PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

Politique de certification
-entreprise-

POUR LES CERTIFICATS QUALIFIES AVEC UTILISATION DE DISPOSITIF SECURISE DE CREATION DE SIGNATURE ELECTRONIQUE

Version 1.0 du 7 novembre 2003

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

conseil.dcssi@sgdn.pm.gouv.fr

Historique des modifications

Version	Date	Objet de la modification	Auteur(s)	Statut
0.1	28/02/2003	Création du document	BCS	Draft
0.2	21/03/03	Mise à jour du document	BCS	Draft
0.3	26/0303	Mise à jour du document	BCS	Draft
0.4	26/05/03	Finalisation du document	BCS	Draft
0.5	2/10/03	Mise à jour suite à commentaires GT EGAP	BCS	Draft
0.6	4/11/03	Mise à jour suite à commentaires GT EGAP	BCS	Draft
1.0	7/11/03	Mise à jour suite à commentaires GT EGAP et ajout du glossaire	BCS	Version finale

Sommaire

1 INTRODUCTION 9

1.1 PRESENTATION GENERALE 9
1.2 IDENTIFICATION 9
1.3 GROUPE D'UTILISATEURS ET APPLICATIONS CONCERNES DU DOMAINE 9
1.3.1 GROUPE D'UTILISATEURS 9
1.3.2 TYPES D'APPLICATIONS CONCERNEES 12
1.4 CONTACTS 12
1.4.1 PERSONNES HABILITEES POUR LA QUALIFICATION DE L'AC 12
1.4.2 PERSONNES A CONTACTER CONCERNANT CE DOCUMENT 12
1.4.3 PERSONNES HABILITEES A DETERMINER LA CONFORMITE DE LA DPC AVEC CE DOCUMENT 12

2 DISPOSITIONS D'ORDRE GENERAL 13

2.1 OBLIGATIONS COMMUNES AUX COMPOSANTES DU PSC 13
2.1.1 OBLIGATIONS QUI INCOMBENT A CHACUN DES ACTEURS 13
2.2 LIMITES DE RESPONSABILITES QUI INCOMBENT A CHACUN DES UTILISATEURS 16
2.3 RESPONSABILITES FINANCIERES 16
2.3.1 INDEMNISATION PAR LE PSC 16
2.3.2 RELATIONS FINANCIERES 16
2.3.3 PROCESSUS ADMINISTRATIFS 16
2.4 INTERPRETATION DE LA LOI 16
2.4.1 LOIS 16
2.4.2 ARBITRAGE DES LITIGES 17
2.5 BAREMES DES PRIX 17
2.5.1 FRAIS DE GENERATION OU DE RENOUVELLEMENT DE CERTIFICAT 17
2.5.2 FRAIS D'ACCES A UN CERTIFICAT 17
2.5.3 FRAIS DE REVOCATION 17
2.5.4 FRAIS POUR D'AUTRES SERVICES 17
2.5.5 POLITIQUE DE REMBOURSEMENT 17
2.6 PUBLICATIONS ET SERVICES ASSOCIES 18
2.6.1 PUBLICATION D'INFORMATIONS CONCERNANT LE PSC 18
2.6.2 FREQUENCE DE PUBLICATION 18
2.6.3 CONTROLE D'ACCES 18
2.6.4 SERVICE DE PUBLICATION 18
2.7 QUALIFICATION ET CONTROLES DE CONFORMITE 19
2.7.1 FREQUENCE DE LA QUALIFICATION ET DES CONTROLES DE CONFORMITE 19
2.7.2 IDENTIFICATION ET QUALIFICATIONS DU CONTROLEUR 19
2.7.3 SUJETS COUVERTS PAR LE CONTROLE DE CONFORMITE 19
2.7.4 MESURES A PRENDRE EN CAS DE NON-CONFORMITE 19
2.7.5 COMMUNICATION DES RESULTATS 20
2.8 POLITIQUE DE CONFIDENTIALITE 20
2.8.1 TYPES D'INFORMATIONS CONSIDEREES COMME CONFIDENTIELLES 20
2.8.2 TYPES D'INFORMATIONS CONSIDEREES COMME NON-CONFIDENTIELLES 21
2.8.3 DIVULGATION DES CAUSES DE REVOCATION ET DE SUSPENSION DES CERTIFICATS 21
2.8.4 DELIVRANCE AUX AUTORITES LEGALES 21
2.8.5 DELIVRANCE A LA DEMANDE DU PROPRIETAIRE 21
2.8.6 AUTRES CIRCONSTANCES DE DELIVRANCES POSSIBLES 21
2.9 DROITS SUR LA PROPRIETE 21

3 IDENTIFICATION ET AUTHENTIFICATION 22

3.1 ENREGISTREMENT INITIAL 22
3.1.1 CONVENTIONS DE NOMS 22
3.1.2 NECESSITE D'UTILISATION DE NOMS EXPLICITES 22
3.1.3 INTERPRETATION DES DIFFERENTES FORMES DE NOMS 22
3.1.4 UNICITE DES NOMS 22
3.1.5 RESOLUTION DES LITIGES SUR LA REVENDICATION D'UN NOM 22
3.1.6 RECONNAISSANCE, AUTHENTIFICATION ET ROLE DES NOMS DE MARQUES 22
3.1.7 PREUVE DE LA POSSESSION D'UNE CLE PRIVEE 22
3.1.8 AUTHENTIFICATION DE L'IDENTITE D'UN ORGANISME 23
3.1.9 AUTHENTIFICATION DE L'IDENTITE D'UN INDIVIDU 23
3.2 RE-GENERATION DE CERTIFICAT APRES EXPIRATION 23
3.3 RE-GENERATION DE CLES APRES REVOCATION 24
3.4 AUTHENTIFICATION D'UNE DEMANDE DE REVOCATION 24

4 BESOINS OPERATIONNELS 26

4.1 DEMANDE DE CERTIFICAT 26
4.2 GENERATION DE CERTIFICAT 27
4.3 ACCEPTATION D'UN CERTIFICAT 28
4.4 SUSPENSION, REVOCATION, EXPIRATION DE CERTIFICAT 28
4.4.1 CAUSES DE REVOCATION 28
4.4.2 QUI PEUT DEMANDER UNE REVOCATION ? 29
4.4.3 PROCEDURE DE DEMANDE DE REVOCATION 29
4.4.4 TEMPS DE TRAITEMENT D'UNE REVOCATION 30
4.4.5 CAUSES POSSIBLES DE SUSPENSION 30
4.4.6 QUI PEUT DEMANDER UNE SUSPENSION ? 30
4.4.7 PROCEDURE DE DEMANDE DE SUSPENSION 30
4.4.8 LIMITES D'UNE PERIODE DE SUSPENSION 30
4.4.9 FREQUENCE DE LA MISE A JOUR DE LA LISTE DES CERTIFICATS REVOQUES 30
4.4.10 EXIGENCES DE CONTROLE DES LISTES DE CERTIFICATS REVOQUES 31
4.4.11 PUBLICATION DES CAUSES DE REVOCATION 31
4.4.12 CONTROLE EN LIGNE DES LISTES DE CERTIFICATS REVOQUES 31
4.4.13 AUTRES FORMES DE PUBLICATION DE LISTES DE CERTIFICATS REVOQUES 31
4.4.14 CONTROLE EN LIGNE DES AUTRES FORMES DE LISTES DE CERTIFICATS REVOQUES 31
4.4.15 BESOINS SPECIFIQUES EN CAS DE REVOCATION POUR COMPROMISSION 32
4.5 AUDIT SECURITE 32
4.5.1 TYPES D'EVENEMENTS ENREGISTRES 32
4.5.2 FREQUENCE DE TRAITEMENT DES JOURNAUX D'EVENEMENT 33
4.5.3 DUREE DE RETENTION D'UN JOURNAL D'EVENEMENTS 33
4.5.4 PROTECTION D'UN JOURNAL D'EVENEMENTS 33
4.5.5 COPIE DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS 33
4.5.6 SYSTEME DE COLLECTE DES JOURNAUX (INTERNE OU EXTERNE) 33
4.5.7 IMPUTABILITE 33
4.5.8 ANALYSE DES VULNERABILITES 33
4.6 ARCHIVES 34
4.6.1 TYPES DE DONNEES A ARCHIVER 34
4.6.2 PERIODE DE RETENTION DES ARCHIVES 34
4.6.3 PROTECTION DES ARCHIVES 34
4.6.4 PROCEDURE DE COPIE DES ARCHIVES 34
4.6.5 BESOIN D'HORODATAGE DES ENREGISTREMENTS 35
4.6.6 SYSTEME DE COLLECTE DES ARCHIVES 35
4.6.7 PROCEDURE DE RECUPERATION DES ARCHIVES 35

4.7 CHANGEMENT DE CLE D'UNE COMPOSANTE 35
4.8 COMPROMISSION ET PLAN ANTI-SINISTRE 35
4.8.1 EN CAS DE CORRUPTION DES RESSOURCES INFORMATIQUES, LOGICIELLES ET/OU INFORMATIQUES 36
4.8.2 EN CAS DE REVOCATION DE LA CLE PUBLIQUE D'UNE COMPOSANTE DU PSC 36
4.8.3 EN CAS DE COMPROMISSION DE CLE D'UNE COMPOSANTE DU PSC 36
4.8.4 MESURES DE SECURITE EN CAS DE SINISTRE 36
4.9 FIN DE VIE D'UNE COMPOSANTE 36

5 CONTROLES DE SECURITE PHYSIQUE, DES PROCEDURES ET DU PERSONNEL 38

5.1 CONTROLES PHYSIQUES 38
5.1.1 SITUATION GEOGRAPHIQUE ET CONSTRUCTION DES SITES 38
5.1.2 ACCES PHYSIQUE 38
5.1.3 ÉLECTRICITE ET AIR CONDITIONNE 38
5.1.4 EXPOSITION A L'EAU 38
5.1.5 PREVENTION ET PROTECTION CONTRE LE FEU 38
5.1.6 CONSERVATION DES SUPPORTS DE DONNEES 38
5.1.7 TRAITEMENT DES DECHETS 38
5.1.8 SITE DE SECOURS 39
5.2 CONTROLE DES PROCEDURES 39
5.2.1 ROLES DE CONFIANCE 39
5.2.2 NOMBRE DE PERSONNES NECESSAIRES A CHAQUE TACHE 39
5.2.3 IDENTIFICATION ET AUTHENTIFICATION DES ROLES 39
5.3 CONTROLE DU PERSONNEL 40
5.3.1 COMPETENCES, QUALIFICATION ET ANTECEDENTS REQUIS 40
5.3.2 PROCEDURES PREALABLES DE CONTROLE 40
5.3.3 EXIGENCES DE FORMATION INITIALE 40
5.3.4 EXIGENCES ET FREQUENCES DES FORMATIONS 40
5.3.5 GESTION DES METIERS 40
5.3.6 SANCTIONS POUR DES ACTIONS NON-AUTORISEES 40
5.3.7 CONTROLE DU PERSONNEL CONTRACTANT 40
5.3.8 DOCUMENTATION FOURNIE AU PERSONNEL 40

6 CONTROLES TECHNIQUES DE SECURITE 42

6.1 GENERATION ET INSTALLATION DE BICLE 42
6.1.1 GENERATION DE BICLE 42
6.1.2 DELIVRANCE DE LA CLE PRIVEE A UN SIGNATAIRE OU A UNE COMPOSANTE DU PSC 42
6.1.3 DELIVRANCE DE CLE PUBLIQUE A UNE AC 42
6.1.4 DELIVRANCE DE LA CLE PUBLIQUE D'UNE AC AUX UTILISATEURS 42
6.1.5 TAILLE DES CLES 42
6.1.6 GENERATION DES PARAMETRES DE CLE PUBLIQUE 43
6.1.7 CONTROLE DE LA QUALITE DES PARAMETRES 43
6.1.8 MODE DE GENERATION DE CLE 43
6.1.9 USAGES DE LA CLE 43
6.2 PROTECTION DE CLE PRIVEE 43
6.2.1 MODULE DE CRYPTOGRAPHIE UTILISANT DES NORMES 43
6.2.2 CONTROLE DE CLE PRIVEE PAR PLUSIEURS PERSONNES 43
6.2.3 SEQUESTRE DE CLE PRIVEE 44
6.2.4 COPIE DE SECOURS DE CLE PRIVEE 44
6.2.5 ARCHIVAGE DE CLE PRIVEE 44
6.2.6 MISE A LA CLE DU MODULE CRYPTOGRAPHIQUE 44

6.2.7 METHODE D'ACTIVATION DE CLE PRIVEE 44
6.2.8 METHODE DE DESACTIVATION DE CLE PRIVEE 44
6.2.9 METHODE DE DESTRUCTION DE CLE PRIVEE 44
6.3 AUTRES ASPECTS DE LA GESTION DES BICLES 45
6.3.1 ARCHIVAGE DES CLES PUBLIQUES 45
6.3.2 DUREE DE VIE DES CLES PUBLIQUES ET PRIVEES 45
6.4 DONNEES D'ACTIVATION 45
6.4.1 GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION 45
6.4.2 PROTECTION DES DONNEES D'ACTIVATION 45
6.4.3 AUTRES ASPECTS SUR LES DONNEES D'ACTIVATION 45
6.5 CONTROLE DE LA SECURITE DES POSTES DE TRAVAIL DU PSC 45
6.5.1 BESOINS DE SECURITE SPECIFIQUES SUR LES POSTES DE TRAVAIL 45
6.5.2 NIVEAU DE SECURITE DU POSTE DE TRAVAIL 46
6.6 CONTROLE PHYSIQUE DU SYSTEME DURANT SON CYCLE DE VIE 46
6.6.1 CONTROLES DES DEVELOPPEMENTS DES SYSTEMES 46
6.6.2 CONTROLES DE LA GESTION DE LA SECURITE 46
6.7 CONTROLES DE SECURITE RESEAU 46
6.8 CONTROLES TECHNIQUES DES MODULES DE CRYPTOGRAPHIE 46

7 PROFILS DES CERTIFICATS ET LISTES DE CERTIFICATS REVOQUES 47

7.1 PROFIL DU CERTIFICAT 47
7.1.1 NUMERO DE VERSION 47
7.1.2 EXTENSIONS DE CERTIFICAT 47
7.1.3 IDENTIFICATEURS D'ALGORITHMES 47
7.1.4 FORMAT DE NOMS 47
7.1.5 CONTRAINTE DE NOMS 47
7.1.6 IDENTIFICATEUR DE POLITIQUE DE CERTIFICATION 47
7.1.7 UTILISATION D'EXTENSION DE CONTRAINTES SUR LES POLITIQUES 47
7.1.8 SYNTAXES ET SEMANTIQUES DES QUALIFICATEURS DE POLITIQUES 47
7.1.9 REGLES DE TRAITEMENT DE L'EXTENSION CRITIQUE "POLITIQUE DE CERTIFICATION" 47
7.2 PROFIL DES LISTES DE CERTIFICATS REVOQUES 47
7.2.1 NUMERO DE VERSION DE LISTE DE CERTIFICATS REVOQUES 47
7.2.2 CRL ET EXTENSION DES CRL 48

8 ADMINISTRATION DES SPECIFICATIONS 49

8.1 PROCEDURE DE MODIFICATION DE CES SPECIFICATIONS 49
8.2 POLITIQUES DE PUBLICATION ET DE NOTIFICATION 49
8.3 PROCEDURES D'APPROBATION DES DPC 49

9 GLOSSAIRE 50

10 ANNEXES 58

10.1 ROLES 58
10.2 ACRONYMES 58
10.3 ACTIONS 59
10.4 DOCUMENTS DE REFERENCES 60

FORMULAIRE DE RECUEIL DE COMMENTAIRES 63

1 Introduction

1.1 Présentation générale

Cette politique de certification est adaptée aux Prestataires de Service de Certification électronique (PSC) délivrant des certificats qualifiés au sens du décret n° 2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique. Ces certificats seront utilisés pour des signatures électroniques ayant des effets juridiques identiques sur des documents numériques à ceux procurés par la signature manuscrite sur les documents papier et qui sont par conséquent recevables en justice (au sens de la directive européenne Art. 5.1). Ces certificats qualifiés sont distribués à des utilisateurs finaux pour sécuriser des applications (cf. §1.3.2) **à l'aide d'un dispositif sécurisé de création de signature (noté DSCS).**

Ce document est conforme aux principes et recommandations définies dans le document « ETSI TS 101 456 v1.2.1 (2002-04), Policy requirements for certification authorities issuing qualified certificates » dont l'OID est : " itu-t (0) identified organization (4) etsi (0) qualified-certificate-policies (1456) policy-identifiers (1) qcp-public-with-sscd (1) ".

