Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral des finances DFF

Office fédéral de l'informatique et de la télécommunication OFIT
Centre de solutions
Cyberadministration
PKI et produits de sécurité

Robert Dietschi

29 avril 2010

AdminPKI - ClassA

Enoncé des pratiques de certification / politique de certification de l'autorité de certification AdminPKI (certificats qualifiés)

OID : 2.16.756.1.17.3.1.4

Projektname: **ClassA**

Projektnummer: **-**

Version: **V2.6**

Status	In Arbeit	in Prüfung	genehmigt zur Nutzung
	☐	☐	☒

Beteiligter Personenkreis	
Autoren:	Dietschi Robert, Karolina Kohout
Genehmigung:	Responsable AdminPKI
Benützer/Anwender:	Abonnés, collaborateurs AdminPKI, auditeurs, tiers
zur Information/Kenntnis:	-

Digitally signed by Daniel Markwalder - Bereichsleiter PKI und Sicherheitsprodukte
Bern, 2011-05-24 (with timestamp)
Reason: Approved Version

Änderungskontrolle, Prüfung, Genehmigung			
Wann	**Version**	**Wer**	**Beschreibung**
01.04.2006	X0.1	R. Dietschi	1ère version
21.08.2006	V1.0	R. Dietschi	
21.09.2006	V1.1	R. Dietschi	Review BIT
01.06.2007	V2.0	R. Dietschi	Review KPMG
30.06.2007	V2.1	R. Dietschi	Post audit KPMG
17.08.2007	V2.2	R. Dietschi	Update Filename & Review KPMG
06.02.2008	V2.3	R. Dietschi	Mise à jour
10.01.2009	V2.4	R. Jusufi	Update CRL
23.03.2010	V2.5	P. Joye	ISIS-MTT Custom DN Longueur de la clef de signature à 2048 bits Validité des certificats d'abonné 1 ou 3 ans TSA
04.05.2011	V2.6	P. Joye	Corrections

Management summary

Ce document est l'énoncé des pratiques de certification [CPS], respectivement la politique de certification [CP] de l'autorité de certification AdminPKI de l'office fédéral de l'informatique et de la télécommunication OFIT. Il décrit les pratiques suivies par l'AdminPKI pour émettre des certificats qualifiés au sens de la loi fédérale sur les services de certification dans le domaine de la signature électronique (Loi sur la signature électronique, SCSE) [1].

Table des matières

1 Introduction 9
1.1 Aperçu 9
1.2 Identification 9
1.3 Groupes d'utilisateurs 10
1.3.1 Autorités de certification 10
1.3.2 Autorité d'enregistrement LRA 11
1.3.3 Abonné 12
1.3.4 Partie utilisatrice 12
1.3.5 Autres participants 13
1.4 Utilisation des certificats 13
1.4.1 Utilisation autorisée 13
1.4.2 Utilisation non autorisée 13
1.5 Administration du document / Personne de contact 13
1.5.1 Administration du document 13
1.5.2 Personne de contact 13
1.5.3 Vérification du contenu 14
1.5.4 Procédure d'approbation 14
1.6 Glossaire et abréviations 15
1.6.1 Glossaire 15
1.6.2 Abréviations 17

2 Service d'information et service d'annuaire 20
2.1 Service de publication et d'archivage 20
2.2 Le service d'information 20
2.3 Actualisation des informations 20
2.4 Contrôle d'accès 21

3 Identification et authentification 22
3.1 Attribution d'un nom 22
3.1.1 Convention de noms 22
3.1.2 Utilisation de noms explicites 22
3.1.3 Anonymat et pseudonymie 23
3.1.4 Règles d'interprétation des diverses formes de noms 23
3.1.5 Unicité des noms 23
3.1.6 Reconnaissance, authentification et rôle des marques de commerce 24
3.2 Enregistrement initial 24
3.2.1 Preuve de la possession d'une clé privée 24
3.2.2 Authentification de l'identité d'une entité administrative 24
3.2.3 Vérification de l'identité du demandeur de certificat 24
3.2.4 Données non vérifiées 25
3.2.5 Vérification de qualités spécifiques de l'abonné 25
3.2.6 Certification croisée (reconnaissance) 25
3.3 Renouvellement du certificat 25
3.4 Authentification d'une demande d'annulation 25

4 Exigences opérationnelles 27
4.1 Demande de certificat 27
4.1.1 Qui peut faire une demande de certificat 27
4.1.2 Processus d'enregistrement 27

4.2 Traitement de la demande de certificat 28
4.2.1 Identification et authentification du demandeur 28
4.2.2 Acceptation/refus de la demande de certificat 28

4.2.3 Traitement de la demande de certificat 28
4.3 Emission du certificat 29
4.3.1 Actions de l'autorité de certification de deuxième niveau durant le processus d'émission 29
4.3.2 Notification de l'émission du certificat au demandeur 29
4.4 Acceptation du certificat 29
4.4.1 Procédure d'acceptation 29
4.4.2 Publication du certificat par l'autorité d'enregistrement AdminCA-A-T01 29
4.4.3 Notification de l'émission du certificat à d'autres entités 30
4.5 Utilisation des clés et du certificat 30
4.5.1 Utilisation des clés et du certificat par l'abonné 30
4.5.2 Utilisation du certificat par les tiers (parties utilisatrices) 30
4.6 Prolongation de la validité du certificat 31
4.7 Remplacement du certificat 31
4.8 Modification du contenu du certificat 31
4.9 Suspension et annulation (révocation) de certificat 31
4.9.1 Motifs d'annulation 31
4.9.2 Qui peut demander l'annulation 32
4.9.3 Procédures de demande d'annulation 32
4.9.4 Délai pour faire une demande d'annulation 33
4.9.5 Délai pour exécuter une demande d'annulation 33
4.9.6 Exigences de contrôle des listes de certificats annulés 33
4.9.7 Fréquence de publication des CRL et des ARL 33
4.9.8 Délai pour publier la CRL 34
4.9.9 Contrôle en ligne de la liste des certificats annulés 34
4.9.10 Exigences liées à la vérification en ligne 34
4.9.11 Autres formes de publication de liste de certificats annulés 34
4.9.12 Remplacement du certificat en cas de compromission des clés 34
4.9.13 Suspension de certificat 34
4.9.14 Qui peut demander l'annulation 34
4.9.15 Procédure de demande de suspension 34
4.9.16 Durée de la suspension 34
4.10 Service de vérification de l'état du certificat 35
4.10.1 Caractéristiques opérationnelles 35
4.10.2 Disponibilité du service 35
4.10.3 Options 35
4.11 Fin des rapports contractuels 35
4.12 Entiercement / recouvrement des clés de signature 35
4.12.1 Politique d'entiercement / recouvrement des clés de signature 35
4.12.2 Clés de sessions et pratiques de recouvrement 35

5 Sécurité physique, sécurité des procédures et du personnel 36
5.1 Contrôles de la sécurité physique 36
5.1.1 Emplacement 36
5.1.2 Accès physique 36
5.1.3 Système électrique et système de conditionnement de l'air 36
5.1.4 Dégâts d'eau 36
5.1.5 Prévention et protection contre les incendies 36
5.1.6 Supports d'information 36
5.1.7 Mise au rebut 37
5.1.8 Entreposage hors site (site de secours) 37
5.2 Contrôle des procédures 37
5.2.1 Rôles de confiance 37
5.2.2 Nombre de personnes requises par tâche 38
5.2.3 Identification et authentification de chaque rôle 39
5.2.4 Séparation des rôles 39

5.3 Contrôle de sécurité du personnel 39
5.3.1 Compétences, qualification et antécédents requis 39
5.3.2 Procédures préalables de contrôle 39
5.3.3 Exigences de formation initiale 39
5.3.4 Exigences et fréquences des formations 40
5.3.5 Rotation des postes 40
5.3.6 Sanctions pour actions non autorisées 40
5.3.7 Personnel lié par contrat à durée limitée 40
5.3.8 Documentation fournie au personnel 40
5.4 Procédure de vérification de la sécurité des systèmes 40
5.4.1 Types d'évènements enregistrés 40
5.4.2 Fréquence du traitement des journaux d'évènements 41
5.4.3 Période de conservation des journaux d'évènements 41
5.4.4 Protection des journaux d'évènements 41
5.4.5 Procédures de sauvegarde des journaux d'évènements 41
5.4.6 Système de collecte des journaux 41
5.4.7 Notification suivant un évènement critique 41
5.4.8 Évaluation de la vulnérabilité 42
5.5 Archivage des certificats et autres documents 42
5.5.1 Types de données à archiver 42
5.5.2 Périodes de rétention des archives 42
5.5.3 Protection des archives 42
5.5.4 Procédure de copie des archives 42
5.5.5 Besoin d'horodatage des archives 42
5.5.6 Système d'archivage 43
5.5.7 Procédures de récupération des archives 43
5.6 Changement de clé d'une composante de l'AdminPKI 43
5.7 Compromission et plan anti-sinistre 43
5.7.1 Gestion des incidents 43
5.7.2 Corruption des ressources informatiques, de logiciels ou de données 43
5.7.3 Compromission des clés de signatures de l'AdminPKI 43
5.7.4 Plan de continuité 44
5.8 Cessation d'activité 44
5.8.1 Cessation d'activité de l'AdminPKI 44
5.8.2 Cessation d'activité d'une autorité d'enregistrement locale 45

6 Contrôles techniques de sécurité 46
6.1 Génération et installation des paires de clés 46
6.1.1 Génération des paires de clés 46
6.1.2 Délivrance de la clé privée à un abonné 46
6.1.3 Délivrance de la clé publique de l'abonné à l'autorité de certification 46
6.1.4 Publication de la clé publique des autorités de certification 46
6.1.5 Exigences cryptographiques 46
6.1.6 Génération des paramètres de clé publique et contrôle de qualité 47
6.1.7 Usage de la clé 47
6.2 Protection de la clé privée et contrôles techniques du module cryptographique. 47
6.2.1 Normes relatives au module cryptographique 47
6.2.2 Contrôle des clés de signature de l'AdminPKI 47
6.2.3 Séquestre de clé privée (key escrow) 47
6.2.4 Copie de secours de clé privée 47
6.2.5 Archivage de clé privée 48
6.2.6 Utilisation de clé privée 48
6.2.7 Protection de la clé de création de signature 48
6.2.8 Méthodes d'activation des clés privées 48
6.2.9 Méthode de désactivation des clés privées 48
6.2.10 Méthode de destruction des clés privées 48

6.2.11 Propriétés des modules cryptographiques 48
6.3 Autres aspects de la gestion des paires de clés 48
6.3.1 Archivage des clés publiques 48
6.3.2 Périodes d'utilisation des clés publiques et privées 49
6.4 Données d'activation 49
6.4.1 Génération et installation des données d'activation 49
6.4.2 Protection des données d'activation 49
6.4.3 Autres aspects des données d'activation 49
6.5 Contrôles de sécurité informatique 49
6.5.1 Besoins de sécurité spécifique sur les postes de travail 49
6.5.2 Niveau de sécurité du poste de travail 50
6.6 Contrôles techniques relatif au cycle de vie 50
6.6.1 Contrôle du développement des systèmes 50
6.6.2 Contrôles de gestion de la sécurité 50
6.6.3 Contrôles de sécurité des composants 50
6.7 Contrôle de sécurité réseau 50
6.8 Service d'horodatage 50

7 Certificats et liste des certificats annulés 51
7.1 Format du certificat d'abonné 51
7.2 Profil de la liste des certificats annulés CRL 53
7.3 OSCP 53

8 Contrôles de conformité 54
8.1 Fréquence et circonstances 54
8.2 Identité et compétences de l'auditeur 54
8.3 Relation entre l'auditeur et l'AdminPKI 54
8.4 Objet de l'inspection 54
8.5 Mesures adoptées lorsque des irrégularités ont été relevées 54
8.6 Communication des résultats 54

9 Conditions cadres 55
9.1 Emoluments 55
9.1.1 Emission et renouvellement du certificat de l'abonné 55
9.2 Responsabilité financière 55
9.2.1 Protection d'assurance 55
9.2.2 Protection d'assurance pour abonnés et les LRA 55
9.3 Protection des données 55
9.3.1 Informations confidentielles 55
9.3.2 Informations non confidentielles 56
9.3.3 Protection des données confidentielles 56
9.4 Données personnelles 56
9.5 Droits sur la propriété intellectuelle 56
9.6 Garanties et assurances 57
9.6.1 Représentations et garanties des autorités de certification de l'AdminPKI 57
9.6.2 Représentations et garanties des autorités d'enregistrement locales LRA 57
9.6.3 Représentations et garanties de l'abonné 57
9.6.4 Représentations et garanties de la partie utilisatrice 57
9.6.5 Représentations et garanties d'autres parties 57
9.7 Limites de la garantie 57
9.8 Responsabilité et limitation de responsabilité 57
9.8.1 Responsabilité et limitation de responsabilité de l'AdminPKI 57
9.8.2 Responsabilité des abonnés 58
9.8.3 Responsabilité des LRA 58
9.9 Indemnisation 58
9.10 Entrée en vigueur, validité, applicabilité 58
9.10.1 Entrée en vigueur 58

9.10.2 Validité 58
9.10.3 Applicabilité en cas de non validité 59
9.11 Information des abonnés 59
9.12 Administration du présent document 59
9.13 Règlement des litiges 59
9.14 Lois applicables 59
9.15 Report de droits et d'obligations 59
9.16 Autres dispositions 59
9.16.1 Langue 59

Annexes 60
9.17 Annexe A - Références 60
9.18 Annexe B - Structure ASN1 61
Annexe B1 - Autorité de certification AdminCA-A-T01 61
Annexe B2 - Certificat d'abonné 64
Annexe B3 - Service d'horodatage (TSA) 66
Annexe B4 - Liste des certificats annulés 68

1 Introduction

1.1 Aperçu

Ce document est l'énoncé des pratiques de certification [CPS], respectivement la politique de certification [CP] de l'autorité de certification AdminPKI de l'office fédéral de l'informatique et de la télécommunication OFIT. Il décrit les pratiques suivies par l'AdminPKI pour émettre des certificats qualifiés[1] au sens de la loi fédérale sur les services de certification dans le domaine de la signature électronique (Loi sur la signature électronique, SCSE) [1].

En vertu de l'article 3, alinéa 3 SCSE, l'OFIT est reconnu en tant qu'unité administrative de la Confédération.

Lorsque l'AdminPKI est mentionnée comme titulaire de droits et d'obligations, c'est la Confédération suisse, représentée par OFIT, qui est visée.

La structure de ce document est reprise du chapitre 6 de la norme RFC 3647 [3].

1.2 Identification

Le présent document porte le titre de : « *Enoncé des pratiques de certification / politique de certification de l'autorité de certification AdminPKI (certificats qualifiés)* ».

Il est identifié par l'OID **2.16.756.1.17.3.1.4**

L'arborescence d'identification ({2 16 756}) est gérée par l'office fédérale de la communication (OFCOM) et est subdivisée en 8 arcs [19]). L'arc {2 16 756 1 n} identifie les noms d'organisation selon la recommandation F.500 de l'UIT [20].

L'identificateur {2 16 756 1 17} identifie le nom d'organisation *Admin* qui est attribué à l'office fédérale de l'informatique et de la télécommunication OFIT.

L'AdminPKI gère l'arc {2 16 756 1 17 3}.

[1] *Les certificats qualifiés sont des certificats de classe A selon la terminologie de l'Administration fédérale*

1.3 Groupes d'utilisateurs

1.3.1 Autorités de certification

La délivrance des certificats qualifiés repose sur une infrastructure de certification AdminPKI[2] à deux niveaux.

