de la CRL.

L'ensemble des informations des certificats sont classées selon trois niveaux de confidentialité et les documents à l'intention du grand public doivent être accessibles sans restrictions.

3. IDENTIFICATION ET AUTHENTIFICATION

3.1. Nommage

3.1.1. Types de nom

3.1.1.1. Noms pour les TLM, les CA racine, les EA et les AA

(35) Dans le certificat du TLM, le nom est composé d'un seul attribut subject_name avec la valeur réservée «EU_TLM».

(36) Pour les CA racine, le nom est composé d'un seul attribut subject_name avec une valeur octroyée par la CPA. L'unicité des noms est établie sous la seule responsabilité de la CPA et le TLM maintient le registre des noms de CA racine dès la notification de la CPA (approbation, révocation/suppression d'une CA racine). Les noms de sujets dans les certificats sont limités à 32 octets. Chaque CA racine propose son nom à la CPA dans le formulaire de demande (flux 14). La CPA est chargée de la vérification de l'unicité des noms. Si le nom n'est pas unique, le formulaire de demande est rejeté (flux 4).

(37) Le nom dans chaque certificat d'EA/AA peut être composé d'un seul attribut subject_name avec une valeur générée par l'émetteur du certificat. L'unicité des noms relève de la seule responsabilité de la CA racine chargée de la délivrance.

(38) Les certificats d'EA et d'AA n'utilisent pas de nom d'une taille supérieure à 32 octets, car les subject_name des certificats sont limités à 32 octets.

(39) Les AT ne contiennent pas de nom.

3.1.1.2. Noms des entités finales

(40) Deux types d'identifiants (ID) uniques sont attribués à chaque station STI-C:

- un ID canonique qui est stocké lors de l'enregistrement initial de la station STI-C sous la responsabilité du fabricant. Cet ID contient une sous-chaîne qui identifie le fabricant ou l'exploitant de sorte que cet identifiant puisse être unique;
- un attribut subject_name, qui peut faire partie de l'EC de la station STI-C, sous la responsabilité de l'EA.

3.1.1.3. Identification des certificats

(41) Les certificats qui respectent le format de [5] sont identifiés en calculant une valeur HashedId8 telle que définie dans [5].

3.1.2. Nécessité d'utiliser des noms explicites

Aucune disposition.

3.1.3. Anonymat et emploi de pseudonymes pour les entités finales

(42) L'AA veille à ce que l'emploi de pseudonymes d'une station STI-C soit établi en fournissant à la station STI-C des AT qui ne contiennent aucun nom et aucune information permettant d'établir le lien entre le sujet et son identité réelle.

3.1.4. Règles d'interprétation des diverses formes de noms

Aucune disposition.

3.1.5. Unicité des noms

(43) Les noms du TLM, des CA racine, des EA, des AA et des ID canoniques pour les stations STI-C sont uniques.

(44) Lors du processus d'enregistrement d'une CA racine donnée dans l'ECTL, le TLM veille à l'unicité de l'identifiant du certificat (HashedId8). Lors du processus de délivrance, la CA racine veille à ce que l'identifiant de certificat (HashedId8) de chaque CA subalterne soit unique.

(45) Le HashedId8 d'un EC est unique au sein de la CA chargée de la délivrance. Le HashedId8 d'un AT ne doit pas nécessairement être unique.

3.2. Validation initiale de l'identité

3.2.1. Méthode visant à prouver la possession d'une clé privée

(46) La CA racine démontre qu'elle détient légitimement la clé privée correspondant à la clé publique dans le certificat autosigné. Le CPOC vérifie cette preuve.

(47) L'EA/AA prouve qu'elle détient légitimement la clé privée correspondant à la clé publique devant figurer dans le certificat. La CA racine vérifie cette preuve.

(48) La possession d'une nouvelle clé privée (pour la régénération) est démontrée par la signature de la demande avec la nouvelle clé privée (signature interne) suivie de la génération d'une signature externe sur la demande signée avec la clé privée actuelle valide (pour garantir l'authenticité de la demande). Le demandeur soumet la demande de certificat signée à la CA chargée de la délivrance au moyen d'une communication sécurisée. La CA chargée de la délivrance vérifie que la signature numérique du demandeur sur le message de demande a été créée à l'aide de la clé privée correspondant à la clé publique jointe à la demande de certificat. La CA racine précise les réponses et la demande de certificat qu'elle soutient dans sa CPS.

3.2.2. Authentification de l'identité d'une organisation

3.2.2.1. Authentification de l'identité d'une organisation de CA racine

(49) Dans un formulaire de demande destiné à la CPA (à savoir flux 14), la CA racine communique l'identité de l'organisation et les informations relatives à l'enregistrement, composées des éléments suivants:

- nom de l'organisation;
- adresse postale;
- adresse électronique;
- nom d'une personne physique à contacter au sein de l'organisation;
- numéro de téléphone;
- empreinte numérique (par exemple la valeur de hachage SHA 256) du certificat de la CA racine en version imprimée;
- informations cryptographiques (par exemple des algorithmes cryptographiques, des longueurs de clé) dans le certificat de CA racine;
- toutes les autorisations que la CA racine est autorisée à utiliser et à communiquer aux sous-CA.

(50) La CPA vérifie l'identité de l'organisation et d'autres informations relatives à l'enregistrement fournies par le demandeur du certificat pour l'ajout d'un certificat de CA racine dans l'ECTL.

(51) La CPA recueille des éléments d'identification directs ou une attestation fournie par une source appropriée et autorisée de l'identité (par exemple le nom) et, le cas échéant, des caractéristiques spécifiques des sujets auxquels un certificat est délivré. Les éléments d'identification peuvent être soumis sous forme de documentation papier ou électronique.

(52) L'identité du sujet doit être vérifiée au moment de l'enregistrement par des moyens appropriés et conformément à la présente politique de certification.

(53) Lors de chaque demande de certificat, les éléments d'identification suivants doivent être fournis:

- nom complet de l'entité organisationnelle (organisation privée, entité publique ou entité non commerciale);
- enregistrement reconnu au niveau national ou autres attributs pouvant être utilisés, dans la mesure du possible, afin de distinguer l'entité organisationnelle d'autres portant le même nom.

Les règles énoncées ci-dessus reposent sur le document TS 102 042 [4]: *La CA veille à ce que les éléments d'identification du souscripteur et du sujet et la précision de leurs noms et des données associées soient soit dûment examinés dans le cadre du service défini soit, le cas échéant, jugés concluants à l'issue de l'examen des attestations fournies par des sources appropriées et autorisées. Elle doit également veiller à ce que les demandes de certificat soient exactes, autorisées et complètes, conformément à l'attestation ou aux éléments d'identification recueillis.*

3.2.2.2. Authentification de l'identité d'une organisation de TLM

(54) L'organisation exploitant le TLM fournit des éléments d'identification et des éléments attestant de l'exactitude du nom et des données associées afin de permettre une vérification appropriée lors de la création initiale et de la régénération de clé du certificat du TLM.

(55) L'identité du sujet est vérifiée au moment de la création du certificat ou de la régénération de clé par des moyens appropriés et conformément à la présente PC.

(56) Les éléments d'identification de l'organisation doivent être fournis conformément à la section 3.2.2.1.

3.2.2.3. Authentification de l'identité d'une organisation de sous-CA

(57) La CA racine vérifie l'identité de l'organisation et d'autres informations relatives à l'enregistrement fournies par les demandeurs du certificat pour les certificats de sous-CA (EA/AA).

(58) Au minimum, la CA racine:

- détermine que l'organisation existe en utilisant au moins une base de données ou un service tiers de preuve d'identité ou bien de la documentation organisationnelle fournie par l'autorité reconnue ou l'agence gouvernementale concernée qui confirme l'existence de l'organisation ou déposée auprès de celle-ci;

- utilise la voie postale ou une procédure comparable pour demander au demandeur du certificat de confirmer certaines informations relatives à l'organisation, de confirmer qu'il a autorisé la demande de certificat et que la personne qui soumet la demande au nom du demandeur est autorisée à le faire. Lorsque le nom d'une personne agissant en qualité de mandataire de l'organisation figure sur le certificat, le demandeur confirme également qu'il emploie cette personne et l'a autorisée à agir en son nom.

(59) Les procédures de validation pour la délivrance de certificats de CA sont documentées dans une CPS de la CA racine.

3.2.2.4. Authentification de l'organisation du souscripteur des entités finales

(60) Avant que le souscripteur des entités finales (fabricant/exploitant) ne puisse s'enregistrer auprès de l'EA de confiance pour permettre à ses entités finales d'envoyer les demandes de certificats EC, l'EA:

- vérifie l'identité de l'organisation du souscripteur et d'autres informations relatives à l'enregistrement fournies par le demandeur du certificat;
- vérifie que le type de station STI-C (à savoir le produit concret sur la base de la marque, du modèle et de la version de la station STI-C) satisfait à l'ensemble des critères d'évaluation de la conformité.

(61) Au minimum, l'EA:

- détermine que l'organisation existe en utilisant au moins une base de données ou un service tiers de preuve d'identité ou bien de la documentation organisationnelle fournie par l'autorité reconnue ou l'agence gouvernementale concernée qui confirme l'existence de l'organisation ou déposée auprès de celle-ci;
- utilise la voie postale ou une procédure comparable pour demander au demandeur du certificat de confirmer certaines informations relatives à l'organisation, de confirmer qu'il a autorisé la demande de certificat et que la personne qui soumet la demande en son nom est autorisée à le faire. Lorsque le nom d'une personne agissant en qualité de mandataire de l'organisation figure sur le certificat, le demandeur confirme également qu'il emploie cette personne et l'a autorisée à agir en son nom.

(62) Les procédures de validation pour l'enregistrement d'une station STI-C par son souscripteur sont documentées dans une CPS de l'EA.

3.2.3. Authentification de l'entité individuelle

3.2.3.1. Authentification de l'entité individuelle du TLM/de la CA

(63) Pour l'authentification d'une entité individuelle (personne physique) identifiée en association avec une personne morale ou une entité organisationnelle (par exemple le souscripteur), les éléments d'identification à fournir sont les suivants:

- nom complet du sujet (y compris le nom de famille et les prénoms, conformément à la législation applicable et aux pratiques nationales d'identification);

- date et lieu de naissance, référence à un document d'identité reconnu au niveau national ou autres caractéristiques de l'abonné pouvant être utilisées, dans la mesure du possible, pour distinguer la personne d'autres portant le même nom;
- nom complet et statut juridique de la personne morale associée ou d'une autre entité organisationnelle (par exemple le souscripteur);
- toute information pertinente relative à l'enregistrement (par exemple le registre des sociétés) de la personne morale associée ou d'une autre entité organisationnelle;
- des éléments prouvant que le sujet est associé à la personne morale ou à une autre entité organisationnelle.

Les éléments peuvent être soumis sous forme de documentation papier ou électronique.

(64) Pour vérifier son identité, le mandataire d'une CA racine, d'une EA, d'une AA ou d'un souscripteur fournit des documents démontrant qu'il travaille pour l'organisation (certificat d'autorisation). Il fournit également un document d'identité officiel.

(65) Pour le processus d'inscription initial (flux 31/32), un représentant de l'EA/AA fournit à la CA racine correspondante toutes les informations nécessaires (voir section 4.1.2).

(66) Le personnel de la CA racine vérifie l'identité du mandataire du demandeur du certificat ainsi que tous les documents associés, en appliquant les exigences relatives au «personnel de confiance», énoncées dans la section 5.2.1. (Le processus de validation des informations relatives à la demande et de génération du certificat par la CA racine est effectué par des «personnes de confiance» à la CA racine, sous la supervision d'au moins deux personnes, étant donné qu'il s'agit d'opérations sensibles au sens de la section 5.2.2).

3.2.3.2. Authentification de l'identité du souscripteur des stations STI-C

(67) Les souscripteurs sont représentés par des utilisateurs finaux autorisés au sein de l'organisation, qui sont enregistrés auprès de l'EA et de l'EA chargées de la délivrance. Ces utilisateurs finaux désignés par des organisations (fabricants ou exploitants) prouvent leur identité et font l'objet d'une authentification avant:

- l'enregistrement de l'EE auprès de son EA correspondante, y compris sa clé publique canonique, son ID canonique (identifiant unique) et les autorisations conformément à l'EE;
- l'enregistrement auprès de l'AA et l'obtention de la preuve d'un accord de souscription qui peut être envoyée à l'EA.

3.2.3.3. Authentification de l'identité des stations STI-C

(68) Les sujets de EE des entités finales s'authentifient lors de la demande d'EC (flux 31) en utilisant leur clé privée canonique pour l'authentification initiale. L'EA vérifie l'authentification à l'aide de la clé publique canonique correspondant à l'EE. Les clés publiques canoniques des EE sont apportées à l'EA avant l'exécution de la demande initiale, par un canal sécurisé entre le fabricant ou l'exploitant de la station STI-C et l'EA (flux 33).

(69) Les sujets d'AT d'entité finale s'authentifient lors de la demande d'AT (flux 32) en utilisant leur clé privée unique d'inscription. L'AA envoie la signature à l'EI (flux 25) pour validation; l'EA la valide et confirme le résultat à l'AA (flux 23).

3.2.4. Renseignements non vérifiés sur le souscripteur

Aucune disposition.

3.2.5. Validation de l'autorité

3.2.5.1. Validation du TLM, de la CA racine, de l'EA et de l'AA

(70) Chaque organisation recense dans la CPS au moins un représentant (par exemple un officier de sécurité) chargé de demander de nouveaux certificats et des renouvellements. Les règles en matière de nommage établies à la section 3.2.3 sont applicables.

3.2.5.2. Validation des souscripteurs de la station STI-C

(71) Au moins une personne physique chargée d'enregistrer les stations STI-C auprès d'une EA (par exemple un agent de sécurité) est reconnue par l'EA et approuvée par cette autorité (voir section 3.2.3).

3.2.5.3. Validation des stations STI-C

(72) Un souscripteur de station STI-C peut enregistrer des stations STI-C auprès d'une EA spécifique (flux 33) pour autant qu'il soit authentifié auprès de cette EA.

Lorsque la station STI-C est enregistrée auprès d'une EA avec un ID canonique unique et une clé publique canonique, elle peut demander un EC à l'aide d'une demande signée avec la clé privée canonique liée à la clé publique canonique enregistrée précédemment.

3.2.6. Critères d'interopérabilité

(73) Pour la communication entre les stations STI-C et les EA (ou AA), la station STI-C doit être en mesure d'établir une communication sécurisée avec les EA (ou AA), c'est-à-dire de mettre en œuvre des fonctions d'authentification, de confidentialité et d'intégrité, comme spécifié à [1]. D'autres protocoles peuvent être utilisés, pour autant que [1] soit mise en œuvre. L'EA et l'AA prennent en charge cette communication sécurisée.

(74) L'EA et l'AA prennent en charge les demandes de certificat et les réponses conformées à [1], qui prévoit un protocole sécurisé de réponse/demande d'AT assurant l'anonymat du demandeur vis-à-vis de l'AA et la séparation des tâches entre l'AA et l'EA. D'autres protocoles peuvent être utilisés, pour autant que [1] soit mise en œuvre. Afin d'empêcher la divulgation de l'identité à long terme des stations STI-C, la communication entre une station STI-C mobile et une EA est confidentielle (par exemple, les données de communication sont chiffrées de bout en bout).

(75) L'AA soumet une demande de validation de l'autorisation (flux 25) pour chaque demande d'autorisation reçue de la part d'un sujet de certificat d'EE. L'EA valide cette demande en ce qui concerne:

- le statut de l'EE à l'EA ;

- la validité de la signature;
- les autorisations et ITS-AID requises,
- le statut de la fourniture d'un service de l'AA au souscripteur.

3.3. Identification et authentification des demandes de régénération de clés

3.3.1. Identification et authentification pour régénération de clé courante

3.3.1.1. Certificats du TLM

(76) Le TLM génère une paire de clés et deux certificats: Un certificat autosigné et un certificat de lien, tel que visé à la section 7.

3.3.1.2. Certificats de la CA racine

Sans objet.