Cette politique de certification peut constituer la base d'élaboration pour une politique de certification de toute AC souhaitant être qualifiée. A ce titre la qualification d'une AC s'appuie sur une politique de certification et un audit.

Il est rappelé les définitions suivantes :

- Données de création de signature électronique : les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique. Dans la suite de la présente PC, ce terme sera remplacé par celui de clé privée.
- Données de vérification de signature électronique : les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique. Dans la suite de la présente PC, ce terme sera remplacé par celui de certificat. Lorsqu'une précision sera nécessaire, le terme sera remplacé par clé publique.

1.2 Identification

Après qualification, l'identification de cette politique de certification sera à déposer auprès de l'AFNOR, qui lui assignera un OID (Object IDentificator).

1.3 Groupe d'utilisateurs et applications concernés du domaine

1.3.1 Groupe d'utilisateurs

❖ Autorité de certification AC

Une AC est une entité responsable du PSC qui dispose d'une plate-forme lui permettant d'enregistrer des utilisateurs finaux, générer, émettre, publier, révoquer et renouveler des certificats qualifiés (dans la suite le terme de certificat qualifié sera remplacé par « certificat »), conformément à sa politique de certification et à ses pratiques de certification, au profit d'utilisateurs finaux et sur la base desquels une communauté d'utilisateurs de ces certificats peut établir sa a confiance.

L'AC peut en plus générer les certificats et les clés privées de l'utilisateur final et distribuer le dispositif sécurisé de création de signature (noté DSCS).

L'AC peut déléguer tout ou partie de ses services, en fonction de sa PC et de ses DPC, à différents acteurs tels qu'un opérateur de prestation d'externalisation, une autorité d'enregistrement ou un service de publication. L'AC peut aussi être en relation avec une Autorité Administrative (Cf. Glossaire) pour l'élaboration et la validation de sa PC et de ses DPC.

La personnalisation et la génération des clés, utilisées dans le DSCS, peuvent être effectuées par l'AC ou le signataire.

L'AC identifie et authentifie l'ARA et le mandataire comme un signataire en tant que personne physique. L'AC est en relation contractuelle avec l'entreprise de l'ARA. Elle peut aussi être en relation contractuelle avec le mandataire.

NB : L'AC n'est pas tenue de mettre en œuvre un service de suspension.

❖ Autorité d'enregistrement AE

Une AE est une entité de l'AC pour laquelle elle authentifie le mandataire et/ ou les demandeurs de certificat et initie des demandes d'opération pour un signataire qui sont :

- l'enregistrement,
- la génération de certificat ;
- la révocation de certificat ;
- le renouvellement de certificat.

L'AE agit conformément à la politique de certification et aux pratiques de certification définies par l'AC, au profit de signataire.

❖ Signataire

Toute personne physique qui détient un certificat qualifié et un dispositif sécurisé de création de signature (DSCS) pour la mise en œuvre de sa clé privée. Il agit soit pour son propre compte, soit pour celui d'une personne physique ou morale qu'il représente dans le cadre de l'application concernée (cf. §1.3.2). Il applique la politique et les pratiques de sécurité édictée par l'ARA. Tant qu'il ne possède pas son certificat, le signataire est appelé un demandeur pour l'ensemble des opérations ayant trait à l'enregistrement.

❖ Autorité Responsable d'Application

L'ARA est un responsable identifié au sein de l'entreprise qui est responsable du domaine d'application de l'entreprise dont font partie les signataires. La garantie de l'ARA vis à vis des signataires et des vérificateurs par rapport à l'application concernée vient de la qualité de la technologie mise en œuvre et du cadre procédurale et contractuel qu'elle définit dans une politique régissant l'application et qu'elle s'engage à respecter. L'ARA à la responsabilité de spécifier et de mettre en oeuvre l'ensemble des procédures et relations contractuelles qui permettent de mentionner les procédures d'enregistrement et de remise de certificat et/ou de biclés et d'utilisation du certificat délivré aux signataires de l'entreprise. Cette spécification peut faire intervenir pour certain point l'AC et le mandataire. Elle établie une relation contractuelle avec l'AC qui reprend les éléments ci-dessus pour la gestion des certificats des signataires générés par le PSC de l'AC.

Lorsque l'entreprise a recours à un mandataire, le contrat entre l'entreprise et le l'AC identifie le mandataire.

❖ Mandataire

Toute personne physique liée par contrat avec l'ARA pour réaliser l'enregistrement des signataires pour le compte de l'entreprise. Le mandataire est en relation directe avec l'AE du PSC. Il réalise l'identification et l'authentification du signataire par rapport faciale suivant les procédures définies par l'ARA. Il transmet la demande de certificat du signataire au PSC afin que le PSC puisse générer un certificat et le transmettre au signataire suivant le contrat liant l'AC et l'entreprise ARA. Le mandataire n'a jamais connaissance de la clé privée associée à la clé publique contenue dans le certificat délivré au signataire ni des données d'activations qui permettent d'activé cette clé privée.
Le recours à un mandataire n'est pas obligatoire pour une entreprise.
Le mandataire est lié, directement ou indirectement, par contrats à l'AC.

❖ Vérificateur

Toute 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 (cf. §1.3.2). Il applique la politique et les pratiques de sécurité édictée par l'ARA. Un utilisateur de certificat ne détient pas forcément de certificat propre.

❖ Opérateur de prestation d'externalisation OPE

L'OPE assure des prestations techniques, en entre autres cryptographiques, nécessaires au processus de gestion de certificat (enregistrement, certification, révocation, publication, …), conformément à la politique de certification et une pratique de certification définie par l'AC. Par exemple, dans le cas d'un opérateur de certification, il peut être en outre techniquement dépositaire de la clé privée de l'AC utilisée pour la signature des certificats. Dans ce cas là, sa responsabilité ne peut être engagée que par l'AC et se limite au respect des procédures établies dans la déclaration des pratiques de certification.
L'opérateur de prestation d'externalisation n'est pas obligatoire au sein d'un PSC. Un PSC peut utiliser plusieurs OPE en fonction des opérations externalisées.

❖ Service de publication SP

Le SP rend disponible les certificats de clés publiques émis par l'AC, aux signataires de certificat conformément à la politique de certification et aux pratiques de certification définie par l'AC. Il permet en autre de connaître la validité d'un certificat, par publication d'une CRL.

1.3.2 Types d'applications concernées

Dans le cadre de la présente PC il s'agit d'applications qui demandent une signature électronique de document pourvu d'un effet légal et/ou réglementaire. Les signatures électroniques sécurisées des utilisateurs finaux, utilisant un DSCS et liées à l'utilisation d'un certificat qualifié, sur les documents électroniques seront légalement et/ou réglementairement équivalentes à des signatures manuelles sur des documents manuscrits conformément à la loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique et au décret n°2001-535. Les certificats d'attribut ne sont pas pris en compte dans ce document, bien que des qualités propres au signataire puissent être comprises dans le certificat délivré par le PSC.
Les certificats délivrés suivant la présente PC ne sont utilisable que dans un cadre professionnel régit par une entreprise (entité légale au sens du commerce). Dans ce contexte l'entreprise peut avoir recours à un mandataire pour authentifier et identifier les signataires de l'entreprise.

1.4 Contacts

1.4.1 Personnes habilitées pour la qualification de l'AC

Conformément à l'article 7 du décret n°2001-272 du 30 mars 2001 pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique, l'AC demande à être reconnue comme qualifiée par un organisme accrédité conformément à l'arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation.

1.4.2 Personnes à contacter concernant ce document

L'AC est responsable de la distribution de la présente politique de certification.

1.4.3 Personnes habilitées à déterminer la conformité de la DPC avec ce document

Un organisme accrédité en charge de la qualification est nommé par l'AC afin de mener les démarches nécessaires à la qualification de l'AC (cf §2.7.2).

2 Dispositions d'ordre général

2.1 Obligations communes aux composantes du PSC

Toutes les entités du PSC :

- N'utilisent leurs clés publiques et privées qu'aux fins pour lesquelles elles ont été émises et avec les outils spécifiés, en vertu de la présente politique.
- Protégent leur clé privée et leurs données d'activation en intégrité et en confidentialité.
- Respectent et appliquent la PC et les DPC mises en œuvre et reconnue par l'AC pour le PSC.
- Respectent le résultat d'un contrôle de conformité interne et/ou externe et remédient aux non-conformités qu'il révèlerait.
- Protègent les informations qu'elles gèrent en fonction du niveau de protection défini par l'AC.
- Utilisent des systèmes et des matériels sécurisés et protégés conformément aux objectifs de sécurité prescrits par l'analyse de risques de l'AC.
- En cas de sinistre, y compris la compromission des données de création de signature électronique, s'assurent de la disponibilité des services minimum du PSC conformément au plan de continuité définit par l'AC.
- En cas de fin de vie du PSC, les entités du PSC appliquent le plan de cessation d'activité définit par l'AC.
- Mettent en œuvre les moyens nécessaires pour enregistrer et conserver pendant une durée appropriée les informations pertinentes concernant un certificat qualifié afin de pouvoir constituer une preuve, de la certification, dans le cadre d'une procédure légale.
- Rendent les opérations qu'elles supportent accessibles à tous les tiers dont l'activité s'inscrit dans le domaine d'intervention fixé par l'AC.
- Disposent d'un ou de plusieurs systèmes d'assurance de la qualité (politique, procédure, responsabilité, poste) et de la sécurité adaptée aux services qu'elles fournissent.
- Emploient un nombre suffisant de personnes, en fonction des postes décrit dans la DPC, nécessaires à la réalisation des services supportées.
- Sont indépendantes de toute autre organisation pour les décisions qui se rapportent à la mise en œuvre, à la préparation, à la continuation ou à l'interruption de leurs services.
- Contrôlent l'accès physique à leurs locaux et limitent cet accès aux personnels autorisés.
- Prennent les dispositions nécessaires pour mettrent en place les mécanismes de contrôle des opérations supportées.
- Les entités du PSC impliquées dans la gestion des opérations de génération et de révocation de certificat ont une autonomie de décision vis à vis de toute autre organisation pour les décisions qui se rapportent à la mise en œuvre, à la préparation, à la continuation ou à l'interruption de ces services.

2.1.1 Obligations qui incombent à chacun des acteurs

❖ Autorité Responsable d'Application

- L'ARA fournit ses exigences sur l'identification à porter dans le certificat des signataires et l'usage des certificats. Les exigences sur l'usage sont entre autre :

  - ✓ Choix de la publication des certificats par le SP du PSC ;
  - ✓ Choix des publications des causes de révocation ;
  - ✓ Choix sur l'usage des clés (signature ou non-répudiation) ;

- ✓ Choix sur le transfert de ses données archivés par le PSC en cas de fin de vie de ce dernier ;
- ✓ Les causes de révocation ;
- ✓ Les personnes autorisées pour la demande de révocation.

➢ Lorsque l'entreprise a recours à un mandataire, l'ARA fournit l'identité du mandataire au PSC et ses limites de pouvoir.

❖ Autorité d'enregistrement

➢ L'AE met à disposition du mandataire ou du signataire l'ensemble des formulaires nécessaires aux opérations réalisables entre le PSC et un signataire.
➢ L'AE authentifie le mandataire ou le signataire pour l'ensemble des opérations impliquant une relation avec le PSC.
➢ L'AE identifie les signataires pour la création des certificats.
➢ L'AE s'assure que les demandes auprès du PSC sont complètes et exactes et effectuées par un mandataire ou un signataire dûment autorisé.
➢ L'AE conserve et protége en confidentialité et en intégrité les données personnelles d'identification transmises lors de l'enregistrement.
➢ L'AE conserve et protége en confidentialité et en intégrité les données personnelles d'authentification du mandataire ou du signataire transmises lors des opérations avec le PSC.
➢ L'AE respecte la législation relative au respect des données d'identification personnelles [L78-19].

❖ Autorité de certification

➢ L'AC est une entité légale au sens de la loi française.
➢ L'AC doit être qualifiée au sens de l'article 7 du décret n°2001-272 du 30 mars 2001 pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.
➢ L'AC rend accessible l'ensemble des services déclarés dans la PC aux maîtrises d'ouvrage d'application, signataires, … qui mettent en œuvre des certificats dans le cadre de la loi du 13 mars 2000.
➢ L'AC est en relation contractuelle avec l'entreprise de l'ARA pour la gestion des certificats des signataires. Elle peut aussi être en relation contractuelle avec le mandataire choisi par l'entreprise. L'AC fournit ses exigences sur l'authentification des différentes opérations qui impliquent le signataire et l'utilisation du certificat à l'ARA.
➢ L'AC détaille dans la ou les DPC toutes les exigences de la PC, en respectant la séparation organisationnelle et fonctionnelle définie dans la PC, sur la base de laquelle elle demande la qualification. De plus, elle s'assure qu'au moins l'un des processus antérieurs à la délivrance du certificat, dans la gestion du certificat par le PSC au profit d'un signataire, met en oeuvre un rapport facial entre le PSC et le signataire permettant de garantir le lien entre la personne physique et le certificat. Lorsqu'un mandataire est utilisé le rapport facial a lieu entre le mandataire et le PSC et le mandataire et le signataire.
➢ L'AC rend disponible, sous une forme claire et compréhensible à l'abonné avant d'entrer dans toute relation contractuelle, les termes et conditions régissant l'AC et l'ensemble des obligations et des conditions d'usage des certificats.
➢ L'AC s'assure que les exigences de la PC et les procédures de la DPC appliquées par chacune des entités sont adéquates et conformes aux normes en vigueur.
➢ L'AC gère et documente les demandes d'accords de certification avec des AC extérieures au domaine de sécurité auquel l'AC appartient.
➢ L'AC définit les procédures applicables dans le cadre d'une procédure légale de remises d'informations concernant un signataire ou une entité du PSC.

- L'AC, dans le cadre de la qualification, est tenu de fournir aux organismes qu'il a choisis tous les éléments nécessaires au bon accomplissement de la procédure d'évaluation.
- En cas d'externalisation de certaines des opérations délivrées par le PSC à un ou plusieurs organismes extérieurs (OPE,…) :
  - ✓ L'AC conserve la responsabilité de tous les aspects des services de certification électronique qu'elle propose.
  - ✓ L'AC spécifie clairement les responsabilités des organismes sous-traitants ou tiers intervenant dans d'autres relations. Pour cela, l'AC s'appuiera sur un cadre contractuel clairement documenté.
  - ✓ L'AC s'assure que les organismes sous-traitants mettent en oeuvre la PC et les DPC reconnues.
- L'AC mène une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de chacune des entités qu'il gère et élabore en conséquence la PC et la DPC correspondant à la couverture de ces risques.
- L'AC génère ses données de création et de vérification de signatures électroniques à l'aide un d'un dispositif matériel évalué certifié EAL 4+ ou équivalent.
- L'AC s'assure que l'intégrité et l'authentification des données de vérification de signature, et de toutes les autres données associées, sont préservées lors de leur distribution aux tiers utilisateurs.
- L'AC génère et renouvelle les certificats des signataires sur demande d'une AE qu'elle reconnaît.
- L'AC s'assure qu'un certificat peut être révoqué en 24 heures maximums sur la base d'une demande de révocation validée et autorisée.
- L'AC assure l'intégrité et la précision des dates utilisées dans les processus qu'elle gère.
- Lorsque l'AC génère les données de création et de vérification de signature électronique du signataire, elle :
  - ✓ s'assure d'une part que la génération des données est sécurisée et d'autre part que leur confidentialité et leur intégrité sont préservées ;
  - ✓ apporte la preuve que les clés ont été générées dans le DSCS qui sera fourni à l'utilisateur ;
  - ✓ ne conserve aucune trace de la donnée de création de signature électronique de signature conformément au i) de l'article 6 II du décret 2001-272 du 30 mars 2001, pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.