Au premier niveau, l'**autorité de certification primaire** *Admin-Root-CA* est chargée de valider le certificat à clé publique des autorités de certification du deuxième niveau.

Au deuxième niveau, les **autorités de certification** sont chargées d'émettre, valider, publier, archiver et gérer les certificats d'abonnés. A l'heure actuelle, seule l'autorité de certification *AdminCA-A-T01* émet et gère des certificats qualifiés pour les abonnés.

L'autorité de certification primaire se différencie des autorités de certification du deuxième niveau avant tout par son certificat qu'elle signe par sa propre clé privée. Il n'existe aucun certificat pour vérifier l'authenticité du certificat de l'autorité primaire. La vérification doit être conduite avec des méthodes alternatives, comme par exemple, en comparant l'empreinte digitale du certificat publié par l'AdminPKI sur son site d'information avec l'empreinte sauvegardée localement par l'application. Le CallCenter de l'office fédéral de l'informatique et de la télécommunication OFIT fournit sur demande l'empreinte du certificat de l'autorité de certification primaire.

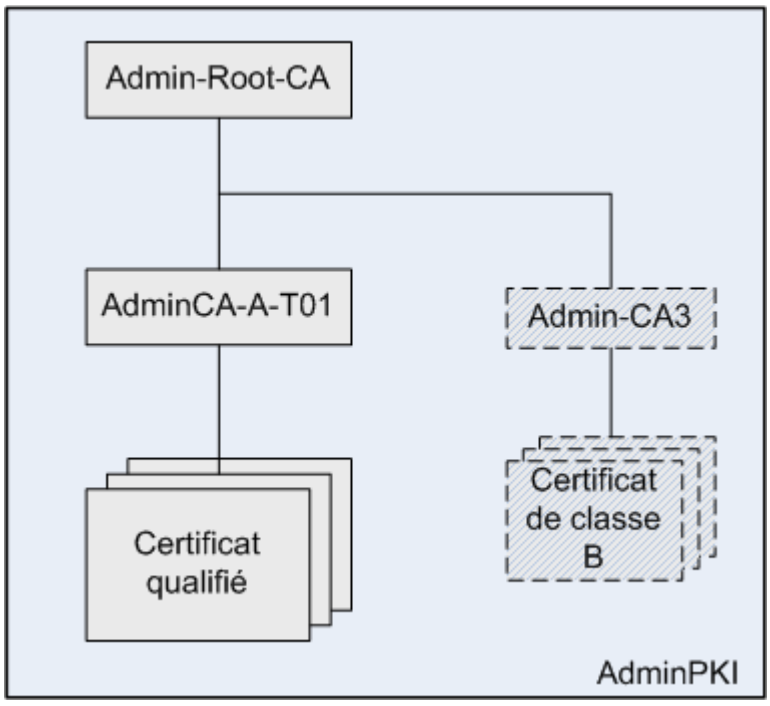

Figure 1: Hiérarchie de certification AdminPKI

[2] *L'infrastructure AdminPKI gère et émet également des certificats de classe B qui sont utilisés à des fins d'authentification, de chiffrement et de signature avancée. Les processus d'émission et de gestion des certificats de classe B sont identiques aux processus d'émission et de gestion des certificats qualifiés.*

Les obligations de l'infrastructure de certification AdminPKI sont de:

- respecter et appliquer les dispositions du présent document
- respecter et appliquer les dispositions du contrat cadre et de la convention qui la lie à ses clients
- mettre en œuvre les moyens techniques et humains qui sont nécessaires à l'exploitation de l'infrastructure
- protéger l'intégrité et la confidentialité de ses propres clés de signature, d'authentification et de chiffrement
- n'utiliser ses propres clés de signature, d'authentification et de chiffrement qu'aux fins pour lesquelles elles sont émises et avec les outils qui sont spécifiés dans le présent document
- tenir un journal des accès physiques et limiter leur accès à une population connue
- garantir la fiabilité des processus :
  - d'enregistrement de l'abonné
  - d'émission et de révocation des certificats
  - de publication de la liste des certificats révoqués.
- utiliser, si nécessaire, tous les moyens dont elles disposent pour informer les abonnés de la révocation du certificat d'une composante de l'infrastructure.

1.3.2 Autorité d'enregistrement LRA

L'autorité d'enregistrement ou autorité d'enregistrement locale [LRA] a pour tâches :

- d'identifier et d'authentifier les demandeurs de certificats
- d'initier les demandes d'opération qui sont:
  - l'enregistrement
  - l'émission du certificat
  - l'annulation (révocation) du certificat
  - le renouvellement du certificat.

La LRA est exploitée par une entité administrative (Administration fédérale, cantonale ou communale). Un contrat cadre et un protocole d'accord (SLA) lient l'AdminPKI et l'autorité d'enregistrement locale.

Les obligations de la LRA sont de:

- respecter et appliquer les dispositions du présent document
- respecter et appliquer les dispositions du contrat cadre et de la convention qui la lie à l'AdminPKI
- mettre en œuvre les moyens techniques et humains qui sont nécessaires à l'exploitation de la composante
- protéger l'intégrité et la confidentialité de ses propres clés de signature, d'authentification et de chiffrement
- n'utiliser ses propres clés de signature, d'authentification et de chiffrement qu'aux fins pour lesquelles elles sont émises et avec les outils qui sont spécifiés dans le présent document.
- respecter la législation relative au traitement et à la conservation des données personnel-

les

- garantir la fiabilité du processus d'enregistrement ; cela concerne en particulier :
  - la vérification des données personnelles du demandeur de certificat
  - la transmission d'une requête d'émission de certificat à l'autorité de certification de deuxième niveau
- informer l'abonné au sujet de ses droits et obligations
- vérifier l'authenticité d'une demande de révocation.
- informer l'abonné que son certificat est publié dans l'annuaire *Admin-Directory*.

1.3.3 Abonné

L'abonné[3] est une personne physique qui détient un certificat qualifié et un dispositif sécurisé de création de signature pour la mise en œuvre de sa clé privée. Il agit pour le compte d'une unité administrative (Administration fédérale, cantonale ou communale), conformément à la loi sur l'organisation du gouvernement et de l'administration (LOGA) 172.010, ainsi qu'à l'Ordonnance sur l'organisation du Département fédéral des finances 172.215.1, et ce dans le cadre de l'application concernée (cf. §1.4).

Dans la phase amont de certification, il est «demandeur» de certificat, dans le contexte du certificat X.509 il est « sujet » et dans la phase aval de certification il est « titulaire » de certificat.

Les obligations spécifiques de l'abonné sont de :

- respecter et appliquer les dispositions du présent document
- utiliser ses clés de signature avec des applications approuvées par l'AdminPKI
- avoir les connaissances de base qui sont nécessaires à une utilisation appropriée des clés de signature et des certificats
- conserver seul le contrôle de ses clés et du dispositif de signature, protéger le code d'activation du dispositif de signature
- prendre les dispositions nécessaires pour empêcher la perte ou le vol du dispositif de signature
- notifier immédiatement à l'autorité locale d'enregistrement ou à l'AdminPKI qu'il sait ou soupçonne que sa clé privée a été compromise
- faire révoquer son certificat si les informations qu'il contient ne sont pas/plus valables.

En signant la notice informative à l'intention de l'abonné, l'abonné confirme avoir pris connaissance de ses droits et obligations.

1.3.4 Partie utilisatrice

La partie utilisatrice est une entité ou une personne physique ou morale qui utilise un certificat et un dispositif de vérification de signature afin de valider un certificat et la signature correspondante dans le cadre d'une application (cf. § 1.4). Un utilisateur de certificat ne détient pas forcément de certificat propre.

Les applications utilisées par la partie utilisatrice doivent vérifier les certificats conformément

[3] *L'abonné peut être également une personne physique qui a besoin d'un certificat qualifié dans le cadre de sa relation avec une administration. Cette personne doit s'adresser à l'administration concernée pour obtenir un certificat qualifié.*

à la procédure de validation des chemins de certification précisés dans la recommandation X.509 de l'UIT - T.

1.3.5 Autres participants

L'office fédéral de la communication OFCOM édicte les prescriptions techniques et administratives concernant les services de certification dans le domaine de la signature électronique (RS 943.032.1).

Le Service Suisse d'accréditation SAS nomme les organismes de reconnaissances (cf. § 8.2) qui sont chargés de vérifier que les fournisseurs de service de certification FSC respectent les exigences de la loi sur la signature électronique.

1.4 Utilisation des certificats

1.4.1 Utilisation autorisée

L'utilisation des certificats émis par l'AdminPKI n'est permise qu'en relation avec des applications autorisées par l'AdminPKI. Il s'agit d'applications certifiées qui respectent les exigences de la loi sur la signature électronique (cf. Art. 6, SCSE) et/ou d'une loi[4] découlant de la directive 1999/93/CE du Parlement Européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électronique.

L'AdminPKI publie sur son site d'information la liste des applications autorisées.

1.4.2 Utilisation non autorisée

Les abonnés ne sont autorisés d'aucune façon, à utiliser leurs certificats à d'autres fins que la signature électronique.

1.5 Administration du document / Personne de contact

1.5.1 Administration du document

L'AdminPKI est garant du contenu, de la gestion et de la publication du présent document (cf. § 9.12)

1.5.2 Personne de contact

Le responsable PKI est la personne de contact :

Office fédéral de l'informatique et de la télécommunication OFIT
Responsable PKI
Centre de solutions - Cyberadministration
Monbijoustrasse 74

[4] *Exemple : Gesetz über die Rahmenbedingungen für elektronischen Signaturen (Signaturgesetz – SigG) du 16 mai 2001.*

CH-3003 Berne

1.5.3 Vérification du contenu

Le responsable PKI et le responsable sécurité de l'AdminPKI sont conjointement tenus de vérifier et de maintenir le contenu du présent document.

1.5.4 Procédure d'approbation

Voir § 9.12.

1.6 Glossaire et abréviations

1.6.1 Glossaire

Abonné	personne physique qui détient un certificat qualifié et un dispositif sécurisé de création de signature. Il agit pour le compte d'une entité (Administration fédérale, cantonale ou communale), conformément à la loi sur l'organisation du gouvernement et de l'administration (LOGA) 172.010, ainsi qu'à l'Ordonnance sur l'organisation du Département fédéral des finances 172.215.1, et ce dans le cadre de l'application concernée. Dans la phase amont de certification, il est « demandeur » de certificat, dans le contexte du certificat X.509 il est « sujet » et dans la phase aval de certification il est « titulaire » de certificat.
Admin-Directory	méta annuaire de l'Administration fédérale où sont publiés et archivés les certificats et les listes de certificats annulés (révoqués).
Autorité de certification de premier niveau	dans une infrastructure de certification de type hiérarchique, l'autorité de certification de premier niveau ou Root se différencie des autres autorités de certification parce que son certificat est signé par sa propre clé privée. Il n'existe aucun certificat pour vérifier l'authenticité du certificat de l'autorité Root. La vérification doit être conduite avec des méthodes alternatives, comme par exemple, en comparant l'empreinte digitale du certificat publié par l'autorité de surveillance avec l'empreinte sauvegardée localement par l'application.
Autorité de certification	autorité de confiance qui délivre et gère des certificats à clé publique et des listes de certificats suspendus et annulés (révoqués) qui sont conformes à la recommandation X.509.
Autorité d'enregistrement	personne ou organisation responsable de l'identification/ l'authentification d'un abonné avant l'émission de certificats à son intention, mais qui ne signe et n'émet pas les certificats. L'autorité d'enregistrement est subordonnée à, au moins, une autorité de certification de deuxième niveau.
Classes de certificats	l'Administration fédérale a défini différentes classes de certificats qui sont désignées par une lettre de A à E. Les classes de certificats se différencient au niveau de la procédure d'identification du demandeur de certificat, du support du certificat et de l'extension de l'utilisation de clés.
Certificat	clé publique d'un abonné, ainsi que d'autres informations connexes, signés numériquement avec la clé privée de l'autorité de certification qui l'a émis. Le format du certificat est conforme à la recommandation X.509.

Certificat de classe A	un certificat de classe A est un certificat qualifié au sens de la loi sur la signature électronique (SCSE).
Certificat qualifié	certificat numérique qui remplit les conditions de l'art. 7 de la loi sur la signature électronique (SCSE).
Custom DN	Champ DN (nom distinctif) d'une personne (abonné), pouvant être adapté à volonté si l'abonné est qualifié pour ce type de certificat
Données d'activation	données personnelles, autres que les clés, qui sont nécessaires à l'activation des modules cryptographiques.
Enregistrement	document faisant état de résultats obtenus ou apportant la preuve de la réalisation d'une activité. Les enregistrements peuvent, par exemple, documenter la traçabilité et apporter la preuve que vérifications, actions préventives et actions correctives ont été réalisées.
fournisseur de services de certification	organisme qui certifie des données dans un environnement électronique et qui délivre à cette fin des certificats numériques.
Identificateur d'objet	identificateur alphanumérique unique, enregistré conformément aux normes internationales en la matière pour désigner un objet ou une classe d'objets spécifiques.
Infrastructure à clé publique	ensemble complet des politiques, processus, environnement serveurs, logiciels et postes de travail servant à l'administration des certificats et des clés.
ISIS-MTT Admission	Spécification définissant le format des données concernant la légitimité (p.ex. rôle ou profession) d'une personne à exercer, à pratiquer une/des activités. Nouvelle dénomination depuis le 20 janvier 2009 : CommonPKI
Intégrité des données	assurance que les données n'ont pas été modifiées entre leur création et leur réception.
Liste des certificats d'autorités de certification annulés (révoquées)	liste de certificats de CA annulés (révoqués) par l'autorité de certification de premier niveau.
Liste des certificats suspendus et annulés (révoqués)	liste tenue à jour par l'autorité de certification contenant les numéros de certificats qui ont été annulés (révoqués) avant que la date de validité soit échue.
Organisme de reconnaissance	organisme qui, selon les règles de l'accréditation est habilité à reconnaître et à surveiller les fournisseurs de services de certification. En Suisse, KPMG AG est l'organisme de reconnaissance.

Partie utilisatrice	entité ou personne physique ou morale qui utilise un certificat et un dispositif de vérification de signature afin de valider un certificat et la signature correspondante dans le cadre d'une application.
Politique en matière de sécurité	une politique de sécurité est un ensemble de règles et de directives élaborées en fonction d'une analyse de risques pour réduire la probabilité des incidents (mesures préventives) et pallier aux effets de ces derniers (mesures correctives), afin de protéger les ressources identifiées comme sensibles pour le fournisseur de services de certification électronique. Les spécifications d'une stratégie et d'une politique en matière de sécurité permettent de définir clairement le niveau de sécurité à atteindre globalement pour un système d'information et spécifiquement pour chaque élément de l'architecture de sécurité.
Publication	opération consistant à mettre un certificat à disposition de tiers (partie utilisatrice) pour leur permettre de vérifier une signature électronique.
Renouvellement d'un certificat	opération effectuée à la demande d'un abonné ou en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat pour l'abonné. La re-génération d'un certificat après révocation n'est pas un renouvellement.
signature électronique	données électroniques jointes ou liées logiquement à d'autres données électroniques et qui servent à vérifier leur authenticité.
signature électronique avancée	signature électronique qui satisfait aux exigences suivantes: 1. être liée uniquement au titulaire 2. permettre d'identifier le titulaire 3. être créée par des moyens que le titulaire peut garder sous son contrôle exclusif 4. être liée aux données auxquelles elle se rapporte de telle sorte que toute modification ultérieure des données soit détectable.
signature électronique qualifiée	signature électronique avancée fondée sur un dispositif sécurisé de création de signature au sens de l'art. 6, al. 1 et 2 de la loi sur la signature électronique (SCSE) et sur un certificat qualifié valable au moment de sa création.