3.3.1.3. Régénération de clé ou renouvellement du certificat d'EA /AA

(77) Avant l'expiration d'un certificat d'EA /AA, l'EA /AA demande un nouveau certificat (flux 21/flux 24) afin de maintenir la continuité de l'usage des certificats. L'EA /AA génère une nouvelle paire de clés pour remplacer celle qui expire et signe la demande de régénération contenant la nouvelle clé publique avec la clé privée actuelle valide («régénération»). L'EA ou l'AA génère une nouvelle paire de clés et signe la demande avec la nouvelle clé privée (signature interne) pour prouver la possession de la nouvelle clé privée. Toute la demande est signée (contresignée) avec la clé privée actuelle valide (signature externe) pour garantir l'intégrité et l'authenticité de la demande. En cas d'utilisation d'une paire de clés de chiffrement et de déchiffrement, il faut prouver la possession de clés privées de déchiffrement prouvée (pour une description détaillée de la régénération, voir section 4.7.3.3).

(78) La méthode d'identification et d'authentification pour la régénération courante est similaire à celle énoncée à la section 3.2.2 en ce qui concerne la délivrance initiale d'une validation initiale de certificat de CA racine.

3.3.1.4. Authentifiants d'inscription des entités finales

(79) Avant l'expiration d'un EC existant, l'EE demande un nouveau certificat (flux 31) afin de maintenir la continuité de l'usage des certificats. L'EE génère une nouvelle paire de clés pour remplacer celle qui expire et demande un nouveau certificat contenant la nouvelle clé publique; la demande est signée avec la clé privée d'EC valide en vigueur.

(80) L'EE peut signer la demande avec la clé privée nouvellement créée (signature interne) pour prouver la possession de la nouvelle clé privée. Toute la demande est ensuite signée (contresignée) avec la clé privée actuelle valide (signature externe) et chiffrée à l'intention de l'EA réceptrice comme spécifié dans [1] pour garantir la confidentialité, l'intégrité et l'authenticité de la demande. D'autres protocoles peuvent être utilisés, pour autant que [1] soit mise en œuvre.

3.3.1.5. Tickets d'autorisation des entités finales

(81) La régénération de clés de certificat pour les AT repose sur le même processus que l'autorisation initiale, tel que défini dans [1]. D'autres protocoles peuvent être utilisés, pour autant que [1] soit mise en œuvre.

3.3.2. Identification et authentification pour régénération de clés après révocation

3.3.2.1. Certificats de CA

(82) L'authentification d'une organisation de CA pour la régénération de clés de certificats de CA racine, d'EA et d'AA après révocation est gérée de la même manière que la délivrance initiale d'un certificat de CA, conformément aux dispositions de la section 3.2.2.

3.3.2.2. Authentifiants d'inscription des entités finales

(83) L'authentification d'une EE pour la régénération de clés de l'EC après révocation est gérée de la même manière que la délivrance initiale d'un certificat d'EE, conformément aux dispositions de la section 3.2.2.

3.3.2.3. Demandes d'autorisation des entités finales

Ne s'applique pas, étant donné que les AT ne sont pas révoqués.

3.4. Identification et authentification des demandes de révocation

3.4.1. Certificats de CA racine/EA /AA

(84) Les demandes de suppression d'un certificat de CA racine de l'ECTL sont authentifiées par la CA racine auprès du TLM (flux 12 et 9). Les demandes de révocation d'un certificat d'EA/AA sont authentifiées par la CA racine concernée et la sous-CA elle-même.

(85) Les procédures acceptables pour l'authentification des demandes de révocation d'un souscripteur comprennent:

- un message écrit et signé sur du papier à lettres d'entreprise émanant du souscripteur qui demande la révocation, faisant référence au certificat à révoquer;
- la communication avec le souscripteur qui fournit des assurances raisonnables que la personne ou l'organisation qui demande la révocation est réellement le souscripteur. En fonction des circonstances, cette communication peut inclure un ou plusieurs des éléments suivants: adresse électronique, adresse postale ou service de messagerie.

3.4.2. Authentifiants d'inscription de la station STI-C

(86) Le souscripteur de la station STI-C peut révoquer l'EC d'une station STI-C précédemment enregistrée auprès d'une EA (flux 34). Le souscripteur qui demande la révocation crée une demande de révocation d'une station STI-C donnée ou d'une liste de stations STI-C. L'EA authentifie la demande de révocation avant de la traiter et confirme la révocation des stations STI-C et de leurs EC.

(87) L'EA peut révoquer l'EC d'une station STI-C conformément aux dispositions de la section 7.3.

3.4.3. Tickets d'autorisation de la station STI-C

(88) Les AT n'étant pas révoqués, leur validité est limitée à une période spécifique. La plage des périodes de validité acceptables dans la présente politique de certification est spécifiée à la section 7.

4. EXIGENCES OPERATIONNELLES DU CYCLE DE VIE DES CERTIFICATS

4.1. Demande de certificat

(89) La présente section définit les exigences applicables à une première demande de délivrance du certificat.

(90) Le terme «demande de certificat» se réfère aux processus suivants:

- enregistrement et mise en place d'un rapport de confiance entre le TLM et la CPA;
- enregistrement et mise en place d'un rapport de confiance entre la CA racine, la CPA et le TLM, y compris l'insertion du premier certificat de CA racine dans l'ECTL;
- enregistrement et mise en place d'un rapport de confiance entre l'EA/AA et la CA racine, y compris la délivrance d'un nouveau certificat EA/AA;
- enregistrement de la station STI-C auprès de l'EA par le fabricant/l'exploitant;
- demande d'EC/AT par la station STI-C.

4.1.1. Qui peut présenter une demande de certificat

4.1.1.1. CA racine

(91) Les CA racine génèrent leurs propres paires de clés et délivrent leur certificat racine elles-mêmes. Une CA racine peut soumettre une demande de certificat par l'intermédiaire de son représentant désigné (flux 14).

4.1.1.2. *TLM*

(92) Le TLM génère ses propres paires de clés et délivre son certificat lui-même. La création initiale du certificat du TLM est traitée par un représentant de l'organisation du TLM sous le contrôle de la CPA.

4.1.1.3. EA et AA

(93) Un mandataire de l'EA ou l'AA peut soumettre la demande de certificat de la sous-CA (EA et/ou AA) au mandataire de la CA racine concernée (flux 27/28).

4.1.1.4. Station STI-C

(94) Les souscripteurs enregistrent chaque station STI-C auprès de l'EA conformément à la section 3.2.5.3.

(95) Chaque station STI-C enregistrée auprès de l'EA peut envoyer des demandes d'EC (flux 31).

(96) Chaque station STI-C peut envoyer des demandes d'AT (flux 32) sans demander l'interaction d'un souscripteur. Avant de demander un AT, une station STI-C doit avoir un EC.

4.1.2. Processus d'inscription et responsabilités

(97) Les autorisations pour la délivrance de certificats par les CA racine et les sous-CA à des fins spéciales (des pouvoirs publics) (c'est-à-dire les stations STI-C mobiles et fixes spéciales) ne peuvent être accordées que par les États membres dans lesquels les organisations sont situées.

4.1.2.1. CA racine

(98) Après avoir été auditées (flux 13 et 36, section 8), les CA racine peuvent demander l'insertion de leur(s) certificat(s) dans l'ECTL auprès de la CPA (flux 14). Le processus d'inscription est fondé sur un formulaire signé de demande manuelle qui doit être physiquement remis à la CPA par le mandataire de la CA racine et qui contient au moins les renseignements mentionnés dans les sections 3.2.2.1, 3.2.3 et 3.2.5.1.

(99) Le formulaire de demande de la CA racine est signé par son mandataire.

(100) Outre le formulaire de demande, le mandataire de la CA racine fournit une copie de la CPS de la CA racine (flux 15) et de son rapport d'audit à la CPA pour approbation (flux 16). En cas d'approbation positive, la CPA génère et envoie un certificat de conformité au CPOC/TLM et à la CA racine correspondante.

(101) Le mandataire des CA racine introduit ensuite son formulaire de demande (contenant l'empreinte numérique du certificat autosigné), le document d'identité officiel et une preuve de l'autorisation au CPOC/TLM. Le certificat autosigné est transmis sous forme électronique au CPOC/TLM. Le CPOC/TLM vérifie tous les documents et le certificat autosigné.

(102) Si les vérifications donnent des résultats positifs, le TLM ajoute le certificat de la CA racine à l'ECTL sur la base de la notification de la CPA (flux 1 et 2). Le processus détaillé est décrit dans la CPS du TLM

(103) Une procédure supplémentaire pour obtenir une approbation de la CPS et du rapport d'audit d'une CA racine auprès d'un organisme national de certains pays devrait être possible.

4.1.2.2. *TLM*

(104) Après avoir été audité, le TLM peut s'inscrire auprès de la CPA. Le processus d'inscription est fondé sur un formulaire signé de demande manuelle qui est physiquement remis à la CPA (flux 38) par le mandataire du TLM et qui contient au moins les renseignements mentionnés dans les sections 3.2.2.2 et 3.2.3.

(105) Le formulaire de demande du TLM est signé par son mandataire.

(106) Premièrement, le TLM génère son certificat autosigné et le transmet de façon sécurisée à la CPA. Le TLM transmet ensuite son formulaire de demande (contenant l'empreinte numérique du certificat autosigné), une copie de sa CPS, un document d'identité officiel, une preuve d'autorisation et son rapport d'audit à la CPA (flux 40). La CPA vérifie tous les documents et le certificat autosigné. Si toutes les vérifications de documents, du certificat autosigné et de l'empreinte donnent des résultats positifs, la CPA confirme le processus d'inscription en envoyant son approbation au TLM et au CPOC (flux 39). La CPA conserve les renseignements relatifs à la demande envoyés par le TLM. Le certificat du TLM est ensuite émis via le CPOC.

4.1.2.3. EA et AA

(107) Au cours du processus d'inscription, l'EA /AA transmet les documents pertinents (par exemple, la CPS et le rapport d'audit) à la CA racine correspondante pour approbation (flux 27/28). Si les contrôles de ces

documents sont positifs, la CA racine envoie une approbation aux sous-CA racine correspondantes (flux 29/30). La sous-CA (EA ou AA) transmet ensuite sa demande signée par voie électronique, et remet physiquement son formulaire de demande (conformément à la section 3.2.2.1), la preuve de l'autorisation et le document d'identité à la CA racine correspondante. Cette dernière vérifie la demande et les documents reçus (formulaire de demande contenant l'empreinte numérique, à savoir la valeur de hachage SHA 256 de la demande de la sous CA, la preuve de l'autorisation et le document d'identité). Si tous les contrôles aboutissent à un résultat positif, la CA racine délivre le certificat à la sous-CA correspondante. Des informations détaillées sur la façon d'effectuer une demande initiale figurent dans sa CPS spécifique.

(108) Outre le formulaire de demande de la sous-CA, le mandataire de la sous-CA joint une copie de la CPS transmise à la CA racine.

(109) Des informations sont communiquées à un auditeur agréé de la PKI aux fins de l'audit conformément à la section 8.

(110) Si une sous-CA est détenue par une entité différente de l'entité qui détient une CA racine, avant l'émission d'une demande de certificat de la sous-CA, l'entité de la sous-CA signe un contrat concernant le service de la CA racine.

4.1.2.4. Station STI-C

(111) L'inscription initiale des sujets des entités finales (stations STI-C) est effectuée auprès de l'EA (flux 33 et 35) par le souscripteur responsable (fabricant/exploitant) après l'authentification réussie de l'organisation du souscripteur et de l'un de ses représentants conformément aux sections 3.2.2.4 et 3.2.5.2.

(112) Une station STI-C peut générer une paire de clés EC (voir section 6.1) et créer une demande d'EC signée conformément à [1]. D'autres protocoles peuvent être utilisés, pour autant que [1] soit mise en œuvre.

(113) Lors de l'enregistrement d'une station STI-C normale (par opposition à une station STI-C fixe ou mobile spéciale), l'EA doit vérifier que les autorisations dans la demande initiale ne sont pas destinées à une utilisation par les pouvoirs publics. Les autorisations pour une utilisation par les pouvoirs publics sont définies par les États membres correspondants. La procédure détaillée pour l'enregistrement et la réponse de l'EA au fabricant/à l'exploitant (flux 33 et 35) est exposée dans la CPS correspondante de l'EA.

(114) Une station STI-C doit être inscrite auprès d'une EA (section 3.2.5.3) par envoi de sa demande EC initiale, conformément à [1].

(115) Lors de l'enregistrement initial par le représentant d'un souscripteur authentifié, l'EA approuve les AT que le sujet de l'entité finale (c'est-à-dire la station STI-C) pourrait obtenir. En outre, chaque entité finale se voit attribuer un niveau de garantie de la confiance, lequel est lié à la certification de l'entité finale conformément à l'un des profils de protection énumérés à la section 6.1.5.2.

(116) Les véhicules ordinaires n'ont qu'une station STI-C enregistrée auprès d'une EA. Les véhicules à usage spécial (tels que les voitures de police et autres véhicules à usage spécial dotés de droits spécifiques) peuvent être inscrits auprès d'une EA supplémentaire ou avoir une station STI-C supplémentaire

pour des autorisations dans le cadre de cet usage spécial. Les véhicules bénéficiant d'une telle dérogation sont définis par les États membres responsables. Les autorisations pour les stations STI-C mobiles et fixes spéciales ne sont accordées que par les États membres responsables. La CPS des CA racine ou des sous-CA délivrant des certificats pour ce type de véhicules dans ces États membres détermine la façon dont le processus de certification s'applique à ces véhicules.

(117) Lorsque le souscripteur est en train de migrer une station STI-C d'une EA à une autre, la station STI-C peut être enregistrée auprès de deux EA (similaires).

(118) Une station STI-C génère une paire de clés AT (voir section 6.1) et crée une demande d'AT conformément à [1]. D'autres protocoles peuvent être utilisés, pour autant que [1] soit mise en œuvre.

(119) Les stations STI-C adressent une demande d'autorisation à l'URL de l'AA (flux 32 et 26) en envoyant au moins les renseignements mentionnés dans la section 3.2.3.3). L'AA et l'EA valident l'autorisation pour chaque demande conformément aux sections 3.2.6 et 4.2.2.5.

4.2. Traitement des demandes de certificat

4.2.1. Exécution des fonctions d'identification et d'authentification

4.2.1.1. Identification et authentification des CA racine

(120) Le mandataire de la CPA est chargé de l'authentification du mandataire de la CA racine et de l'approbation de son processus d'inscription conformément à la section 3.

4.2.1.2. Identification et authentification du TLM

(121) Le mandataire de la CPA est chargé de l'authentification du mandataire du TLM et de l'approbation de son formulaire de demande de processus d'inscription conformément à la section 3.

4.2.1.3. Identification et authentification de l'EA et l'AA

(122) La CA racine correspondante est chargée de l'authentification du mandataire de l'EA/AA et de l'approbation de son formulaire de demande de processus d'inscription conformément à la section 3.

(123) La CA racine confirme sa validation positive du formulaire de demande à l'EA/AA. L'EA/AA peut ensuite envoyer une demande de certificat à la CA racine (flux 21/24), qui délivre les certificats à l'EA/AA correspondante (flux 18/19).

4.2.1.4. Identification et authentification du souscripteur EE

(124) Avant qu'une station STI-C puisse demander un certificat EC, le souscripteur EE transmet de façon sécurisée les renseignements d'identification de la station STI-C à l'EA (flux 33). L'EA vérifie la demande et, si le résultat est positif, enregistre les renseignements relatifs à la station STI-C dans sa base de données centrale et confirme cet enregistrement au souscripteur EE (flux 35). Cette opération n'est effectuée qu'une seule fois par le fabricant ou l'exploitant pour chaque station STI-C. Une fois qu'une station STI-C est enregistrée par une EA, elle peut demander un seul certificat EC (flux 31) à la fois. L'EA

authentifie les renseignements contenus dans la demande de certificat EC et vérifie qu'ils sont valides pour une station STI-C.

4.2.1.5. Tickets d'autorisation

(125) Lors de demandes d'autorisation (flux 32), conformément à [1], l'AA doit authentifier l'EA de laquelle la station STI-C a reçu son EC. D'autres protocoles peuvent être utilisés, pour autant que [1] soit mise en œuvre. Si l'AA n'est pas en mesure d'authentifier l'EA , la demande est rejetée (flux 26). L'AA doit impérativement posséder le certificat EA pour authentifier l'EA et vérifier sa réponse (flux 25 et 23, section 3.2.5.3).