❖ Service de Publication

- Le SP garantit les conditions de mises à jour et de disponibilités (24 heures sur 24 et 7 jours sur 7) pour l'ensemble des données qu'il publie.
- Lorsque cela est nécessaire le SP protège en intégrité les données qu'il publie.
- Le SP authentifie toutes les entités du PSC qui lui communiquent des données à publier.

❖ Mandataire

- Le mandataire communique toutes les informations nécessaires au PSC, exactes et à jour, pour toutes opérations avec le PSC qui requièrent une authentification et une identification du signataire conformément aux procédures définis entre l'AC et l'ARA.

❖ Signataire

- Le signataire communique toutes les informations nécessaires au mandataire ou au PSC, exactes et à jour pour toutes opérations avec le PSC qui requièrent une authentification.

- Le signataire, ou toutes autres personnes désignées par lui, informe l'entité du PSC chargée de la révocation dès qu'il a connaissance d'une compromission ou une suspicion de compromission de sa donnée de création de signature ou d'une modification de toutes informations contenues dans la donnée de vérification de signature.
- Le signataire informe l'entité chargée de l'enregistrement, dès qu'il a connaissance d'un changement ou d'une inexactitude de l'une des informations contenues dans son certificat.
- Le signataire respecte le contrat ou la convention qui lie l'entreprise et le PSC selon laquelle son certificat est géré.
- Le signataire respecte les conditions d'utilisation de données de création et de vérification de signature électronique et de son certificat.
- Lorsque le signataire génère ses données de création et de vérification de signature électronique, il :
  - ✓ s'assure que la biclé respecte les recommandations algorithmiques définis dans [SR 002 176].
  - ✓ il utilise un DSCS évalué certifié conformément à la procédure n°872 /SGDN/DCSSI/SDR du 7 avril 2003.

2.2 Limites de responsabilités qui incombent à chacun des utilisateurs

L'AC n'est pas responsable du préjudice causé par un usage du certificat dépassant les limites fixées à son utilisation ou à la valeur des transactions pour lesquelles il peut être utilisé, à condition que la présence de ces limites dans le certificat ait été clairement portée à la connaissance des utilisateurs.

2.3 Responsabilités financières

Lorsque cela s'applique, les responsabilités financières entre les composantes, le PSC et les signataires doivent figurer dans le contrat ou la convention liant les différentes parties ainsi que dans la DPC. Les entités du PSC doivent avoir une stabilité financière et les ressources nécessaires pour opérer conformément à la PC. Lorsqu'une entité du PSC délègue une partie de ses services, la composante qui prend en charge ces services doit aussi respecter ces exigences financières.

2.3.1 Indemnisation par le PSC

Le cas échéant, cette rubrique doit être renseignée et apparaître dans la DPC, le contrat ou la convention liant les différentes parties.

2.3.2 Relations financières

Le cas échéant, cette rubrique doit être renseignée et apparaître dans la DPC, le contrat ou la convention liant les différentes parties.

2.3.3 Processus administratifs

Le cas échéant, cette rubrique doit être renseignée et apparaître dans la DPC, le contrat ou la convention liant les différentes parties.

2.4 Interprétation de la loi

2.4.1 Lois

Les textes applicables sont entre autres :

- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Art. 323-1 à 323-3 du Code pénal).
- Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique ;
- Décret 2001-272 du 30 mars 2001, pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique ;
- Décret no 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information ;
- Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification et à l'accréditation des organismes chargés de l'évaluation ;
- Arrêté [à compléter] modifiant l'arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification et à l'accréditation des organismes chargés de l'évaluation.

2.4.2 Arbitrage des litiges

L'AC est responsable de la résolution des litiges. En priorité un compromis est recherché par l'AC en vue de résoudre les litiges conformément à ces responsabilités.

2.5 Barèmes des prix

Le coût éventuel des services fournis par une composante doit apparaître dans le contrat ou la convention liant les différentes parties.

2.5.1 Frais de génération ou de renouvellement de certificat

Le cas échéant, cette rubrique doit être renseignée et apparaître dans la DPC, le contrat ou la convention liant les différentes parties.

2.5.2 Frais d'accès à un certificat

Le cas échéant, cette rubrique doit être renseignée et apparaître dans la DPC, le contrat ou la convention liant les différentes parties.

2.5.3 Frais de révocation

Le cas échéant, cette rubrique doit être renseignée et apparaître dans la DPC, le contrat ou la convention liant les différentes parties.

2.5.4 Frais pour d'autres services

Le cas échéant, cette rubrique doit être renseignée et apparaître dans la DPC, le contrat ou la convention liant les différentes parties.

2.5.5 Politique de remboursement

Le cas échéant, cette rubrique doit être renseignée et apparaître dans la DPC, le contrat ou la convention liant les différentes parties.

2.6 Publications et services associés

2.6.1 Publication d'informations concernant le PSC

Les informations publiées concernant le PSC sont les suivantes :

- La PC en identifiant clairement l'usage associé ;
- Les procédures de validation de certificat (contenant les exigences sur la vérification du statut du certificat) ;
- La limite de responsabilité du PSC ;
- La période de temps d'archivage des données d'enregistrement et des accords ;
- Le contenu des accords ;
- La période de temps d'archivages des journaux ;
- Les procédures de résolution des litiges ;
- Les dispositions légales en vigueur ;
- L'ensemble des obligations et des conditions d'usage des certificats des signataires ;
- Le schéma de qualification utilisé et le résultat de conformité de la PC ;
- Formulaires de demande de certification ;
- Formulaires de demande de révocation ;
- Condensat des certificats des AC.

Le SP assure que la publication des informations ci-dessus est effectuée de manière à garantir l'intégrité, la lisibilité, la compréhensibilité et la clarté des données listés ci-dessus.

2.6.2 Fréquence de publication

La publication des informations concernant le PSC doit être mise à jour suite à toute modification des spécifications.
Les délais de mise à jour des listes de certificats publiées sont définis dans VAR_TEMPS : :F_MAJ_LISTE.

Le SP est disponible 24H/24H et 7j/7j et est public et accessible de manière internationale.

2.6.3 Contrôle d'accès

Le SP est responsable de la mise en œuvre et de l'application d'une politique de sécurité adaptée aux contrôles d'accès, à sa publication, pour l'ajout, le retrait ou la modification de toute information (Cf. 2.6.1 et CRL). L'accès en écriture est réservé aux fonctions internes du PSC.
La modification des informations de révocation nécessite réservé à l'AC. L'information de révocation doit être protégée en intégrité par l'AC et authentifiée par le SP.

2.6.4 Service de Publication

Le SP assure que la publication des listes de certificat valides aux signataires et aux vérificateurs répond au minimum aux exigences suivantes :

- le certificat est accessible pour une récupération uniquement dans les cas où le consentement du signataire a été obtenu conformément au § 2.8.4.
- les termes et les conditions d'emploi sont accessibles aux signataires et aux vérificateurs pour un certificat donné suivant le besoin d'en connaître.
- une fois le certificat généré, il est accessible dans son intégralité par le signataire pour lequel il a été généré et garantit intègre.

2.7 Qualification et contrôles de conformité

2.7.1 Fréquence de la qualification et des contrôles de conformité

Qualification :

La qualification du PSC (telle qu'elle est définie en 1.4) doit précéder sa première mise en service. La qualification est délivrée pour une période de trois ans avec une vérification de tous les ans.

Contrôle de conformité :

L'AC doit procéder à un contrôle de conformité avant la première mise en service d'une composante. Ce contrôle doit ensuite être pratiqué de manière régulière VAR_TEMPS : : F_CONFORM.

2.7.2 Identification et qualifications du contrôleur

Qualification :

L'AC choisi un organisme accrédité pour procéder à l'évaluation des services qu'il propose.

Contrôle de conformité :

L'AC désigne un contrôleur compétent en sécurité des systèmes d'information, n'appartenant pas à la composante contrôlée et dûment autorisé à pratiquer ces contrôles.

2.7.3 Sujets couverts par le contrôle de conformité

Qualification :

Il se déroule conformément à l'arrêté [à compléter] modifiant l'arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification et à l'accréditation des organismes chargés de l'évaluation.

Selon l'article 7 de l'arrêté: « L'évaluation est effectuée par l'organisme aux frais du prestataire de services de certification. Son objet est notamment est de vérifier que les services offerts par le prestataire respectent en tous points les exigences fixées par l'article 6 du décret du 30 mars 2001 susvisé ainsi que les normes, prescription techniques et règles de bonne pratique applicables en matière de certification électronique. »

Contrôle de conformité :

Le contrôle de conformité porte sur les points suivants du présent document :

- 3 Identification et authentification ;
- 4 Besoins opérationnels ;
- 5 Contrôle de sécurité physique, contrôle des procédures, contrôles du personnel ;
- 6 Contrôles techniques de sécurité ;
- 7 Profils des certificats et CRL ;
- 8 Administration des spécifications.

2.7.4 Mesures à prendre en cas de non-conformité

Contrôle de conformité :

A l'issue du contrôle de conformité, le contrôleur rend à l'autorité administrative, un avis parmi les suivants : « réussite », « échec », « à confirmer».
Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- En cas d'échec, et selon l'importance des non-conformités, le contrôleur propose à l'autorité administrative des sanctions qui peuvent être l'interdiction d'exercer, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la sanction à appliquer est effectué par l'autorité administrative et doit respecter les politiques de sécurité internes à l'administration concernée.
- En cas de résultat « A confirmer », l'Autorité administrative remet à la composante un avis précisant sous quel délai les non-conformités doivent être réparées. Puis, un contrôle de « confirmation » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'Autorité administrative remet à la composante contrôlée un avis d'autorisation d'exercice de sa fonction.

2.7.5 Communication des résultats

Qualification :

Selon l'article 9 de l'arrêté : « L'organisme accrédité reconnaît ou non la qualification du prestataire de service de certification électronique au vu du rapport d'évaluation et des éventuelles observations du prestataire. Lorsqu'il reconnaît la qualification du prestataire, l'organisme accrédité délivre une attestation qui décrit les prestations de services couvertes par la qualification ainsi que la durée, qui ne peut excéder un an, pendant laquelle l'attestation est valable.
Les prestataires dont la qualification est reconnue communiquent à toute personne qui en fait la demande une copie de l'attestation délivrée par l'organisme accrédité. »

Contrôle de conformité :

Les résultats des contrôles de conformité sont communiqués à la composante contrôlée ainsi qu'à l'Autorité administrative compétente. Ils peuvent également être communiqués à d'autres entités ayant le besoin d'en connaître et dont le nom doit être précisé.

2.8 Politique de confidentialité

2.8.1 Types d'informations considérées comme confidentielles

Sous l'autorité de l'AC, chacune des entités met en place et tient à jour l'inventaire de toutes les informations qu'elle détient et leur attribue un niveau de protection adéquat, en fonction des résultats de l'analyse de risque de l'AC, à l'aide d'une classification qui définit les règles de manipulation par les rôles autorisés au sein de l'entité.

A titre indicatif :

- Archives de journaux d'événements
  Sensible
- Archives des conventions cryptographiques utilisées (paramètres, valeurs d'initialisations)
  Confidentielles
- Clés privées propres à l'AC
  Confidentielles
- Données d'identification d'un utilisateur (identifiants nominatifs)

Confidentielles à caractère privatif.

- Journaux d'audit
  Diffusion restreinte
- Données d'activation de la donnée de création de signature électronique de l'utilisateur
  Diffusion restreinte

2.8.2 Types d'informations considérées comme non-confidentielles

Les informations concernant le PSC et citées en 2.6.1, et celles publiées par le SP (cf. § 2.6.4) sont considérées comme non confidentielles. Les procédures internes de fonctionnement sont non confidentielles au sein du PSC.

2.8.3 Divulgation des causes de révocation et de suspension des certificats

Suivant les spécifications du § 7.1, cette cause peut apparaître dans la CRL. Si toutefois cette information doit rester confidentielle, l'AE peut donner à l'AC comme cause de révocation une " raison inconnue " ("Unknown"). Pour le traitement de l'extension "Cause de révocation", cf § 7.2.2 (CRL et extension de CRL).

La divulgation des causes de révocation et de suspension des certificats est effectuée suite à un accord du signataire.

2.8.4 Délivrance aux autorités légales

En aucun cas, le recouvrement de clé de signature ne doit être possible. L'AC est responsable de la diffusion d'informations (par exemple, quand cela est utilisé, le lien entre un signataire et son certificat qualifié) sur les signataires dans le cadre d'une commission rogatoire ou d'une autre autorisation légale.

2.8.5 Délivrance à la demande du propriétaire

Les informations relatives à un signataire et définies comme confidentielles en 2.8.1 ne peuvent être divulguées qu'à leur propriétaire ou à un tiers, sur demande du propriétaire. Dans le cas d'une AC en fin de vie (dans les conditions définies au § 4.8.3), un consentement doit être donné par l'ARA pour que les informations utilisées pour son enregistrement soient conservées et communiquées à une tierce partie. De même, le signataire doit donner son consentement à la publication de son certificat.

2.8.6 Autres circonstances de délivrances possibles

Les informations relatives à un signataire et définies comme confidentielles en 2.8.1 peuvent être divulguées à leur AC ou à un tiers défini dans la DPC.

2.9 Droits sur la propriété

L'AC précise dans sa DPC les mesures mises en place sur la protection juridique des ses biens.

3 Identification et authentification

3.1 Enregistrement initial

3.1.1 Conventions de noms

Les noms utilisés sont décrits selon la norme X500.
Dans chaque certificat X509V3 l'émetteur (issuer) et le signataire (subject) sont identifiés par un nom distinctif ("Distinguish Name" ou DN) (Cf. 3.1.2) qui doit être unique (Cf. 3.1.4). L'identifiant porté dans le certificat est construit à partir du nom du signataire ou d'un pseudonyme, conformément aux exigences du décret [D2001-272], récupéré par l'AE lors de l'authentification du signataire (Cf. § 3.1.9). Lorsqu'un pseudonyme est utilisé, il doit être identifié comme tel dans le DN.

3.1.2 Nécessité d'utilisation de noms explicites

L'unicité du DN porté dans le certificat d'un signataire doit être vérifiée dans le domaine de sécurité durant tout le temps de vie de l'AC. Cette unicité s'établit sur une liste limitée d'attributs du DN (cf 3.1.1). Le contexte d'interprétation du DN étant déterminé par le champ « Country Name », une politique de définition du contenu du DN doit être élaborée.

3.1.3 Interprétation des différentes formes de noms

L'AC prend en compte les exigences de l'ARA pour la construction des DN portés dans le certificat du signataire.

3.1.4 Unicité des noms

L'unicité d'un certificat est basée sur l'unicité de son numéro de série pour une AC donnée. L'unicité de nom au sein d'un domaine doit être garantie pour éviter toute ambiguïté.

Durant le cycle de vie d'une AC, un DN contenu dans un certificat ne peut être attribué à un autre signataire.

3.1.5 Résolution des litiges sur la revendication d'un nom

Lorsque le nom à inclure dans un certificat provoque un litige avec un autre utilisateur, l'AE à qui la demande de certification a été formulée en informe l'AC qui est responsable de la résolution de ce litige. La réglementation en vigueur permet la résolution de ces litiges. A défaut, et sur demande du plaignant, l'AC est responsable de la résolution du litige conformément au § 2.4.2.