1.6.2 Abréviations

SIGLES	DESCRIPTION	ACRONYMS	DESCRIPTION
AC	Autorité de certification	CA	Certification Authority

SIGLES	DESCRIPTION	ACRONYMS	DESCRIPTION
AE	Autorité d'enregistrement	RA	Registration Authority
ASC	Alimentation sans coupure	UPS	Uninterrupted Power Supply
ASD	Algorithme de signature numérique	DSA	Digital Signature Algorithm
CB	Organisme de certification	CB	Certification Body
DN	Nom distinctif	DN	Distinguished Name
EPC	Énoncé des pratiques de certification	CPS	Certificate Practice Statement
FSC	Fournisseur de services de certification	CSP	
FIPS	Federal Information Processing Standard	FIPS	Federal Information Processing Standard
ICP	Infrastructure des clés publiques	PKI	Public Key Infrastructure
IDO	Identificateur d'objet	OID	Object Identifier
ISIS-MTT	Industrial Signature Interoperability and Mailtrust Specification	ISIS-MTT	Industrial Signature Interoperability and Mailtrust Specification
LAR	Liste des autorités annulées (révoquées)	ARL	Authority Revocation List
LRC	Liste de révocation de certificats	CRL	Certificate Revocation List
ND	Nom distinctif	DN	Distinghished Name
NIP	Numéro d'identification personnel	PIN	Personal Identification Number
OFCOM	Office fédéral de la télécommunication	OFCOM	
OFIT	office fédéral de l'informatique et de	-	

SIGLES	DESCRIPTION	ACRONYMS	DESCRIPTION
	la télécommunication		
PC	Politique de certification	CP	Certificate Policy
PKCS	Norme relative à la cryptographie à clé publique	PKCS	Public-key Cryptography Standard
PKIX	Infrastructure à clé publique (conforme à la norme X.509)	PKIX	Public Key Infrastructure X509
RFC	Document RFC (Request For Comments)	RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (type d'algorithme)	RSA	Rivest-Shamir-Adleman
SAS	Service Suisse d'accréditation	SAS	Swiss Accreditation Service
SHA-1	Secure Hash Algorithm	SHA-1	Secure Hash Algorithm
SLA	Accord de niveau de service	SLA	Service Level Agreement
UIT	Union internationale des télécommunications	ITU	International Telecommunication Union
USIC	Unité de stratégie informatique de la Confédération	-	

2 Service d'information et service d'annuaire

2.1 Service de publication et d'archivage

Les certificats de l'AdminPKI, ainsi que les listes des certificats annulés sont publiés et archivés dans le Meta annuaire électronique *Admin-Directory*. *Admin-Directory* est un service d'annuaire conforme à la norme X.500 de l'UIT-T.

Le service d'annuaire *Admin-Directory version Intranet* est accessible depuis le réseau Intranet de l'Administration fédérale à l'adresse http://intranet.annuaires.admin.ch ou à l'aide du protocole LDAP (port 389) depuis Internet.

La version publique de l'*Admin-Directory* (*Admin-Directory Public*) est accessible depuis l'Internet (protocole LDAP). La version publique ne contient qu'une partie des données de la version Intranet.

2.2 Le service d'information

Le service d'information sert à publier:

- l'énoncé des pratiques de certification, respectivement la politique de certification de l'autorité de certification AdminPKI (ce document)
- la directive d'enregistrement de la LRA
- la notice informative à l'intention de l'abonné
- les certificats des autorités de certification
- la liste des certificats annulés CRL
- toutes les modifications et/ou extensions qui se rapportent aux autorités de certification
- la mise en œuvre et en service d'une nouvelle autorité de certification de deuxième niveau dédiée à la émission de certificats qualifiés
- la liste des applications autorisées pour signer électroniquement des documents
- le lien de la liste des certificats révoqués
- le lien sur les documents juridiques
- l'Url du Service d'accréditation suisse SAS
- l'Url du Recueil systématique du droit fédéral (lois et ordonnances de la Confédération Suisse)

Le service est accessible à l'adresse http://www.pki.admin.ch/

2.3 Actualisation des informations

Les dates de publication des documents liés à l'AdminPKI coïncident avec la date d'entrée en vigueur.

L'Admin-Root-CA met à jour sa ARL au minimum une fois par année et immédiatement après avoir annulé le certificat d'une autorité de certification de deuxième niveau.

L'AdminCA-A-T01 met à jour sa CRL au minimum tous les 3 (trois) jours et immédiatement après l'annulation d'un certificat d'abonné.

Après chaque annulation, la CRL et/ou l'ARL est publiée sans retard. L'AdminPKI n'offre pas de service en ligne (OCSP) pour vérifier la validité d'un certificat.

2.4 Contrôle d'accès

A l'exception de données personnelles liées à des applications, l'ensemble des données de l'annuaire *Admin-Directory version Intranet* est accessible, en lecture, depuis le réseau de l'Administration fédérale.

L'ensemble des données de l'annuaire *Admin-Directory Public* est accessible depuis le réseau Internet. L'annuaire *Admin-Directory Public* est une réplication partielle (protocole DISP) de l'annuaire *Admin-Directory Intranet.*

3 Identification et authentification

L'AdminPKI délègue les tâches d'identification et d'authentification des abonnés aux autorités d'enregistrement locales LRA (cf. § 1.3.2).

Le présent chapitre décrit les pratiques édictées par l'AdminPKI et suivies par les autorités d'enregistrement locales afin d'identifier et authentifier les abonnés[5].

3.1 Attribution d'un nom

3.1.1 Convention de noms

Dans chaque certificat émis par l'autorité de certification de deuxième niveau *AdminCA-A-T01* (cf. § 1.3.1), l'émetteur (issuer) et le signataire (subject) sont identifiés par un « nom de forme distinctive » (DN distinguished name). Le DN, qui se présente sous la forme d'une chaîne imprimable[6] X.501 et non vide, doit être conforme aux dispositions de la directive technique I006 (DT20) de l'Unité de stratégie informatique de la Confédération [USIC] [9].

L'extension « Custom DN » permet de choisir librement le nom de forme distinctive en respectant les dispositions de la directive technique I006 (DT20) de l'Unité de stratégie informatique de la Confédération [USIC] [9].

Les attributs autorisées dans le champ „Custom DN" sont :

- Country : c
- Organization : o
- Telephone : t
- Organizational Unit : ou
- Common Name : cn
- Location : l
- Email Address : e
- Surname : sn
- Given Name : gn
- Pseudonym : pseudonym

Les abonnés avec extension « Custom DN » ainsi que leurs certificats ne sont pas enregistrés dans l'annuaire *Admin-Directory*, mais dans la base de données de l'AdminPKI.

3.1.2 Utilisation de noms explicites

Voir directive technique I006 (DT20) de l'Unité de stratégie informatique de la Confédération [USIC] [9].

L'abonné (cf. 1.3.3) est une personne physique qui agit pour le compte d'une unité administrative (Administration fédérale, cantonale ou communale). L'abonné est identifié par son

[5] *Abonné : cf. 1.3.3*

[6] *Jeu de caractères T.50*

nom, son prénom et un code unique (voir également chapitre 3.1.5). A l'exception de certificats émis avec l'extension « Custom DN », le certificat de l'abonné ne contient aucune information relative à sa fonction, à un éventuel titre et/ou à une unité d'organisation.

Dans le cas de pseudonymes, le nom distinctif de l'abonné inclut le mot PSEUDO.

3.1.3 Anonymat et pseudonymie

L'utilisation de pseudonyme est soumise à autorisation de **l'**AdminPKI.

3.1.4 Règles d'interprétation des diverses formes de noms

La conversion des caractères spéciaux du jeu de caractères T.61 en T.50 est spécifiée dans la table ci-dessous:

T.61	T.50
+	-
/	-
à	a
À	A
á	a
Á	A
â	a
Â	A
ä	ae
Ä	Ae
æ	ae
Æ	Ae
ç	c
è	e
È	E
é	e
É	E
ê	e
Ê	E

T.61	T.50
ë	e
Ë	E
ì	i
Ì	I
î	i
Î	I
ï	i
Ï	I
Ñ	N
ñ	n
ò	o
Ò	O
ó	o
Ó	O
ô	o
Ô	O
ö	oe
Ö	Oe
Ø	O

T.61	T.50
ø	o
œ	oe
Œ	Oe
Š	S
š	s
ß	ss
ù	u
Ù	U
ú	u
Ú	U
û	u
Û	U
ü	ue
Ü	Ue
ý	y
ÿ	y
Ÿ	Y

3.1.5 Unicité des noms

L'AdminPKI assigne à l'attribut du sujet du certificat, conformément aux dispositions de la directive technique I006, une valeur unique se composant du nom et du prénom du demandeur du certificat et d'un code haché. Pour l'Administration fédérale, le code haché est obtenu à l'aide du numéro de personnel. Pour les cantons, le code haché est obtenu à l'aide d'un numéro identifiant le canton, éventuellement d'un numéro identifiant la commune et du numéro de personnel.

Lorsque le nom à inclure dans un certificat provoque un litige avec un autre utilisateur, l'autorité d'enregistrement, à qui la demande de certification a été formulée, en informe l'AdminPKI. L'AdminPKI est responsable de la résolution de ce litige.

3.1.6 Reconnaissance, authentification et rôle des marques de commerce

Sans objet.

Le certificat d'abonné ne contient pas d'informations relatives à une marque de commerce.

3.2 Enregistrement initial

3.2.1 Preuve de la possession d'une clé privée

Les clés de signature sont générées (cf. 4.1) dans un dispositif de création de signature (carte à puce) tel que défini au § 6.1 du présent document. La génération des clés est initialisée par l'autorité d'enregistrement locale en présence du demandeur de certificat.

Les données d'activation (PIN et PUK), permettant de générer et d'activer l'usage des clés de signature, doivent être spécifiées par le demandeur de certificat et elles sont en sa seule possession.

De facto, le demandeur de certificat est en possession des clés de signature.

3.2.2 Authentification de l'identité d'une entité administrative

Sans objet.

A l'exception de certificats émis avec l'extension « Custom DN », le certificat ne contient aucune information relative à la qualité de l'abonné de représenter une personne morale déterminée.

3.2.3 Vérification de l'identité du demandeur de certificat

Afin de garantir la véracité du lien entre une paire de clés cryptographiques, plus précisément entre une clé publique et un abonné, l'AdminPKI doit s'assurer de l'identité du demandeur de certificat de visu et au moyen de documents officiels et valables, tels que passeport ou carte d'identité.

La tâche d'identifier les demandeurs de certificats et de réunir les informations nécessaires à l'émission d'un certificat est déléguée à l'autorité d'enregistrement locale.

L'autorité d'enregistrement locale doit:

- vérifier le contenu du formulaire de demande de certificat
- vérifier que le demandeur fait l'objet d'un enregistrement dans le service d'annuaire *Admin-Directory*
- s'assurer que le nom du demandeur dans l'annuaire soit identique à celui de la pièce

d'identité présentée[7]

- scanner la pièce d'identité présentée
- vérifier la véracité du nom de forme distinctive dans le cas d'un certificat émis avec l'extension « Custom DN » (p.ex. patente, unité organisationnelle, etc.)

La copie électronique de la pièce d'identité est jointe à la demande électronique de certificat qui est soumise à l'AdminCA-A-T01.

3.2.4 Données non vérifiées

Toutes les informations qui sont nécessaires à l'identification du demandeur sont vérifiées. Aucune autre information n'est vérifiée par l'autorité locale d'enregistrement.

3.2.5 Vérification de qualités spécifiques de l'abonné

Sans objet.

Le certificat ne contient aucune information relative à la qualité de l'abonné de représenter une personne morale déterminée.

3.2.6 Certification croisée (reconnaissance)

Une autorité de certification de deuxième niveau qui émet des certificats qualifiés au sens de la loi sur la signature électronique n'est pas autorisée à reconnaître (certification croisée) d'autres autorités de certification.

3.3 Renouvellement du certificat

La procédure qui permet de renouveler un certificat est identique à la procédure qui permet d'obtenir un premier certificat. L'abonné doit se représenter devant une autorité d'enregistrement locale à des fins d'identification et d'authentification.

Une nouvelle paire de clés de signature est générée.

3.4 Authentification d'une demande d'annulation

La procédure de demande d'annulation est décrite au chapitre 4.9.3.

L'abonné peut demander l'annulation de son certificat :

- en se présentant en personne devant l'autorité d'enregistrement locale
- en envoyant sa demande d'annulation par courrier postal
- en signant sa demande d'annulation à l'aide de sa clé de signature, à condition que la demande de révocation ne soit pas due à une compromission ou suspicion de compromission, perte ou vol de données de création de signature

[7] *Admin-Directory n'accepte pas les caractères spéciaux du jeu de caractères T.61. Avant de comparer les noms, l'autorité d'enregistrement locale doit convertir les caractères spéciaux selon les règles d'interprétation des diverses formes de noms (cf. § 3.1.4. En cas de doute, l'autorité d'enregistrement locale doit s'adresser au responsable sécurité de AdminPKI*

- en contactant le CallCenter de l'office fédéral de l'informatique et de la télécommunication
- à l'aide d'une application Web accessible depuis le site d'information de l'AdminPKI www.pki.admin.ch

L'autorité d'enregistrement locale s'assure de l'identité et de l'autorisation du demandeur en confrontant les éléments contenus dans le dossier de demande de certificat et ceux présentés par l'abonné.

L'unité administrative (cf. 1.3.3) peut demander la révocation d'un certificat en envoyant par courrier postal une requête de révocation dûment motivée.

L'autorité d'enregistrement locale peut décider d'annuler les certificats d'un abonné.

4 Exigences opérationnelles

4.1 Demande de certificat

4.1.1 Qui peut faire une demande de certificat

Tout collaborateur d'une unité administrative (Administration fédérale, cantonal ou communale) conformément à la loi sur l'organisation du gouvernement et de l'administration (LOGA) 172.010, ainsi qu'à l'Ordonnance sur l'organisation du Département fédéral des finances 172.215.1 qui a signé un contrat cadre et a conclu un protocole d'accord avec l'AdminPKI, peut faire une demande de certificat (cf. 1.3.3). Les données personnelles du demandeur de certificat (nom, prénom, code haché distinctif, adresse de messagerie électronique) sont publiées dans l'annuaire Admin-Directory.

4.1.2 Processus d'enregistrement

L'obtention d'un certificat se déroule en quatre phases : identification et authentification du demandeur (1), génération de la requête (2), validation de la requête (3) et délivrance du certificat (4).

La tâche d'identification/authentification du demandeur de certificat est déléguée à l'autorité d'enregistrement locale qui doit s'assurer de l'identité du demandeur de visu et au moyen de documents officiels et valables (passeport et carte d'identité). L'autorité d'enregistrement locale doit scanner la pièce d'identité présentée. Ce document est joint à la requête de certificat qui est transmise à l'autorité de certification de deuxième niveau. L'autorité d'enregistrement doit également vérifier l'authenticité de la requête (contrôle du formulaire de requête, contrôle des données dans l'annuaire *Admin-Directory*).

L'autorité d'enregistrement locale doit informer le demandeur au sujet de ses obligations et de sa responsabilité liées à l'utilisation des certificats et du dispositif de création de signature.

Les clés de signature sont générées dans le dispositif de création de signature (carte à puce). Les données d'activation qui permettent de générer et d'activer l'usage des clés de signature (PIN et PUK), doivent être spécifiées par le demandeur de certificat et elles sont en sa seule possession.

Les requêtes de certificats authentifiées sont validées par l'autorité d'enregistrement locale et transmises à l'autorité de certification de deuxième niveau pour exécution. Le certificat est émis et délivré au demandeur.