(126) L'EA authentifie la station STI-C demandant un AT en vérifiant son EC (flux 25 et 23).

4.2.2. Approbation ou rejet des demandes de certificat

4.2.2.1. Approbation ou rejet des certificats de la CA racine

(127) Le TLM insère/supprime les certificats de la CA racine dans l'ECTL conformément à l'approbation de la CPA (flux 1/2).

(128) Le TLM doit vérifier la signature, les renseignements et l'encodage des certificats de la CA racine après avoir reçu une approbation de la CPA (flux 1). Après la validation et l'approbation de la CPA, le TLM met le certificat racine correspondant sur l'ECTL et notifie la CPA (flux 5).

4.2.2.2. *Approbation ou rejet du certificat du TLM*

(129) La CPA est responsable de l'approbation ou du rejet des certificats du TLM.

4.2.2.3. *Approbation ou rejet des certificats de l'EA et de l'AA*

(130) La CA racine vérifie les demandes de certificat des sous-CA (flux 21/24) et les rapports correspondants (délivrés par l'auditeur agréé de la PKI) lorsqu'elle les reçoit (flux 36, section 8) de la sous-CA de la CA racine correspondante. Si le résultat de la vérification est positif, la CA racine correspondante délivre un certificat à l'EA/AA (flux 18/19); dans le cas contraire, la demande est rejetée et aucun certificat n'est délivré à l'EA /AA.

4.2.2.4. Approbation ou rejet de l'EC

(131) L'EA vérifie et valide les demandes d'EC conformément aux sections 3.2.3.2 et 3.2.5.3.

(132) Si la demande de certificat conformément à [1] est correcte et valide, l'EA génère le certificat demandé.

(133) Si la demande de certificat n'est pas valide, l'EA la refuse et envoie une réponse exposant le motif de refus conformément à [1]. Si une station STI-C souhaite toujours obtenir un EC, elle dépose une nouvelle demande de certificat. D'autres protocoles peuvent être utilisés, pour autant que [1] soit mise en œuvre.

4.2.2.5. Approbation ou rejet de l'AT

(134) La demande de certificat est vérifiée par l'EA. L'AA établit la communication avec l'EA pour valider la demande (flux 25). L'EA authentifie la station STI-C à l'origine de la demande et détermine si elle est en droit de recevoir l'AT demandé selon la CP (par exemple, en vérifiant le statut de révocation et la

validité de la durée/région, les autorisations; le niveau de garantie, etc.). L'EA retourne une réponse de validation (flux 23) et, si cette réponse est positive, l'AA génère le certificat demandé et le transmet à la station STI-C. Si la demande d'AT n'est pas correcte ou si la réponse de validation de l'EA est négative, l'AA rejette la demande. Si une station STI-C souhaite toujours obtenir un AT, elle dépose une nouvelle demande d'autorisation.

4.2.3. Délai de traitement des demandes de certificat

4.2.3.1. Demande de certificat de CA racine

(135) Le traitement du processus d'identification et d'authentification d'une demande de certificat a lieu pendant les jours ouvrables et est soumis à un délai maximal prévu dans la CPS de la CA racine.

4.2.3.2. *Demande de certificat du TLM*

(136) Le traitement de la demande de certificat du TLM est soumis à un délai maximal prévu dans la CPS du TLM.

4.2.3.3. *Demande de certificat de l'EA et de l'AA*

(137) Le traitement du processus d'identification et d'authentification d'une demande de certificat a lieu pendant les jours ouvrables conformément à l'accord et au contrat entre la CA racine de l'État membre/de l'organisation privée et la sous-CA. Le temps de traitement de la demande de certificat de la sous-CA est soumis à un délai maximal prévu dans la CPS de la sous-CA.

4.2.3.4. *Demande d'EC*

(138) Le traitement des demandes d'EC est soumis à un délai maximal prévu dans la CPS de l'EA.

4.2.3.5. *Demande d'AT*

(139) Le traitement des demandes d'AT est soumis à un délai maximal prévu dans la CPS de l'AA.

4.3. Délivrance des certificats

4.3.1. Tâches de la CA lors de la délivrance des certificats

4.3.1.1. Délivrance de certificat par la CA racine

(140) Les CA racine délivrent leurs propres certificats de CA racine autosignés, leurs certificats de lien, leurs certificats de sous-CA et CRL.

(141) Après approbation de la CPA (flux 4), la CA racine envoie son certificat au TLM via le CPOC, pour qu'il soit ajouté à l'ECTL (flux 11 et 8) (voir section 4.1.2.1). Le TLM vérifie si la CPA a approuvé le certificat (flux 1).

4.3.1.2. *Délivrance de certificat du TLM*

(142) Le TLM délivre son propre certificat de TLM et de lien autosigné et l'envoie au CPOC (flux 6).

4.3.1.3. Délivrance de certificat d'EA et AA

(143) Les sous-CA génèrent une demande de certificat signée et la transmettent à la CA racine correspondante (flux 21 et 24). La CA racine vérifie la demande et délivre un certificat à la sous-CA à l'origine de la demande, conformément à [5], dans les plus brefs délais, comme prévu dans la CPS pour les pratiques

opérationnelles habituelles, mais au plus tard cinq jours ouvrables après réception de la demande.

(144) La CA racine met à jour le répertoire contenant les certificats des sous-CA.

4.3.1.4. Délivrance de l'EC

(145) La station STI-C transmet une demande d'EC à l'EA conformément à [1]. L'EA authentifie et vérifie que les informations contenues dans la demande de certificat sont valides pour une station STI-C. D'autres protocoles peuvent être utilisés, pour autant que [1] soit mise en œuvre.

(146) Si le résultat de la validation est positif, l'EA délivre un certificat conformément à l'enregistrement de la station STI-C (voir 4.2.1.4) et l'envoie à la station STI-C en utilisant un message de réponse d'EC conformément à [1]. D'autres protocoles peuvent être utilisés, pour autant que [1] soit mise en œuvre.

(147) S'il n'existe pas d'enregistrement, l'EA génère un code d'erreur et l'envoie à la station STI-C en utilisant un message de réponse d'EC conformément à [1]. D'autres protocoles peuvent être utilisés, pour autant que [1] soit mise en œuvre.

(148) Les demandes et les réponses d'EC sont chiffrées afin de garantir la confidentialité et sont signées afin de garantir l'authentification et l'intégrité.

4.3.1.5. Délivrance d'AT

(149) La station STI-C envoie un message de demande d'AT à l'AA conformément à [1]. L'AA envoie une demande de validation de l'AT, conformément à [1], à l'EA. L'EA envoie une réponse de validation de l'AT à l'AA. Si cette réponse est positive, l'AA génère un AT et l'envoie à la station STI-C en utilisant un message de réponse d'AT conformément à [1]. En cas de réponse négative, l'AA génère un code d'erreur et l'envoie à la station STI-C en utilisant un message de réponse d'AT conformément à [1]. D'autres protocoles peuvent être utilisés, pour autant que [1] soit mise en œuvre.

(150) Les demandes et les réponses d'AT sont chiffrées (cela n'est nécessaire que pour les stations mobiles STI-C mobiles) afin de garantir la confidentialité et sont signées afin de garantir l'authentification et l'intégrité.

4.3.2. Notification au souscripteur de la délivrance des certificats par la CA

Sans objet.

4.4. Acceptation des certificats

4.4.1. Acceptation des certificats

4.4.1.1. CA racine

Sans objet.

4.4.1.2. *TLM*

Sans objet.

4.4.1.3. EA et AA

(151) L'EA/AA vérifie le type de certificat, la signature et les informations figurant dans le certificat reçu. L'EA/AA rejette tous les certificats de l'EA/AA qui ne sont pas correctement vérifiés et émet une nouvelle demande.

4.4.1.4. Station STI-C

(152) La station STI-C vérifie la réponse d'EC/AT reçue de l'EA/AA par rapport à sa demande initiale, y compris la signature et la chaîne de certification. Elle rejette toutes les réponses d'EC/AT qui ne sont pas correctement vérifiées. En pareils cas, elle doit envoyer une nouvelle demande d'EC/AT.

4.4.2. Publication du certificat

(153) Les certificats du TLM et leurs certificats de lien sont mis à la disposition de tous les participants par l'intermédiaire du CPOC.

(154) Les certificats de la CA racine sont publiés par le CPOC via l'ECTL, qui est signé par le TLM.

(155) Les certificats des sous-CA (EA et AA) sont publiés par la CA racine.

(156) Les EC et les AT ne sont pas publiés.

4.4.3. Notification de la délivrance des certificats

Il n'y a pas de notifications de délivrance.

4.5. Utilisation des paires de clés et des certificats

4.5.1. ***Utilisation de la clé privée et du certificat***

4.5.1.1. Utilisation de la clé privée et du certificat pour le TLM

(157) Le TLM utilise ses clés privées pour signer ses propres certificats (du TLM et de lien) et l'ECTL.

(158) Le certificat du TLM est utilisé par les participants à une PKI afin de vérifier l'ECTL et d'authentifier le TLM.

4.5.1.2. Utilisation de la clé privée et du certificat pour les CA racine

(159) Les CA racine utilisent leurs clés privées pour signer leurs propres certificats, les CRL, les certificats de lien et les certificats de l'EA/AA.

(160) Les certificats de la CA racine sont utilisés par les participants à la PKI afin de vérifier les certificats de l'AA et de l'EA connexes, les certificats de lien et les CRL.

4.5.1.3. Utilisation de la clé privée et du certificat pour les EA et les AA

(161) Les EA utilisent leurs clés privées pour signer les EC et pour le déchiffrement des demandes d'inscription.

(162) Les certificats d'EA sont utilisés pour vérifier la signature des EC connexes et pour le chiffrement des demandes d'EC et d'AT par les EE tels que défini dans [1].

(163) Les AA utilisent leurs clés privées pour signer les AT et déchiffrer les demandes d'AT.

(164) Les certificats des AA sont utilisés par les EE pour vérifier les AT connexes et chiffrer les demandes d'AT tel que défini dans [1].

4.5.1.4. Utilisation de la clé privée et du certificat pour l'entité finale

(165) Les EE utilisent la clé privée correspondant à un EC valide afin de signer une nouvelle demande d'inscription telle que définie dans [1]. La nouvelle clé privée est utilisée pour créer la signature interne dans la demande afin de prouver la possession de la clé privée correspondant à la nouvelle clé publique d'EC.

(166) Les EE utilisent la clé privée correspondant à un EC valide afin de signer une demande d'autorisation telle que définie dans [1]. La clé privée correspondant au nouvel AT doit être utilisée pour créer la signature interne dans la demande afin de prouver la possession de la clé privée correspondant à la nouvelle clé publique de l'AT.

(167) Les EE utilisent la clé privée correspondant à un AT approprié afin de signer les messages des STI-C tels que définis dans [5].

4.5.2. ***Utilisation du certificat et de la clé publique par une partie utilisatrice***

(168) Les parties utilisatrices utilisent la voie de certification de confiance et les clés publiques qui y sont associées aux fins visées dans les certificats et pour authentifier l'identité commune de confiance des EC et des AT.

(169) Les certificats de la CA racine, de l'EA et de l'AA, les EC et les AT ne sont pas utilisés sans vérification préliminaire par une partie utilisatrice.

4.6. Renouvellement de certificat

Non autorisé.

4.7. Régénération de clés de certificat

4.7.1. Circonstances de la régénération des clés de certificat

(170) La régénération des clés de certificat a lieu lorsqu'un certificat atteint la fin de sa durée de vie ou lorsqu'une clé privée arrive à la fin de son utilisation opérationnelle, mais que la relation de confiance avec la CA existe toujours. Une nouvelle paire de clés et le certificat correspondant sont générés et délivrés dans tous les cas.

4.7.2. Qui peut demander la régénération

4.7.2.1. CA racine

(171) La CA racine ne demande pas de régénération. Le processus de régénération est un processus interne pour la CA racine car c'est elle-même qui signe son certificat. La CA racine procède à une régénération soit avec des certificats de lien, soit par une nouvelle délivrance (voir section 4.3.1.1).

4.7.2.2. *TLM*

(172) Le TML ne demande pas de régénération. Le processus de régénération est interne pour le TML car c'est lui-même qui signe son certificat.

4.7.2.3. EA et AA

(173) Il convient que la demande de certificat de la sous-CA soit soumise en temps utile afin d'avoir la certitude que le nouveau certificat de sous-CA et la paire de clés de sous-CA seront opérationnels avant l'expiration de la clé de sous-CA privée en vigueur. La date de dépôt doit également tenir compte du délai requis pour l'approbation.

4.7.2.4. station STI-C

Sans objet.

4.7.3. Traitement des demandes de régénération des clés de certificat

4.7.3.1. Certificat du TLM

(174) Le TLM décide de la régénération des clés sur la base des exigences énoncées aux sections 6.1 et 7.2. Le processus détaillé est exposé dans sa CPS.

(175) Le TLM exécute le processus de régénération des clés en temps utile afin que les nouveaux certificats du TLM et certificat de lien puissent être diffusés à tous les participants avant l'expiration du certificat de TLM en vigueur.

(176) Le TLM utilise les certificats de lien pour la régénération des clés et afin de garantir la relation de confiance du nouveau certificat autosigné. Le certificat du TLM et le certificat de lien nouvellement générés sont transférés au CPOC.

4.7.3.2. Certificat de CA racine

(177) La CA racine décide de la régénération des clés sur la base des exigences énoncées aux sections 6.1.5 et 7.2. Le processus détaillé doit être défini dans sa CPS.

(178) La CA racine exécute le processus de régénération des clés en temps utile (avant l'expiration du certificat de la CA racine) afin de permettre l'insertion du nouveau certificat dans l'ECTL avant le début de la validité du certificat de la CA racine (voir section 5.6.2). Le processus de régénération des clés est effectué soit via les certificats de lien, soit comme une demande initiale.

4.7.3.3. certificats d'EA et d'AA

(179) L'EA ou l'AA demande un nouveau certificat comme suit:

Étape	**Indications**	**Demande de régénération des clés**
1	**Génération de paires de clés**	Les sous-CA (EA et AA) génèrent de nouvelles paires de clés conformément à la section 6.1.
2	**Génération de demande de certificat et signature interne**	La sous-CA génère une demande de certificat à partir de la clé publique nouvellement générée, en prenant en considération le système de dénomination (subject_info) de la section 3, l'algorithme de signature, les SSP (autorisations spécifiques de service) et les paramètres facultatifs supplémentaires, et génère la signature interne avec la nouvelle clé privée correspondante. Si une clé de chiffrement est requise, la sous-CA doit également prouver la possession de la clé de déchiffrement correspondante.
3	**Générer une signature externe**	L'ensemble de la demande est signée avec la clé privée valide en vigueur afin de garantir l'authenticité de la demande signée.
4	**Envoyer une demande à la CA racine**	La demande signée est présentée à la CA racine correspondante.
5	**Vérification de la demande**	La CA racine correspondante vérifie l'intégrité et l'authenticité de la demande. Elle vérifie d'abord la signature externe. Si le résultat de cette vérification est positif, elle vérifie la signature interne. Lorsqu'il existe une preuve de possession de la clé de déchiffrement privée, elle vérifie également cette preuve.
6	**Accepter ou rejeter la**	Si tous les contrôles aboutissent à un résultat positif, la CA racine

	demande	accepte la demande; dans le cas contraire, elle la rejette.
7	**Générer et délivrer un certificat**	La CA racine génère un nouveau certificat et le remet à la sous-CA qui en fait la demande.
8	**Envoyer la réponse**	La sous-CA envoie un message sur le statut (quant à la réception ou non du certificat) à la CA racine.

Tableau 3: Processus de régénération des clés pour les EA et les AA

(180) Au cours de la régénération automatique des clés pour les sous-CA, la CA racine veille à ce que le demandeur soit bien en possession de sa clé privée. Des protocoles appropriés pour la preuve de possession des clés de déchiffrement privées sont appliqués, par exemple comme définis dans le RFC 4210 et 4211. Pour les clés de signature privées, la signature interne doit être utilisée.