3.1.6 Reconnaissance, authentification et rôle des noms de marques

Sans objet.

3.1.7 Preuve de la possession d'une clé privée

Lorsque le signataire génère lui-même ses données de création et de vérification de signature électronique alors il fournit une preuve :

- De possession de sa donnée de création de signature électronique correspondant à la donnée de vérification de signature électronique contenue dans le certificat.

- Que la donnée de création de signature électronique a été générée dans le DSCS (cette preuve est apporté par l'utilisation d'un produit conforme aux exigences du § 6.1.8).

Dans le cas d'une génération de donnée de création et de vérification de signature électronique par le PSC, cette preuve est apportée par le processus de génération et de remise de clé au signataire (cf. § 6.1.1 et § 6.1.2).

3.1.8 Authentification de l'identité d'un organisme

L'AE vérifie l'identité et les attributs spécifiques à l'organisme auquel le signataire prétend appartenir qui lui sont fournit dans la demande (Cf. § 4.1).
L'authentification d'un organisme est réalisée par rapport facial auprès de l'AE, ou par une méthode apportant un degré d'assurance équivalent. L'authentification d'un organisme par l'AE permet d'identifier l'organisme de façon unique et non ambiguë et requiert la présentation de documents officiels d'identités de l'entreprise.

3.1.9 Authentification de l'identité d'un individu

L'AE vérifie l'identité et les attributs spécifiques fournis par le demandeur dans la demande de certificat (Cf. § 4.1).
L'authentification est réalisée par rapport facial auprès de l'AE ou par une méthode apportant un degré d'assurance équivalent. L'authentification d'un signataire par l'AE permet d'identifier la personne à laquelle un certificat électronique est délivré de façon unique et non ambiguë et de créer le DN correspondant comme défini au § 3.1.1. Cette authentification et identification requièrent de la part du signataire la présentation d'un document officiel d'identité. Le document officiel d'identité présenté par le signataire doit être rapproché directement ou indirectement de la personne physique concernée.
De même, l'AE vérifie les attributs dont se prévaut le signataire ainsi que l'ensemble des autres informations contenues dans le certificat avec un degré d'assurance identique à l'authentification du signataire lorsque cela à un sens (Cf. par exemple le 3.1.8).

Lorsque l'entreprise à recours à un mandataire, c'est le mandataire qui effectue le travail de l'AE auprès du signataire. L'AE authentifie ensuite le mandataire dans les mêmes conditions décrites ci-dessus.

3.2 Re-génération de certificat après expiration

La période de validité d'un certificat relevant de cette politique est précisée par la variable VAR_TEMPS::T_VALID_CERT (cette durée peut être écourtée à la demande du signataire ou d'une personne autorisée). La re-génération de certificat après expiration requiert une authentification du signataire. Cette authentification peut être effectuée :

- Par la même procédure que lors de la première demande de certificat dès lors qu'une des informations contenues dans le certificat ou utilisée lors de la première authentification est modifiée.
- Par une procédure apportant un degré d'assurance équivalent à celui de la procédure définie aux § 3.1.9 et § 3.1.8 (par la signature de la demande de renouvellement par la donnée de création de signature électronique dont le certificat correspondant arrive en fin de validité).

Si cela s'applique, la période de validité d'un certificat est limitée par la date d'expiration de l'habilitation de son porteur.

L'AE vérifie que l'identité et les attributs du signataire à inclure dans le nouveau certificat sont toujours valides.

La réutilisation de la clé publique du signataire pour une nouvelle émission de certificat n'est possible que si cela est jugé pertinent du point de vue de sa sécurité cryptographique et si la donnée de création de signature électronique n'est pas compromise.

Lorsque l'entreprise à recours à un mandataire, c'est le mandataire qui effectue le travail de l'AE auprès du signataire. L'AE authentifie ensuite le mandataire dans les mêmes conditions décrites ci-dessus.

3.3 Re-génération de clés après révocation

En cas de révocation de certificat pour cause de compromission ou suspicion de compromission des données de création de signature, perte ou vol, de nouvelles données de création et de vérification de signature électronique doivent être générées. Le signataire doit s'authentifier auprès de l'AE pour disposer d'un nouveau certificat. La procédure d'authentification à mettre en œuvre est alors la même que lors d'un premier enregistrement (cf.§ 3.1.8 et § 3.1.9).

Si le certificat est révoqué pour une autre cause (modification d'informations contenues dans le certificat, révocation de l'autorité de certification, etc.), la re-génération de certificat après expiration requiert une authentification du signataire. Cette authentification peut être effectuée :

- Par la même procédure que lors de la première demande de certificat.
- Par une procédure apportant un degré d'assurance équivalent à celui de la procédure définie aux § 3.1.9 et § 3.1.8 (par la signature de la demande de renouvellement par la donnée de création de signature électronique dont le certificat correspondant arrive en fin de validité).

Si cela s'applique, la période de validité d'un certificat est limitée par la date d'expiration de l'habilitation de son porteur.

L'AE vérifie que l'identité et les attributs du signataire à inclure dans le nouveau certificat sont toujours valides.
La réutilisation de la donnée de vérification de signature électronique pour une nouvelle émission de certificat n'est possible que si cela est jugé pertinent du point de vu de sa sécurité cryptographique et si la donnée de création de signature électronique n'est pas compromise.

Lorsque l'entreprise à recours à un mandataire, c'est le mandataire qui effectue le travail de l'AE auprès du signataire. L'AE authentifie ensuite le mandataire dans les mêmes conditions décrites ci-dessus.

3.4 Authentification d'une demande de révocation

Si la demande de révocation est due à une compromission ou suspicion de compromission, perte, vol de donnée de création de signature électronique du signataire, l'authentification de la demande de révocation ne peut être effectuée avec la donnée de création de signature électronique compromise. L'authentification peut être réalisée par une procédure apportant un degré d'assurance équivalent à celui de la procédure définie au § 3.1.9 et § 3.1.8

Si la demande de révocation est provoquée par une autre cause (modification d'informations contenues dans le certificat, révocation de l'AC, etc.), le signataire peut s'authentifier :

- en signant sa demande avec sa donnée de création de signature électronique,
- en se présentant en personne auprès de l'AE,
- ou en utilisant la même procédure que lors d'un premier enregistrement auprès du PSC.

L'AE s'assure de l'identité et de l'autorisation du signataire en confrontant les éléments contenus dans le dossier de demande de certificat (Cf. § 4.1) et ceux présentée par le signataire.

Lorsque l'entreprise à recours à un mandataire, c'est le mandataire qui peut effectuer l'authentification du signataire. Le PSC authentifie ensuite le mandataire dans les mêmes conditions décrites ci-dessus.

4 Besoins opérationnels

4.1 Demande de certificat

L'AE s'assure de l'exactitude et de la complétude de la demande de certificat du signataire et que celui-ci ou le mandataire est habilité à déposer la demande. L'AE informe le signataire de manière complète et exacte sur les conditions d'emploi de son certificat. Cette information est accessible au signataire conformément au § 2.6.1.

Le signataire fournit les renseignements ci-dessous auprès du mandataire ou de l'AE :

- Nom patronymique complet du titulaire ;
- Date et lieu de naissance du titulaire, conformément aux dispositions nationales établies pour l'enregistrement des naissances ;
- Nom à utiliser dans le certificat ;
- Preuve de l'autorisation d'associer des attributs ou des droits à un certificat ;
- Preuve du grade ou du poste occupé par le demandeur ;
- Adresse, ou toutes autres informations, permettant de contacter le signataire.

Si le signataire procède à une demande pour un dispositif :

- Référence permettant d'identifier le dispositif ou le système matériel, par exemple un nom de domaine.
- Lorsque cela s'applique, le nom complet et statut légal de la personne morale contrôlant le dispositif ou le système matériel.
- Numéro ou code d'identification de la personne morale concernée.

Le signataire fournit aussi la liste des informations suivantes :

- Choix de la publication de son certificat par le SP ;
- Choix des publications des causes de révocation (si proposé par le PSC) ;
- Choix sur le transfert[1] de ses données archivés par le PSC en cas de fin de vie de ce dernier.

Le signataire fournit les renseignements ci-dessous auprès de l'AE ou du mandataire :

- Le numéro ou code d'identification de la personne morale concernée ;
- Nom complet et statut légal de la personne morale concernée ;
- Un document établissant le lien entre le titulaire et la personne morale ;
- L'identification de son autorité hiérarchique (au sein de son organisme), autorité qui aura le pouvoir par exemple de révoquer son certificat en son nom cf. 4.4.2 et 4.4.6 ;
- Référence au contrat entre l'AC et l'ARA au titre duquel le certificat est délivré ;
- Si l'organisme est une société anonyme ou une société de personnes et capitaux :
  - ✓ Nom, raison sociale ;
  - ✓ Adresse du siège social et numéro de téléphone ;
  - ✓ Numéro SIRET ;
  - ✓ Extrait du registre du commerce où la société est enregistrée ;
  - ✓ Composition et répartition du capital de la société ;
- Si l'organisme est une société de personnes :

[1] (vision juridique à apporter sur ce point - données personnelles -)

- ✓ Nom, dénomination ;
- ✓ Adresse et numéro de téléphone ;
- ✓ Numéro SIRET ;
- ✓ Extrait du registre du commerce où la société est enregistrée ;
- ✓ Fiche individuelle d'état civil et de nationalité de chaque associé ;
- ✓ Composition et répartition des parts sociales de la société ;

- Si l'organisme est une entreprise individuelle :
  - ✓ Nom, dénomination ;
  - ✓ Fiche individuelle d'état civil et de nationalité de l'entrepreneur ;
  - ✓ Adresse et numéro de téléphone ;
  - ✓ Numéro SIRET ;
  - ✓ Extrait du registre du commerce où l'entreprise est enregistrée ;
- Si l'organisme est une entité administrative :
  - ✓ Nom ;
  - ✓ Adresse ;
  - ✓ Numéro de téléphone ;
  - ✓ Référence des textes portant création de l'organisme ;

L'AE journalise les caractéristiques et les références des documents présentés par le signataire nécessaires à l'authentification et à la création de l'identité (Cf.§ 3.1.1) portée dans le certificat conformément au § 4.6.1 et aux recommandations de la CNIL.

Cette politique de certification ne prend pas en compte la gestion des certificats d'attribut.

La procédure de demande de renouvellement est identique à celle de la demande initiale définie dans ce paragraphe.

4.2 Génération de certificat

L'ARA ou le mandataire donne au PSC son acceptation sur les termes de la présente PC et de la DPC (qui est utilisé pour mettre en œuvre cette PC) qui lui incombent conformément au § 4.3.
L'AE authentifie conformément au § 3.1.8 et au § 3.1.9 une demande de certificat d'un signataire ou d'un mandataire renseigné suivant les conditions du § 4.1.
Si le signataire génère ses données de création et de vérification de signature électronique, alors l'AE doit s'assurer conformément au § 3.1.7 que le signataire détient la donnée de création de signature correspondant à la donnée de vérification qu'il remet conformément au § 6.1.3.

Le processus de génération de certificats est le suivant :

- L'AE transmet la demande de certificat à l'AC ;
- L'AC authentifie l'AE de manière à être sûre qu'elle est dûment autorisée à effectuer ce type d'opération et traite la demande de certificat ;
- Si l'AC génère les clés de signature du signataire, alors le processus de génération de certificat doit être lié de manière sécurisée au processus de génération de clé et effectué conformément au § 6.1.1.
- L'AC signe, à l'aide de sa clé privée, un certificat dont le contenu est défini au § 7.1 ;
- La génération de certificat s'effectue avec une ressource matérielle (Cf. 6.1.8) et dans ses locaux sécurisés conformément au § 5 ;
- L'AC transmet le certificat au signataire (Cf. § 6.1.2).
- Le signataire ou le mandataire notifie à l'AC s'il accepte ou non le certificat conformément au § 4.3 (acceptation du certificat) ;

- Si l'AC à généré les clés du signataire, alors elle remet aussi la clé privée au signataire conformément au § 6.1.4 ;
- Si l'ARA a donné son accord pour sa publication, l'AC transmet le certificat au SP qui, après avoir authentifié l'AC, publie le certificat du signataire.

L'ensemble des communications entre les différentes entités du PSC est protégé en confidentialité et en intégrité.

Au cours du processus de génération de certificat, le PSC doit mettre en œuvre un rapport facial entre le signataire et le PSC afin de s'assurer que l'ensemble des procédures de génération, de renouvellement de certificat, d'enregistrement et de génération des données de création et de vérification de signature électronique sont liés de sorte à garantir l'intégrité du lien entre le contenu du certificat, le signataire et sa donnée de création de signature électronique correspondant au certificat.

La procédure de régénération de certificat est identique à celle définie dans ce paragraphe. Elle implique la signature d'un nouveau contrat (Cf. § 4.3) incluant les modifications éventuelles et la révocation de l'ancien certificat. L'authentification de cette demande est effectuée par l'AE conformément aux § 3.2 et § 3.3.

4.3 Acceptation d'un certificat

Acceptation des termes entre l'AC et l'ARA :

A l'établissement de l'accord entre l'AC et l'ARA, l'ARA notifie à l'AC qu'il accepte les conditions de la PC et de la DPC en signant un accord (papier ou électronique) qui manifeste :

- Son adhésion aux conditions d'utilisation et de gestion par le PSC de son certificat et le cas échéant de ses données de création et de vérification de signature électronique conformément à cette PC.
- Son accord sur les conditions de publication ou non de son certificat (cf. § 2.6.1).
- l'accord du signataire sur la conservation des données qu'il fournit conformément au § 4.1 pour son enregistrement.
- Son consentement sur les obligations qui lui incombent.
- Son accord sur la communication par le PSC de l'ensemble des informations, liées au signataire et conservées par l'AE, à une tierce partie dans le cas de cessation d'activité sous les mêmes conditions définies dans la présente PC.
- Sa confirmation de l'exactitude des informations contenues dans le certificat.

Acceptation de certificat :

A la réception de son certificat le signataire notifie à l'AC qu'il accepte son certificat en signant un accord (papier ou électronique) contenant son consentement sur le contenu du certificat. L'ensemble des acceptations définies ci-dessus peuvent être demandées de manière séparée au cours de la mise en œuvre de la procédure de génération du certificat du signataire défini au § 4.2.

Le PSC archive ces données conformément au § 4.6.1.

4.4 Suspension, révocation, expiration de certificat

4.4.1 Causes de révocation

Les causes de révocation pour un signataire sont les suivantes :

- Changement d'informations contenues dans le certificat.
- Compromission, suspicion de compromission, vol ou perte de la clé privée.
- Compromission, suspicion de compromission du certificat du signataire.
- Cessation du liant entre le porteur et l'identité morale le supportant.
- Décès du porteur, perte du droit de signature pour raison légale ou cessation d'activité de l'organisme porteur du certificat.
- Non-respect du contrat ou de la convention liant un signataire au PSC.
- Révocation du certificat de l'AC émettrice du certificat.

Les causes de révocations pour une AC sont les suivantes :

- Décision suite à un contrôle de conformité.
- Non-respect de la politique de certification et de la déclaration des pratiques de certification par l'AC.
- Cessation d'activité de l'AC.
- Compromission, suspicion de compromission de certificat de l'AC.
- Compromission, suspicion de compromission, vol, perte de la clé privée d'une AC.
- Compromission de clé publique d'une AC.

4.4.2 Qui peut demander une révocation ?

Les personnes pouvant demander une révocation sont :

- Le signataire pour son certificat ;
- Les personnes désignées par l'ARA à cet effet dans son dossier d'enregistrement cf. § 4.1 ;
- L'ARA qui est en relation contractuelle avec l'AC ;
- Le mandataire ;
- L'AC peut demander la révocation d'une de ses entités (si cela s'applique).