Les processus de génération de certificats avec l'extension « Custom DN » ou avec l'admission ISIS-MTT diffèrent du processus ordinaire dans le fait que les données personnelles sont introduites dans la base de données de l'AdminPKI, et non dans l'annuaire AdminDirectory. Ce processus exige deux officiers LRA avec des rôles distincts.

Cas particuliers « Custom DN » :

- Définition du champ « Custom DN » de l'abonné et attribution des droits d'émissions à un officier LRA par un autre officier LRA.

Cas particuliers ISIS-MTT :

- Gestion préalable du registre des professions et attribution des droits d'émissions à un officier LRA par un autre officier LRA.

- un second officier LRA qui a reçu les droits de gérer un abonné éligible pour ISIS-MTT Admission

4.2 Traitement de la demande de certificat

Des informations complémentaires sont disponibles dans les directives d'enregistrement de l'AdminPKI pour la LRA [21].

4.2.1 Identification et authentification du demandeur

La tâche d'identification/authentification du demandeur de certificat est déléguée à l'autorité d'enregistrement locale qui doit s'assurer de l'identité du demandeur de visu et au moyen de documents officiels et valables (passeport et carte d'identité). L'autorité d'enregistrement locale doit scanner la pièce d'identité présentée. Ce document est joint à la requête de certificat qui est transmise à l'autorité de certification de deuxième niveau.

4.2.2 Acceptation/refus de la demande de certificat

Toute personne dont les données personnelles sont publiées dans l'annulaire *Admin-Directory* peut remplir le formulaire de requête de certificat et l'adresser à l'autorité d'enregistrement locale

L'autorité d'enregistrement locale doit vérifier l'authenticité de la requête (contrôle du formulaire de requête, contrôle des données dans l'annuaire *Admin-Directory*, contrôle de l'identité du demandeur). Au cas où les données sont incomplètes et/ou le demandeur de certificat n'est pas identifiable, l'autorité d'enregistrement locale interrompt le processus de traitement de la requête.

4.2.3 Traitement de la demande de certificat

L'autorité d'enregistrement locale doit :

- vérifier l'authenticité et le contenu de la demande de certificat, respectivement, accepter/refuser la demande
- vérifier l'identité du demandeur de certificat
- initialiser le processus de génération des clés dans le dispositif de signature
- émettre/valider la demande de certificat
- transmettre la demande de certificat à l'autorité de certification de deuxième niveau pour exécution
- déposer la demande dans le dossier du demandeur de certificat.

Les demandes de certificats, validées par l'autorité d'enregistrement locale, sont traitées en temps réel (dès réception) et automatiquement par l'autorité de certification de deuxième niveau. L'autorité de certification de deuxième niveau doit :

- vérifier l'authenticité et l'intégrité de la demande de certificat
- accepter/refuser la demande

- émettre le certificat.

4.3 Emission du certificat

4.3.1 Actions de l'autorité de certification de deuxième niveau durant le processus d'émission

Les demandes de certificats, soumises par l'autorité d'enregistrement, sont traitées en temps réel et automatiquement par l'autorité de certification de deuxième niveau.

L'autorité de certification de deuxième niveau doit :

- vérifier l'authenticité et l'intégrité des demandes de certificat
- vérifier l'unicité de la clé publique à certifier
- émettre et valider le certificat en le signant à l'aide de sa clé de signature
- publier et archiver le certificat dans l'annuaire Admin-Directory. Le consentement de l'unité administrative qui emploie l'abonné est nécessaire pour publier le certificat dans la version publique de l'Admin-Directory
- transmettre le certificat à l'autorité d'enregistrement locale afin de le sauvegarder sur le dispositif de signature du demandeur de certificat.

4.3.2 Notification de l'émission du certificat au demandeur

L'émission du certificat est notifiée au demandeur à l'aide d'un message électronique. Pour ce faire, l'adresse de messagerie électronique contenue dans le certificat est utilisée.

4.4 Acceptation du certificat

4.4.1 Procédure d'acceptation

En signant la notice informative à l'intention de l'abonné, l'abonné confirme avoir pris connaissance de ses droits et obligations. Plus précisément, par sa signature il manifeste :

- son adhésion aux conditions d'utilisation et de gestion par l'AdminCA-A-T01 de son certificat et le cas échéant de ses données de création et de vérification de signature électronique conformément au présent document
- son accord sur les conditions de publication de son certificat
- son accord sur la conservation de données personnelles et de certification par l'autorité d'enregistrement locale
- son consentement sur les obligations qui lui incombent
- sa confirmation de l'exactitude des informations contenues dans le certificat.

En cas de cessation d'activité de l'AdminPKI, l'abonné accepte également que son dossier soit transféré au fournisseur de services de certification qui reprend les tâches de certification de l'AdminPKI.

4.4.2 Publication du certificat par l'autorité d'enregistrement AdminCA-A-T01

Les certificats émis sont publiés dans l'annuaire *Admin-Directory* version Intranet (accessible

depuis le réseau de l'Administration fédérale). Sur demande, ils sont également publiés dans l'annuaire *Admin-Directory* version Internet.

4.4.3 Notification de l'émission du certificat à d'autres entités

L'émission des certificats est notifiée aux unités administratives cantonales et communales qui ont signé un contrat cadre et conclu un protocole d'accord avec AdminPKI.

4.5 Utilisation des clés et du certificat

Le domaine d'utilisation des clés de signature et du certificat qualifié est spécifié au chapitre 1.4. Les clés de signature et le certificat qualifié correspondant sont réservés exclusivement à la signature électronique de documents et à la vérification de ladite signature électronique.

4.5.1 Utilisation des clés et du certificat par l'abonné

Les abonnés sont autorisés à utiliser leurs clés privées avec les applications informatiques qui sont approuvées et publiées par le service d'information de l'AdminPKI

L'utilisation des clés par l'abonné est soumise aux conditions suivantes :

- l'abonné doit utiliser ses clés privées pour des applications approuvées et à des fins appropriées
- l'abonné a les connaissances de base qui sont nécessaires à une utilisation appropriée des clés de signature et des certificats
- l'abonné utilise un dispositif de signature approuvé par l'AdminPKI. Une liste des dispositifs de signature approuvés est publiée sur le site d'information
- l'abonné doit être au courant de sa responsabilité et de ses obligations qui sont stipulées dans le présent document
- l'abonné doit conserver seul le contrôle de ses clés et du dispositif de signature. Il doit prendre les précautions nécessaires pour en empêcher la perte, la divulgation à des tiers, la modification et l'utilisation non autorisée
- l'abonné doit notifier immédiatement à l'autorité d'enregistrement locale ou au CallCenter de l'office fédéral de l'informatique et de la télécommunication OFIT qu'il sait ou soupçonne que sa clé privée a été compromise
- l'abonné n'est pas autorisé, de quelque façon que ce soit, à utiliser son certificat à d'autre fin que la signature électronique
- l'abonné doit faire révoquer son certificat si les informations qu'il contient ne sont plus valables.

4.5.2 Utilisation du certificat par les tiers (parties utilisatrices)

L'utilisation du certificat par les tiers est soumise aux conditions suivantes :

- le tiers a connaissance du contenu de la CP/CPS
- le tiers dispose des connaissances de base qui sont nécessaires à une utilisation appropriée des certificats
- le tiers doit utiliser un dispositif de vérification de signatures approuvé par l'AdminPKI
- le tiers doit vérifier la validité du certificat avant de l'utiliser conformément à la procédure

de validation des chemins de certification précisés dans la recommandation X.509 de l'UIT - T.

4.6 Prolongation de la validité du certificat

L'abonné qui veut faire prolonger la validité d'un certificat (cf. RFC3647 [3] , chapitre 4.4.6), doit faire une nouvelle requête de certificat et se représenter devant l'autorité d'enregistrement locale à des fins d'identification. Les dispositions des chapitres 4.1, 4.2, 4.3 4.4 et 4.5 s'appliquent.

Cette requête de certificat implique la génération d'une nouvelle paire de clés de signature dans le dispositif de signature de l'abonné.

4.7 Remplacement du certificat

L'abonné, qui veut remplacer un certificat valable, échu ou révoqué (cf. RFC3647 [3] , chapitre 4.4.7), doit faire une nouvelle requête de certificat et se représenter devant l'autorité d'enregistrement locale à des fins d'identification. Les dispositions des chapitres 4.1, 4.2, 4.3 4.4 et 4.5 s'appliquent.

Cette requête de certificat implique la génération d'une nouvelle paire de clés de signature dans le dispositif de signature de l'abonné.

4.8 Modification du contenu du certificat

L'abonné, qui veut faire modifier le contenu d'un certificat valable (cf. RFC3647 [3] , chapitre 4.4.8), doit faire une nouvelle requête de certificat et se représenter devant l'autorité d'enregistrement locale à des fins d'identification. Les dispositions des chapitres 4.1, 4.2, 4.3 4.4 et 4.5 s'appliquent.

Cette requête de certificat implique la génération d'une nouvelle paire de clés de signature dans le dispositif de signature de l'abonné.

4.9 Suspension et annulation (révocation) de certificat

Le certificat d'abonné peut être annulé (révoqué) ; l'annulation est définitive.

La suspension de certificat n'est pas autorisée (cf. § 3.4 des prescriptions techniques et administratives concernant les services de certification dans le domaine de la signature électronique [2]).

4.9.1 Motifs d'annulation

L'autorité de certification de deuxième niveau peut annuler un certificat pour les raisons suivantes :

- il y a compromission présumée ou réelle des clés privées ou des codes d'activation (PIN/PUK)
- la véracité du lien entre la clé de signature et l'abonné ne peut plus être garantie
- le certificat contient des informations qui ne sont plus valables
- l'abonné a reçu un certificat de manière illicite

- il y a eu renvoi ou suspension de l'abonné
- un terme ou un contrat a pris fin
- l'abonné n'a pas respecté ses obligations ou d'autres conventions, règlements ou lois qui pourraient être en vigueurs
- l'unité administrative qui emploie l'abonné n'a pas respectée ses obligations
- l'autorité d'enregistrement locale qui a validé la demande de certificat n'a pas respecté ses obligations
- le dispositif de signature est défectueux
- l'abonné a perdu son dispositif de signature
- L'AdminPKI cesse ses activités de certification.

4.9.2 Qui peut demander l'annulation

L'autorité de certification de deuxième niveau accepte les demandes d'annulation de certificat de :

- de l'abonné
- de l'autorité d'enregistrement locale qui a émis/validé la demande de certificat
- de l'entité administrative qui emploie l'abonné
- du responsable de la sécurité de l'AdminPKI.

Un certificat peut également être annulé suite à une décision judiciaire. Cette demande d'annulation doit être faite par écrit au responsable de l'AdminPKI (cf. 1.5) et être motivée.

L'autorité d'enregistrement locale et le responsable de l'AdminPKI doivent s'assurer que le demandeur a qualité pour demander l'annulation.

4.9.3 Procédures de demande d'annulation

4.9.3.1 Annulation causée par la compromission de clés de signature

La procédure ci-après doit être suivie lorsque la clé privée d'un abonné est compromise :

1. L'abonné doit initialiser le processus d'annulation. Il peut adresser sa demande d'annulation :
   - à l'autorité d'enregistrement locale (pendant les heures de bureaux),
   - au CallCenter de l'office fédéral de l'informatique et de la communication (hors des heures de bureau). Si le CallCenter n'est pas atteignable, il peut faire sa demande à l'aide d'une application Web disponible sur le site d'information de l'AdminPKI : www.pki.admin.ch.
   - par messagerie électronique sécurisé
2. L'autorité d'enregistrement locale, respectivement le CallCenter doit authentifier la demande d'annulation en demandant à l'abonné de se présenter personnellement ou en fournissant le mot de passe d'annulation.

   Si la demande a été envoyée dans une communication électronique comportant une signature numérique, l'autorité d'enregistrement locale l'authentifie en vérifiant la signature numérique.
3. La demande d'annulation est déposée dans le dossier de l'abonné.
4. La demande d'annulation est transmise à l'autorité de certification de deuxième niveau

pour exécution.

5. L'autorité de certification de deuxième niveau traite les demandes d'annulation qui sont authentifiables automatiquement.
6. L'autorité de certification de deuxième niveau informe l'autorité d'enregistrement, respectivement l'abonné de l'exécution de l'annulation.

L'autorité d'enregistrement locale doit effectuer une enquête afin de connaître les circonstances qui ont conduit à la compromission des clés de l'abonné et décider si l'abonné peut faire une nouvelle demande de certificat.

4.9.3.2 Annulation causée par la perte du dispositif de signature ou en cas de dommage

En cas de perte du dispositif de signature, la procédure est identique à la procédure de demande d'annulation pour cause de compromission des clés signature (cf. 4.9.3.1). La même procédure s'applique si le dispositif de signature est endommagé.

L'autorité d'enregistrement locale doit effectuer une enquête afin de connaître les circonstances liées à la perte du dispositif de signature et décider si l'abonné peut faire une nouvelle demande de certificat.

4.9.3.3 Annulation pour cause de non-conformité

Si l'abonné ne respecte pas ses obligations, l'autorité d'enregistrement locale doit annuler les certificats. La procédure d'annulation pour cause de non-conformité est identique à la procédure d'annulation pour cause de compromission des clés de signature (cf. 4.9.3.1).

L'autorité d'enregistrement locale accepte des demandes d'annulation provenant de l'entité administrative qui emploie l'abonné ou du responsable sécurité de l'AdminPKI.

L'autorité d'enregistrement locale doit effectuer une enquête afin de déterminer pourquoi un abonné ne respecte pas ses obligations et décider si l'abonné peut faire une nouvelle demande de certificat.

4.9.4 Délai pour faire une demande d'annulation

En cas de compromission de ses clés de signature ou en cas de perte du dispositif de signature, l'abonné doit demander l'annulation de son certificat sans attente.

4.9.5 Délai pour exécuter une demande d'annulation

L'autorité de certification de deuxième niveau traite les demandes d'annulation authentifiées automatiquement et dès réception.

Après chaque révocation, l'autorité de certification de deuxième niveau génère une liste des certificats annulés et la publie sans retard dans l'Admin-Directory.

4.9.6 Exigences de contrôle des listes de certificats annulés

Dès la réception d'un message signé, il appartient à la partie utilisatrice de vérifier la validité du certificat du signataire et la validité de l'émetteur de la CRL.

4.9.7 Fréquence de publication des CRL et des ARL

L'Admin-Root-CA met à jour son ARL une fois par année et après avoir annulé le certificat d'une autorité de certification de deuxième niveau et une fois par année si aucun certificat

d'autorité de certification n'est annulé durant cette période.

L'autorité de certification de deuxième niveau met à jour sa CRL :

- après chaque annulation de certificat
- tous les 3 (trois) jours si aucun certificat n'est annulé durant cette période.

4.9.8 Délai pour publier la CRL

L'autorité de certification de deuxième niveau publie une nouvelle CRL au plus tard 24h après réception d'une demande d'annulation.

4.9.9 Contrôle en ligne de la liste des certificats annulés

L'autorité de certification de deuxième niveau n'offre pas de service de vérification en ligne de type OCSP (cf. [3], chapitre 4.4.9).

4.9.10 Exigences liées à la vérification en ligne

Sans objet.

4.9.11 Autres formes de publication de liste de certificats annulés

L'autorité de certification de deuxième niveau n'offre pas d'alternative aux CRL et ARL.

4.9.12 Remplacement du certificat en cas de compromission des clés

Voir chapitres 4.7 et 4.9.3.1.

4.9.13 Suspension de certificat

L'annulation (révocation) d'un certificat est définitive. La suspension de certificats n'est pas autorisée (cf. [2], chapitre 3.4.1, h).

4.9.14 Qui peut demander l'annulation

Sans objet, cf. 4.9.13.