4.7.3.4. Certificats de la station STI-C

Sans objet pour les AT.

4.8. Modification d'un certificat

Non autorisée.

4.9. Révocation et suspension de certificat

Voir section 7

4.10. Services d'état des certificats

4.10.1. Caractéristiques opérationnelles

Sans objet

4.10.2. Disponibilité du service

Sans objet

4.10.3. Caractéristiques optionnelles

Sans objet

4.11. Fin de la souscription

Sans objet

4.12. Séquestre et récupération des clés

4.12.1. Souscripteur

4.12.1.1. Quelles paires de clés peuvent être mises sous séquestre

Sans objet.

4.12.1.2. Qui peut présenter une demande de récupération

Sans objet.

4.12.1.3. Processus de récupération et responsabilités

Sans objet.

4.12.1.4. Identification et authentification

Sans objet.

4.12.1.5. Approbation ou rejet des demandes de récupération

Sans objet.

4.12.1.6. Actions KEA et KRA pendant la récupération de la paire de clés

Sans objet.

4.12.1.7. Disponibilité de KEA et KRA

Sans objet.

4.12.2. Politique et pratiques d'encapsulation et de récupération des clés de session

Sans objet.

5. INSTALLATION, GESTION ET CONTROLES OPERATIONNELS

(181) La PKI est composée de la CA racine, de l'EA/AA, du CPOC et du TLM, y compris leurs composants de TIC (par exemple, les réseaux et les serveurs).

(182) Dans la présente section, l'entité responsable d'un élément de la PLK est identifiée par l'élément lui-même. En d'autres termes, la phrase «la CA est chargée d'exécuter l'audit» est équivalente à «l'entité ou le personnel qui gère la CA est chargé d'exécuter...».

(183) L'expression «éléments du modèle de confiance des STI-C» comprend la CA racine, le TLM, l'EA/AA, le CPOC et le réseau sécurisé.

5.1. Contrôles physiques

(184) Toutes les opérations du modèle de confiance des STI-C sont menées dans un environnement physiquement protégé, qui dissuade, prévient et détecte l'utilisation et l'accès non autorisés des informations et systèmes sensibles ou leur divulgation. Les éléments du modèle de confiance des STI-C utilisent des contrôles de sécurité physique conformément aux normes ISO 27001 et ISO 27005.

(185) Les entités qui gèrent les éléments du modèle de confiance des STI-C décrivent les contrôles de sécurité physiques, des procédures et du personnel dans leur CPS. En particulier, la CPS couvre des informations sur l'emplacement du site et la construction des bâtiments ainsi que leurs contrôles de sécurité physiques garantissant un accès contrôlé à tous les locaux utilisés dans l'installation des entités du modèle de confiance des STI-C.

5.1.1. Emplacement et construction des installations

5.1.1.1. CA racine, CPOC, TLM

(186) L'emplacement et la construction de l'installation abritant l'équipement et les données de la CA racine, du CPOC et du TLM (HSM, données d'activation, sauvegarde de la paire de clés, ordinateur, journaux de vérification, scénario de la cérémonie des clés, demande de certificat, etc.) sont compatibles avec les installations utilisées pour héberger les informations sensibles et de grande valeur. La CA racine est exploitée dans une zone physique dédiée, séparée des autres zones physiques des composantes de la PKI.

(187) La CA racine, le CPOC et le TLM mettent en œuvre des politiques et procédures visant à garantir le maintien d'un niveau élevé de sécurité dans l'environnement physique dans lequel l'équipement de la CA racine est installé afin de garantir:

- qu'il est isolé des réseaux extérieurs au modèle de confiance;
- qu'il est scindé en une série de (au moins deux) périmètres physiques de plus en plus sécurisés;
- que les données sensibles (HSM, sauvegarde de paires de clés, données d'activation, etc.) sont stockées dans un coffre dédié situé dans une zone physique dédiée sous un contrôle d'accès multiple.

(188) Les techniques de sécurité employées sont conçues pour résister à un grand nombre de différentes formes d'attaque qui peuvent être combinées. Les mécanismes utilisés incluent au moins:

- des alarmes périmétriques, une télévision en circuit fermé, des murs renforcés et des détecteurs de mouvement;
- une authentification à deux facteurs (par exemple, carte à puce et code PIN) pour chaque personne et un badge pour pénétrer dans les installations de la CA racine et dans la zone physique sécurisée et les quitter.

(189) La CA racine, le CPOC et le TLM utilisent un personnel autorisé pour surveiller constamment l'équipement des installations 7 jours sur 7, 24h sur 24, 365 jours par an. L'environnement opérationnel (par ex. les installations physiques) n'est jamais laissé sans surveillance. Le personnel de l'environnement opérationnel n'a jamais accès aux zones sécurisées de la CA racine ou des sous-CA à moins d'y être autorisé.

5.1.1.2. *EA/AA*

(190) Les mêmes dispositions que celles qui figurent à la section 5.1.1.1 s'appliquent.

5.1.2. Accès physique

5.1.2.1. CA racine, CPOC, TLM

(191) L'équipement et les données (HSM, données d'activation, sauvegarde de paires de clés, ordinateur, journal, scénario de la cérémonie des clés, demande de certificat, etc.) sont toujours protégés contre un accès non autorisé. Les mécanismes de sécurité physique pour les équipements, au minimum:

- exercent une surveillance continue, soit manuellement soit par voie électronique, pour repérer toute intrusion non autorisée;
- garantissent qu'aucun accès non autorisé au matériel et aux données d'activation n'est permis;
- garantissent que tous les supports amovibles et documents papier contenant des informations sensibles en texte clair sont stockés dans un conteneur sécurisé;
- garantissent qu'aucune personne non autorisée à titre permanent entrant dans des zones sécurisées n'est laissée hors de la surveillance d'un

membre du personnel autorisé de la CA racine, du CPOC et des installations du TLM;

- garantissent qu'un registre d'accès est maintenu et contrôlé périodiquement;
- fournissent au moins deux couches de sécurité progressivement renforcée, par exemple au niveau du périmètre, du bâtiment et de la salle opérationnelle;
- requièrent deux contrôles de l'accès physique des rôles de confiance pour le HSM et les données d'activation cryptographiques.

(192) Un contrôle de sécurité des installations abritant l'équipement est effectué s'il est prévu de le laisser sans surveillance. Au minimum, le contrôle permet de vérifier que:

- l'équipement est dans un état approprié pour le mode de fonctionnement en vigueur;
- pour les composantes hors ligne, tout l'équipement est arrêté;
- tous les conteneurs de sécurité (enveloppe inviolable, coffre, etc.) sont correctement sécurisés;
- les systèmes de sécurité physiques (par exemple, verrous de portes, couvercles d'aération, électricité) fonctionnent correctement;
- la zone est protégée contre un accès non autorisé.

(193) Les modules cryptographiques amovibles sont désactivés avant le stockage. Lorsqu'ils ne sont pas utilisés, ces modules et les données d'activation utilisées pour y accéder ou les activer sont placés dans un coffre. Les données d'activation sont mémorisées ou enregistrées et stockées d'une manière correspondant à la sécurité assurée au module cryptographique. Elles ne sont pas stockées avec le module cryptographique, afin d'éviter qu'une seule personne n'ait accès à la clé privée.

(194) Une personne ou un groupe assumant de rôles de confiance sont explicitement chargés d'effectuer ces contrôles. Lorsque la responsabilité est confiée à un groupe de personnes, un journal est tenu et identifie la personne qui effectue chaque vérification. Si les installations ne sont pas constamment occupées, la dernière personne à partir paraphe un registre de sortie indiquant la date et l'heure, et confirme que tous les mécanismes de protection physiques nécessaires sont en place et activés.

5.1.2.2. *EA/AA*

(195) Les mêmes dispositions de la section 5.1.2.1 s'appliquent.

5.1.3. Alimentation électrique et climatisation

(196) Les installations sécurisées des éléments du modèle de confiance des STI-C (CA racine, CPOC, TLM, EA et AA) sont équipées d'un accès fiable à l'alimentation électrique afin de garantir un fonctionnement sans défaillance ou avec des défaillances mineures. Des installations principales et de secours sont requises en cas de panne d'alimentation externe et il convient d'assurer un arrêt ordonné de l'équipement du modèle de confiance des STIC en cas d'absence d'alimentation. Les installations du modèle de confiance des STI-C sont

équipées de systèmes de chauffage/ventilation/climatisation permettant de maintenir la température et l'humidité relative de l'équipement du modèle de confiance des STI-C dans la plage de fonctionnement. La CPS de l'élément du modèle de confiance des STI-C décrira en détail le plan et les processus de mise en œuvre de ces exigences.

5.1.4. Exposition à l'eau

(197) Les installations sécurisées des éléments du modèle de confiance des STI-C (CA racine, CPOC, TLM, EA et AA) doivent être protégées de manière à réduire au maximum les conséquences d'une exposition à l'eau. Pour cette raison, il convient d'éviter les canalisations d'eau et les tuyaux d'écoulement. La CPS de l'élément du modèle de confiance des STI-C décrira en détail le plan et les processus de mise en œuvre de ces exigences.

5.1.5. Prévention et protection contre les incendies

(198) Pour éviter une exposition dommageable au feu ou à la fumée, les installations sécurisées des éléments du modèle de confiance des STIC (CA racine, CPOC, TLM, EA et AA) sont construites et équipées en conséquence et des procédures sont mises en œuvre pour répondre aux menaces liées au feu. Le stockage des supports doit être protégé contre les incendies dans des conteneurs appropriés.

(199) Les éléments du modèle de confiance des STI-C protègent les supports physiques contenant des sauvegardes des données de système essentielles ou toute autre information sensible contre les risques de l'environnement ainsi que l'utilisation non autorisée, l'accès et la divulgation. La CPS de l'élément du modèle de confiance des STI-C décrira en détail le plan et les processus de mise en œuvre de ces exigences.

5.1.6. Gestion des supports

(200) Les supports utilisés dans les éléments du modèle de confiance des STI-C (CA racine, CPOC, TLM, EA et AA) sont manipulés de manière sécurisée afin d'être protégés de tout dommage, vol et accès non autorisé. Des procédures de gestion des supports sont mises en œuvre afin de protéger les supports contre l'obsolescence et la détérioration au cours de la période pendant laquelle les enregistrements doivent être conservés.

(201) Les données sensibles sont protégées contre les accès résultant d'une réutilisation d'objets de stockage (par exemple, des fichiers supprimés), qui pourraient rendre les données sensibles accessibles à des utilisateurs non autorisés.

(202) Un inventaire de toutes les ressources d'information est tenu et les exigences définies pour la protection de ces ressources sont cohérentes avec l'analyse de risque. La CPS de l'élément du modèle de confiance des STI-C décrira en détail le plan et les processus de mise en œuvre de ces exigences.

5.1.7. Élimination des déchets

(203) Les éléments du modèle de confiance des STI-C (CA racine, CPOC, TLM, EA et AA) mettent en œuvre des procédures d'élimination sûre et irréversible des déchets (papier, supports ou tout autre déchet) afin d'empêcher que des déchets contenant des informations confidentielles/privées ne fassent l'objet d'une utilisation non autorisée, d'un accès ou d'une divulgation. Tous les supports

utilisés pour le stockage des informations sensibles, telles que des clés, des données d'activation ou des fichiers, sont détruits avant d'être évacués pour leur élimination. La CPS de l'élément du modèle de confiance des STI-C décrira en détail le plan et les processus de mise en œuvre de ces exigences.

5.1.8. Sauvegarde hors site

5.1.8.1. CA racine, CPOC et TLM

(204) Des sauvegardes complètes des composantes de la CA racine, du CPOC et du TLM, suffisantes pour permettre une récupération en cas de panne du système, sont effectuées hors ligne après le déploiement de la CA racine, du CPOC et du TLM, et après la création de chaque nouvelle paire de clés. Des copies de sauvegarde des renseignements opérationnels essentiels (paire de clés et CRL) et des logiciels sont effectuées régulièrement. Des dispositifs de sauvegarde adéquats sont fournis de façon à ce que tous les renseignements opérationnels essentiels et les logiciels puissent être récupérés après un sinistre ou une défaillance des supports. Les modalités de sauvegarde pour les systèmes individuels sont régulièrement mises à l'épreuve afin de s'assurer qu'elles satisfont aux exigences du plan de continuité des activités. Au moins une copie de sauvegarde complète est stockée dans un emplacement hors site (récupération après sinistre). La copie de sauvegarde est stockée sur un site présentant des contrôles physiques et des procédures équivalents à ceux du système opérationnel de la PKI.

(205) Les données de sauvegarde sont soumises aux mêmes exigences d'accès que les données opérationnelles. Les données de sauvegarde sont chiffrées et stockées hors site. En cas de perte totale des données, les informations requises pour remettre la CA racine, le CPOC et le TLM en exploitation sont entièrement récupérées à partir des données de sauvegarde.

(206) Le matériel privé de la CA racine, du CPOC et du TLM signé avec clé n'est pas sauvegardé au moyen de mécanismes de sauvegarde standard, mais en utilisant la fonction de sauvegarde du module cryptographique.

5.1.8.2. *EA/AA*

(207) Les processus décrits dans la section 5.1.8.1 s'appliquent à la présente section.

5.2. Contrôles des procédures

La présente section décrit les exigences applicables aux rôles, aux fonctions et à l'identification des membres du personnel.

5.2.1. Rôles de confiance

(208) Les membres du personnel, les contractants et les consultants qui se voient assigner des rôles de confiance sont considérés comme des «personnes de confiance». Les personnes souhaitant devenir des personnes de confiance pour obtenir un poste de confiance respectent les exigences de contrôle de la présente politique de certification.

(209) Les personnes de confiance contrôlent ou ont accès aux opérations d'authentification ou cryptographiques susceptibles d'affecter sensiblement:

- la validation des informations contenues dans des demandes de certificats;

- l’acceptation, le rejet ou autre traitement des demandes de certificats, des demandes de déchéance ou des demandes de renouvellement;
- la délivrance ou la révocation des certificats, y compris le personnel ayant accès à des parties restreintes de leur répertoire ou le traitement des informations ou des demandes relatives aux souscripteurs.

(210) Les rôles de confiance comprennent, mais sans s’y limiter:

- le service à la clientèle;
- l’administration du système;
- l’ingénierie désignée;
- les cadres chargés de la gestion de la fiabilité de l’infrastructure.

(211) La CA fournit des descriptions claires de tous les rôles de confiance dans sa CPS.

5.2.2. Nombre de personnes requises par tâche

(212) Les éléments du modèle de confiance des STI-C établissent, maintiennent et appliquent des procédures de contrôle rigoureuses pour garantir la séparation des tâches fondées sur les rôles de confiance et veiller à ce que plusieurs personnes de confiance soient requises pour exécuter les tâches sensibles. Les éléments du modèle de confiance des STI-C (TLM, CPOC, CA racine, EA et AA) doivent satisfaire à [4] ainsi qu’aux exigences énoncées dans les paragraphes suivants.

(213) Une politique et des procédures de contrôle sont en place pour garantir une séparation des tâches fondée sur les responsabilités inhérentes au poste. Les tâches les plus sensibles, telles que l’accès au matériel cryptographique de la CA (HSM) et à son matériel connexe signé avec clé, ainsi que leur gestion, doivent requérir l’autorisation de plusieurs personnes de confiance.

(214) Ces procédures de contrôle internes sont conçues de façon à ce qu’au moins deux personnes de confiance soient requises pour avoir un accès physique ou logique au dispositif. Les restrictions relatives à l’accès au matériel cryptographique de la CA doivent être strictement appliquées par plusieurs personnes de confiance tout au long de son cycle de vie, de la réception et l’inspection à l’entrée à la destruction logique et/ou physique finale. Une fois qu’un module est activé avec des clés opérationnelles, de nouveaux contrôles de l’accès sont invoqués pour maintenir un contrôle fractionné sur l’accès tant physique que logique au dispositif.

5.2.3. Identification et authentification pour chaque rôle

(215) Toutes les personnes assignées à un rôle, telles que décrites dans la présente CP, sont identifiées et authentifiées de manière à garantir que le rôle leur permet d’exécuter leurs tâches de la PKI.