4.4.3 Procédure de demande de révocation

La procédure de révocation se déroule comme suit :

- L'AE authentifie conformément au § 3.4 une demande de révocation de la part d'une personne autorisée (Cf. au § 4.4.2) et contrôle la cause de la demande conformément au § 4.4.1. L'AE définit les modalités de confirmation d'une demande ou d'un rapport de révocation. Les demandes de révocation doivent être traitées à la réception de la demande par l'AE.
- L'AE transmet la demande à l'AC.
- L'AC authentifie l'AE de manière à être sure qu'elle est dûment autorisée à effectuer ce type d'opération et traite la demande de révocation.
- L'AC révoque le certificat. Lorsque la suspension est utilisée dans la procédure de révocation, alors le certificat est suspendu pendant la vérification de la demande de révocation. A cette occasion une confirmation peut être demandée au signataire ou au mandataire si la demande a été effectuée par un tiers autorisé.
- L'AC génère une nouvelle CRL ou une delta CRL de telle sorte à garantir son intégrité et son authenticité (signé par l'AC ou par une autorité désignée par l'AC).
- L'AC transmet la liste des certificats révoqués au SP.

L'ensemble des communications entre les différentes entités du PSC est protégé en confidentialité et en intégrité.

La CRL n'est pas le seul moyen que peut utiliser l'AC pour révoquer un certificat de signataire.
Le temps de traitement de la révocation s'effectue dans un délai conforme au § 4.4.4.

Le signataire dont le certificat est révoqué et l'ARA doit être informé du nouveau statut de son certificat par le PSC.
Une fois que le certificat est révoqué, il ne peut être réutilisé, la révocation est définitive.

4.4.4 Temps de traitement d'une révocation

Le temps de traitement des demandes de révocation à partir de la réception de la demande par l'AE s'effectue dans un délai de VAR_TEMPS : :T_REVOC (au maximum 1 jour).

Le service de révocation doit être disponible 24/24 et 7/7. Dans le cas d'une défaillance matérielle ou autre, en dehors des limites de responsabilité, le PSC devra prendre les mesures nécessaires au rétablissement du service de révocation dans un temps d'indisponibilité inférieur à celui défini dans la DPC.

4.4.5 Causes possibles de suspension

Les causes de suspensions du certificat d'un signataire :

- Pendant la période de vérification de la révocation.
- La DPC devra préciser les autres causes de suspension.

4.4.6 Qui peut demander une suspension ?

Les personnes pouvant demander une suspension sont :

- Le signataire pour son certificat,
- Les personnes désignées par le signataire à cet effet dans son dossier d'enregistrement cf. § 4.1.
- L'AC peut demander la révocation d'une de ses entités (si cela s'applique).

4.4.7 Procédure de demande de suspension

Soit la suspension est utilisée lors de la procédure de révocation, alors Cf. § 4.4.3, soit elle est utilisée pour des raisons autres et dans ce cas la procédure est identique ou apporte un degré d'assurance équivalent à celle définie au § 4.4.3.

4.4.8 Limites d'une période de suspension

Si un certificat est suspendu avant d'être révoqué, cette durée ne doit pas excéder le temps nécessaire pour confirmer la révocation.

4.4.9 Fréquence de la mise à jour de la liste des certificats révoqués

Les délais de mise à jour des listes de certificats révoqués, VAR_TEMPS : :F_MAJ_CRL, s'effectue au plus en 24H. La variable VAR_TEMPS : : NEXT_CRL donne une date informative sur la date d'émission de la prochaine CRL.

La modification des informations de révocation est soumise à contrôle d'accès, elle donne lieu à l'émission d'une trace imputable et opposable, donc signée.

Quand elles sont utilisées, les CRL doivent :

- Contenir la date de la prochaine CRL.
- Une nouvelle CRL peut être publiée avant la date de la prochaine CRL.
- Etre signées par l'AC ou par une autorité désignée par l'AC.

Les listes de révocation publiées doivent :

- Etre renouvelées au moins tous les jours.
- Préciser une date pour la CRL suivante et émettre une autre CRL avant cette date.

Les informations liées au statut de révocation doivent être publiques et internationalement accessibles.

4.4.10 Exigences de contrôle des listes de certificats révoqués

Dès la réception d'un message signé ou avant l'envoi d'un message chiffré, il appartient au signataire de vérifier le statut du certificat dans la CRL. De même, il lui appartient de vérifier la validité de la CRL (signature et validité de l'émetteur de la CRL).

4.4.11 Publication des causes de révocation

Les causes de révocation d'un certificat peuvent apparaître dans la CRL conformément aux exigences du § 2.8.3.

La divulgation des causes de révocation et de suspension des certificats est effectuée suite à un accord du signataire.

4.4.12 Contrôle en ligne des listes de certificats révoqués

L'information consistant à savoir si un certificat a un statut révoqué ou non doit être disponible 24h/24h et 7j/7j, VAR_TEMPS : :T_DISPO_PUB , être public et disponible de façon internationale.

Dans le cas d'une défaillance matérielle ou autre, dans les limites de responsabilité du PSC, ce dernier devra prendre les mesures nécessaires au rétablissement du service de révocation dans un temps d'indisponibilité inférieur à celui défini dans la DPC.

Le SP rend publiquement accessible l'information de révocation ou la délivre sur demande.

4.4.13 Autres formes de publication de listes de certificats révoqués

D'autres formes de publication que celle proposée par le SP peuvent compléter le service de base du PSC (copie de la liste des CRL au niveau de l'AC ou de l'AE, mise à disposition d'un standard téléphonique, etc.). Pour la publication de l'information relative à la révocation d'un certificat, il est possible d'utiliser un service en ligne de divulgation d'information relative à la révocation (par exemple OCSP).
Les exigences relatives aux autres formes de publication sont identiques à celles définies pour la gestion de la CRL (Cf. § 4.4.12 pour VAR_TEMPS : :F_MAJ_CRL_BIS).

4.4.14 Contrôle en ligne des autres formes de listes de certificats révoqués

Les exigences sont identiques à celles définies au § 4.4.12.

4.4.15 Besoins spécifiques en cas de révocation pour compromission

En cas de révocation pour compromission ou suspicion de compromission de clé, la mise à jour de la CRL doit être réalisée selon la politique exprimée en 4.4.3. Cependant, des mesures particulières peuvent être prises. En cas de révocation pour cause de compromission de clé, il sera indiqué à l'autorité chargée de la révocation la date à laquelle l'on suppose que la compromission a eu lieu. VAR_TEMPS : :T_INVALID.

4.5 Audit sécurité

4.5.1 Types d'événements enregistrés

Les données enregistrées sont :

❖ Informations minimales pour tout événement :

- Date et heure de l'opération
- Destinataire de l'opération
- Nom de l'exécutant
- Nom des personnes présentes
- Nom du signataire ou du mandataire de l'opération
- Résultat de l'événement
- Type de l'opération
- Cause de l'événement

❖ Événements physiques dont la trace n'est pas fournie automatiquement par le système.

- Autres registres dépendant de la configuration du site physique, à préciser dans la DPC tels que:
  - ✓ journaux des accès des personnes,
  - ✓ changements concernant les personnes,
  - ✓ changement de configuration du système,
- Registre des accès physiques aux postes de travail du PSC

❖ Opérations menées sur les postes informatiques du PSC et relatives aux opérations rendues par le PSC

- Informations communes :
  - ✓ Démarrage et arrêt de l'application
  - ✓ Changements de mots de passe
  - ✓ Création et transmission de récépissés
  - ✓ Modification de paramètres de configuration de l'outil de certification
  - ✓ Modifications de droits d'accès
  - ✓ Remise à zéro du journal d'audit
  - ✓ Suspension ou révocation de certificat
  - ✓ Communications avec le service de publication

- Enregistrement :
  - ✓ Enregistrement d'un nouvel utilisateur (dans la base de données interne)
  - ✓ Éventuellement demande de renouvellement

- Génération de certificat :
  - ✓ Destruction de secrets

- ✓ Génération de certificat de l'AC et des signataires
- ✓ Génération des données de création et de vérification de l'AC

- Révocation de certificat :
  - ✓ Demande de révocation
  - ✓ Rapport de révocation

- Si l'AC génère les données de création et de vérification de signature électronique :
  - ✓ Demande de génération des données de création et de vérification de signature électronique
  - ✓ Génération des données de création et de vérification de signature électronique
  - ✓ Conservation des données de création et de vérification de signature électronique
  - ✓ Transmission des données de création et de vérification de signature électronique

❖ Opérations menées sur les postes informatiques et matériels du réseau du PSC

- Cf. §6.5.1

4.5.2 Fréquence de traitement des journaux d'événement

L'analyse du contenu des journaux d'événements doit être effectuée de manière régulière VAR_TEMPS : :F_JOURNX).

4.5.3 Durée de rétention d'un journal d'événements

Les journaux sont archivés et répondent donc aux spécifications exprimées en 4.6.2.

4.5.4 Protection d'un journal d'événements

Les journaux d'événements doivent être protégés en intégrité, contre la perte, la destruction et la falsification et le système de datage des événements sur le poste de travail est sûr et non modifiable. La définition de la sensibilité des journaux d'événements (sensible ou classifié) dépend de la nature des informations traitées et du métier et est définie au § 2.8.1. Elle peut entraîner un besoin de protection en confidentialité.

4.5.5 Copie de sauvegarde des journaux d'événements

Une copie de sauvegarde des journaux d'événements est réalisée, elle doit être protégée au même niveau que les originaux (4.5.4.).

4.5.6 Système de collecte des journaux (interne ou externe)

Le système de collecte des journaux peut être interne ou externe à l'AC. Il doit se déclencher au démarrage du système informatique et rester actif jusqu'à son extinction. Le contournement du processus de journalisation est impossible.

4.5.7 Imputabilité

L'imputabilité d'une action revient à la personne, l'organisme ou le système l'ayant exécutée et dont le nom figure dans le champ "nom de l'exécutant" du journal d'événements.

4.5.8 Analyse des vulnérabilités

Une procédure interne d'analyse du contenu des journaux d'événements doit permettre de détecter les vulnérabilités du système et prévenir les attaques potentielles sur le système. Cette procédure doit

figurer dans la DPC du PSC. L'AC est informée mensuellement des anomalies détectées. En cas d'anomalie critique, elle est avisée immédiatement.

4.6 Archives

4.6.1 Types de données à archiver

L'AC archive toutes les données qui pourraient être utiles à la preuve de la certification d'un signataire. Ces données à archiver, et documenter, sont les suivantes :

- Accords contractuels ou conventions avec d'autre PSC
- Certificats du signataire et de composantes
- CRL
- Demandes de révocation et leurs résultats
- Données d'identifications personnelles du signataire (y compris quand cela est utilisé le lien entre un signataire et son certificat qualifié) dont le numéro de référence et les limitations de validité et d'usage des pièces d'identité officielles utilisées lors de l'enregistrement.
- Journaux d'événements des entités du PSC en relation avec les opérations propres aux certificats et le cas échant aux données de création et de vérification de signature électronique.
- Logiciels et fichiers de configuration des différentes composantes
- Récépissés des communications internes et externes au PSC
- Ensemble de tous les éléments utiles à l'enregistrement d'un signataire demandé dans la demande de certificat (Cf. 4.1) et pour son authentification (Cf. § 3.1.8 et § 3.1.9).
- Nature des documents présentés par le signataire, le mandataire et l'ARA.
- Emplacement où sont conservées les copies des formulaires remplis par le signataire ou mandataire, y compris le document manifestant l'acceptation (Cf. § 4.3) de l'ARA aux conditions d'utilisation et au contenu du certificat (Cf. § 4.3).
- Identité de la personne morale au nom de laquelle a lieu la demande (Cf. § 3.1.8).
- Méthode utilisée pour valider les documents d'identité (Cf. DPC).

4.6.2 Période de rétention des archives

Elle résulte d'un compromis entre le besoin et les contraintes de moyens de conservation. La durée de conservation des informations relatives à l'authentification du signataire dépend des obligations légales de conservation de preuves pour les transactions sécurisées à l'aide du certificat qualifié du signataire et de besoins pour faire la preuve de l'authentification du signataire. Dans la plupart des cas, des clauses limitant la période de contestation possible de la transaction sont susceptibles de déterminer la durée minimale de conservation des informations.
La DPC contient la liste des durées de conservation pour chacune des informations listées au § 4.6.1 VAR_TEMPS : :T_ARCHIVES.

4.6.3 Protection des archives

Les archives doivent être protégées en intégrité et en disponibilité, (la disponibilité doit permettre de réaliser la condition T_RECUP_ARCH). La définition de la sensibilité des journaux d'événements (sensible ou classifié) dépend de la nature des informations traitées et du métier. Elle doit être définie au cas par cas. Elle peut causer un besoin de protection en confidentialité.

4.6.4 Procédure de copie des archives

Pas de spécification.

4.6.5 Besoin d'horodatage des enregistrements

Il est recommandé que l'AC définisse dans sa DPC la précision de l'horloge pour dater les évènements enregistrés et archivés (Cf. § 4.5.1 et 4.6.1) et comment elle atteint cette précision.

4.6.6 Système de collecte des archives

Cf. DPC.

4.6.7 Procédure de récupération des archives

Une composante ne peut récupérer et consulter que ses propres archives. Le processus de récupération doit faire l'objet d'une procédure interne de fonctionnement ou doit figurer dans la DPC de la composante. La récupération doit être effectuée sous un délai minimal VAR_TEMPS : : T_RECUP_ARCH.

4.7 Changement de clé d'une composante

Lorsqu'une composante renouvelle ses clés, elle en informe ses utilisateurs, selon le besoin d'en connaître, ainsi que l'AC du PSC, sous une période minimale donnée VAR_TEMPS : :T_CHG_KEY. Selon la nature du changement (fin de période de validité de clés, renouvellement de clé suite à une révocation, etc.), les mesures prises doivent respecter les procédures de traitement énoncées dans les chapitres correspondants (§4.2, 3.2, 3.3).

4.8 Compromission et plan anti-sinistre

La DPC doit contenir une référence à un plan de continuité qui contient un plan anti-sinistre, spécifié dans une politique de sécurité de chacune des entités du PSC, qui permet de s'assurer contre toute perte, dommage ou compromission des biens du PSC ainsi que contre toute interruption de service. Cette référence indique ses modalités de déclenchement, de création de rapports d'incidents et les personnes responsables de ce plan doivent être indiquées dans la DPC. Ce plan doit être régulièrement testé. VAR_TEMPS : : F_TEST_PLAN.

Ce plan de continuité permet de garantir une disponibilité, avec les mêmes contraintes d'origines définies dans la présente PC, pour les services suivants :

- Publication des certificats en cours de validité,
- Révocation des certificats (génération et diffusion de l'information de révocation)

Le PSC met en œuvre les mesures nécessaires permettant d'éviter toute compromission ou vol des informations ou des matériels qu'il détient ainsi que la continuité de la protection des infrastructures physiques pour les opérations de génération de certificat, préparation du DSCS du signataire et de révocation.

Le PSC dispose d'un plan de reprise d'activité en cas de sinistre qui prend en compte les paramètres suivants :

- Délai minimum de recouvrement de ses services
- Mise en service d'un site miroir (optionnel)
- Politique de sécurité et de protection des secrets
- Procédures de secours
- Tests pratiques, formation et entraînement des personnels

4.8.1 En cas de corruption des ressources informatiques, logicielles et/ou informatiques

En cas de corruption des ressources informatiques, logicielles et/ou données se référer au plan anti-sinistre. (cf. 4.8).

4.8.2 En cas de révocation de la clé publique d'une composante du PSC

La révocation de la clé publique d'une composante doit être géré dans le cadre de la fin de vie de cette composante (cf. § 4.8.3).