4.9.15 Procédure de demande de suspension

Sans objet, cf. 4.9.13.

4.9.16 Durée de la suspension

Sans objet, cf. 4.9.13.

4.10 Service de vérification de l'état du certificat

4.10.1 Caractéristiques opérationnelles

Le service de vérification de l'état des certificats est basé sur la liste des certificats annulés CRL. La CRL contient les certificats annulés dont la date d'échéance n'est pas dépassée. La CRL est publiée par :

- le service d'annuaire *Admin-Directory*
- le service d'information à l'adresse www.pki.admin.ch

4.10.2 Disponibilité du service

La disponibilité du service de vérification de l'état des certificats est de 99% durant les heures de bureau. Hors des heures de bureau, le service est disponible sans garantie. Dans 80% des cas, une défaillance du service de certification ne doit pas excéder 24h.

4.10.3 Options

Pas d'options.

4.11 Fin des rapports contractuels

La fin des rapports contractuels est réglée dans le contrat cadre et la convention qui lie l'AdminPKI à ses clients.

4.12 Entiercement / recouvrement des clés de signature

Les dispositions d'application de la loi sur la signature électronique (cf. [1]) interdisent à l'AdminPKI de faire une copie des clés de signature des abonnés et d'offrir un service de recouvrement des clés de signatures.

4.12.1 Politique d'entiercement / recouvrement des clés de signature

Sans objet, cf. 4.12.

4.12.2 Clés de sessions et pratiques de recouvrement

Sans objet, cf. 4.12.

5 Sécurité physique, sécurité des procédures et du personnel

5.1 Contrôles de la sécurité physique

5.1.1 Emplacement

L'infrastructure de certification l'AdminPKI est exploitée dans les locaux de l'office fédéral de l'informatique et de la télécommunication OFIT. Le périmètre réservé à l'infrastructure de certification l'AdminPKI est sécurisé.

5.1.2 Accès physique

L'accès physique à l'infrastructure de certification est réglé dans la directive de contrôle d'accès.

Seules les personnes en possession d'un badge délivré par le responsable de la sécurité peuvent accéder au local contenant les équipements informatiques de l'AdminPKI. L'accès est interdit à toute personne non accompagnée par un collaborateur de l'AdminPKI.

Des détecteurs de mouvement sont raccordés au centre de surveillance de l'immeuble.

5.1.3 Système électrique et système de conditionnement de l'air

Le local de l'infrastructure de certification est muni d'un système de conditionnement de l'air pour la régulation de la température et de l'humidité.

Tous les composants électriques sont branchés à un bloc d'alimentation sans coupure, qui conditionne également l'alimentation électrique.

5.1.4 Dégâts d'eau

Le local de l'infrastructure de certification est équipé de détecteurs d'eau qui sont branchés à la station de surveillance de l'immeuble.

En cas d'alarme, les équipements informatiques de l'infrastructure de certification sont stoppés automatiquement et l'alimentation électrique est débranchée, à l'exception du cas où une alarme est déclenchée par le détecteur placé directement sous l'installation de climatisation, ceci afin d'évier une trop grand sensibilité due à quelques gouttes d'humidité

5.1.5 Prévention et protection contre les incendies

Le local de l'infrastructure de certification est muni de détecteurs de fumée et de chaleur qui sont branchés à la station de surveillance de l'immeuble.

5.1.6 Supports d'information

Tous les supports contenant de l'information de l'infrastructure de certification, sont déposés dans un coffre-fort résistant au feu situé dans le local réservé à l'infrastructure de certifica-

tion.

5.1.7 Mise au rebut

Les entités de l'AdminPKI utilisent des mécanismes de destruction des supports en fonction de la classification des informations, papiers (tels que des broyeurs) et des supports magnétiques (broyeurs).

5.1.8 Entreposage hors site (site de secours)

L'AdminPKI dispose d'un site de secours, si besoin est, pour assurer la continuité des opérations.

L'AdminPKI utilise deux installations de stockage de données protégées, hors site.

5.2 Contrôle des procédures

5.2.1 Rôles de confiance

Afin de veiller à la séparation des tâches critiques, on distingue 7 (sept) rôles de confiance au sein de l'AdminPKI. Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où cela ne dégrade pas la sécurité des services offerts.

Les rôles de confiance sont :

1. Le mandant

   Le mandant représente l'AdminPKI auprès de la direction de l'Office Fédéral de l'Informatique et des Télécommunications (OFIT). Il supporte la responsabilité générale de l'AdminPKI. Ses tâches principales dans le cadre de l'AdminPKI sont d'approuver les politiques de sécurité et de certification et de garantir l'exploitation de l'infrastructure.

2. Le responsable PKI

   Le responsable PKI est responsable pour la mise en œuvre des obligations de l'AdminPKI. Cela comprend en particulier, la collaboration à la planification stratégique, la relation avec la clientèle et les fournisseurs, la conduite des collaborateurs de l'équipe AdminPKI.

3. Le responsable du développement

   Le responsable du développement de l'AdminPKI est responsable pour le soutien technique et l'amélioration des services de l'AdminPKI. Il réalise les objectifs stratégiques définis par le mandant et le responsable PKI.

   Il est responsable pour l'architecture, le design et l'implémentation des techniques PKI. Il effectue une veille technologique sur le marché, organise les mise à jour des nouvelles versions et coordonne les installations de ces dernières. Il est également responsable de la maintenance de la base de données CMDB ainsi que du standard A006.

4. L'officier de sécurité

   L'officier de sécurité est responsable du respect des bases légales, de l'application de la politique de sécurité physique et fonctionnelle de AdminPKI et de son environnement. Il gère les contrôles d'accès physique à la plate-forme, il est habilité à prendre connaissance des archives et analyse les journaux d'évènements.

5. Le responsable de l'exploitation

Le responsable de l'exploitation est responsable de l'ensemble des services délivrés par l'AdminPKI. En particulier, il a pour tâches de conclure les contrats de supports avec les fournisseurs, d'assurer la disponibilité de l'infrastructure de certification et de coordonner les travaux de l'équipe d'exploitation de l'AdminPKI

6. L'équipe d'exploitation

   Elle est chargée de la mise en route, de la configuration et de la maintenance de la plate-forme informatique de la composante. Elle assure l'administration du système et du réseau de la plate-forme sur laquelle repose totalement ou partiellement l'enregistrement, la génération et la révocation des certificats et les autres services fournis par l'AdminPKI.

   Elle surveille le bon fonctionnement de l'AdminPKI et redémarre si nécessaire les services de certification.

7. Le responsable du service d'annuaire

   Le responsable du service d'annuaire est responsable pour l'exploitation et la disponibilité du service d'annuaire conformément aux accords SLAs.

8. Le responsable du service d'information

   Il est responsable pour la publication des informations pertinentes en faveur des clients. Il est en outre responsable du site Internet http://www.pki.admin.ch et répond aux questions que les clients adressent à pki-info@bit.admin.ch

9. Le contrôleur

   Le contrôleur**,** désigné par le responsable sécurité de l'AdminPKI, est chargé de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des politiques de certification, des pratiques de certification et des services effectivement fournis par l'AdminPKI.

10. Le collaborateur de l'autorité d'enregistrement locale (Officier LRA)

    L'officier LRA est chargé d'identifier les demandeurs de certificats et de personnaliser le dispositif de création de signature (carte à puce).

5.2.2 Nombre de personnes requises par tâche

A l'exception des tâches exécutées par les opérateurs (cf. § 5.2.1), toutes les tâches font appel au minimum à deux personnes opérant de concert.

Le cas de l'autorité d'enregistrement locale est particulier, puisque l'officier LRA exécute ses tâches seulement en présence du demandeur de certificat.

Les procédures suivantes font appel à trois personnes opérant de concert :

- mises à jour des clés de signatures de l'infrastructure de certification
- remplacement des modules de sauvegarde des clés de signature de l'infrastructure de certification
- mise en service des copies de secours des clés de signature

Les processus de génération de certificats avec l'extension « Custom DN » ou avec l'admission ISIS-MTT exigent deux officiers LRA avec des rôles distincts :

Cas « Custom DN » :

- un premier officier LRA qui a le droit de gérer les « Custom DN » et qui définit quel officier LRA peut générer des certificats pour un abonné précis
- un second officier LRA qui a reçu les droits de gérer un abonné « Custom DN »

Cas ISIS-MTT :

- un premier officier LRA qui a le droit de gérer le registre des professions
- un second officier LRA qui a reçu les droits de gérer un abonné éligible pour ISIS-MTT Admission

5.2.3 Identification et authentification de chaque rôle

L'AdminPKI a mis en place une gestion des droits d'accès pour identifier et authentifier son personnel réalisant une action en fonction de son rôle. Cette gestion des droits est réalisée par des mécanismes de sécurité permettant de séparer les différentes fonctions de confiance identifiées aux chapitres 5.2.1 et 5.2.2 suivant les objectifs de sécurité définis au chapitre 6.5.

5.2.4 Séparation des rôles

Le responsable du service attribue les rôles aux collaborateurs de l'AdminPKI. Il veille à éviter tout conflit d'intérêt.

5.3 Contrôle de sécurité du personnel

5.3.1 Compétences, qualification et antécédents requis

Les collaborateurs de l'AdminPKI sont des collaborateurs de l'Administration fédérale nommés pour une période indéterminée. Ils possèdent la formation générale, le savoir-faire, l'expérience et les qualifications requises pour la fourniture de service de certification. Normalement, ils sont affectés à temps plein aux tâches liées à leurs responsabilités dans le cadre de l'infrastructure de certification. Chaque collaborateur est personnellement informé par le responsable du service de l'étendue et des limites de sa sphère de responsabilité.

Le contrat de travail de chaque collaborateur contient une clause de confidentialité.

Les collaborateurs des autorités d'enregistrement locales sont des collaborateurs d'une unité administrative (Administration fédérale, cantonale ou communale); ils sont assujettis à un processus de certification avant d'être nommés.

5.3.2 Procédures préalables de contrôle

Avant d'être nommé, les collaborateurs de l'AdminPKI et des autorités d'enregistrement locales doivent être soumis à un contrôle de sécurité relatif aux personnes selon l'article 10, alinéa 1, lettre a. de l'ordonnance sur les contrôles de sécurité relatifs aux personnes [13].

5.3.3 Exigences de formation initiale

Les collaborateurs de l'AdminPKI sont formés aux logiciels, matériels et procédures internes de fonctionnement de la composante pour laquelle ils opèrent. Les collaborateurs doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

5.3.4 Exigences et fréquences des formations

Tout nouveau collaborateur suit une formation initiale au système, aux politiques de sécurité, au plan de secours, aux logiciels et opérations qu'il met en œuvre.

Chaque collaborateur doit assister à une formation après toute évolution importante du système, de l'organisation, des outils et des procédures.

5.3.5 Rotation des postes

Sans objet à l'heure actuelle.

5.3.6 Sanctions pour actions non autorisées

Les sanctions à appliquer lorsqu'un collaborateur de L'AdminPKI abuse de ses droits ou effectue une opération non conforme à ses attributions sont réglées dans la loi fédérale sur la responsabilité de la Confédération, des membres de ses autorités et de ses fonctionnaires (RS 170.323).

5.3.7 Personnel lié par contrat à durée limitée

Les exigences en matière de sécurité du personnel engagé de manière temporaire et du personnel des fournisseurs sont identiques à ceux qui s'appliquent aux collaborateurs de l'administration fédérale (cf. § 5.3.1, § 5.3.2, § 5.3.3 et § 5.3.4)

5.3.8 Documentation fournie au personnel

Le personnel a accès à l'ensemble de la documentation de L'AdminPKI, en particulier aux documents suivants :

- Enoncé des pratiques de certification / politique de certification de l'autorité de certification AdminPKI (ce document)
- politique de sécurité
- manuel d'exploitation et d'organisation
- manuels concernant le matériel et les logiciels systèmes et d'applications

5.4 Procédure de vérification de la sécurité des systèmes

5.4.1 Types d'évènements enregistrés

Les évènements qui sont liés à l'émission et à la gestion des certificats sont enregistrés automatiquement et/ou manuellement à des fins de vérification.

Les données suivantes sont enregistrées :

Système :

- opérations menées sur les postes informatiques et matériels du réseau de l'AdminPKI
- tentatives non autorisées d'accès aux réseaux et aux équipements informatiques de l'infrastructure de certification

Certification :

- enregistrement : enregistrement d'un nouvel abonné, demande de renouvellement
- génération de certificat : de l'autorité de certification, de l'abonné
- annulation de certificat : demande de révocation, rapport de révocation
- opérations menées sur les postes informatiques et relatives aux opérations rendues par L'AdminPKI : démarrage et arrêt de l'application, changement de mot de passe, modification de paramètres de configuration de l'outil de certification
- accès physique au centre de gestion des clés et à d'autres établissements connexes
- destruction des clés, des données sur l'activation et des autres renseignements désignés
- changements de personnel.

Les informations suivantes sont enregistrées par évènement : date et heure de l'opération, destinataire de l'opération, nom de l'exécutant, nom des personnes présentes, nom du demandeur de l'opération, résultat de l'évènement, type de l'opération, cause de l'évènement.

5.4.2 Fréquence du traitement des journaux d'évènements

Les journaux d'évènements sont analysés en ligne par un logiciel chargé de la surveillance de l'infrastructure de certification. Au minimum une fois par semaine, le responsable sécurité analyse de manière ciblée les journaux d'évènements.

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements « système » et les journaux d'évènements « applicatifs » sont conservés au minimum durant 11 ans.

5.4.4 Protection des journaux d'évènements

Les journaux d'évènements sont sauvegardés sur un serveur dédié. Seuls les collaborateurs de l'AdminPKI autorisés et authentifiés ont accès aux journaux d'évènements.

Les informations stockées hors site sont chiffrées.

5.4.5 Procédures de sauvegarde des journaux d'évènements

Les journaux d'évènements sont sauvegardés tous les jours dans le cadre de la sauvegarde courante du système hôte de l'AdminPKI.

5.4.6 Système de collecte des journaux

Un serveur interne à l'infrastructure de certification collecte l'ensemble des journaux d'évènement.

5.4.7 Notification suivant un évènement critique

Le logiciel chargé d'analyse des journaux d'évènements informe le responsable de sécurité et les opérateurs responsables de l'exploitation en cas d'évènement critique.

5.4.8 Évaluation de la vulnérabilité

Au minimum une fois par semaine, un logiciel analyse les composants de l'AdminPKI dans le but de détecter les éventuelles vulnérabilités et de prévenir les attaques potentielles sur l'infrastructure de certification.

En cas d'anomalie critique, le responsable sécurité est immédiatement avisé.

5.5 Archivage des certificats et autres documents

5.5.1 Types de données à archiver

L'AdminPKI archive l'ensemble des données et journaux d'évènements qui sont liés à l'émission et à la gestion des certificats. Il s'agit en particulier des :

- accords contractuels ou conventions avec les clients de l'AdminPKI et les exploitants des autorités d'enregistrement locales
- certificats d'abonnés et de composants de l'AdminPKI
- de l'ensemble des listes de certificats annulés (CRL) qui ont été émises
- des demandes de révocation et rapports d'enquêtes, si existant
- données d'identifications personnelles de l'abonné, ensemble des éléments utiles à l'enregistrement, nature des documents présentés par le demandeur de certificats
- journaux d'évènements
- rapports d'audit
- rapports d'incidents
- rapports d'analyse de vulnérabilités

5.5.2 Périodes de rétention des archives

Les archives de l'AdminPKI sont conservées au minimum pour une durée de 11 (onze) ans.

5.5.3 Protection des archives

Les journaux applicatifs sont signés par l'application de certification, puis ils sont chiffrés avant d'être sauvegardés et chiffrés.