(216) Les éléments du modèle de confiance des STI-C vérifient et confirment l’identité et l’autorisation de toutes les personnes souhaitant devenir des personnes de confiance avant qu’elles ne se voient:

- délivrer leurs dispositifs d’accès et l’accès aux installations requises;

- accorder les authentifiants électroniques pour accéder à des fonctions spécifiques sur les systèmes de la CA et les exécuter.

(217) La CPS décrit les mécanismes utilisés pour identifier et authentifier les personnes.

5.2.4. Rôles nécessitant une séparation des tâches

(218) Les rôles nécessitant une séparation des tâches sont notamment (liste non exhaustive):

- l'acceptation, le rejet et la révocation des demandes, et autre traitement de demandes de certificats de la CA;
- la création, la délivrance et la destruction d'un certificat de la CA.

(219) La séparation des tâches peut être réalisée au travers de l'équipement de la PKI et/ou de procédures. Aucune personne ne peut se voir attribuer plus d'une identité, sauf autorisation de la CA racine.

(220) La partie de la CA racine et de la CA concernée par la gestion de la création et de la révocation des certificats est indépendante des autres organisations pour ses décisions relatives à l'établissement, à la prestation, au maintien et à la suspension de services conformément aux politiques de certification applicables. En particulier, son encadrement supérieur, son encadrement et son personnel investis de rôle de confiance sont exempts de toute pression commerciale, financière ou autre, susceptible d'influencer négativement la confiance dans les services qu'elle fournit.

(221) L'EA et l'AA qui servent les stations STI-C mobiles sont des entités opérationnelles distinctes, avec une infrastructure informatique et des équipes de gestion informatique distinctes. Conformément au RGPD, l'EA et l'AA n'échangent aucune donnée à caractère personnel, sauf pour l'autorisation des demandes d'AT. Elles transfèrent les données relatives à l'approbation des demandes d'AT en utilisant uniquement le protocole de validation des autorisations de [1], sur une interface sécurisée réservée. D'autres protocoles peuvent être utilisés, pour autant que [1] soit mise en œuvre.

(222) Les fichiers journaux stockés par l'EA et l'AA ne peuvent être utilisés qu'aux seules fins de la révocation des EC présentant un comportement anormal sur la base des AT dans des messages CAM/DENM malveillants interceptés. Après l'identification d'un message CAM/DENM comme étant malveillant, l'AA examinera la clé de vérification de l'AT dans ses journaux de délivrance et soumettra une demande de révocation à l'EA contenant la signature chiffrée sous la clé privée de l'EC qui a été utilisée lors de la délivrance de l'AT. Tous les fichiers journaux doivent être suffisamment protégés contre l'accès par des parties non autorisées et ne peuvent être partagés avec d'autres entités ou autorités.

Remarque: Au moment de la rédaction de la présente version de la CP, la fonction d'anomalie de comportement n'a pas été mise au point. L'éventuelle mise au point de la fonction d'anomalie de comportement est envisagée dans le cadre de futures révisions de la politique.

5.3. Contrôles du personnel

5.3.1. Exigences en matière de qualifications, d'expérience et d'habilitation de sécurité

(223) Les éléments du modèle de confiance des STI-C emploient un personnel en nombre suffisant, possédant l'expertise, l'expérience et les qualifications requises pour les fonctions inhérentes au poste et les services offerts. Le personnel d'une PKI satisfait à ces exigences en faisant valoir une formation et des références officielles et/ou une expérience concrète. Les rôles de confiance et les responsabilités, tels que précisés dans la CPS, sont documentés dans les descriptions de poste et clairement définis. Pour les sous-traitants du personnel d'une PKI, les descriptions de poste sont conçues afin de garantir la séparation des tâches et des privilèges, et la sensibilité du poste est déterminée sur la base des tâches et des niveaux d'accès, d'un examen des antécédents ainsi que de la formation et de la sensibilisation du personnel.

5.3.2. Procédures de vérification des antécédents

(224) Les éléments du modèle de confiance des STI-C procèdent à la vérification des antécédents concernant les membres du personnel désireux de devenir des personnes de confiance. Les vérifications des antécédents sont réitérées pour le personnel occupant des postes de confiance au moins tous les cinq ans.

(225) Les facteurs suivants (liste non exhaustive), mis en évidence lors d'une vérification des antécédents, peuvent être considérés comme des motifs de rejet d'une candidature à un poste de confiance ou d'adoption de mesures à l'encontre d'une personne de confiance existante:

- des déclarations erronées faites par le candidat ou la personne de confiance;
- des références professionnelles très négatives ou peu fiables;
- certaines condamnations pénales;
- des indices d'une absence de responsabilité financière.

(226) Les rapports contenant ces informations sont évalués par le personnel des ressources humaines, qui prend des mesures raisonnables compte tenu de la nature, de l'ampleur et de la fréquence du comportement mis au jour par la vérification des antécédents. Cette action peut inclure des mesures allant jusqu'à l'annulation des offres d'emploi faites aux candidats pour des postes de confiance ou à la résiliation du contrat de travail des personnes de confiance existantes. L'utilisation d'informations révélées dans le cadre d'une vérification des antécédents est soumise à la législation applicable.

(227) Une enquête sur les antécédents des personnes souhaitant devenir des personnes de confiance inclut, sans s'y limiter:

- la confirmation d'un emploi antérieur;
- une vérification des références professionnelles couvrant une durée d'emploi d'au moins cinq ans;
- une confirmation du diplôme le plus élevé ou le plus pertinent obtenu;
- une recherche de casier judiciaire.

5.3.3. Exigences en matière de formation

(228) Les éléments du modèle de confiance des STI-C dispensent aux membres de leur personnel la formation requise pour qu'ils puissent s'acquitter avec compétence et de manière satisfaisante de leurs responsabilités liées aux opérations de la CA.

(229) Les programmes de formation sont réexaminés régulièrement et les formations abordent des questions qui intéressent les fonctions exercées par les membres de leur personnel.

(230) Les programmes de formation abordent des questions importantes pour l'environnement spécifique de la personne en formation, notamment:

- les principes et les mécanismes de sécurité du modèle de confiance des STI-C;
- les versions du matériel et du logiciel utilisés;
- l'ensemble des tâches dont la personne est supposée s'acquitter, et les procédures et séquences d'établissement de rapports internes et externes;
- les processus d'entreprise et flux de travail d'une PKI;
- le signalement et le traitement des incidents et compromissions;
- les procédures de récupération et continuité des activités après sinistre;
- des connaissances informatiques suffisantes.

5.3.4. Fréquence et exigences en matière de recyclage

(231) Les personnes assignées à des rôles de confiance sont tenues de rafraîchir de façon continue à l'aide d'un environnement de formation les connaissances qu'elles ont acquises par la formation. La formation doit être répétée autant de fois que nécessaire et au moins tous les deux ans.

(232) Les éléments du modèle de confiance des STI-C offrent aux membres de leur personnel une formation de remise à niveau et des mises à jour dans la mesure et avec la fréquence requises pour garantir le maintien du niveau de compétence requis dont ils ont besoin pour s'acquitter avec compétence et de manière satisfaisante de leurs responsabilités inhérentes au poste.

(233) Les personnes occupant des rôles de confiance sont informées des modifications intervenant dans les opérations de la PKI, le cas échéant. Toute modification significative apportée aux opérations est accompagnée d'un plan de formation (sensibilisation) et l'exécution de ce plan est documentée.

5.3.5. Fréquence et séquence de rotation des postes

(234) Aucune stipulation tant que les compétences techniques, l'expérience et les droits d'accès sont assurés. Les administrateurs des éléments du modèle de confiance des STI-C veillent à ce que les changements dans le personnel n'affectent pas la sécurité du système.

5.3.6. Sanctions pour des actions non autorisées

(235) Chaque élément du modèle de confiance des STI-C doit élaborer un processus disciplinaire formel afin de garantir que les actions non autorisées sont dûment

sanctionnées. Dans les cas les plus graves, l'assignation des rôles et les privilèges correspondants doivent être retirés.

5.3.7. Exigences concernant les contractants indépendants

(236) Les éléments du modèle de confiance des STI-C ne peuvent autoriser des contractants ou des consultants indépendants à devenir des personnes de confiance que dans la mesure où des relations de sous-traitance clairement définies l'exigent et à condition que l'entité ait confiance dans ces contractants ou consultants au même titre que s'ils faisaient partie de son personnel et que ceux-ci se conforment aux exigences applicables aux membres du personnel.

(237) Dans le cas contraire, les contractants et consultants indépendants n'ont accès aux installations sécurisées de la PKI des STI-C que s'ils sont escortés et sous la surveillance directe de personnes de confiance.

5.3.8. Documentation fournie au personnel

(238) Les éléments du modèle de confiance des STI-C dispensent aux membres de leur personnel la formation requise et leur donnent accès à la documentation qui leur est nécessaire pour s'acquitter avec compétence et de manière satisfaisante de leurs responsabilités inhérentes au poste.

5.4. Procédures relatives aux journaux d'audit

(239) La présente section définit les exigences en ce qui concerne les types d'événements à enregistrer et la gestion des journaux d'audit.

5.4.1. Types d'événements à enregistrer et à signaler par chaque CA

(240) Un représentant de la CA vérifie régulièrement les journaux, les événements et les procédures de la CA.

(241) Les éléments du modèle de confiance des STI-C enregistrent les types suivants d'événements d'audit (le cas échéant):

- accès aux installations physiques: l'accès par des personnes physiques aux installations sera enregistré par stockage des demandes d'accès à l'aide de cartes à puce. Un événement sera créé pour chaque enregistrement créé;
- gestion des rôles de confiance: tout changement dans la définition et le niveau d'accès des différents rôles sera enregistré, y compris la modification des attributs des rôles. Un événement sera créé pour chaque enregistrement créé;
- accès logique: un événement sera créé lorsqu'une entité (par ex. un programme) a accès aux zones sensibles (c.-à-d. réseaux et serveurs);
- gestion de sauvegarde: un événement est créé chaque fois qu'une sauvegarde est effectuée, avec ou sans succès;
- gestion des journaux: les journaux seront conservés. Un événement est créé lorsque le journal excède une taille déterminée;
- données du processus d'authentification pour les souscripteurs et les éléments du modèle de confiance des STI-C: des événements seront créés pour chaque demande d'authentification effectuée par les souscripteurs et les éléments du modèle de confiance des STI-C;

- acceptation et rejet des demandes de certificats, y compris la création et le renouvellement de certificats: un événement sera créé périodiquement avec une liste des demandes de certificats acceptées et rejetées au cours des sept derniers jours;
- enregistrement des fabricants: un événement sera créé lorsqu'un fabricant est enregistré;
- enregistrement d'une station STI-C: un événement sera créé lorsqu'une station STI-C est enregistrée;
- gestion du HSM: un événement sera créé lorsqu'une violation de la sécurité du HSM est enregistrée;
- gestion informatique et de réseau, dans la mesure où elle concerne les systèmes de la PKI: un événement sera créé lorsqu'un serveur de la PKI est arrêté ou relancé;
- gestion de la sécurité (tentatives fructueuses et infructueuses d'accès au système de la PKI, réalisation d'actions relatives à la PKI et au système de sécurité, changements du profil de sécurité, pannes du système, pannes de matériel et autres anomalies, activités relatives au pare-feu et au routeur; et entrées dans les installations de la PKI et sorties);
- les données liées aux événements seront conservées pendant au moins cinq ans, sauf si des règles nationales supplémentaires sont applicables.

(242) Conformément au RGPD, les journaux d'audit ne permettent pas l'accès aux données relatives à la vie privée en ce qui concerne les véhicules privés équipés d'une station STI-C.

(243) Dans la mesure du possible, les journaux d'audit de sécurité sont collectés automatiquement. Lorsque cela n'est pas possible, un journal, un formulaire papier ou un autre mécanisme physique est utilisé. Tous les journaux d'audit de sécurité, tant électroniques que non électroniques, sont conservés et mis à disposition au cours des audits de conformité.

(244) Chaque événement lié au cycle de vie du certificat est journalisé de manière à pouvoir être attribué à la personne qui l'a exécuté. Toutes les données relatives à une identité personnelle sont chiffrées et protégées contre les accès non autorisés.

(245) Au minimum, chaque enregistrement d'audit comprend les éléments suivants (enregistrés automatiquement ou manuellement pour chaque événement vérifiable):

- type d'événement (à partir de la liste ci-dessus);
- date et heure certifiées auxquelles l'événement s'est produit;
- résultat de l'événement — réussite ou échec s'il y a lieu;
- identité de l'entité et/ou de l'exploitant qui a causé l'événement, le cas échéant;
- identité de l'entité à laquelle l'événement s'adresse.

5.4.2. Fréquence de traitement des journaux

(246) Les journaux d'audit sont examinés en réponse à des alertes fondées sur des irrégularités et des incidents dans les systèmes de la CA et le sont en outre périodiquement, chaque année.

(247) Le traitement des journaux d'audit consiste à passer ces journaux en revue et à justifier par des documents tous les événements significatifs dans une synthèse des journaux d'audit. Les revues des journaux d'audit comprennent une vérification que le journal n'a pas été altéré, un contrôle de toutes les entrées du journal et une enquête sur toute alerte ou irrégularité dans les journaux. Les mesures prises sur la base des revues des journaux d'audit sont documentées.

(248) Le journal d'audit est archivé au moins une fois par semaine. Un administrateur l'archive manuellement si l'espace libre du disque pour le journal d'audit est inférieur au volume escompté des données du journal d'audit produites au cours de la semaine.

5.4.3. Période de conservation des journaux d'audit

(249) Les enregistrements de journaux relatifs aux cycles de vie des certificats sont conservés pendant au moins cinq ans après l'expiration du certificat correspondant.

5.4.4. Protection des journaux d'audit

(250) L'intégrité et la confidentialité du journal d'audit sont garanties par un mécanisme de contrôle de l'accès basé sur les rôles. Seuls les administrateurs peuvent accéder aux journaux d'audit internes; les utilisateurs disposant d'une autorisation appropriée peuvent également accéder aux journaux d'audit relatifs au cycle de vie des certificats via une page web avec un identifiant de connexion. L'accès doit être accordé avec une authentification multi-utilisateurs (au moins deux utilisateurs) et à deux niveaux au moins. Il y a lieu de garantir techniquement que les utilisateurs ne peuvent pas accéder à leurs propres fichiers journaux.

(251) Chaque entrée aux journaux est signée avec une clé provenant du HSM.

(252) Les journaux des événements contenant des informations pouvant conduire à une identification personnelle, telle qu'un véhicule privé, sont chiffrés de manière à ce que seules les personnes autorisées puissent les lire.

(253) Les événements sont journalisés de manière à ce qu'ils ne puissent pas être facilement supprimés ou détruits (sauf pour un transfert vers des supports de longue durée) au cours de la période pendant laquelle les journaux doivent être conservés.

(254) Les journaux d'événements sont protégés de manière à rester lisibles pendant toute la durée de leur stockage.

5.4.5. Procédures de sauvegarde des journaux d'audit

(255) Les journaux d'audit et les synthèses sont sauvegardés via des mécanismes de sauvegarde d'entreprise, sous le contrôle des rôles de confiance autorisés, séparés de la génération de la source de leurs composantes. Les sauvegardes des journaux d'audit sont protégées avec le même niveau de confiance qui s'applique aux journaux originaux.

5.4.6. Système de collecte des audits (interne ou externe)

(256) L'équipement des éléments du modèle de confiance des STI-C active les processus d'audit au démarrage du système et ne les désactive qu'à l'arrêt du système. Si les processus d'audit ne sont pas disponibles, l'élément du modèle de confiance des STI-C suspend son fonctionnement.

(257) À la fin de chaque période d'exploitation et lors de la régénération des clés de certificats, le statut collectif des équipements doit être signalé au gestionnaire des opérations et à l'organe régissant les opérations de l'élément de la PKI correspondant.

5.4.7. Notification du sujet ayant causé un événement

(258) Lorsqu'un événement est journalisé par le système de collecte de l'audit, cela garantit que l'événement est lié à un rôle de confiance.