4.8.3 En cas de compromission de clé d'une composante du PSC

En cas de révocation d'un certificat d'une composante pour compromission ou suspicion de compromission de données de création de signature électronique :

- Informer de la compromission de ses données l'ARA et les vérificateurs, de même que les PSC avec lesquels elle est liée par contrat ou toute autre forme de relation établie.
- Informer que les certificats et les informations relatifs à la révocation des certificats signés avec les données de création de signature électronique compromises peuvent ne plus être valides. Les certificats qu'elle a émis au moins depuis la date de connaissance de la compromission de ses données de création de signature électronique, sont révoqués.
- Lorsque l'AC est informée de la compromission des données de création de signature d'un autre PSC, avec lequel des accords ou des conventions existent, elle révoque sans délai tout certificat émis pour ce PSC suivant les clauses contractuelles les liants.

L'AC propose un contrôle et prononce la remise en service de la composante avec de nouvelles données de création de signature électronique.

4.8.4 Mesures de sécurité en cas de sinistre

Cette rubrique doit être renseignée et apparaître dans le plan anti-sinistre du PSC (cf. § 4.8).

4.9 Fin de vie d'une composante

Avant toute cessation d'activité du PSC, les actions suivantes doivent au minimum être mises en oeuvre :

- Communiquer son intention de cessation d'activité conformément VAR_TEMPS : :T_FIN_VIE aux signataires, vérificateurs et PSC avec lesquels l'AC est liée par accord ou convention ou par toutes autres formes contractuelles. Pour sa diffusion d'information, l'AC n'est pas tenue d'avoir eu des relations avec les vérificateurs.
- L'AC s'assure que le préjudice engendré par la cessation d'activité est aussi réduit que possible pour les signataires et les vérificateurs.
- L'AC retire toutes autorisations aux entités externalisées supportant des opérations du PSC en relation avec la gestion des certificats.
- L'AC doit prendre les dispositions nécessaires afin de transférer ses obligations et ses limites de responsabilité en terme de conservation (Cf. § 4.6) des informations d'enregistrements, de journalisation des évènements (Cf. § 4.5) et ce pour une durée, définie dans la DPC, garantie aux signataires et aux vérificateurs.
- L'AC détruit, ou archive conformément au § 6.2.5, ses données de création de signature électronique conformément au § 6.2.9.

- L'AC doit prendre les dispositions nécessaires pour débloquer, si nécessaire en cas de faillite ou par incapacité propre, la provision budgétaire prévue pour lui permettre de réaliser les opérations de transfert nécessaires.
- L'AC précise les mesures à prendre en prévision de sa cessation éventuelle d'activité dans la DPC qui inclut :

  - ✓ La désignation des entités concernées.
  - ✓ Le transfert d'obligation et de limites de responsabilités.
  - ✓ Le traitement de l'information relative à la révocation des certificats non expirés à la date de cessation d'activité.

Note :

Les opérations suivantes peuvent également être mises en œuvre :

- En cas de fin de vie d'une AC
  - ✓ Faire révoquer son certificat par une autorité de certification supérieure (en tenant compte des spécifications du § 4.4.15)
  - ✓ Révoquer les certificats valides qu'elle a signés, uniquement pour une fin de vie due à une compromission ou suspicion de compromission de clé, une perte ou un vol (en tenant compte des spécification du § 4.4.15)
- Une entité qui cesse son activité remet ses archives à l'AC.

5 Contrôles de sécurité physique, des procédures et du personnel

5.1 Contrôles physiques

5.1.1 Situation géographique et construction des sites

La situation géographique et la construction des sites qui hébergent l'ensemble des services du PSC sont définies en fonction des objectifs de l'analyse de risques menée sur le PSC. Tous les autres services supportés par l'AC en relation avec la certification ou la validation sont aussi à sécuriser avec le même degré d'assurance. Les exigences qui couvrent les objectifs de sécurité de l'analyse de risque sont déclinées dans les § 5.1 et 4.8.

5.1.2 Accès physique

L'accès physique à une composante et aux ressources du PSC est protégé contre toutes personnes non autorisées de manière à détecter, enregistrer et réagir à ces intrusions. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. Le contrôle d'accès est nominatif et s'effectue sur autorisation pour les installations utiles à la génération de certificat, des données de création et de vérification de signature électronique et des codes d'activation associés si besoin est, et la gestion des révocations.
Chaque entité définit un périmètre de sécurité dédié à l'accueil des installations et des informations utiles aux services qu'elle supporte afin de se protéger contre leur vol, leur destruction, leur usurpation, leur sortie non-autorisées et leur altération. Lorsqu'une entité du PSC partage une partie de ses locaux avec un autre organisme, les locaux communs doivent être exclus du périmètre de sécurité.

5.1.3 Électricité et air conditionné

La prévention physique contre des incidents matériels est effectuée en accord avec les recommandations des constructeurs de matériels. Cette spécification doit être complétée au niveau de la DPC du PSC et adaptée à l'environnement physique de chaque entité.

5.1.4 Exposition à l'eau

La prévention physique contre le dégât des eaux est effectuée en accord avec la politique de sécurité de la composante. Cette spécification doit être complétée au niveau de la DPC du PSC et adaptée à l'environnement physique de chaque entité.

5.1.5 Prévention et protection contre le feu

La prévention physique contre l'incendie est effectuée en accord avec la politique de sécurité de l'entité. Cette spécification doit être complétée au niveau de la DPC du PSC et adaptée à l'environnement physique de chaque entité.

5.1.6 Conservation des supports de données

Les supports sont conservés dans des enceintes sécurisées (coffres-forts, etc.) dont l'accès est contrôlé.

5.1.7 Traitement des déchets

Les entités du PSC utilisent des mécanismes de destruction des supports, en fonction de la classification des informations, papiers (tels que des broyeurs) et des supports magnétiques

(incinération). La réforme des matériels ayant appartenu à la plate-forme du PSC au préalable assure la non ré-utilisabilité des informations qu'il contient (chiffrement de l'ensemble du disque dur, autres).

5.1.8 Site de secours

Le plan anti-sinistre, décrit en 4.8 définit l'existence et la gestion du site de secours, si besoin est, pour assurer la continuité des opérations.

5.2 Contrôle des procédures

5.2.1 Rôles de confiance

L'annexe « Rôles » précise comment et sous quelles conditions ces rôles peuvent être cumulés par un même exploitant. Afin de veiller à la séparation des tâches critiques, on distingue quatre rôles au sein des composantes du PSC. Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où cela ne dégrade pas la sécurité des services offerts.

5.2.2 Nombre de personnes nécessaires à chaque tâche

Les opérations associées à chaque composante du PSC sont données dans le § 1.3.1 de cette PC. Selon le type d'opérations supporté, le nombre et le type de rôles et de personnes devant nécessairement être présentes (en tant qu'acteurs ou témoins) peut être différent. L'annexe "Rôles par opérations" de la DPC permet de définir un nombre d'exploitants minimum nécessaire par type d'opérations. De même, la DPC devra préciser la répartition des obligations incombant à chacune des entités sur chacun des rôles.

Pour la génération de certificat et la révocation le PSC sépare ses opérations de sécurité des opérations normales. Les tâches effectuées dans le cadre des opérations de sécurité doivent inclure :

- Les procédures et les obligations opérationnelles ;
- La prévision de charge et la tolérance des systèmes sécurisés ;
- La protection contre les virus et autre logiciel compromettant ou non-autorisé ;
- L'entretien à l'intérieur du périmètre de sécurité ;
- La gestion de réseau ;
- La collecte et le traitement des journaux et des archives permettant l'audit et l'analyse des évènements ;
- La manipulation et la sécurité des informations et des biens ;
- La communication de données et de logiciels.

Ces tâches doivent être effectuées dans le cadre des opérations de sécurité mais peuvent être menées à bien par du personnel non spécialisé à condition que ce personnel soit supervisé conformément au § 5.1.2 et au § 5.2.3.

5.2.3 Identification et authentification des rôles

Chaque entité du PSC met en place une gestion des droits d'accès pour identifier et authentifier son personnel réalisant une action en fonction d'un rôle, Cf. § 5.2.1, ayant trait à la gestion d'un certificat, (Cf. § 5.2.2). Cette gestion des droits est réalisée par des mécanismes de sécurité permettant de séparer les différentes fonctions de confiance identifiées aux § 5.2.1 et § 5.2.2 (y compris la séparation entre les opérations courantes et l'administration de la sécurité) suivant les objectifs de sécurité définis au § 6.5.1.

5.3 Contrôle du personnel

5.3.1 Compétences, qualification et antécédents requis

Tous les personnels du PSC signent une clause de confidentialité avec leur employeur. Le nom et la fonction de tous les employés doivent être explicitement précisés dans la DPC. Les composantes s'engagent à ce que les compétences professionnelles de leurs personnels correspondent à leurs attributions. L'honnêteté des personnels du PSC doit être prouvée conformément au § 5.3.2. Pour cela, le PSC s'engage à mettre en œuvre tous les moyens légaux dont elle dispose.
Le personnel d'encadrement possède l'expertise appropriée à son rôle et est familier aux procédures de sécurité en vigueur au sein du PSC.

5.3.2 Procédures préalables de contrôle

Les personnels du PSC ne doivent pas avoir fait l'objet de condamnation en contradiction avec leurs attributions. Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflits d'intérêts préjudiciables à l'impartialité des opérations au sein de chacune des composantes.

5.3.3 Exigences de formation initiale

Le personnel doit être formé aux logiciels, matériels et procédures internes de fonctionnement de la composante pour laquelle il opère. Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité. Pour ce faire, l'AC formalise des documents spécifiant les rôles et responsabilités du personnel.

5.3.4 Exigences et fréquences des formations

Tout nouvel employé suit une formation initiale au système, aux politiques de sécurité, au plan de secours, aux logiciels et opérations qu'il met en œuvre. Chaque employé devra assister à une formation après toute évolution importante du système, de l'organisation, des outils, des procédures.. VAR_TEMPS : : F_TEST_FORM.

5.3.5 Gestion des métiers

En terme de gestion de carrière pour un exploitant donné, les règles à appliquer sont celles pratiquées par l'organisme employeur. Un personnel identifié de la direction du PSC ou de chacune des entités du PSC à la charge de nommer les personnels autorisés à exercer une fonction de confiance. Tous les personnels du PSC qui occupent un poste de travail, identifié comme « sensible » par l'analyse de risque de l'AC, signent une clause de confidentialité avec l'AC.

5.3.6 Sanctions pour des actions non-autorisées

Le responsable de sécurité de l'entité propose à l'autorité administrative les sanctions à appliquer lorsqu'une personne abuse de ses droits ou effectue une opération non conforme à ses attributions. La gravité de la sanction dépendra de la gravité de la faute.

5.3.7 Contrôle du personnel contractant

Les personnels contractants doivent respecter les mêmes conditions que celles énoncées dans les rubriques 5.3.1, 5.3.2, 5.3.3 et 5.3.4.

5.3.8 Documentation fournie au personnel

Les documents dont doit disposer le personnel sont les suivants :

- Déclaration des Pratiques de Certification propre au domaine de certification
- Documents constructeurs des matériels et logiciels utilisés
- Politiques de certification supportée par la composante à laquelle il appartient
- Procédures internes de fonctionnement

Les informations ci-dessus sont délivrées aux personnels en fonction du besoin d'en connaître.

6 Contrôles techniques de sécurité

6.1 Génération et installation de biclé

6.1.1 Génération de biclé

L'AC génère et utilise sa biclé de signature dans un module cryptographique qui est évalué conformément au § 6.1.8 en respectant les exigences de protection physique et les spécifications sur les rôles à mettre en œuvre pour l'initialisation de l'AC (Cf. § 5.2.2).

Si le PSC génère les données du signataire, alors il procède en respectant les conditions de génération des données de création et de vérification de signature électronique dans un module cryptographique qui est évalué conformément au § 6.1.8 en respectant les exigences de protection physique et les spécifications sur les rôles à mettre en œuvre pour l'initialisation de l'AC (Cf. § 5.2.2).

Si le signataire génère sa biclé, alors il procède à l'aide d'un module cryptographique évalué et certifié qui respecte les conditions définis au § 6.1.8.

6.1.2 Délivrance de la clé privée à un signataire ou à une composante du PSC

La délivrance s'effectue de manière à garantir la confidentialité et l'intégrité de la donnée de création de signature électronique et à ne la délivrer qu'au signataire concerné. La remise de la clé privée doit être séparée dans le temps ou dans l'espace de la remise de la donnée d'activation associée. Les données de création et de vérification de signature électronique sont conservées de telles sorte à garantir leur confidentialité et leur intégrité avant d'être délivrées au signataire.

6.1.3 Délivrance de clé publique à une AC

La délivrance de la donnée de vérification de signature d'un signataire à l'AC s'effectue de telle sorte à garantir l'intégrité de bout en bout et à en authentifier l'origine.
Le signataire fournit la preuve de la possession de la clé privée à l'AC lors de l'enregistrement (cf. §3.1.7).

6.1.4 Délivrance de la clé publique d'une AC aux utilisateurs

La délivrance de la donnée de vérification de signature d'une AC à ses partenaires (signataire, vérificateur, …) s'effectue de telle sorte à garantir l'intégrité de bout en bout et à en authentifier l'origine (la clé publique de l'AC peut par exemple être contenue dans le dispositif de vérification de l'utilisateur de certificat).

Le certificat de l'AC ne peut être considéré à lui seul comme un élément de confiance, il doit :

- Soit être signé par une autre autorité ;
- Soit être accompagné d'une déclaration signalant qu'il s'agit de la bonne clé publique ;
- Soit par la délivrance, cf. § 2.6.1, d'un condensat par une source de confiance.

6.1.5 Taille des clés

L'entité (signataire ou composante du PSC) qui génère les données de création et de vérification de signature électronique utilise une taille de clé et un algorithme qui sont au minimum conformes au

guide de l'EESSI sur les algorithmes recommandés pour la signature électronique sécurisée [SR 002 176].

6.1.6 Génération des paramètres de clé publique

L'entité (signataire ou composante du PSC) qui génère les données de création de signature électronique génère au cours du même processus les données de vérifications de signatures électroniques.

6.1.7 Contrôle de la qualité des paramètres

L'entité (signataire ou composante du PSC) qui génère les données de création et de vérification de signature électronique s'assure qu'elles remplissent les conditions énoncées dans le guide de l'EESSI sur les algorithmes recommandés pour la signature électronique sécurisée [SR 002 176].

6.1.8 Mode de génération de clé

Pour l'AC, la génération, l'utilisation et le stockage des clés de l'autorité de certification utilisées pour signer les certificats et signer les informations d'état de révocation des certificats doivent être effectués au sein d'un module cryptographique sécurisé qui doit être conforme aux exigences de l'annexe de l'arrêté du [à compléter]. Pour l'AC, la ressource cryptographique pour la signature de certificat est matérielle.

Par ailleurs, si le prestataire de service de certification génère les clés du signataire, le module cryptographique utilisé pour cette fonction doit être certifié conforme aux exigences définies à l'article 3.I du décret 2001-272 pour cette fonction, tel que spécifié dans la procédure [SIG/P/01.1].

Si le signataire génère sa biclé, alors il procède à l'aide d'un DSCS évalué et certifié conformément à la procédure [SIG/P/01.1].

6.1.9 Usages de la clé

L'AC s'engage et s'assure que ses données de création de signature électronique ne peuvent être utilisées qu'à des fins de signature de certificat de signataire et de CRL.
L'utilisation de l'extension « Key usage » du certificat de l'AC et des certificats de signataire doit être conforme aux exigences du document de l'ETSI [TS 101 862].
L'utilisation de l'extension « Key usage » du certificat du signataire doit prendre la valeur « non-répudiation ».

6.2 Protection de clé privée

6.2.1 Module de cryptographie utilisant des normes

L'entité (signataire ou composante du PSC) qui génère les données de création et de vérification de signature électronique respecte les conditions de génération des clés de signature afin d'être conforme au guide de l'EESSI sur les algorithmes recommandés pour la signature électronique sécurisée [SR 002 176].