Seul le responsable sécurité a accès aux données archivées.

5.5.4 Procédure de copie des archives

L'AdminPKI utilise deux installations de stockage/archivage de données protégées, hors site.

5.5.5 Besoin d'horodatage des archives

Chaque évènement enregistré et archivé est daté. L'heure est assurée par une horloge de référence hébergée par un système informatique local. Tous les composants de l'infrastructure centrale de l'AdminPKI sont synchronisés sur cette horloge.

5.5.6 Système d'archivage

Le système d'archivage est interne à l'AdminPKI.

5.5.7 Procédures de récupération des archives

La récupération, respectivement l'analyse des fichiers d'archives doivent être approuvées par le responsable sécurité.

5.6 Changement de clé d'une composante de l'AdminPKI

La validité des clés utilisées par les composantes de l'AdminPKI et les collaborateurs de l'AdminPKI est surveillée par l'ingénieur système. La génération de nouvelles clés et l'émission des certificats doivent être autorisés par le responsable sécurité.

Selon la nature du changement (fin de période de validité, renouvellement des clés suite à une révocation, etc.), les mesures prises doivent respecter les procédures de traitement énoncés dans les chapitres 4.2, 3.2 et 3.3.

Lorsqu'une composante renouvelle ses clés, elle en informe, si nécessaire, ses utilisateurs.

5.7 Compromission et plan anti-sinistre

5.7.1 Gestion des incidents

La procédure de gestion des incidents est édictée par le responsable de la sécurité et communiquée à l'ensemble des collaborateurs de l'infrastructure de certification.

5.7.2 Corruption des ressources informatiques, de logiciels ou de données

L'AdminPKI met en œuvre les mesures nécessaires permettant d'éviter toute compromission ou vol des informations ou matériel qu'il détient. En cas de vol, compromission, respectivement suspicion de compromission, le plan de reprise/continuité des activités est déclenché par le responsable sécurité.

Le responsable de la sécurité de l'infrastructure de certification travaille en étroite collaboration avec le délégué à la sécurité informatique de l'office fédérale de l'informatique et de la télécommunication.

En cas de nécessité, l'AdminPKI dispose d'un site de secours opérationnel dans les cinq jours qui suivent la destruction de son site à Berne.

5.7.3 Compromission des clés de signatures de l'AdminPKI

En cas de compromission, respectivement suspicion de compromission des clés des autorités de certification de premier et de deuxième niveau, le responsable PKI est immédiatement informé. Après analyse de la situation, le responsable PKI déclenche, si nécessaire, la procédure de révocation de l'ensemble des certificats d'abonné concernés. Ceci implique de :

- informer les abonnés
- informer le Service Suisse d'accréditation et l'organisme de reconnaissance

- révoquer le certificat de l'autorité de certification et les certificats d'abonnés
- générer de nouvelles clés de signature pour l'autorité de certification
- informer les autorités d'enregistrement locales
- émettre les certificats d'abonnés.

5.7.4 Plan de continuité

Le plan de continuité de l'AdminPKI est mis en œuvre suite à un sinistre. Il a pour but de garantir une disponibilité avec les mêmes contraintes d'origines pour les services de base par ordre de priorité : (1) révocation des certificats (génération et diffusion de l'information de révocation) et (2) émission de nouveaux certificats.

Il traite les points suivants :

- corruption des ressources informatiques, de logiciels ou de données
- révocation du certificat d'une composante de l'AdminPKI
- compromission de la clé d'une entité de l'AdminPKI
- poursuite/reprise des activités suite à un sinistre.

Il prend en compte les paramètres suivants :

- délai minimum de recouvrement des services
- mise en service d'un site miroir
- politique de sécurité
- tests pratiques, formation et entraînement du personnel.

Le plan de continuité est strictement confidentiel.

5.8 Cessation d'activité

5.8.1 Cessation d'activité de l'AdminPKI

Conformément à l'art. 10 de l'ordonnance 943.032 sur les services de certification dans le domaine de la signature électronique l'AdminPKI informe l'autorité de surveillance (SAS), l'organisme de certification (CB) et ses clients au minimum 30 (trente) jours avant la fin de ses activités de certification[8].

Les certificats valides sont annulés et une liste de certificats annulés [CRL] est générée et publiée sur le site d'information de l'AdminPKI pour une durée minimale de 11 ans.

Les clés de signatures de l'AdminPKI et les copies de sauvegardes sont détruites.

Les informations relatives à la certification sont archivées à l'office fédéral de l'informatique et de la télécommunication pour une durée minimale de 11 ans à partir du dernier jour des opérations.

[8] *AdminPKI ne prévoit pas de transférer son service de certification à un autre fournisseur de service de certification*

5.8.2 Cessation d'activité d'une autorité d'enregistrement locale

L'AdminPKI informe l'organisme de reconnaissance (CB) de la cessation des activités d'une autorité d'enregistrement locale, respectivement le transfert des activités à une autre autorité d'enregistrement locale.

Les informations relatives à la certification sont soit transférées à une autre autorité d'enregistrement locale soit archivées à l'office fédérale de l'informatique et de la télécommunication pour une durée minimale de 11ans.

6 Contrôles techniques de sécurité

6.1 Génération et installation des paires de clés

6.1.1 Génération des paires de clés

La génération, l'utilisation et le stockage des clés des autorités de premier et deuxième niveau, utilisées pour signer les certificats et les listes des certificats annulés, sont effectués au sein d'un module cryptographique sécurisé (Hardware Security Modul) qui est conforme à la norme FIPS 140-1 Level 4.

La génération, l'utilisation et le stockage des clés de signature des abonnés sont effectués au sein d'un module cryptographique sécurisé (Hardware Security Modul) qui est conforme à la norme EAL4+.

6.1.2 Délivrance de la clé privée à un abonné

Les clés de signatures sont générées dans le dispositif sécurisé de signature de l'abonné (cf. § 6.1). Seul l'abonné a le contrôle de ce dispositif.

6.1.3 Délivrance de la clé publique de l'abonné à l'autorité de certification

La clé publique de l'abonné est inclue dans la demande de certification et est transférée à l'autorité de certification à l'aide d'un protocole sécurisé.

6.1.4 Publication de la clé publique des autorités de certification

L'AdminPKI remet à ses clients un compact disc contenant les certificats des autorités de certification (cf. § 1.3.1). Le CallCenter de l'office fédéral de l'informatique et de la télécommunication OFIT fournit sur demande l'empreinte du certificat de l'autorité de certification primaire.

Les certificats des autorités de certification de l'AdminPKI sont publiés :

- par le service de publication et d'archivage Admin-Directory (cf. § 2.1)
- par le site d'information de l'AdminPKI (cf. § 2.2)

6.1.5 Exigences cryptographiques

Les algorithmes de signature et de hachage sont spécifiés par le responsable sécurité.

L'algorithme de hachage est SHA1.

La taille des clés de signature RSA utilisées par les autorités de certification de premier et de deuxième niveau est de 2048 bits, de même que pour les clés de signature des abonnés.

Le responsable sécurité de l'AdminPKI vérifie une fois par année si la taille des clés reste adaptée ou doit être augmentée.

6.1.6 Génération des paramètres de clé publique et contrôle de qualité

Les clés de signatures des abonnés sont générées dans un dispositif sécurisé de signature qui est conforme à la norme EAL4+, alors que les clés de signature des autorités de certification de premier et de deuxième niveau sont générés dans un module Hardware qui est conforme à la norme FIPS 140-1 Level 4.

6.1.7 Usage de la clé

L'AdminPKI s'engage et s'assure que ses clés de signatures ne peuvent être utilisées qu'à des fins de signature de certificat d'abonné et de CRL (liste des certificats annulés).

Les clés de signature de l'abonné ne peuvent être utilisées qu'à des fins de signature et en relation avec des applications autorisées par l'AdminPKI (cf. § 1.4.1)

L'extension « Key usage » d'un certificat d'abonné a la valeur de « non répudiation ».

6.2 Protection de la clé privée et contrôles techniques du module cryptographique

6.2.1 Normes relatives au module cryptographique

Les autorités de certification de premier et de deuxième niveau et les abonnés utilisent des modules de génération de clés et de signature qui sont conformes à la norme FIPS (cf. § 6.1) et à la norme EAL4+.

6.2.2 Contrôle des clés de signature de l'AdminPKI

Les activités liées d'une part, à la mise en / hors service, au remplacement des modules cryptographiques et d'autre part, aux processus de génération, de sauvegarde et de recouvrement des clés de signature de l'AdminPKI nécessitent la présence de 3 (trois) collaborateurs de l'AdminPKI (cf. § 5.2 et 5.3)

6.2.3 Séquestre de clé privée (key escrow)

Les clés privées ne sont pas séquestrées.

6.2.4 Copie de secours de clé privée

Les copies de secours des clés de signature des autorités de certification de premier et deuxième niveau sont protégées avec un niveau de sécurité aussi important que les clés en usage.

Au cas où les clés de signature ne sont plus utilisées, les clés de signatures doivent être révoquées et les copies de secours correspondantes doivent être détruites.

En aucun cas, les clés de signature de l'abonné ne font l'objet d'une copie de secours.

6.2.5 Archivage de clé privée

Les clés de signature (clé privée) ne sont pas archivées.

6.2.6 Utilisation de clé privée

Les clés de signature en usage ne quittent pas le dispositif de création de signature.

6.2.7 Protection de la clé de création de signature

Les clés de signature sont stockées dans le module de création de signature (cf. § 6.1). Elles sont chiffrées et protégées par un code d'accès.

6.2.8 Méthodes d'activation des clés privées

Les clés de signature de l'autorité de deuxième niveau sont activées lors du lancement de l'application PKI. Le lancement de l'application est exécuté par le responsable sécurité.

Le code d'activation PIN permet d'activer la clé de signature de l'abonné.

6.2.9 Méthode de désactivation des clés privées

Les clés de création de signature de l'autorité de deuxième niveau sont désactivées lors de la fermeture de l'application PKI.

6.2.10 Méthode de destruction des clés privées

La méthode de destruction des données de création de signature est propre à la ressource cryptographique et est matérielle. Cette méthode garantit que les données de création de signature une fois détruite ne puissent plus être retrouvées. Le processus de destruction des données de création de signature doit être approuvé par le responsable sécurité.

6.2.11 Propriétés des modules cryptographiques

Voir chapitre § 6.2.1.

6.3 Autres aspects de la gestion des paires de clés

6.3.1 Archivage des clés publiques

Les données de vérification de signature (clé publique) sont archivées au minimum pour une durée de 11 (onze) ans.

6.3.2 Périodes d'utilisation des clés publiques et privées

La période de validité des certificats émis par l'AdminPKI est de :

- 20 (vingt) ans pour l'autorité de certification primaire (root):
- 10 (dix) ans pour les autorités de certification de deuxième niveau
- 1 (une) année ou 3 (trois) ans pour les certificats d'abonné.

La période d'utilisation des clés de création de signature est de :

- 7 (sept) ans pour les autorités de certification de deuxième niveau
- 3 (trois) ans pour les abonnés.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

L'abonné détermine ses données d'activation (PIN et PUK) et les active au début du processus de génération de ses données de création et de vérification de sa signature.

6.4.2 Protection des données d'activation

L'abonné doit protéger ses données de création de signature en confidentialité et en intégrité.

Les autorités d'enregistrement locales doivent informer les abonnés des conséquences de la divulgation de leurs données d'activation. Ils doivent également leur indiquer comment choisir un mot de passe.

6.4.3 Autres aspects des données d'activation

Les données d'activation doivent comporter au minimum 8 caractères.

6.5 Contrôles de sécurité informatique

6.5.1 Besoins de sécurité spécifique sur les postes de travail

L'AdminPKI met en oeuvre un certain nombre de contrôles liés aux logiciels de l'application PKI, tels que :

- contrôle d'accès aux services des logiciels de l'application PKI
- séparation obligatoire des tâches pour les fonctions de la PKI
- identification et authentifications des collaborateurs de l'AdminPKI
- journalisation des évènements, vérification périodiques des journaux
- filtrage des entrées/sorties réseaux

6.5.2 Niveau de sécurité du poste de travail

L'analyse des risques liés aux services de certification menée par l'AdminPKI a permis de définir le niveau de sécurité des systèmes et matériels (postes de travail) pour les différentes entités de l'AdminPKI.

6.6 Contrôles techniques relatif au cycle de vie

6.6.1 Contrôle du développement des systèmes

Une analyse des risques est menée avant tout développement d'une composante de l'AdminPKI.

L'utilisation de produits de confiance qui sont sécurisés et protégés contre toute modification non autorisée est une priorité.

6.6.2 Contrôles de gestion de la sécurité

Toute évolution de l'infrastructure de certification AdminPKI doit être documentée, doit apparaître dans les procédures de fonctionnement, doit être conforme au schéma de maintenance de l'assurance dans les produits évalués et doit être approuvée par le responsable sécurité.

L'AdminPKI s'assure que :

- des procédures de contrôle portant sur les modifications existent
- la sécurité du dispositif matériel n'est pas altérée par un tiers ou de toute autre manière lors de son transport
- la sécurité du dispositif matériel n'est pas altérée par un tiers ou de toute autre manière pendant la durée de son utilisation ou de sa conservation éventuelle
- le dispositif matériel fonctionne correctement
- la capacité de traitement et de stockage répond aux besoins des abonnés
- la montée en charge et du maintien du système à niveau.

6.6.3 Contrôles de sécurité des composants

Le responsable sécurité vérifie régulièrement l'intégrité des composants de l'infrastructure de certification AdminPKI.

6.7 Contrôle de sécurité réseau

Le réseau AdminPKI est un segment exclusif qui est rattaché par une passerelle au réseau BV-Netz de l'Administration fédérale. La passerelle est configurée pour n'accepter que les protocoles nécessaires au fonctionnement de l'AdminPKI.

6.8 Service d'horodatage

L'AdminPKI offre un service d'horodatage. Les règles liées à l'exploitation de l'AdminPKI s'applique à l'autorité d'horodatage. De plus amples informations sont disponibles en [14].

7 Certificats et liste des certificats annulés

Les certificats et les listes des certificats annulés [CRL] émis par l'AdminPKI sont conformes aux exigences des prescriptions techniques et administratives concernant les services de certification dans le domaine de la signature électronique (cf. [2], § 3.4).

L'AdminPKI n'offre pas de service en ligne de type OCSP.

7.1 Format du certificat d'abonné

La structure ASN1 du certificat d'abonné est décrite à l'annexe B2.

La structure du certificat se compose d'un certificat de base et de champs additionnels (extensions).

Le certificat de base contient les champs suivants dans la séquence tsbCertificate conformément à l'art. 7 de la SCSE [1] et à la norme RFC 3280, chapitre 4.1 :

- Version du certificat contient le numéro 2 qui désigne un certificat de version 3.
- Numéro de série du certificat : contient un nombre entier servant à désigner le numéro de série du certificat. L'AdminCA-A-T01 est responsable du contenu de ce champ.
- Identifiant de l'algorithme de signature utilisé pour signer le certificat : contient l'identificateur d'objet 1 2 840 113549 1 1 5 qui désigne l'algorithme shaWithRSAEncryption
- Nom du fournisseur de service de certification CSP : contient le nom distinctif de l'AdminCA-A-T01 :

  CN = AdminCA-A-T01, OU = Certification Authorities, OU= Services, O = admin, C = ch
- Durée de validité du certificat d'abonné : contient la période pendant laquelle le certificat d'abonné est présumé valide. Le champ notBefore indique la date d'entrée en vigueur du certificat, le champ notafter indique la date d'expiration. La période de validité des certificats d'abonné ne doit pas dépasser 3 (trois) ans.
- Nom du titulaire du certificat (abonné) : contient le nom distinctif de l'abonné, par exemple :

  C = ch, O = admin, OU = Weisse Seiten, CN = User Test NQW5PM
- Clé et algorithme de vérification de la signature du titulaire de certificat : contient l'identificateur d'objet 1 2 8 840 113549 1 1 1 qui désigne l'algorithme rsaEncryption et la clé publique de l'abonné.