5.4.8. Évaluation des vulnérabilités

(259) Le rôle chargé de réaliser l'audit et les rôles chargés de réaliser les opérations du système de la PKI dans les éléments du modèle de confiance des STI-C expliquent tous les événements significatifs dans une synthèse des journaux d'audit. Ces revues comprennent une vérification que le journal n'a pas été altéré et qu'il n'y a pas de discontinuité ou d'autre perte de données d'audit, puis un bref contrôle de toutes les entrées du journal, assorti d'une enquête plus approfondie de toutes les alertes ou irrégularités dans les journaux. Les mesures prises à la suite de ces revues sont documentées.

(260) Les éléments du modèle de confiance STI-C:

- mettent en œuvre des contrôles de détection et de prévention organisationnels et/ou techniques sous le contrôle des éléments du modèle de confiance des STI-C afin de protéger les systèmes de la PKI contre les virus et les logiciels malveillants;
- documentent et suivent un processus de correction des vulnérabilités qui couvre l'identification, l'examen, la réponse et la correction des vulnérabilités;
- subissent ou exécutent une analyse des vulnérabilités:
  - après toute modification du système ou du réseau déterminée par les éléments du modèle de confiance des STI-C comme étant importante pour les composantes de la PKI; et
  - au moins une fois par mois, sur les adresses IP publiques et privées indiquées par la CA, le CPOC comme étant les systèmes de la PKI,
- subissent un essai de pénétration sur les systèmes de la PKI, au moins une fois par an et après des mises à jour ou des modifications des infrastructures ou des applications, déterminées par les éléments du modèle de confiance des STI-C comme étant significatives pour la composante de la PKI de la CA;
- pour les systèmes en ligne, enregistrent les éléments prouvant que chaque analyse des vulnérabilités et essai de pénétration ont été réalisés par une personne ou une entité (ou un groupe collectif de ces dernières) disposant des compétences, des outils, des connaissances, du code de déontologie et de l'indépendance nécessaires pour fournir un essai de vulnérabilité ou de pénétration fiable;
- repèrent les vulnérabilités et y remédient conformément aux politiques d'entreprise en matière de cybersécurité et à la méthodologie d'atténuation des risques.

5.5. Archivage des enregistrements

5.5.1. Types d'enregistrements archivés

(261) Les éléments du modèle de confiance des STI-C archivent des enregistrements suffisamment détaillés pour permettre d'établir la validité d'une signature et le bon fonctionnement de la PKI. Au minimum, les enregistrements des événements de la PKI suivants sont archivés (le cas échéant):

- journal des accès physiques aux installations des éléments du modèle de confiance des STI-C (au minimum un an);
- journal de gestion des rôles de confiance pour les éléments du modèle de confiance des STI-C (minimum dix ans);
- journal des accès informatiques pour les éléments du modèle de confiance des STI-C (minimum cinq ans);
- journal de la création, de l'utilisation et de la destruction des clés de la CA (minimum cinq ans) (pas pour le TLM et le CPOC);

- journal de la création, de l'utilisation et de la destruction des certificats (minimum deux ans);
- journal des demandes de la CPA (minimum deux ans);
- journal de la gestion des données d'activation pour les éléments du modèle de confiance des STI-C (minimum cinq ans);
- journal informatique et de réseau pour les éléments du modèle de confiance des STI-C (minimum cinq ans);
- documentation de la PKI pour les éléments du modèle de confiance des STI-C (minimum cinq ans);
- rapport des incidents de sécurité et d'audit pour les éléments du modèle de confiance des STI-C (minimum dix ans);
- équipement, logiciels et configuration du système (minimum cinq ans).

(262) Les éléments du modèle de confiance des STI-C conservent les documents suivants relatifs aux demandes de certificats et à leur vérification, et tous les certificats des TLM, des CA racine et des CA ainsi que leur CRL, au moins sept ans après l'expiration de la validité de tout certificat basé sur ces documents:

- documents d'audit de la PKI conservés par les éléments du modèle de confiance des STI-C;
- documents de la CPS conservés par les éléments du modèle de confiance des STI-C;
- contrat entre la CPA et d'autres entités conservé par les éléments du modèle de confiance des STI-C;
- certificats (ou autres informations de révocation) conservés par la CA et le TLM;
- enregistrements des demandes de certificats dans le système de la CA racine (non applicable au TLM);
- autres données ou applications permettant de vérifier le contenu des archives;
- tous travaux liés aux éléments du modèle de confiance des STI-C et aux auditeurs de la conformité ou provenant de ceux-ci.

(263) L'entité de la CA conserve tous les documents relatifs aux demandes de certificats et à leur vérification, et tous les certificats ainsi que leur révocation, pendant au moins sept ans après l'expiration de la validité de tout certificat fondé sur ces documents.

5.5.2. Période de conservation des archives

(264) Sans préjudice des réglementations exigeant une période d'archivage plus longue, les éléments du modèle de confiance des STI-C conservent tous les enregistrements pendant au moins cinq ans après l'expiration du certificat correspondant.

5.5.3. Protection des archives

(265) Les éléments du modèle de confiance des STI-C conservent l'archive des enregistrements dans une installation de stockage sûre et sécurisée séparée de l'équipement de la CA, avec des contrôles de sécurité physique et procédurale équivalents ou supérieurs à ceux de la PKI.

(266) L'archive est stockée dans un système fiable qui garantit sa protection contre toute consultation, modification, suppression ou autre altération non autorisée.

(267) Les supports contenant les données d'archive et les applications requises pour les traiter sont maintenus de façon à ce qu'il soit possible d'y accéder pendant la période prévue dans la présente CP.

5.5.4. Archives système et stockage

(268) Les éléments du modèle de confiance des STI-C sauvegardent au fur et à mesure les archives système de ces informations sur une base quotidienne et effectuent des sauvegardes intégrales sur une base hebdomadaire. Des copies des enregistrements papier sont conservées dans une installation sécurisée hors site.

5.5.5. Exigences d'horodatage des enregistrements

(269) Les éléments du modèle de confiance des STI-C qui gèrent une base de données des révocations veillent à ce que les enregistrements contiennent des informations relatives à l'heure et à la date de création des enregistrements de révocation. L'intégrité de ces informations sera mise en œuvre à l'aide de solutions basées sur la cryptographie.

5.5.6. Système de collecte des archives (interne ou externe)

(270) Le système de collecte des archives est interne.

5.5.7. Procédures d'obtention et de vérification des informations archivées

(271) Tous les éléments du modèle de confiance des STI-C ne permettent l'accès aux archives qu'aux personnes de confiance autorisées. Les CA racine et les CA décrivent les procédures pour la création, la vérification, l'assemblage, la transmission et le stockage des informations archivées dans la CPS.

(272) L'équipement de la CA racine et de la CA vérifie l'intégrité des informations avant leur restauration.

5.6. Changement de clés pour les éléments du modèle de confiance des STI-C

(273) Les éléments suivants du modèle de confiance des STI-C appliquent des exigences spécifiques pour leur changement de clés: certificats du TLM, de la CA racine et de l'EA/AA.

*5.6.1. **TLM***

(274) Le TLM efface sa clé privée à l'expiration du certificat correspondant. Il génère une nouvelle paire de clés et le certificat du TLM correspondant avant la désactivation de la clé privée valide en vigueur. Il veille à ce que le nouveau certificat (de lien) soit inséré dans l'ECTL à temps pour être distribué à toutes les stations STI-C avant de devenir valide. Le certificat de lien et le nouveau certificat autosigné sont transférés au CPOC.

5.6.2. CA racine

(275) La CA racine désactive et supprime la clé privée en vigueur (y compris les clés de sauvegarde), de sorte qu'elle ne délivrera pas de certificats d'EA/AA dont la validité s'étend au-delà de la validité du certificat de la CA racine.

(276) La CA racine génère une nouvelle paire de clés et les certificats de la CA racine et de lien correspondants avant la désactivation de la clé privée en vigueur (y compris des clés de sauvegarde) et l'envoie au TLM pour insertion dans l'ECTL. La période de validité du nouveau certificat de la CA racine débute lors de la désactivation prévue de la clé privée en vigueur. La CA racine veille à ce que le nouveau certificat soit inséré dans l'ECTL à temps pour être distribué à toutes les stations STI-C avant de devenir valide.

(277) La CA racine active la nouvelle clé privée lorsque le certificat de la CA racine correspondant devient valide.

5.6.3. Certificat d'EA/AA

(278) L'EA/AA désactive la clé privée en vigueur de façon à ne pas délivrer d'EC/AT dont la validité s'étend au-delà de la validité du certificat d'EA/AA.

(279) L'EA/AA génère une nouvelle paire de clés et demande un certificat d'EA/AA correspondant avant la désactivation de la clé privée en vigueur. La durée de validité du nouveau certificat d'EA/AA débute lors de la désactivation prévue de la clé privée en vigueur. L'EA/AA veille à ce que le nouveau certificat puisse être publié à temps pour être distribué à toutes les stations STI-C avant de devenir valide.

(280) L'EA/AA active la nouvelle clé privée lorsque le certificat d'EA/AA devient valide.

5.6.4. Auditeur

Aucune disposition

5.7. Compromission et reprise après sinistre

5.7.1. Traitement des incidents et des compromissions

(281) Les éléments du modèle de confiance des STI-C contrôlent leurs équipements sur une base continue, de façon à détecter d'éventuelles tentatives de piratage ou d'autres formes de compromission. Lorsqu'un tel événement se produit, ils enquêtent afin de déterminer la nature et le degré du préjudice.

(282) Si le personnel chargé de la gestion de la CA racine ou du TLM détecte une possible tentative de piratage ou une autre forme de compromission, il enquête afin de déterminer la nature et le degré du préjudice. En cas de compromission de la clé privée, le certificat de la CA racine est révoqué. Les experts en sécurité informatique de la CPA évaluent la portée du préjudice éventuel afin de déterminer s'il est nécessaire de rétablir la PKI, si seuls certains certificats doivent être révoqués et/ou si la PKI a été compromise. En outre, la CPA détermine quels sont les services qui doivent être maintenus (révocation et informations sur le statut du certificat) et de quelle façon, conformément au plan de continuité des activités de la CPA.

(283) Les incidents, la compromission et la continuité des activités sont couverts dans la CPS, qui peut également s'appuyer sur d'autres ressources et plans d'entreprise pour sa mise en œuvre.

(284) Si le personnel chargé de la gestion de l'EA/de l'AA/du CPOC détecte une possible tentative de piratage ou une autre forme de compromission, il enquête afin de déterminer la nature et le degré du préjudice. Le personnel chargé de la gestion de l'entité de la CA ou du CPOC évalue l'ampleur du préjudice éventuel afin de déterminer si la composante de la PKI doit être rétablie, si seuls certains certificats doivent être révoqués et/ou si la composante de la PKI a été compromise. En outre, l'entité de la sous-CA détermine quels services doivent être maintenus et de quelle façon, conformément au plan de continuité des activités de l'entité de la sous-CA. En cas de compromission d'une composante de la PKI, l'entité de la CA alerte sa propre CA racine et le TLM par l'intermédiaire du CPOC.

(285) Les incidents, la compromission et la continuité des activités sont couverts dans la CPS de la CA racine ou du TLM, ou d'autres documents pertinents dans le cas du CPOC, qui peut également s'appuyer sur d'autres ressources et plans d'entreprise pour leur mise en œuvre.

(286) La CA racine et la CA alertent, en fournissant des informations précises sur les conséquences de l'incident, chaque représentant des États membres et chaque CA racine avec lesquels elles ont signé un accord dans le cadre des STI-C, afin de leur permettre d'activer leur propre plan de gestion des incidents.

5.7.2. Corruption des ressources informatiques, des logiciels et/ou des données

(287) Si un sinistre qui empêche le bon fonctionnement d'un élément du modèle de confiance des STI-C est découvert, cet élément suspend son fonctionnement et examine si la clé privée a été compromise (sauf le CPOC). Le matériel défectueux est remplacé le plus rapidement possible et les procédures décrites dans les sections 5.7.3 et 5.7.4 s'appliquent.

(288) La corruption des ressources informatiques, des logiciels et/ou des données est signalée à la CA racine dans les 24 heures pour les niveaux de risque les plus élevés. Tous les autres événements doivent être inclus dans le rapport périodique de la CA racine, des EA et des AA.

5.7.3. Procédures en cas de compromission de la clé privée d'une entité

(289) Si la clé privée d'une CA racine est compromise, perdue, détruite ou soupçonnée d'être compromise, la CA racine:

- suspend son fonctionnement;
- lance le plan de rétablissement après sinistre et de migration;
- révoque son certificat de CA racine;
- enquête sur le «problème de clé» qui a généré la compromission et informe la CPA, qui révoquera le certificat de CA racine par l'intermédiaire du TLM (voir section 7);
- alerte tous les souscripteurs avec lesquels elle a conclu un accord.

(290) Si une clé de l'EA/AA est compromise, perdue, détruite ou soupçonnée d'être compromise, l'EA/AA:

- suspend son fonctionnement;
- révoque son propre certificat;
- enquête sur le «problème de clé» et informe la CA racine;
- alerte les souscripteurs avec lesquels il existe un accord.

(291) Si la clé de l'EC ou de l'AT d'une station STI-C est compromise, perdue, détruite ou soupçonnée d'être compromise, l'EA/AA auxquelles la station STI-C a souscrit:

- révoque l'EC de la STI concernée;
- enquête sur le «problème de clé» et informe la CA racine;
- alerte les souscripteurs avec lesquels elle a conclu un accord.

(292) Lorsque l'un des algorithmes ou des paramètres associés utilisés par la CA racine et/ou la CA ou les stations STI-C ne suffit plus pour le restant de son usage prévu, la CPA (avec une recommandation des experts en cryptographie) informe l'entité de la CA racine avec laquelle elle a conclu un accord et modifie les algorithmes utilisés. (Pour plus de détails, voir la section 6 et les CPS de la CA racine et de la sous-CA).

5.7.4. Capacités en matière de continuité des activités après un sinistre

(293) Les éléments du modèle de confiance des STI-C exploitant des installations sécurisées pour les opérations de la CA élaborent, testent, maintiennent et mettent en œuvre un plan de rétablissement après sinistre visant à atténuer les effets de tout sinistre d'origine naturelle ou humaine. Ces plans couvrent la restauration des services des systèmes d'information et des principales fonctions opérationnelles.

(294) Après un incident d'un certain niveau de risque, la CA compromise doit être auditée à nouveau par un auditeur agréé de la PKI (voir section 8).

(295) Lorsque la CA compromise n'est pas en mesure de fonctionner plus longtemps (par exemple, à la suite d'un grave incident), un plan de migration doit être établi pour le transfert de ses fonctions à une autre CA racine. La CA racine de l'UE est au moins disponible pour soutenir le plan de migration. La CA compromise cesse ses fonctions.

(296) Les CA racine incluent le plan de rétablissement après sinistre et le plan de migration dans la CPS.

5.8. Cessation et transfert

*5.8.1. **TLM***

(297) Le TLM ne met pas fin à son fonctionnement, mais une entité gérant le TLM peut reprendre une autre entité.

(298) En cas de changement de l'entité de gestion:

- il demande l'approbation de la CPA pour un changement de gestion du TLM, de l'ancienne entité à la nouvelle entité;
- la CPA approuve le changement de gestion du TLM;

- tous les journaux d'audit et les enregistrements archivés sont transférés de l'ancienne entité de gestion à la nouvelle entité.

5.8.2. CA racine

(299) La CA racine ne cesse/débute pas son fonctionnement avant d'avoir établi un plan de migration (prévu dans la CPS correspondante) qui garantit un fonctionnement continu à tous les souscripteurs.

(300) En cas de cessation du service de la CA racine, la CA racine:

- informe la CPA;
- informe le TLM afin qu'il puisse supprimer le certificat de la CA racine de l'ECTL;
- révoque la CA racine correspondante en délivrant une CRL sur laquelle elle figure;
- alerte les CA racine avec lesquelles elle a conclu un accord pour le renouvellement des certificats d'EA/AA;
- détruit la clé privée de la CA racine;
- communique les dernières informations relatives au statut de révocation (CRL signée par la CA racine) à la partie utilisatrice, en indiquant clairement qu'il s'agit des dernières informations de révocation;
- archive tous les journaux d'audit et autres enregistrements avant la cessation de la PKI;
- transfère les enregistrements archivés à l'autorité appropriée.