6.2.2 Contrôle de clé privée par plusieurs personnes

Le contrôle de la donnée de création de signature électronique de l'AC par plusieurs personnes (systèmes où n exploitants parmi m doivent signer) doit être utilisé, conformément aux spécifications

du § 5.2.2 (Annexe "Rôles par opérations") sur le nombre de personnes devant approuver une action. Trois rôles minimums sont requis pour le contrôle de la clé privée de signature.

6.2.3 Séquestre de clé privée

En aucun cas, les données de création de signature électronique des signataires et des entités du PSC ne doivent être séquestrées par le PSC.

6.2.4 Copie de secours de clé privée

Les copies de secours de clés privées de signature de l'AC sont protégées avec un niveau de sécurité aussi important que les clés en usages conformément aux § 6.1.1, § 6.2.2 et § 6.2.7.
Après la période de fin de validité, toutes les copies de la donnée de création de signature électronique de l'AC doivent être détruites conformément au § 6.2.9.
En aucun cas, les données de création de signature électronique des signataires et des entités du PSC ne doivent faire l'objet de copie de secours par le PSC.

6.2.5 Archivage de clé privée

Après la période de fin de validité de données de création de signature électronique de l'AC sont archivées de telle sorte qu'elles ne puissent plus être réutilisées qu'à des fins de preuve.
Quand les clés de l'AC sont contenues dans une ressource matérielle dédiée, un contrôle d'accès doit exister pour interdire l'export des clés en dehors du dispositif.
En aucun cas, les données de création de signature électronique des signataires et des entités du PSC ne doivent être archivées par le PSC.

6.2.6 Mise à la clé du module cryptographique

Lorsque la donnée de création de signature de l'AC est en dehors du dispositif de création de signature de l'AC, elle doit être protégée à un niveau au moins équivalent à celui dont elle dispose lorsqu'elle est contenue dans le dispositif de création de signature.
Lorsque l'AC génère la biclé du signataire, la préparation et la réactivation du DSCS du signataire est contrôlée par l'AC de manière à en garantir l'intégrité et la confidentialité par l'AC afin d'éviter toute forme de compromission et d'en garantir la seule connaissance au signataire.

6.2.7 Méthode d'activation de clé privée

L'activation du module cryptographique de l'AC de signature des certificats requiert la présence de deux rôles de confiance, détenant chacun une clé privée valide, conformément aux spécifications du chapitre "Rôles par opérations" sur le nombre de personnes devant approuver une action.

6.2.8 Méthode de désactivation de clé privée

La désactivation de la donnée de création de signature s'effectue à la déconnexion de l'utilisateur ou après une certaine période d'inactivité. Elle dépend aussi du fonctionnement du module cryptographique (qui peut lui aussi désactiver la clé privée dans certains cas particuliers). Après sa désactivation, le module cryptographique doit être retiré et conservé dans un lieu protégé (coffre-fort, etc.).

6.2.9 Méthode de destruction de clé privée

La méthode de destruction des données de création de signature électronique de l'AC est une caractéristique propre à la ressource cryptographique de l'AC et doit être matérielle. Cette méthode doit garantir que ses données de création de signature électronique une fois détruites ne puissent plus être retrouvées.

6.3 Autres aspects de la gestion des biclés

6.3.1 Archivage des clés publiques

L'archivage des clés publiques revient à l'archivage des certificats. Ces derniers doivent être archivés et conservés pour une période donnée. VAR_TEMPS : :T_A_CERT.

6.3.2 Durée de vie des clés publiques et privées

La crypto période d'une clé privée doit être inférieure ou égale à la crypto période de la clé publique correspondante. De préférence, la période de validité du certificat de l'AC est plus longue que la période de validité des certificats émis VAR_TEMPS : :T_VALID_KPRIV, VAR_TEMPS : :T_VALID_KPUB. La période de validité d'une clé publique est limitée par la date d'expiration de l'habilitation de son porteur.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

L'entité (AC, AE ou signataire) qui génère le code d'activation procède de manière à garantir que seul l'utilisateur de la clé privée associée peut en avoir connaissance. Pour ce faire, il procède suivant les normes et standards en vigueur. La remise de la donnée d'activation doit être séparée dans le temps ou dans l'espace de la remise de la clé privée associée.

6.4.2 Protection des données d'activation

La donnée d'activation est une donnée secrète que le porteur protége en confidentialité et en intégrité. Lorsque le PSC génère la donnée d'activation du signataire, alors elle la protège en confidentialité et en intégrité jusqu'à sa distribution au signataire.

6.4.3 Autres aspects sur les données d'activation

L'utilisation de mots de passe requiert un contrôle de leur constitution (par exemple, longueur d'au moins 8 caractères, présence d'au moins un caractère spécial, etc.).

6.5 Contrôle de la sécurité des postes de travail du PSC

6.5.1 Besoins de sécurité spécifiques sur les postes de travail

Les besoins de sécurité suivants doivent permettre d'évaluer le niveau de sécurité des postes de travail des composantes du PSC :

- Journalisation (imputabilité et nature des actions effectuées) des évènements en fonction des rôles et des opérations
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur).
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapides des droits d'accès
- Identification et authentification des utilisateurs du poste de travail
- Protection contre les virus informatiques et toutes formes de logiciels compromettant ou non-autorisé et mise à jour des logiciels
- Protection des supports d'informations contre les dommages, le vol et la compromission même par réutilisation et l'usurpation

- Filtrage des entrées/sorties réseau
- Mise en gestion de la configuration du système d'information

6.5.2 Niveau de sécurité du poste de travail

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

6.6 Contrôle physique du système durant son cycle de vie

6.6.1 Contrôles des développements des systèmes

Le développement d'un système permettant de mettre en œuvre les entités du PSC doit utiliser une méthode éprouvée. Le PSC utilise des systèmes et des produits de confiance sécurisés et protégés contre toute modification non autorisée.
L'AC peut s'assurer que chacune de ses entités satisfait aux exigences de sécurité correspondantes en utilisant, par exemple, des systèmes et/ou des matériels conformes à un ou plusieurs profils de protection appropriés, définis dans le cadre de la norme ISO 15408 ou une norme équivalente.
Une analyse de risque doit être menée avant tout développement de système de façon à prendre en considération les objectifs de sécurité dès la phase de spécification.

6.6.2 Contrôles de la gestion de la sécurité

Toute évolution du système doit être autorisée par l'AC, documentée, doit apparaître dans les procédures de fonctionnement internes au PSC et être conforme au schéma de maintenance de l'assurance dans les produits évalués.

L'AC s'assure :

- Des procédures de contrôle portant sur les modifications (mise à jour, correction, patch,…) existent.
- Que la sécurité du dispositif matériel n'est pas altérée par un tiers ou de toute autre manière lors de son transport.
- Que 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.
- Que le dispositif matériel fonctionne correctement.
- Que la capacité de traitements et de stockage répond au besoin des signataires.
- De la montée en charge et du maintien du système à niveau.

6.7 Contrôles de sécurité réseau

L'interconnexion vers des réseaux publics doit être protégée (par exemple, par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein du PSC).
Le PSC protège les données sensibles (Cf. § 2.8.1), notamment les informations liées à l'enregistrement du signataire, lorsqu'elles sont communiquées par le biais d'un réseau non sécurisé.
La configuration des composants du réseau local sont l'objet d'audit régulier par le contrôleur (cf. § 5.2.1).

6.8 Contrôles techniques des modules de cryptographie

cf. 6.2.

7 Profils des certificats et listes de certificats révoqués

7.1 Profil du certificat

Les champs de base définis dans la recommandation X.509 v3 spécifiés dans le document ETSI TS 101 862 "Qualified certificate profile" et l'article 6.2 du décret 2001-272.

7.1.1 Numéro de version

Cf. 7.1.

7.1.2 Extensions de certificat

Le traitement des extensions suit les règles de l'annexe "Extensions" (pour le certificat).

7.1.3 Identificateurs d'algorithmes

Les identificateurs d'algorithmes doivent être inscrits auprès d'un registre.

7.1.4 Format de noms

Les noms doivent respecter les règles édictées au § 3.1.1.

7.1.5 Contrainte de noms

Cf. 7.1.

7.1.6 Identificateur de Politique de Certification

L'AC met l'OID de sa politique de certification dans son certificat.

7.1.7 Utilisation d'extension de contraintes sur les politiques

Cf. 7.1.

7.1.8 Syntaxes et sémantiques des qualificateurs de politiques

Cf. 7.1.

7.1.9 Règles de traitement de l'extension critique "Politique de Certification"

Cf. 7.1.

7.2 Profil des Listes de certificats révoqués

7.2.1 Numéro de version de liste de certificats révoqués

Les champs de base définis dans la recommandation X.509 v3 sont spécifiés dans le document ETSI TS 101 862 "Qualified certificate profile" et dans l'article 6.2 du décret 2001-272.

7.2.2 CRL et extension des CRL

Les champs de base définis dans la recommandation X.509 v3 spécifiés dans le document ETSI TS 101 862 "Qualified certificate profile" et l'article 6.2 du décret 2001-272.

8 Administration des spécifications

8.1 Procédure de modification de ces spécifications

L'AC doit prévenir les entités du PSC ainsi que l'ARA et le mandataire et les vérificateurs, de même que les PSC avec lesquels des accords de reconnaissance ont été conclus, des modifications qu'elle entend mener sur la PC et la DPC dés lors que celles-ci peuvent affecter ces accords ou le niveau de sécurité offert par le PSC. De plus l'AC doit faire approuver conformément au § 8.2 les évolutions de son référentiel de sécurité. Dés lors que l'AC est qualifiée, elle doit se conformer aux exigences des procédures de qualification (Cf. § 2.7) pour le maintien de sa qualification.

8.2 Politiques de publication et de notification

L'AC ne rend public que les détails de ses DPC aux signataires et/ou mandataire ou l'ARA et aux vérificateurs dans la mesure où ceux-ci servent à établir la conformité à la PC. De même l'AC diffuse l'information provenant de la PC et de la DPC aux personnels conformément au § 5.3.8. L'AC peut s'appuyer sur le SP qui doit mettre ces éléments à la disposition du mandataire et des signataires et des tiers utilisateurs, de même que toutes documentations pertinentes.

L'ensemble de ces informations est disponible dans un langage compréhensible par les signataires et les vérificateurs, peut être communiqué par exemple sous forme des conditions générales de services de l'AC (en anglais PDS PKI Disclosure Statement).
Si des informations doivent être publiées en dehors du périmètre du PSC, leur nature doit être spécifiée dans la DPC. Si des informations sensibles ou classifiées figurent dans la PC ou la DPC, elles peuvent être omises dans la version publiée des documents.

8.3 Procédures d'approbation des DPC

L'AC est responsable de l'adéquation des DPC avec la ou les PC supportées ainsi que de son implémentation correcte. Pour ce faire elle procède par un contrôle de conformité comme décrit au § 2.7.

9 Glossaire

Accord entre domaines
Accord portant sur les échanges entre deux domaines distincts. Les termes de l'accord portent sur l'interopérabilité des IGC et des applications communicantes.
Σ
Accord de reconnaissance entre IGC
Accord par lequel une IGC d'un domaine reconnaît la totalité ou une partie préalablement identifiée des certificats d'un autre domaine.
Σ
Accréditation
Autorisation et approbation délivrées par une instance désignée par arrêté du ministre chargé de l'industrie à une organisation ou à un individu, et permettant à ceux-ci de réaliser une évaluation en vue de la qualification des PSC.
Σ
Autorité Administrative (AA)
Autorité responsable de l'IGC et possédant un pouvoir décisionnaire au sein de l'IGC. Elle est garante de l'application de la politique de sécurité du domaine d'application qui régit l'IGC. Cette politique de sécurité englobe la ou les politiques de certification des IGC du domaine d'application. Elle valide les pratiques de certification respectées par les différentes composantes de l'IGC : AC, AE, SP, OC. Elle peut éventuellement être confondue avec l'AC.
Σ
Autorité de certification (AC)
Autorité chargée par un ou plusieurs utilisateurs de créer et d'attribuer les certificats. Cette autorité peut, facultativement, créer les clés d'utilisateur. [9594-8]
L'AC est l'entité responsable du PSC. Elle peut sous-traiter uen partie de ses activités à d'autres entités du PSC.
Elle peut demander à être qualifiée.
Σ
Autorité de certification racine (ACR)
Autorité de certification (AC) prise comme référence par une communauté d'utilisateurs et les AC d'une IGC. Elle est un élément essentiel de la confiance qui peut être accordée à l'IGC dans un contexte donné.
Σ
Autorité compétente
Responsable hiérarchique du signataire ou du correspondant local de sécurité du domaine d'application.
Σ
Autorité d'Enregistrement (AE)
Entité dont le but est de soutenir localement un ensemble d'entités d'extrémités physiquement éloignées de l'autorité de certification à laquelle elles sont subordonnées. Une autorité d'enregistrement remplit en partie des fonctions de l'administrateur de l'autorité de certification directement responsable d'un ensemble d'entités d'extrémité subordonnées. Ces fonctions comprennent :
l'enregistrement, l'annulation de l'enregistrement et la modification des attributs des entités d'extrémité subordonnées ;
l'autorisation des demandes de récupération des certificats ;
l'approbation et l'autorisation des demandes de révocation de certificats ;
la remise physique des jetons individuels au personnel autorisé à les détenir ;

l'enregistrement, l'annulation de l'enregistrement et l'attribution de privilèges au personnel de l'autorité d'enregistrement locale.

Une autorité d'enregistrement n'est généralement pas habilitée à émettre des certificats ou des liste des certificats révoqués ni à connaître les clés privées des entités d'extrémité.
L'expression générique « autorité d'enregistrement » peut être modifiée pour les IGC individuelles (par exemple autorité locale d'enregistrement, autorité d'enregistrement d'organisation) et chacune de ces IGC peut mettre en œuvre un ensemble modifié des fonctions décrites ci-dessus.
∑
Autorité Responsable d'Application (ARA)
L'autorité responsable d'application est responsable du domaine d'application. La garantie de l'autorité responsable d'application vis à vis des signataires et des utilisateurs de certificats par rapport à l'application concernée vient de la qualité de la technologie mise en œuvre et du cadre réglementaire et contractuel qu'elle définit dans une politique régissant l'application et qu'elle s'engage à respecter. L'élaboration et la mise en œuvre de la politique de sécurité, qui est un volet de la politique régissant l'application, du domaine d'application est confié à l'autorité administrative. Elle délègue la responsabilité de l'authentification des utilisateurs finaux à l'autorité administrative (AA).
∑
Bi-clé
Un bi-clé est un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptologie basée sur des algorithmes asymétriques. Quatre types de bi-clés interviennent dans une infrastructure de gestion de clés :
Les bi-clés d'intégrité, dont la clé privée est utilisée à des fins de contrôle d'accès, de non-répudiation et de signature et la clé publique à des fins de vérification,
les bi-clés de certification, sont nécessaires au fonctionnement d'une IGC ;
les bi-clés de confidentialité, grâce auxquels des messages ou des données sont protégés en confidentialité ;
les bi-clés d'échange de clés qui permettent de transporter les clés (symétriques ou asymétriques).
∑
Centre d'élaboration de clés (CEC)
Plate-forme technique offrant des services de génération de clés et paramètres cryptographiques pour le compte de signataires ou de composantes de l'IGC.
∑
Certificat
Clé publique d'un utilisateur, ainsi que certaines autres informations rendues infalsifiables par chiffrement avec la clé privée d'une autorité de certification (AC) qui l'a délivré. [9594-8]
Un certificat contient des informations telles que :

- l'identité du porteur de certificat,
- la clé publique du porteur de certificat,
- la durée de vie du certificat,
- l'identité de l'autorité de certification qui l'a émis,
- la signature de l'AC qui l'a émis.