Le certificat d'abonné contient les extensions suivantes de la séquence *tbsCertificate* conformément au document RFC 3280 [8], chapitre 4.2. :

- Identificateur de clé d'autorité (*authorityKeyIdentifier*)
  - identifie la clé publique devant être utilisée pour vérifier la signature d'un certificat
  - extension non critique
- Utilisation de clé (*key usage*)
  - identifie la clé publique devant être utilisée pour vérifier la signature d'un certificat
  - extension critique

- Politique de certification (*certificatePolicies*)
  - inclut le champ policyQualifiers, à l'intérieur duquel les qualificatifs CPS Pointer et User Notice permettent respectivement de pointer vers les pratiques de certification du CSP et la notice à destination des utilisateurs

    L'identificateur d'objet est {2.16.756.1.17.3.2.17}

    Les pratiques de certifications sont disponibles à l'adresse http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_1_4.pdf
  - extension non critique
- Points de distribution de la liste des certificats annulés (CRLDistributionPoints)
  - identifie le ou les points de répartitions de la liste de certificats suspendus et révoqués
  - extension non critique
- Point d'accès au certificat du fournisseur de services de certification (AuthorityInformation Access)
  - extension non critique
- Mention précisant que le certificat est délivré à titre de certificat qualifié (qcStatements)
  - identificateur d'objet tel que défini dans la norme ETSI 101 862 0 (cf. annexe [18])
  - extension critique
  - identificateur d'objet : {0.4.0.1862.1.1}
- Mention précisant que la clé de signature est protégée par un dispositif sécurisé de création de signature (qcStatements)
  - identificateur d'objet tel que défini dans la norme ETSI 101 862 0 (cf. annexe [18]) : {0.4.0.1862.1.4}
  - extension critique
- Valeur limite des transactions (qcStatements)
  - identificateur d'objet tel que défini dans la norme ETSI 101 862 0 (cf. annexe [18]) : {0.4.0.1862.1.2}
  - extension critique
- Extension d'autre nom d'émetteur
  - identificateur d'objet : {2.5.29.18}
  - nom alternatif : { O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA}
  - extension non critique

7.2 Profil de la liste des certificats annulés CRL

La structure ASN1 de la liste des certificats annulés est décrite à l'annexe B4.

La liste des certificats annulés [CRL] contient les champs tbsCertList, signatureAlgorithm et signatureValue conformément au document RFC 3280 [17], chapitre 5.

La séquence tbsCertList contient les champs suivants :

- version, dont la valeur est 1 pour indiquer qu'il s'agit d'une CRL version 2
- signature : identificateur de l'algorithme utilisé pour signer la CRL
- issuer : contient le nom distinctif de l'AdminCA-A-T01
- thisUpdate : heure de publication de la CRL
- nextUpdate : heure de publication de la prochaine CRL
- revokedCertificates, comprenant le numéro de série du certificat et la date d'annulation;

La CRL contient les extensions non critiques authorityKeyIdentifier et cRLNumber à l'intérieur de la séquence tbsCertList conformément au document RFC 3280 [17], chapitre 5.2.

7.3 OSCP

L'AdminPKI n'offre pas de service en ligne de type OCSP.

8 Contrôles de conformité

8.1 Fréquence et circonstances

La surveillance des fournisseurs reconnus est réglée par la loi sur la signature électronique. Elle est assurée par l'organisme de reconnaissance selon les règles de l'accréditation.

Indépendamment de la surveillance exercée par l'organisme de surveillance, les composantes de l'AdminPKI doivent démontrées au responsable sécurité, au moins tous les 12 mois, qu'elles respectent tout à fait les exigences du présent document.

Cette règle ne s'applique pas aux autorités locales d'enregistrement qui sont contrôlées, au minimum, une fois tous les 3 ans.

8.2 Identité et compétences de l'auditeur

L'organisme de reconnaissance est la société KPMG Klynveld Peat Marwick Goerdeler SA, Zurich.

Le responsable sécurité de l'AdminPKI mandate une société indépendante pour exécuter les audits internes.

8.3 Relation entre l'auditeur et l'AdminPKI

L'organisme de reconnaissance est une société indépendante qui sur la base de mandat exécute les contrôles de conformité.

Les audits internes sont exécutés par une société indépendante qui reçoit un mandat de l'AdminPKI.

8.4 Objet de l'inspection

L'objet de l'inspection est déterminé par l'organisme de reconnaissance.

Les audits internes sont de la compétence du responsable sécurité. Le responsable sécurité peut coordonner le contenu des audits internes avec l'organisme de reconnaissance.

8.5 Mesures adoptées lorsque des irrégularités ont été relevées

Le responsable PKI et le responsable sécurité décident, en accord avec l'organisme de reconnaissance, des mesures à adopter pour corriger/éliminer les irrégularités constatées lors des audits.

8.6 Communication des résultats

Les mesures à adopter pour éliminer/corriger des irrégularités constatées lors des audits sont communiquées aux unités administratives (Administration fédérale, cantonale ou communale) concernées.

La publication des rapports d'audit n'est pas prévue.

9 Conditions cadres

9.1 Emoluments

9.1.1 Emission et renouvellement du certificat de l'abonné

Les émoluments liés à l'émission, au renouvellement, à la gestion, à la publication et à l'utilisation des certificats sont fixés dans la convention qui lie l'AdminPKI et l'unité administrative (Administration fédérale, cantonale ou communale) qui emploie l'abonné (cf. § 1.3.3).

Les coûts engendrés par l'exploitation d'une autorité d'enregistrement locale LRA (procédure d'enregistrement, support utilisateur, fourniture de matériel « cryptoki », etc.) sont à la charge de l'unité administrative (Administration fédérale, cantonale ou communale) qui exploite la LRA.

Les coûts engendrés chez la partie utilisatrice sont à la charge de ladite partie utilisatrice.

9.2 Responsabilité financière

9.2.1 Protection d'assurance

L'OFIT est une partie juridiquement non indépendante de la Confédération suisse. La Confédération suisse est par conséquent détentrice des droits et des obligations, et donc personne responsable au sens de l'art. 16 SCSE et responsable de la protection d'assurance au sens de l'art. 2 OSCSE.

La déclaration de garantie du 1er juin 2006 selon art. 2, al. 2 OSCSE du Département fédéral des finances remplace l'assurance selon art. 2, al.1 OSCSE. Cette déclaration stipule que la Confédération suisse supporte elle-même les risques découlant des activités de l'OFIT en tant que fournisseur de service de certification dans le domaine de la signature électronique et que, par conséquent, renonce à la conclusion d'une assurance.

9.2.2 Protection d'assurance pour abonnés et les LRA

Les abonnés ainsi que les autorités d'enregistrement locales LRA veillent à une protection d'assurance suffisante de leur responsabilité découlant de la législation relative à la signature électronique.

9.3 Protection des données

9.3.1 Informations confidentielles

Toutes les informations relatives aux utilisateurs des services de certification de l'AdminPKI qui n'apparaissent ni dans le certificat de l'abonné ni dans la liste des certificats annulés sont considérées comme confidentielles.

9.3.2 Informations non confidentielles

Les informations qui composent les certificats et le contenu des listes de certificats annulés sont considérées comme non confidentielles.

Les informations qui découlent du contenu du certificat sont également considérées comme non confidentielles.

9.3.3 Protection des données confidentielles

L'AdminPKI prend les mesures nécessaires pour protéger les informations confidentielles qu'elle détient.

Les données confidentielles ne sont utilisées et ne font l'objet de communication extérieure que:

- lors de l'exécution des prestations de services définies dans le présent document
- pour répondre aux exigences légales
- pour l'exécution de travaux ou de prestations de services confiés à des prestataires.

9.4 Données personnelles

L'AdminPKI et les autorités d'enregistrement locales appliquent les dispositions pertinentes de la loi sur la protection des données et de la loi sur la signature électronique.

L'AdminPKI et les autorités d'enregistrement locales ne peuvent traiter que les données personnelles nécessaires à l'accomplissement de leurs tâches. Tout commerce de ces données est interdit.

9.5 Droits sur la propriété intellectuelle

L'AdminPKI est détenteur de la propriété intellectuelle des documents suivants :

- AdminPKI – Classe A Enoncé des pratiques de certification / politique de certification de l'autorité de certification AdminPKI (certificats qualifiés)
- Directives d'enregistrement de l'AdminPKI
- Contrats et autres conventions qui lient l'AdminPKI à ses clients (unité administrative fédérale, cantonale ou communale)
- Certificats émis

La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement par écrit par l'AdminPKI ou ses ayants droit, sont strictement interdites.

En aucun cas, l'unité administrative (Administration fédérale, cantonale ou communale) qui emploie l'abonné ou l'abonné n'acquiert la propriété du certificat émis par l'AdminPKI. Il n'en acquiert que le droit d'usage.

9.6 Garanties et assurances

9.6.1 Représentations et garanties des autorités de certification de l'AdminPKI

L'AdminPKI s'engage à respecter les exigences découlant de la loi sur la signature électronique (SCSE) et du présent document (cf. § 1.3.1).

9.6.2 Représentations et garanties des autorités d'enregistrement locales LRA

Les LRA sont contractuellement tenues de respecter toutes les exigences découlant de la loi sur la signature électronique ainsi que du présent document (cf. § 1.3.2).

9.6.3 Représentations et garanties de l'abonné

Les abonnés s'engagent à respecter les exigences découlant du présent document (cf. § 1.3.3).

9.6.4 Représentations et garanties de la partie utilisatrice

La « partie utilisatrice » s'engage à respecter ses engagements découlant de la loi et du présent document (cf. § 1.3.4).

9.6.5 Représentations et garanties d'autres parties

Sans objet.

9.7 Limites de la garantie

Toute autre garantie est exclue.

9.8 Responsabilité et limitation de responsabilité

9.8.1 Responsabilité et limitation de responsabilité de l'AdminPKI

L'AdminPKI est responsable au sens de l'art. 16 OSCSE envers l'abonné et les tiers ayant utilisé un certificat qualifié valable pour tous dommages qu'ils subissent en raison de la non observation par l'AdminPKI des obligations découlant de la loi sur la signature électronique et des dispositions d'exécution correspondantes.

L'AdminPKI décline toute responsabilité, si les certificats qu'elle émet sont utilisés à d'autres fins que celles mentionnées dans le présent document.

Dans tous les autres cas, la responsabilité l'AdminPKI est la suivante :

- en cas de violation de contrat, l'AdminPKI est responsable des dommages prouvés, pour autant qu'elle ne démontre pas qu'elle n'a pas commis de faute

- en cas de négligence légère, la responsabilité de l'AdminPKI est limitée à CHF. 100'000.- par sinistre et par année civile pour les dommages matériels
- en cas de négligence légère, la responsabilité de l'AdminPKI est limitée à la contre-valeur des prestations convenues pendant l'année en cours, mais au maximum CHF 50'000.- par sinistre et par année civile pour les dommages pécuniaires.

Toute responsabilité pour dommages consécutifs, manque à gagner et pertes de données est expressément exclue.

L'AdminPKI n'est pas responsable des dommages et retards consécutifs résultant de cas de force majeure, d'événements naturels (p.ex. foudre, dangers naturels), de pannes de courant, de conflits armés, de guerre, de grèves, de restrictions imprévisibles des autorités, de contournement de systèmes de verrouillage, d'applications de connexion à distance, d'attaques de pirates informatiques, d'attaques de virus (y compris chevaux de Troie et similaires) visant des installations de traitement de données, etc. Si l'AdminPKI ne peut pas remplir ses engagements en raisons de tels événements, la réalisation du contrat ou le délai pour la réalisation du contrat sont reportés en fonction de l'événement. L'AdminPKI se dégage de toute responsabilité concernant les dommages consécutifs au report de la réalisation du contrat.

9.8.2 Responsabilité des abonnés

La responsabilité des abonnés, en tant qu'employés de la Confédération ou d'un canton, est engagée conformément aux lois sur la responsabilité applicables de la Confédération et du canton pour les dommages liés à une utilisation illicite de la clé de signature.

9.8.3 Responsabilité des LRA

La responsabilité des LRA est définie dans la convention contractuelle avec l'AdminPKI, sous réserve de l'art. 16 OSCSE.

9.9 Indemnisation

L'AdminPKI ne statue pas d'indemnisation, sous réserve des dispositions des chapitres 9.6 / 9.8.

9.10 Entrée en vigueur, validité, applicabilité

9.10.1 Entrée en vigueur

Le présent document entre en vigueur le jour de sa publication sur le site d'information de l'AdminPKI (cf. § 2.2).

9.10.2 Validité

Ce document est valable :

- jusqu'à ce qu'il soit remplacé par une nouvelle version

ou

- jusqu'à ce que l'AdminPKI cesse ses activités en tant que fournisseur de services de cer-

tification

9.10.3 Applicabilité en cas de non validité

Les dispositions relatives à la loi sur la protection des données et à l'archivage restent applicables, même si ce document perd sa validité.

9.11 Information des abonnés

L'AdminPKI utilise la messagerie électronique pour communiquer avec les abonnés.

9.12 Administration du présent document

Le responsable PKI peut apporter des modifications typographiques ou remanier toute section du présent document et le publier à nouveau, sans avis.

La modification de tout élément du présent document, de nature autre que typographique ou de remaniement de texte, doit faire l'objet d'un préavis de 30 jours. Le responsable sécurité et l'organisme de reconnaissance (cf. 8.2) participe aux processus de révision et d'approbation.

Les abonnés sont, si nécessaire, informés des changements effectués.

9.13 Règlement des litiges

Le règlement des litiges est spécifié dans le contrat cadre et la convention qui lie l'AdminPKI avec les bénéficiaires de services de certification.

9.14 Lois applicables

Le droit suisse s'applique, en particulier la loi sur la signature électronique. Le for judiciaire est Berne.

9.15 Report de droits et d'obligations

L'abonné ne peut pas transmettre ses droits et obligations.

Les droits et obligations relevant de l'Office fédéral de l'informatique et de la télécommunication peuvent également être reportés à d'autres services internes de l'Administration.

9.16 Autres dispositions

9.16.1 Langue

La version française de ce document fait foi en cas de litige.

Annexes

9.17 Annexe A - Références

[1] Loi fédérale sur les services de certification dans le domaine de la signature électronique (Loi sur la signature électronique, SCSE) du 19 décembre 2003 (Etat le 1er août 2008)

[2] Prescriptions techniques et administratives concernant les services de certification dans le domaine de la signature électronique (RS 943.032.1) du (Etat 21.11.2006)

[3] RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

[4] Loi fédérale sur la protection des données (LPD) du 19 juin 1992 (Etat le 12 décembre 2006)

[5] UIT-T X.500, L'annuaire : Vue d'ensemble des concepts, modèles et services

[6] UIT-TX.509, L'annuaire : Cadre d'authentification, UIT-T

[7] RFC 2459, Infrastructure de clés publiques X.509 Internet, Certificat et profil LRC, janvier 1999

[8] RFC 2510, Infrastructure de clés publiques X.509 Internet, Protocoles de gestion des certificats, mars 1999

[9] I006 – DT20, Structure de Admin-Directory, USIC www.isb.admin.ch

[10] FIPS 140-1: Security Requirements for Cryptographic Modules, National Institute of Standards and Technology, Federal Information Processing Standards, 1994

[11] RFC 2526, Public Key Infrastructure Certificate Policy and Certificate Practices Framework, march 1999

[12] Notice informative à l'intention des usagers de l'AdminPKI Class A

[13] Ordonnance sur les contrôles de sécurité relatifs aux personnes (OCSP)

[14] Time-Stamping Authority Policy

[15] Loi fédérale du 6 octobre 1995 sur les entraves au commerce, LETC et les dispositions d'exécution pertinentes.