(301) Le TLM supprime le certificat de la CA racine correspondant de l'ECTL.

*5.8.3. **EA/AA***

(302) En cas de cessation du service de l'EA/AA, l'entité de l'EA/AA donne un préavis de cessation. Une EA ou AA ne cesse/débute pas son fonctionnement avant d'avoir établi un plan de migration (prévu dans la CPS correspondante) qui garantit un fonctionnement continu à tous les souscripteurs. L'EA/AA:

- informe la CA racine par lettre recommandée;
- détruit la clé privée de la CA;
- transfère sa base de données à l'entité désignée par la CA racine;
- cesse de délivrer des certificats;
- pendant le transfert de sa base de données et jusqu'à ce que la base de données soit pleinement opérationnelle dans une nouvelle entité, maintient la capacité d'autoriser des demandes émanant de l'autorité de protection de la vie privée responsable;
- lorsqu'une sous-CA a été compromise, la CA racine révoque la sous-CA et émet une nouvelle CRL avec une liste des sous-CA révoquées;
- archive tous les journaux d'audit et autres enregistrements avant de résilier la PKI;

- transfère les enregistrements archivés à une entité désignée par la CA racine.

(303) En cas de cessation des services de la CA, la CA est chargée de conserver tous les enregistrements pertinents concernant les composantes de la CA et de la PKI.

6. CONTROLES TECHNIQUES DE SECURITE

6.1. Génération et installation des paires de clés

6.1.1. TLM, CA racine, EA et AA

(304) Le processus de génération des paires de clés satisfait aux exigences suivantes:

- chaque participant est en mesure de générer ses propres paires de clés conformément aux sections 6.1.4 et 6.1.5;
- le processus de dérivation des clés de chiffrement symétriques et d'une clé MAC pour les demandes de certificat (ECIES) se déroule conformément à [1] et [5];
- le processus de génération des clés utilise les algorithmes et les longueurs de clés décrits dans les sections 6.1.4.1 et 6.1.4.2;
- le processus de génération des paires de clés est soumis aux exigences du «stockage sécurisé des clés privées» (voir section 6.1.5);
- les CA racine et leurs souscripteurs (sous-CA) veillent à ce que l'intégrité et l'authenticité de leurs clés publiques et de tout paramètre associé soient préservées durant la distribution aux entités enregistrées des sous-CA.

6.1.2. EE — station STI-C mobile

(305) Chaque station STI-C mobile génère ses propres paires de clés conformément aux sections 6.1.4 et 6.1.5.

(306) Le processus de dérivation des clés de chiffrement symétriques et d'une clé MAC pour les demandes de certificat (ECIES) se déroule conformément à [1] et [5].

(307) Les processus de génération des clés utilisent les algorithmes et les longueurs de clés décrits dans les sections 6.1.4.1 et 6.1.4.2.

(308) Les processus de génération des paires de clés sont soumis aux exigences du «stockage sécurisé des clés privées» (voir section 6.1.5).

6.1.3. EE — station STI-C fixe

(309) Chaque station STI-C fixe génère sa propre paire de clés conformément aux sections 6.1.4 et 6.1.5.

(310) Les processus de génération des clés utilisent les algorithmes et les longueurs de clés décrits dans les sections 6.1.4.1 et 6.1.4.2.

(311) Les processus de génération des paires de clés sont soumis aux exigences du «stockage sécurisé des clés privées» (voir section 6.1.5).

6.1.4. Exigences cryptographiques

(312) Tous les participants à la PKI satisfont aux exigences cryptographiques énoncées dans les paragraphes suivants en ce qui concerne l'algorithme de signature, la longueur des clés, le générateur de nombre aléatoire et les certificats de lien.

6.1.4.1. *Algorithme et longueur de la clé - algorithmes de signature*

(313) Tous les participants à la PKI (TLM, CA racine, EA, AA et stations STI-C) sont en mesure de générer des paires de clés et d'utiliser la clé privée pour la signature des opérations avec des algorithmes sélectionnés au plus tard deux ans après l'entrée en vigueur du présent règlement, conformément au tableau 4.

(314) Tous les participants à la PKI qui doivent vérifier l'intégrité de l'ECTL, des certificats et/ou des messages signés conformément à leur rôle, tel que défini à la section 1.3.6, prennent en charge les algorithmes correspondants énumérés au tableau 5 pour vérification. En particulier, les stations STI-C sont capables de vérifier l'intégrité de l'ECTL.

	TLM	CA racine	EA	AA	Station STI-C
ECDSA_nistP256_with_SHA 256	-	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA 256	-	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA 384	X	X	X	-	-
X indique une prise en charge obligatoire					

Tableau 4: Génération de paires de clés et utilisation d'une clé privée pour la signature des opérations

	TLM	CA racine	EA	AA	Station STI-C
ECDSA_nistP256_with_SHA 256	X	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA 256	X	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA 384	X	X	X	X	X
X indique une prise en charge obligatoire					

Tableau 5: Aperçu de la vérification

(315) Si la CPA en décide ainsi, sur la base de nouvelles faiblesses cryptographiques détectées, toutes les stations STI-C sont en mesure de passer à l'un des deux algorithmes (ECDSA_nistP256_with_SHA 256 ou ECDSA_brainpoolP256_with_SHA 256) dès que possible. Le ou les algorithmes qui sont concrètement utilisés sont déterminés dans la CPS de la CA qui délivre le certificat pour la clé publique correspondante, conformément à la présente CP.

6.1.4.2. *Algorithme et longueur de la clé - algorithmes de chiffrement pour l'inscription et l'autorisation*

(316) Tous les participants à la PKI (EA, AA et stations STI-C) sont en mesure d'utiliser les clés publiques pour chiffrer les demandes/réponses d'inscription et d'autorisation avec des algorithmes sélectionnés au plus tard deux ans après l'entrée en vigueur du présent règlement, conformément au tableau 6. Le ou les algorithmes qui sont concrètement utilisés sont déterminés dans la CPS de la CA qui délivre le certificat pour la clé publique correspondante, conformément à la présente CP.

(317) Les algorithmes mentionnés dans le tableau 6 indiquent la longueur de la clé et la longueur de l'algorithme de hachage et sont mis en œuvre conformément à [5].

	TLM	CA racine	EA	AA	Station STI-C
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES 128_CCM	-	-	X	X	X
X indique une prise en charge obligatoire					

Tableau 6: Utilisation des clés publiques pour le chiffrement des questions/réponses d'inscription et d'autorisation

(318) Tous les participants à la PKI (EA, AA et stations STI-C) sont en mesure de générer des paires de clés et d'utiliser la clé privée pour déchiffrer les demandes/réponses d'inscription et d'autorisation avec des algorithmes sélectionnés au plus tard deux ans après l'entrée en vigueur du présent règlement, conformément au tableau 7.

	TLM	CA racine	EA	AA	Station STI-C
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES 128_CCM	-	-	X	X	X
X indique une prise en charge obligatoire					

Tableau 7: Génération de paires de clés et utilisation de clé privée pour le déchiffrement des demandes/réponses d'inscription et d'autorisation

6.1.4.3. *Crypto-agilité*

(319) Les exigences concernant les longueurs de clés et les algorithmes doivent être modifiées au fil du temps afin de maintenir un niveau de sécurité approprié. La CPA surveille la nécessité de ces modifications compte tenu des vulnérabilités réelles et des dernières avancées de la cryptographie. Elle rédigera, approuvera et publiera une mise à jour de la présente politique de certification si elle décide que les algorithmes cryptographiques doivent être mis à jour. Si une nouvelle édition de la présente CP signale un changement d'algorithme et/ou de longueur de clé, la CPA adoptera une stratégie de migration comprenant des périodes de transition au cours desquelles les anciens algorithmes et longueurs de clés doivent être pris en charge.

(320) Afin de permettre et de faciliter le transfert vers de nouveaux algorithmes et/ou longueurs de clés, il est recommandé que tous les participants à la PKI mettent en œuvre des matériels et/ou des logiciels capables de soutenir un changement de longueurs de clés et d'algorithmes.

(321) Les modifications des certificats racine et du TLM sont prises en charge et exécutées à l'aide de certificats de lien (voir section 4.6) qui sont utilisés pour couvrir la période de transition entre les anciens et les nouveaux certificats racine («migration du modèle de confiance»).

6.1.5. Stockage sécurisé de clés privées

La présente section décrit les exigences pour le stockage sécurisé et la génération de paires de clés et de nombres aléatoires pour les CA et les entités finales. Ces exigences sont définies pour les modules cryptographiques et décrites dans les sous-sections suivantes.

6.1.5.1. *Niveau CA racine, sous-CA et TLM*

(322) Un module cryptographique est utilisé pour:

- générer, utiliser, administrer et stocker les clés privées;
- générer et utiliser des nombres aléatoires (l'évaluation de la fonction de génération de nombres aléatoires fait partie de l'évaluation et de la certification de la sécurité);

- créer des sauvegardes des clés privées conformément à la section 6.1.6;
- supprimer des clés privées.

Le module cryptographique est certifié avec l'un des profils de protection (PP) suivants, présentant un niveau d'assurance EAL-4 ou supérieur:

- PP pour HSM:
  - CEN EN 419 221-2: Profils de protection pour modules cryptographiques utilisés par les prestataires de services de confiance – Partie 2: Module cryptographique utilisé par le prestataire de services de certification pour les opérations de signature avec sauvegarde;
  - CEN EN 419 221-4: Profils de protection pour modules cryptographiques utilisés par les prestataires de services de confiance – Partie 4: Module cryptographique utilisé par le prestataire de services de certification pour les opérations de signature sans sauvegarde;
  - CEN EN 419 221-5: Profils de protection pour les modules cryptographiques de prestataires de services de confiance – Partie 5: Module cryptographique pour les services de confiance;
- PP pour cartes à puces:
  - CEN EN 419211-2: Profils de protection des dispositifs sécurisés de création de signature – Partie 2: Dispositif avec génération de clé;
  - CEN EN 419211-3: Profils de protection des dispositifs sécurisés de création de signature – Partie 3: Dispositif avec import de clé.

Un accès manuel au module cryptographique exige une authentification à deux facteurs de l'administrateur. En outre, cela requiert la participation de deux personnes autorisées.

La mise en œuvre d'un module cryptographique garantit que les clés ne sont pas accessibles en dehors du module cryptographique. Le module cryptographique comporte un mécanisme de contrôle de l'accès afin de prévenir toute utilisation non autorisée des clés privées.

6.1.5.2. *Entité finale*

(323) Un module cryptographique pour EE est utilisé pour:

- générer, utiliser, administrer et stocker les clés privées;
- générer et utiliser des nombres aléatoires (l'évaluation de la fonction de génération de nombres aléatoires fait partie de l'évaluation et de la certification de la sécurité);
- assurer la suppression d'une clé privée.

(324) Le module cryptographique est protégé contre un retrait, un remplacement et une modification non autorisés. Tous les PP et les documents correspondants applicables pour la certification de la sécurité du module cryptographique sont évalués, validés et certifiés conformément à la norme ISO 15408, en appliquant

l'accord sur la reconnaissance mutuelle des certificats d'évaluation de la sécurité en matière de technologies de l'information («Mutual Recognition Agreement of Information Technology Security Evaluation Certificates») du groupe des hauts fonctionnaires pour la sécurité des systèmes d'information («Senior Officials Group on Information Systems Security», SOG-IS).

(325) Étant donné l'importance que revêt le maintien du niveau de sécurité le plus élevé possible, des certificats de sécurité pour le module cryptographique sont délivrés au titre du régime de certification «critères communs» (ISO 15048) par un organisme d'évaluation de la conformité reconnu par le comité de gestion dans le cadre de l'accord du SOG-IS, ou délivrés par un organisme d'évaluation de la conformité accrédité par une autorité nationale de certification de cybersécurité d'un État membre. Cet organisme d'évaluation de la conformité offre au moins des conditions d'évaluation de la sécurité équivalentes à celles qui sont prévues par l'accord de reconnaissance mutuelle du SOG-IS.

Note: le lien entre le module cryptographique et la station STI-C est protégé.

6.1.6. Sauvegarde de clés privées

(326) La génération, le stockage et l'utilisation des sauvegardes de clés privées satisfont aux exigences au moins du niveau de sécurité requis pour les clés originales.

(327) Les sauvegardes des clés privées sont effectuées par les CA racine, les EA et les AA.

(328) Les sauvegardes des clés privées ne sont pas effectuées pour les EC et les AT.

6.1.7. Destruction de clés privées

(329) Les CA racine, les EA, les AA et les stations STI-C mobiles et fixes détruisent leur clé privée et toute sauvegarde correspondante, si une nouvelle paire de clés et le certificat correspondant ont été générés et installés avec succès, et si le délai de chevauchement (le cas échéant — pour la CA uniquement) a expiré. La clé privée est détruite en utilisant le mécanisme proposé par le module cryptographique utilisé pour le stockage de clés ou comme décrit dans le PP correspondant tel que mentionné à la section 6.1.5.2.

6.2. Données d'activation

(330) Les données d'activation font référence aux facteurs d'authentification requis pour exploiter les modules cryptographiques afin d'empêcher tout accès non autorisé. L'utilisation des données d'activation d'un dispositif cryptographique de la CA requiert une action par deux personnes autorisées.

6.3. Contrôles de sécurité informatique

(331) Les contrôles de sécurité informatique des CA sont conçus conformément au niveau de sécurité élevé en se conformant aux exigences de la norme ISO/IEC 27002.

6.4. Contrôles techniques tout au long du cycle de vie

(332) Les contrôles techniques de la CA couvrent tout le cycle de vie de la CA. En particulier, cela inclut les exigences de la section 6.1.4.3 («Crypto-agilité»).

6.5. Contrôles de sécurité du réseau

(333) Les réseaux des CA (CA racine, EA et AA) sont renforcés contre les attaques conformément aux exigences et aux orientations pour la mise en œuvre de la norme ISO/IEC 27001 et de la norme ISO/IEC 27002.

(334) La disponibilité des réseaux de la CA est conçue en fonction du trafic estimé.

7. PROFILS DE CERTIFICATS, CRL ET ECTL

7.1. Profil de certificats

(335) Les profils de certificats définis dans [5] sont utilisés pour les TLM, les certificats racines, les certificats de l'EA, les certificats de l'AA, les AT et les EC. Les EA publiques nationales peuvent utiliser d'autres profils de certificat pour les EC.

(336) Les certificats de la CA racine, de l'EA et de l'AA indiquent les autorisations pour lesquelles ces CA (CA racine, EA et AA) sont autorisées à délivrer des certificats.

(337) Sur la base de [5]:

- chaque CA racine utilise sa propre clé privée de signature pour émettre des CRL;
- le TLM utilise sa propre clé privée de signature pour émettre l'ECTL.

7.2. Validité des certificats

(338) Tous les profils de certificats des STI-C comprennent une date de délivrance et d'expiration, qui représentent le délai de validité du certificat. À chaque niveau de la PKI, des certificats sont générés avec une avance suffisante avant l'expiration.

(339) Le délai de validité des certificats de la CA et de l'EC inclut un délai de chevauchement. Les certificats du TLM et de la CA racine sont délivrés et placés sur l'ECTL trois mois au maximum et un mois au moins avant le début de leur validité déterminé en fonction du moment indiqué dans le certificat. Cette phase de préchargement est requise pour distribuer les certificats en toute sécurité à toutes les parties utilisatrices correspondantes, conformément à la section 2.2. Cela garantit que, à compter du début du délai de chevauchement, toutes les parties utilisatrices sont déjà en mesure de vérifier les messages émis avec un nouveau certificat.

(340) Au début du délai de chevauchement, les certificats successifs de la CA, de l'EC et de l'AT sont délivrés (le cas échéant), distribués et installés par les parties utilisatrices correspondantes. Pendant le délai de chevauchement, le certificat en vigueur est utilisé uniquement à des fins de vérification.

(341) Étant donné que les périodes de validité énumérées dans le tableau 8 ne doivent pas dépasser la période de validité du certificat supérieur, les restrictions suivantes s'appliquent:

- maximumvalidity(Root CA) = privatekeyusage(Root CA) + maximumvalidity(EA,AA);
- maximumvalidity(EA) = privatekeyusage(EA) + maximumvalidity(EC);

- maximumvalidity(AA) = privatekeyusage(AA) + preloadingperiod(AT).

(342) La validité des certificats de lien (racine et TML) commence avec l'utilisation de la clé privée correspondante et s'achève à la fin de la durée de validité maximale de la CA racine ou du TLM.

(343) Le tableau 8 montre le délai de validité maximale pour les certificats des CA des STI-C (pour les périodes de validité des AT, voir section 7.2.1).

Entité	Période max. d'utilisation de la clé privée	Durée de validité maximale
CA racine	3 ans	8 ans
EA	2 ans	5 ans
AA	4 ans	5 ans
EC	3 ans	3 ans
TLM	3 ans	4 ans

Tableau 8: Périodes de validité des certificats dans le modèle de confiance des STI-C

7.2.1. Certificats de pseudonymes

(344) Dans ce contexte, des pseudonymes sont mis en œuvre par les AT. En conséquence, la présente section fait référence aux AT plutôt qu'aux pseudonymes.

(345) Les exigences énoncées dans la présente section s'appliquent uniquement aux AT des stations STI-C mobiles qui envoient des messages CAM et DENM, lorsque le risque lié à la confidentialité de la localisation est présent. Aucune exigence spécifique concernant les certificats AT ne s'applique aux AT pour les stations STI-C fixes et mobiles utilisées pour assurer des fonctions spéciales lorsque la confidentialité de la localisation n'est pas applicable (par exemple, les véhicules d'urgence et les véhicules des forces de l'ordre identifiés).

(346) On entend par:

- «période de validité pour les AT», la période pendant laquelle un AT est valide, à savoir la période entre sa date d'entrée en vigueur et sa date d'expiration;
- «période de préchargement pour les AT», la période pendant laquelle les stations STI-C ont la possibilité d'obtenir des AT avant le début de la période de validité (préchargement). La période de préchargement est le délai maximal autorisé entre la demande d'AT à la date ultime de validité de tout AT demandé;
- «période d'utilisation pour les AT», la période durant laquelle un AT est effectivement utilisé pour signer les messages CAM/DENM;
- «nombre maximal d'AT parallèles», le nombre d'AT parmi lesquels une station STI-C peut choisir, à tout moment donné, lors de la signature d'un message CAM/DENM, c'est-à-dire le nombre d'AT différents délivrés à une station STI-C qui sont valides en même temps.

(347) Les exigences suivantes s'appliquent:

- la période de préchargement pour les AT n'excède pas trois mois;
- la période de validité pour les AT ne dépasse pas une semaine;
- le nombre maximal d'AT parallèles ne dépasse pas 100 par station STI-C;
- la période d'utilisation d'un AT dépend de la stratégie de changement des AT et du laps de temps durant lequel un véhicule est en intervention, mais elle est limitée par le nombre maximal d'AT parallèles et par la période de validité. Plus précisément, la période d'utilisation moyenne pour une station STI-C est au moins égale à la durée de service du véhicule pendant une période de validité divisée par le nombre maximal d'AT parallèles.

7.2.2. Tickets d'autorisation pour les stations STI-C fixes

(348) Les définitions de la section 7.2.1 et les exigences suivantes s'appliquent:

- la période de préchargement pour les AT n'excède pas trois mois;
- le nombre maximal d'AT parallèles ne dépasse pas deux par station STI-C.

7.3. Révocation de certificats

7.3.1. Révocation de certificats de la CA, l'EA et l'AA

Les certificats de la CA racine, de l'EA et de l'AA sont révocables. Les certificats révoqués des CA racine, des EA et des AA sont publiés sur une CRL dès que possible et sans retard indu. Cette CRL est signée par son CA racine correspondante et utilise le profil décrit à la section 7.4. Pour la révocation des certificats de la CA racine, la CA racine correspondante émet une CRL sur laquelle elle figure. En outre, en cas de compromission de la sécurité, la section 5.7.3 s'applique. En outre, le TLM retire les CA racine révoquées de la liste de confiance et émet une nouvelle liste de confiance. Les certificats périmés sont retirés de la CRL correspondante et de la liste de confiance.

(349) Les certificats sont révoqués lorsque:

- les CA racine ont des raisons de croire ou de soupçonner fortement que la clé privée correspondante a été compromise;
- les CA racine ont été informées que le contrat conclu avec le souscripteur a été résilié;
- les informations (telles que le nom et les associations entre la CA et le sujet) dans le certificat sont inexactes ou ont changé;
- un incident de sécurité a lieu, qui affecte le titulaire du certificat;
- un audit (voir section 8) conduit à un résultat négatif.

(350) Le souscripteur informe immédiatement la CA d'une compromission connue ou suspectée de sa clé privée. Il convient de s'assurer que seules les demandes authentifiées donnent lieu à des certificats révoqués.

7.3.2. Révocation de certificats d'inscription

(351) La révocation des EC peut être initiée par le souscripteur de la station STI-C (flux 34) et est mise en œuvre moyennant une liste noire interne portant un

horodatage, qui est générée et maintenue par chaque EA dans une base de données des révocations. La liste noire n'est jamais publiée, est tenue confidentielle et est seulement utilisée par l'EA correspondante afin de vérifier la validité des EC correspondants dans le cadre des demandes d'AT et de nouveaux EC.

7.3.3. Révocation de tickets d'autorisation

(352) Comme les AT ne sont pas révoqués par les CA correspondantes, ils ont une durée de vie courte et ne peuvent pas être délivrés trop longtemps avant de devenir valides. Les valeurs des paramètres du cycle de vie des certificats admissibles sont énoncées à la section 7.2.

7.4. Liste de révocation de certificats

(353) Le format et le contenu de la CRL émise par des CA racine sont indiqués dans [1].

7.5. Liste de confiance européenne des certificats

(354) Le format et le contenu de l'ECTL émise par le TLM sont indiqués dans [1].

8. VERIFICATION DE LA CONFORMITE ET AUTRES EVALUATIONS

8.1. Sujets faisant l'objet d'audits et fondement des audits

(355) Un audit de conformité a pour objectif de vérifier que le TML, les CA racine, les EA et les AA fonctionnent conformément à la présente CP. Le TLM, les CA racine, les EA et les AA sélectionnent un auditeur agréé de la PKI et agissant indépendamment pour évaluer leur CPS. L'audit est combiné avec une évaluation au titre des normes ISO/IEC 27001 et ISO/IEC 27002.

(356) Un audit de conformité est ordonné, pour une CA racine, par la CA racine elle-même (flux 13) et, pour une sous-CA, par son EA/AA subordonnée.

(357) Un audit de conformité pour le TLM est ordonné par la CPA (flux 38).

(358) Lorsqu'il est demandé, un audit de conformité est effectué par un auditeur agréé de la PKI sur l'un des niveaux suivants:

(1) conformité des CPS du TLM, de la CA racine, de l'EA ou de l'AA à la présente CP;

(2) conformité des pratiques visées du TLM, de la CA racine, de l'EA ou de l'AA à leur CPS avant l'exploitation;

(3) conformité des pratiques et activités opérationnelles du TLM, de la CA racine, de l'EA ou de l'AA à leur CPS pendant l'exploitation.

(359) L'audit couvre toutes les exigences de la présente CP à respecter par le TLM, les CA racine, les EA et les AA devant faire l'objet de l'audit. Il porte également sur le fonctionnement de la CA dans la PKI des STI-C, y compris sur tous les processus mentionnés dans sa CPS, les locaux et les personnes responsables.

(360) L'auditeur agréé de la PKI fournit un rapport détaillé de l'audit à la CA racine (flux 36), à l'EA, à l'AA ou à la CPA (flux 16 et 40), le cas échéant.

8.2. Fréquence des audits

(361) Une CA racine, un TLM, une EA ou AA commande un audit de conformité pour elle/lui-même auprès d'un auditeur de la PKI indépendant et agréé dans les cas suivants:

- lors de sa première mise en place (conformité de niveaux 1 et 2);
- lors de toute modification de la CP. La CPA définit le contenu du changement de la CP et le calendrier du déploiement et détermine les besoins d'audit (y compris le niveau de conformité nécessaire) en conséquence;
- lors de toute modification de sa CPS (conformité de niveaux 1, 2 et 3). Étant donné que les entités de gestion des CA racine, du TLM et des EA/AA décident des modifications de la mise en œuvre qui suivent la mise à jour de leur CPS, elles commandent un audit de conformité avant de mettre en œuvre ces modifications. En cas de modifications mineures de la CPS (par exemple de nature rédactionnelle), l'entité de gestion peut envoyer à la CPA une demande dûment justifiée pour qu'elle l'autorise à ne pas effectuer les audits de conformité de niveau 1, 2 ou 3;
- régulièrement, et au moins tous les trois ans, durant son exploitation (conformité de niveau 3).

8.3. Identité/qualifications de l'auditeur

(362) La CA devant faire l'objet d'un audit sélectionne une entreprise/organisation («organe d'audit») agissant de manière indépendante et accréditée ou des auditeurs agréés de la PKI qui procéderont à son audit conformément à la présente CP. L'organe d'audit est agréé et certifié par un membre de l'organisme européen d'accréditation[1].

8.4. Lien entre l'auditeur et l'entité soumise à audit

(363) L'auditeur agréé de la PKI est indépendant de l'entité soumise à audit.

8.5. Mesures prises à la suite du constat de lacunes

(364) Lorsqu'un rapport d'audit conclut à la non-conformité du TLM, la CPA ordonne au TLM de prendre des mesures préventives/correctives immédiates.

(365) Lorsqu'une CA racine faisant l'objet d'un rapport d'audit non conforme introduit une nouvelle demande, la CPA rejette la demande et transmet un rejet correspondant à la CA racine (flux 4). En pareils cas, la CA racine sera suspendue. Elle doit prendre des mesures correctives, commander à nouveau un audit et faire une nouvelle demande d'approbation de la CPA. La CA racine n'est pas autorisée à délivrer des certificats pendant la période de suspension.

(366) En cas d'audit régulier de la CA racine ou de modification à la CPS de la CA racine, et en fonction de la nature de la non-conformité décrite dans le rapport d'audit, la CPA peut décider de révoquer la CA racine et de communiquer cette décision au TLM (flux 2), entraînant la suppression du certificat de la CA racine de l'ECTL et l'insertion de la CA racine sur la CRL. La CPA transmet un rejet correspondant à la CA racine (flux 4). La CA racine doit prendre des

[1] La liste des membres de l'organisme européen d'accréditation figure sur cette page: http://www.european-accreditation.org/ea-members

mesures correctives, commander à nouveau un audit complet (niveaux 1 à 3) et introduire une nouvelle demande d'approbation de la CPA. Il se peut aussi que la CPA décide de ne pas révoquer la CA racine, mais de lui accorder un délai de grâce au cours duquel la CA racine prend des mesures correctives, commande à nouveau un audit et soumet à nouveau le rapport d'audit à la CPA. Le cas échéant, le fonctionnement de la CA racine doit être suspendu et elle n'est pas autorisée à délivrer des certificats et des CRL.

(367) Dans le cas de l'audit d'une EA/AA, la CA racine décide d'accepter ou non le rapport. En fonction du résultat de l'audit, la CA racine décide s'il y a lieu de révoquer ou non le certificat d'EA/AA conformément aux règles de la CPS de la CA racine. La CA racine garantit à tout moment la conformité de l'EA/AA à la présente CP.

8.6. Communication des résultats

(368) La CA racine et le TLM transmettent le rapport d'audit à la CPA (flux 16). La CA racine et le TLM conservent tous les rapports d'audit qu'ils ont commandés. La CPA envoie une approbation ou un rejet correspondant (flux 4) à la CA racine et au TLM.

(369) La CA racine envoie un certificat de conformité à l'EA/AA correspondante.

9. AUTRES DISPOSITIONS

9.1. Redevances

(370) L'un des principes du modèle de confiance des STI-C mis en œuvre est que les CA racine, conjointement, financent intégralement les coûts de fonctionnement périodiques et récurrents de la CPA et des éléments centraux (TLM et CPOC) relatifs aux activités exposées dans la présente CP.

(371) Les CA racine (y compris la CA racine de l'UE) sont habilitées à percevoir des redevances auprès de leurs sous-CA.

(372) Tout au long de leur période d'exploitation, chaque participant du modèle de confiance des STI-C a accès à au moins une AC racine, EA et AA sur une base non discriminatoire.

(373) Chaque CA racine est autorisée à répercuter les redevances qu'elle paie pour la CPA et les éléments centraux (TLM et CPOC) sur les participants enregistrés du modèle de confiance des STI-C, y compris les stations STI-C inscrites et autorisées.

9.2. Responsabilité financière

(374) L'établissement initial d'une CA racine couvre une période d'au moins trois années d'exploitation, afin qu'elle puisse devenir membre du modèle de confiance des STI-C de l'UE. La CPS de l'exploitant d'une CA racine contient également des dispositions détaillées relatives à la révocation ou à la fermeture de la CA racine.

(375) Chaque CA racine doit démontrer la viabilité financière de l'entité juridique qui la met en œuvre pendant au moins trois ans. Ce plan de viabilité financière fait partie de la série initiale de documents nécessaires à l'inscription et doit être mis à jour tous les trois ans et communiqué à la CPA.

(376) Chaque CA racine doit signaler la structure des redevances appliquées aux EA/AA et aux stations STI-C inscrites et autorisées chaque année au gestionnaire des opérations et à la CPA afin de démontrer sa viabilité financière.

(377) Toutes les entités financières et juridiques responsables de la CA racine, de l'EA, de l'AA et des éléments centraux (CPOC et TLM) du modèle de confiance des STI-C doivent couvrir leurs tâches opérationnelles par des niveaux d'assurance adéquats permettant de compenser les erreurs opérationnelles et le coût financier du rétablissement de leurs fonctions en cas de défaillance de l'un des éléments techniques.

9.3. Confidentialité des informations opérationnelles

(378) Les éléments suivants sont tenus confidentiels et privés:

- enregistrements des demandes de la CA racine, de l'EA, de l'AA, approuvées ou rejetées;
- rapports d'audit de la CA racine, de l'EA, de l'AA et du TLM;
- plans de rétablissement après sinistre de la CA racine, de l'EA, de l'AA, du CPOC et du TLM;
- clés privées des éléments du modèle de confiance des STI-C (stations STI-C, TLM, EA, AA, CA racine);
- toute autre information considérée comme confidentielle par la CPA, les CA racine, l'EA, l'AA, le TLM et le CPOC.

9.4. Plan en matière de protection de la vie privée

(379) Les CPS des CA racine et les EA/AA établissent le plan et les exigences pour le traitement des données à caractère personnel et la protection de la vie privée sur la base du RGPD et d'autres cadres législatifs (par exemple nationaux) applicables.

10. REFERENCES

La présente annexe fait référence aux documents suivants:

[1] ETSI TS 102 941 V1.2.1, «Systèmes de transport intelligents (STI) – sécurité, confiance et gestion de la vie privée» [Intelligent transport systems (ITS) – security, trust and privacy management].

[2] ETSI TS 102 940 V1.3.1, «Systèmes de transport intelligents (STI) – sécurité, architecture de sécurité pour les communications STI et gestion de la sécurité» [Intelligent transport systems (ITS) – security, ITS communications security architecture and security management].

[3] «Politique de certification et cadre de pratiques de certifications» [Certificate policy and certification practices framework] (RFC 3647, 1999).

[4] ETSI TS 102 042 V2.4.1, «Exigences politiques pour les autorités de certification délivrant des certificats à clés publiques» [Policy requirements for certification authorities issuing public key certificates].

[5] ETSI TS 103 097 V1.3.1, «Systèmes de transport intelligents (STI) – sécurité, en-tête de sécurité et formats des certificats» [Intelligent transport systems (ITS) – security, security header and certificate formats].

[6] Calder A., *Information security based on ISO 27001/ISO 1779: a management guide*, Van Haren Publishing, 2006.

[7] ISO, I., & Std, I. E. C. (2011). ISO 27005 (2011) – Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information. ISO.