[16] AdminPKI Class B, énoncé des pratiques de certification de l'autorité de certification Admin-CA3

[17] RFC 3280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[18] ETSI TS 101 862, v1.3.2 (2004-06), Qualified Certificate Profile

[19] RS 784.101.113 / 2.7 Prescriptions techniques et administratives concernant la gestion des paramètres de communication

[20] UIT-T F.500 Version 08-1992 Services publics internationaux d'annuaire

[21] Directives d'enregistrement de l'AdminPKI pour la LRA

[22] Richtlinien bezüglich des Verfahrens bei Einstellung der Geschäftstätigkeit einer anerkannten CSP, Ausgabe 1. Januar 2009

9.18 Annexe B - Structure ASN1

Annexe B1 - Autorité de certification AdminCA-A-T01

X.509 Field	OIDs/Values	Comments
version	2	v3 cert
serialNumber	xxxxx	Integer value defined at key ceremony
signature {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncryption
parameters	NULL},	
issuer {	{2.5.4.3:Admin-Root-CA}, {2.5.4.11:Certification Authorities}, {2.5.4.11:Services}, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
validity {		
notBefore	"YYMMDDHHMMSSZ",	UTC TIME, ETSI TS 102 280
notAfter	"YYMMDDHHMMSSZ"},	UTC TIME, ETSI TS 102 280
subject {	{2.5.4.3:AdminCA-A-T01}, {2.5.4.11:Certification Authorities}, {2.5.4.11:Services}, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
subjectPublicKeyInfo {		
algorithm {	{1.2.840.113549.1.1.1},	rsaEncryption
parameters	NULL},	
subjectPublicKey {	…..},	BIT STRING 2048 bit
extensions {		
authorityKeyIdentifier {		
extnId	{2.5.29.35},	
extnValue	…..},	OCTET STRING, 160 bit SHA1 of root subjectPublicKey BIT STRING
subjectKeyIdentifier {		
extnId	{2.5.29.14}	
extnValue	…..},	OCTET STRING, 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage {		
extnId	{2.5.29.15},	
critical	TRUE,	BOOLEAN
extnValue	'000001100},	certSign, crlSign
certificatePolicies {		
extnId	{2.5.29.32},	
extnValue	{2.16.756.1.17.3.1.0},	
extnId	{{1.3.6.1.5.5.7.2.2},	
extnValue	{This is the Admin-Root-CA CPS},	UTF8String, id-qt-unotice RFC 3280

X.509 Field	OIDs/Values	Comments
extnId	{1.3.6.1.5.5.7.2.1},	
extnValue	{ http://www.pki.admin.ch/PKI/links/CPS_2_16_756_1_17_3_1_0.pdf}},	IA5String, cps
issuerAltName {		
extnId	{2.5.29.18},	UTF8String, directoryName
extnValue	{O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA}},	
basicConstraints {		
extnId	{2.5.29.19},	
critical	TRUE,	BOOLEAN
extnValue	{cA TRUE},	BOOLEAN
pathLenConstraint	0 },	INTEGER, no child CA
crlDistributionPoints {		
extnId	{2.5.29.31},	
extnValue	{http://www.pki.admin.ch/crl/Admin-Root-CA.crl ldap://admindir.admin.ch/cn=Admin-Root-CA,ou=Certification Authorities,ou=Services,o=Admin,c=CH c=ch,o=Admin,ou=Services,ou=Certification Authorities,cn=Admin-Root-CA},	uri IA5String ldap uri IA5String X509 name, IA5String CA inherits Admin-Root-CA CDPs
AuthorityInfoAcess {		SEQUENCE {
extnId	{1.3.6.1.5.5.7.1.1},	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessmethod	{1.3.6.1.5.5.7.48.2},	id-ad-calssuers
accessLocation	http://www.pki.admin.ch/aia/Admin-Root-CA.crt	uri IA5String
AccessDescription	SEQUENCE {	
AccessMethod	{1.3.6.1.5.5.7.48.1},	id-ad-ocsp
accessLocation	http://ocsp.pki.admin.ch}}},	uri IA5String
qcStatments {		
etxnId	{1.3.6.1.5.5.7.1.3},	
critical	FLASE	BOOLEAN
extnValue	SEQUENCE OF {	OCTET STRING
QCStatment	SEQUENCE	
statmentId	{0.4.0.1862.1.1}}}}}	qcs-Qccompliance
signatureAlgorithm {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncryption
parameters	NULL},	
signature	…..	2048 bit BIT STRING

```
KeyUsage ::= BIT STRING {
           digitalSignature        (0),
           nonRepudiation          (1),
           keyEncipherment         (2),
           dataEncipherment        (3),
           keyAgreement            (4),
           keyCertSign             (5),
           cRLSign                 (6),
           encipherOnly            (7),
           decipherOnly            (8) }
```

Table 1: KeyUsage bit

Usage	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Digital Signature, Non repudiation	x	x							
Data Encipherement			x	x					
Key Agreement					x				
Cert Sign, CRL sign						x	x		

Annexe B2 - Certificat d'abonné

X.509 Field	OIDs/Values	Comments
version	2	v3 cert
serialNumber	xxxxx	Integer value defined at key ceremony
signature {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncryption
parameters	NULL},	
issuer {	{2.5.4.3:AdminCA-A-T01}, {2.5.4.11:Certification Authorities}, {2.5.4.11:Services}, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
validity {		
notBefore	"YYMMDDHHMMSSZ",	UTC TIME, ETSI TS 102 280
notAfter	"YYMMDDHHMMSSZ"},	UTC TIME, ETSI TS 102 280 (3 years)
subject {	{RDN},	Printable String (UTF8String), directoryName
subjectPublicKeyInfo {		
algorithm {	{1.2.840.113549.1.1.1},	rsaEncryption
parameters	NULL},	
subjectPublicKey {	…..},	BIT STRING 2048 bit
extensions {		
authorityKeyIdentifier {		
extnId	{2.5.29.35},	
extnValue	…..},	OCTET STRING, 160 bit SHA1 of root subjectPublicKey BIT STRING
subjectAltName {		
extnId	{2.5.29.17},	
extnValue	…..},	SEQUENCE, CONTEXT SPECIFIC RFC822 Name
subjectKeyIdentifier {		
extnId	{2.5.29.14}	
extnValue	…..},	OCTET STRING, 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage {		
extnId	{2.5.29.15},	
critical	TRUE,	BOOLEAN
extnValue	'010000000},	nonRep
certificatePolicies {		
extnId	{2.5.29.32},	
extnValue	{2.16.756.1.17.3.2.17},	
extnId	{{1.3.6.1.5.5.7.2.2},	
extnValue	{This is the QC EE ClassA CPS},	UTF8String, id-qt-unotice RFC 3280
extnId	{1.3.6.1.5.5.7.2.1},	
extnValue	{http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_1_4.pdf}	IA5String, cps

X.509 Field	OIDs/Values	Comments
	},	
issuerAltName {		
extnId	{2.5.29.18},	UTF8String, directoryName
extnValue	{ O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA}},	
crlDistributionPoints {		
extnId	{2.5.29.31},	
extnValue	{http://www.pki.admin.ch/crl/AdminCA-A-T01.crl ldap://admindir.admin.ch/cn=AdminCA-A-T01,ou=Certification Authorities,ou=Services,o=Admin,c=CH c=ch,o=Admin,ou=Services,ou=Certification Authorities,cn=AdminCA-A-T01},	uri IA5String ldap uri IA5String X509 name, IA5String CA inherits Admin-Root-CA CDPs
AuthorityInfoAcess {		SEQUENCE {
extnId	{1.3.6.1.5.5.7.1.1},	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessmethod	{1.3.6.1.5.5.7.48.2},	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/AdminCA-A-T01.crt	uri IA5String
AccessDescription	SEQUENCE {	
AccessMethod	{1.3.6.1.5.5.7.48.1},	id-ad-ocsp
accessLocation	http://ocsp.pki.admin.ch}}},	uri IA5String
qcStatments {		
extnId	{1.3.6.1.5.5.7.1.3},	
extnValue	SEQUENCE OF {	OCTET STRING
QCStatment	SEQUENCE {	
statmentId	{0.4.0.1862.1.1}},	qcs-QcCompliance
QCStatment	SEQUENCE {	
statmentId	{0.4.0.1862.1.2},	qcs-QcLimitValue
statmentInfo	SEQUENCE {	monetary value
currency	CHF,	ISO 4217 currency codes
amount	xx,	CHF defined at registration time
exponent	xx}}},	INTEGER defined at registration time
QCStatment	SEQUENCE {	
statmentId	{0.4.0.1862.1.4}}}}}	qcs-QcSSCD
admissions	{1.3.36.8.3.3}	Optional ISIS MTT Common PKI admissions extension
signatureAlgorithm {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncryption
parameters	NULL},	

Annexe B3 - Service d'horodatage (TSA)

X.509 Field	OIDs/Values	Comments
version	2	v3 cert
serialNumber	xxxxx	Integer value defined at key ceremony
signature {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncryption
parameters	NULL},	
issuer {	{2.5.4.3: AdminCA-A-T01}, 2.5.4.11:Certification Authorities}, {2.5.4.11:Services}, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
validity {		
notBefore	"YYMMDDHHMMSSZ",	UTC TIME, ETSI TS 102 280
notAfter	"YYMMDDHHMMSSZ"},	UTC TIME, ETSI TS 102 280
subject {	{2.5.4.3: TSA-A-T01}, {2.5.4.11: Server }, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
subjectPublicKeyInfo {		
algorithm {	{1.2.840.113549.1.1.1},	rsaEncryption
parameters	NULL},	
subjectPublicKey {	…..},	BIT STRING 2048 bit
extensions {		
authorityKeyIdentifier {		
extnId	{2.5.29.35},	
extnValue	…..},	OCTET STRING, 160 bit SHA1 of AdminCA-A-T01 subjectPublicKey BIT STRING
subjectKeyIdentifier {		
extnId	{2.5.29.14}	
extnValue	…..},	OCTET STRING, 160 bit SHA1 of self subjectPublicKey BIT STRING
keyUsage {		
extnId	{2.5.29.15},	
critical	TRUE,	BOOLEAN
extnValue	'000000010},	nonRepudiation
extendedkeyUsage {		
extnId	{2.5.29.37},	
critical	TRUE,	BOOLEAN
extnValue	'1 3 6 1 5 5 7 3 8},	timeStamping
basicConstraints {		
extnId	{2.5.29.19},	
critical	TRUE,	BOOLEAN
extnValue	{cA FALSE},	BOOLEAN
lengConstraint	0},	INTEGER

X.509 Field	OIDs/Values	Comments
certificatePolicies {		
extnId	{2.5.29.32},	
extnValue	{2.16.756.1.17.3.2.18},	
extnId	{{1.3.6.1.5.5.7.2.2},	
extnValue	{This is the TSA CPS},	UTF8String, id-qt-unotice RFC 3280
extnId	{1.3.6.1.5.5.7.2.1},	
extnValue	{http://www.pki.admin.ch/policy/CPS_2_16_756_1_17_3_1_4.pdf} },	IA5String, cps
issuerAltName {		
extnId	{2.5.29.18},	UTF8String, directoryName
extnValue	{ O=ZertES Recognition Body: KPMG Klynveld Peat Marwick Goerdeler SA}},	
crlDistributionPoints {		
extnId	{2.5.29.31},	
extnValue	{http://www.pki.admin.ch/crl/AdminCA-A-T01.crl ldap://admindir.admin.ch/cn=AdminCA-A-T01,ou=Certification Authorities,ou=Services,o=Admin,c=CH c=ch,o=Admin,ou=Services,ou=Certification Authorities,cn=AdminCA-A-T01},	uri IA5String ldap uri IA5String X509 name, IA5String CA inherits AdminCA-A-T01 CDPs
AuthorityInfoAcess {		SEQUENCE {
extnId	{1.3.6.1.5.5.7.1.1},	OCTET STRING
extnValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessmethod	{1.3.6.1.5.5.7.48.2},	id-ad-caIssuers
accessLocation	http://www.pki.admin.ch/aia/AdminCA-A-T01.crt}}}},	uri IA5String
SubjectInfoAccess {		
extId	{1 3 6 1 5 5 7 1 11},	OCTET STRING
extValue	SEQUENCE OF {	OCTET STRING
AccessDescription	SEQUENCE {	
accessMethod	{1 3 6 1 5 5 7 48 3},	id-ad-timeStamping
accessLocation	“http://tsa.pki.admin.ch”}}}}}	uri, IA5String
signatureAlgorithm {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncryption
parameters	NULL},	
signature	…..	2048 bit BIT STRING

Annexe B4 - Liste des certificats annulés

X.509 Field	OIDs/Values	Comments
version	2	v3 CRL
signature {		
algorithm	{1.2.840.113549.1.1.5}	sha1WithRSAEncryption
parameters	NULL},	
issuer {	{2.5.4.3:AdminCA-A-T01}, {2.5.4.11:Certification Authorities}, {2.5.4.11:Services}, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
thisUpdate	"YYMMDDHHMMSSZ",	UTC TIME, ETSI TS 102 280
nextUpdate	"YYMMDDHHMMSSZ"},	UTC TIME, ETSI TS 102 280
subject {	{2.5.4.3: AdminCA-A-T01}, {2.5.4.11: Server }, {2.5.4.11:Services}, {2.5.4.10:Admin}, {2.5.4.6:CH}},	Printable String (UTF8String), directoryName
revokedCertificates {	SEQUENCE OF SEQUENCE	
{		
userCert serialNumber	xxxx	INTEGER
revocationDate	"YYMMDDHHMMSSZ",	UTC TIME, ETSI TS 102 280
crlEntryExtensions {{	SEQUENCE OF SEQUENCE	OPTIONAL
invalidityDate	2.5.29.24	
generalizedTime	"YYMMDDHHMMSSZ",	UTC TIME, ETSI TS 102 280
	}}	
{	Context Specific	
{	SEQUENCE	
{	SEQUENCE	
crlNumber	2.5.29.20	INTEGER
	}}}	
signature	…..	2048 bit BIT STRING

Informationen / Informations / Informazioni / Informations

Form / Forme / Forma	Elektronisches Dokument im PDF Format qualifiziert elektronisch signiert nach schweizerischem Recht. / Document électronique en format PDF avec signature électronique qualifiée selon le droit suisse. / Documento elettronico in formato PDF con firma elettronica qualificata conforme al diritto svizzero. / Electronic document in PDF format with qualified electronic signature according to Swiss law. Rechtsgrundlage / Base légale / Base legale / Legal basis: SR/RS 943.03
Gültigkeit / Validité / Validità / Validity	Dieses elektronische Dokument ist nur in elektronischer Form gültig und überprüfbar. / Ce document électronique n'est que valide et vérifiable en forme électronique. / Questo documento elettronico è valido e può essere verificato solamente in forma elettronica. / This electronic document is valid and can be verified only in electronic form.
Überprüfung / Vérification / Verificazione / Verification	Überprüfung: Integrität/Herkunft des Dokuments, Gültigkeit der elektronischen Signatur und des Zeitstempels. / Vérification: Intégrité et origine du document, validité de la signature et de l'horodatage. / Verificazione: Integrità e origine del documento, validità della firma elettronica e del timestamp. / Verification: Integrity and origin of the document, validity of electronic signature and timestamp. https://www.e-service.admin.ch/validator/upload/FullQualified