Un format standard de certificat est normalisé dans la recommandation X509 v3[3].
∑
Certificat d'AC
Certificat d'une autorité de certification fournit par une autre autorité de certification. [9594-8]
∑

Certificat auto-signé
Certificat d'une autorité de certification signé par cette même autorité de certification. [RFC 2459]
Σ
Certificat électronique qualifié
Un certificat électronique répondant aux exigences définies à l'article 6 du [D2001-272].
Σ
Certificat feuille
Certificat terminal du chemin de certification (opposé au certificat de l'AC racine).
Σ
Chaîne de certification
Voir Chemin de certification.
Σ
Chemin de certification
Suite ordonnée de certificats liés les uns aux autres.
Généralement, le chemin relie un certificat feuille à un certificat auto-signé.
Σ
Clé publique
Clé composante d'un bi-clé asymétrique d'une entité qui peut être rendue publique. [ISO/IEC 9798-1]
Σ
Clé privée
Clé composante d'un bi-clé asymétrique d'une entité qui doit uniquement être utilisée par cette entité. [ISO/IEC 9798-1]
Σ
Composante
Plate-forme constituée d'au moins un poste informatique, une application, un moyen de cryptologie et jouant un rôle déterminé au sein de l'IGC. Une composante peut être l'autorité de certification (AC), une autorité d'enregistrement (AE), etc.
Σ
Contremarque de temps
Ensemble de données qui associe une représentation d'une donnée à un instant particulier, dans le but d'établir une preuve indiquant une date à laquelle la donnée existait.
Σ
Contrôle de conformité
Action qui consiste à réaliser un examen le plus exhaustif possible afin de vérifier l'application et le maintient des Déclarations des Pratiques de Certification et de la réglementation au sein d'un organisme conformément aux Politiques de Certification mises en œuvre par l'autorité de certification (AC).
Σ
Croisement de certificat
Action de reconnaître et garantir les certificats émis par une autre IGC. Le croisement de certificat consiste aujourd'hui à certifier la clé publique de l'autorité de certification (AC), appartenant à l'autre IGC.
Σ
Condensat, Condensé
Voir haché.
Σ
Déclaration des Pratiques de Certification (DPC)
Déclaration des pratiques mises en œuvre par une autorité de certification pour émettre et gérer des certificats. [RFC 2527]
Il peut comporter des parties confidentielles.
Σ

Délivrance de clé privée
Dans le cas où un centre de génération de clés est utilisé pour la génération du bi-clé de confidentialité d'un signataire, la remise de la clé privée à son porteur doit être protégée en intégrité et en confidentialité.
∑
Domaine
Groupe d'entités assujetties à la même politique de sécurité et relevant d'une même autorité chargée de mettre en œuvre cette politique.
∑
Domaine d'application
Ensemble constitué de personnels, de systèmes d'information (IGC, applications, réseaux,…) et de moyens. Par exemple : ministère, direction d'un ministère, sociétés, opérateurs de certification.
∑
Domaine de certification
Périmètre d'application de la politique de certification de l'IGC.
∑
Données d'activation
Données privées associées à un signataire permettant de mettre en œuvre sa clé privée.
∑
Données de création de signature électronique
Les éléments propres au signataire, tels que des clés cryptographiques privées, utilisés par lui pour créer une signature électronique. [D2001-272]
∑
Données de vérification de signature électronique
Les éléments, tels que des clés cryptographiques publiques, utilisés pour vérifier la signature électronique. [D2001-272]
∑
Données d'identifications personnelles
Informations relatives à une personne et permettant de connaître avec précision et sans ambiguïté son identité.
∑
Dispositif de vérification de signature électronique
Un matériel ou un logiciel destiné à mettre en application les données de vérification de signature électronique. [D2001-272]
∑
Dispositif de création de signature électronique
Un matériel ou un logiciel destiné à mettre en application les données de création de signature électronique. [D2001-272]
∑
Dispositif sécurisé de création de signature électronique
Un dispositif de création de signature électronique qui satisfait aux exigences définies au I de l'article 3 du [D2001-272].
∑
Édition d'un gabarit de certificat
Opération effectuée par une autorité d'enregistrement (AE) et qui consiste à rassembler un ensemble d'informations publiques sur une entité (son nom, la valeur de sa clé publique, l'algorithme asymétrique mis en œuvre, etc.) ainsi que des données propres au type du certificat désiré (politique de certification, nom de l'autorité de certification). Cette action est le résultat de l'acte d'enregistrement d'un demandeur auprès de l'AE.
∑
Émission d'un certificat

Délivrance par une AC d'un certificat à un signataire ou à une composante de l'IGC.
∑
Enregistrement
Action qui consiste pour une autorité d'enregistrement à renseigner le profil d'un demandeur de certificat et à en vérifier la véracité, conformément à une politique de certification.∑
∑
Entité
Utilisateur, processus ou système faisant partie de l'infrastructure de gestion des clés ou de l'application utilisateur. Les exemples donnés ici comprennent les systèmes et applications d'extrémité (désignés comme entités d'extrémité) et des composantes de l'infrastructure comme les autorités de certification et les autorités d'enregistrement.
∑
Exploitant
Personne travaillant pour le compte de l'IGC et disposant de droits d'accès à une autorité associés aux rôles qui lui sont attribués.
∑
Génération d'un certificat
Processus de création d'un certificat à partir d'éléments spécifiques à l'application et au signataire. Action réalisée au moyen d'une signature du certificat par une autorité de certification (AC).
∑
Haché, condensat, condensé
Résultat d'une fonction de hachage à sens unique (on ne peut pas revenir au message initial), c'est-à-dire d'une fonction calculant une empreinte d'un message de telle sorte qu'une modification même infime du message entraîne la modification de l'empreinte.
∑
Infrastructure de gestion de clés (IGC)
Ensemble organisé de composantes fournissant des services de gestion des clés cryptographiques et de certificats de clés publiques au profit d'une communauté d'utilisateurs (signataires, vérificateurs…).
∑
Interopérabilité
Capacité de deux IGC à constituer un domaine de confiance partagée.
∑
Journalisation
Fait d'enregistrer dans un fichier dédié à cet effet certains types d'événements provenant d'une application ou du système d'exploitation d'un poste informatique. Le fichier résultant rend possible la traçabilité et l'imputabilité des opérations effectuées.
∑
Liste des Certificats Révoqués (CRL)
Liste contenant les identifiants des certificats révoqués ou invalides. Lors d'une révocation, l'AC ajoute l'identifiant du certificat à révoquer dans la CRL, la signe et la transmet au service de publication. Il appartient à l'utilisateur qui souhaite connaître l'état d'un certificat de vérifier la présence de l'identifiant correspondant dans la liste.
∑
Liste des Autorités de certification Révoquées (ARL)
Une ARL est une CRL qui ne contient que des identifiants de certificats d'AC révoqués et pas de certificats feuilles.
∑
Opérateur de Certification (OC)

L'opérateur de certification assure les prestations techniques pour le compte de l'AC. La responsabilité de l'OC est d'exécuter les actions demandées par l'AE et de répondre aux exigences définies par l'AC. Sa responsabilité se limite au respect des procédures établies dans la DPC.

Σ

Opérateur de prestation d'externalisation (OPE)

L'OPE assure des prestations techniques, entre autre cryptographiques, nécessaires au processus de gestion de certificat (enregistrement, certification, révocation, publication,…) conformément à une PC. Dans le cas de l'AC, l'OPE est un OC.
Sa responsabilité se limite au respect des procédures établies dans la DPC.

Σ

Paramètres de clés publiques

Données publiques relatives à la mise en œuvre de l'algorithme asymétrique de cryptographie.

Σ

Politique de certification (PC)

Ensemble de règles, identifié par un nom, relatives à l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications ayant des besoins de sécurité communs. [9594-8]

Σ

Prestataire de service de certification (PSC)

Toute personne ou entité qui délivre des certificats au public ou lui fournit d'autres services liés aux signatures électroniques.
C'est une IGC qui délivre des certificats, elle peut être composée d'une AC, d'une AE et d'un SP.

Σ

Publication d'un certificat

Fait de rendre disponible un certificat via un média (par ex. annuaire, serveur d'information, support amovible,…)

Σ

Qualification des prestataires de services de certification électronique

L'acte par lequel un tiers, dit organisme de qualification, atteste qu'un prestataire de services de certification électronique fournit des prestations conformes à des exigences particulières de qualité. [D2001-272]
La qualification vaut présomption de conformité aux exigences de l'article 6 du décret 2001-272.

Σ

Rapport facial

Action de se présenter en personne auprès d'une composante de l'IGC dans le but de prouver son identité ou son accord.

Σ

Renouvellement de certificat

Action effectuée à la demande d'un signataire et en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat pour un porteur. La re-génération de certificat après révocation n'est pas un renouvellement.

Σ

Révocation de certificat

Processus consistant à indiquer qu'un certificat est devenu invalide. Cette action peut être la conséquence de différents types d'événements tels que le changement de nom de l'entité, le changement de l'association entre l'entité et l'AC, la compromission ou la suspicion de compromission de la clé privée.
Action demandée par une AC, une AE, le porteur de certificat ou son AA.

∑

Service de publication

Le service de publication rend disponible les certificats de clés publiques émis par une AC, à l'ensemble des utilisateurs potentiels de ces certificats. Il publie une liste de certificats reconnus comme valides et une liste de certificats révoqués (CRL). Ce service peut être rendu par un annuaire (par exemple, de type X500), un serveur d'information (Web), une délivrance de la main à la main, une application de messagerie, etc.

∑

Signataire

Toute personne physique, agissant pour son propre compte ou pour celui de la personne physique ou morale qu'elle représente, qui met en oeuvre un dispositif de création de signature électronique. [D2001-272]

Le signataire est appelé demandeur de certificat lorsqu'il effectue une demande de certificat auprès d'une AE. Il est appelé porteur de certificat dès l'instant où il dispose d'un certificat émis par l'IGC. Un signataire ne peut émettre de certificat pour le compte d'autrui. ∑

∑

Signature électronique

Une donnée qui résulte de l'usage d'un procédé répondant aux conditions définies à la première phrase du second alinéa de l'article 1316-4 du code civil : « Lorsqu'elle est électronique, elle consiste en l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache. ». [D2001-272]

∑

Signature électronique sécurisée

Une signature électronique qui satisfait, en outre, aux exigences suivantes :

- être propre au signataire ;
- être créée par des moyens que le signataire puisse garder sous son contrôle exclusif ;
- garantir avec l'acte auquel elle s'attache un lien tel que toute modification ultérieure de l'acte soit détectable. [D2001-272]

∑

Suspension de certificat

Action demandée par une AC, une AE, le porteur de certificat ou son Autorité administrative (AA) et dont le résultat est la suspension de la validité d'un certificat pour une période donnée.

∑

Tampon d'horodatage

Voir contremarque de temps.

∑

Technique cryptographique asymétrique

Technique cryptographique utilisant deux transformations connexes, une transformation publique (définie par la clé publique) et une transformation secrète (définie par la clé privée). Ces deux transformations ont pour propriété de rendre impossible de déduire par ordinateur la transformation secrète, en raison de la transformation publique. [ISO/IEC 11770-1]

∑

Tierce Partie de Confiance (TPC)

Organisme gérant pour le compte d'autrui des conventions secrètes de moyens ou de prestations de cryptologie permettant d'assurer des fonctions de confidentialité. **Erreur ! Source du renvoi introuvable.**

∑

Validation de certificat

Service offrant l'assurance que les informations contenues dans le certificat ont été validées par une autorité de confiance. La validation d'un certificat inclut entre autres la vérification de sa

période de validité, de son état (révoqué ou non), et la vérification de la signature de l'AC génératrice. Elle inclut également la validation du certificat de l'AC génératrice.
∑
Vérificateur
Toute entité (utilisateur humain, organisme ou entité des technologies de l'information) utilisant un certificat de clé publique. Synonyme : utilisateur de certificat.
∑
Vérification de signature
La vérification d'une signature consiste à déchiffrer la signature d'un message, en mettant en œuvre la clé publique de l'émetteur. Si le clair obtenu est identique au haché calculé à partir du message reçu, alors il est garanti que le message est intègre et qu'il a été signé par le porteur de la clé privée correspondante à la clé publique utilisée pour la vérification.
La vérification d'une information signée nécessite des vérifications supplémentaires notamment la datation de l'information, le rôle du signataire, les conditions éventuelles de non-répudiation.

10 Annexes

10.1 Rôles

Responsable de sécurité : le responsable de sécurité est responsable de l'application de la politique de sécurité physique et fonctionnelle d'une composante du PSC et de son environnement. Il gère les contrôles d'accès physiques à la plate-forme de la composante, et est chargé de mettre en œuvre la politique de sécurité régissant la composante. Il est habilité à prendre connaissance des archives et analyse les journaux d'événements

Administrateur : un administrateur met en œuvre les politiques de certification et déclarations des pratiques de certification du PSC au sein de la composante qu'il administre. Il est responsable de l'ensemble des services rendus par cette composante. Il approuve la création, la révocation et la suspension des certificats

Ingénieur système : il est chargé de la mise en route, de la configuration et de la maintenance technique de la plate-forme informatique de la composante. Il 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 éventuellement fournis par le PSC.

Opérateur : l'opérateur d'une composante (AE, AC) réalise l'exploitation des services offerts par la composante, dans le cadre de ses attributions.

Contrôleur : personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des politiques de certification, des déclarations des pratiques de certification et des services effectivement fournis par la composante du PSC.

10.2 Acronymes

AA	Autorité administrative
AC	Autorité de certification
AE	Autorité d'enregistrement
ARL	Liste des Autorités de certification Révoquées
CEC	Centre d'élaboration de clés
CNIL	Commission Nationale de l'Informatique et des Libertés
CPSSI	Cahiers de Prescriptions de Sécurité des Systèmes d'Information
CRL	Certificate Revocation List (Liste des Certificats Révoqués)
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
DN	Distinguish Name
DPC	Déclaration des Pratiques de Certification
DSCS	Dispositif sécurisé de création de signature électronique
IGC	Infrastructure de Gestion de clé
ISO	International Organization for Standardization
ITU	International Telecommunications Union
OC	Opérateur de Certification
OID	Object IDentifier
OPE	Opérateur de Préstation d'Externalisation

PC	Politique de certification
PKIX	Public Key Infrastructure Working Group (Groupe de travail de l'IETF)
PSSI	Politique de Sécurité des Systèmes d'Information
PSC	Prestataire de Services de Certification
PV	Procés Verbal
SP	Service de Publication
SSCD	Secure Signature Creation Divice
TPC	Tierce Partie de Confiance
UTC	Coordinated Universal Time

10.3Actions

Accréditation	Action de garantir qu'une composante est reconnue par une autorité compétente et peut exercer son activité au sein d'une IGC dont elle respecte les modes de fonctionnement (PC et DPC).
Agrément	Reconnaissance formelle que le produit ou système évalué peut protéger des informations jusqu'à un niveau spécifié dans des conditions d'emploi définies au sein d'une administration [IGI900].
Contrôle de conformité	Action qui consiste à réaliser un examen le plus exhaustif possible afin de vérifier l'application stricte des procédures et de la réglementation au sein d'un organisme.
Croisement de certificat	Action de reconnaître et garantir les certificats émis par une autre IGC. Le croisement de certificat consiste aujourd'hui à certifier la clé publique d'une AC appartenant à l'autre IGC.
Édition d'un gabarit de certificat	Opération effectuée par une AE et qui consiste à rassembler un ensemble d'informations publiques sur une entité (son nom, la valeur de sa clé publique, l'algorithme asymétrique mis en œuvre, etc.) ainsi que des données propres au type du certificat désiré (politique de certification, nom de l'autorité de certification). Cette action est le résultat de l'acte d'enregistrement d'un demandeur auprès de l'AE.
Émission d'un certificat	Fait d'exporter un certificat à l'extérieur d'une AC (pour une délivrance à l'utilisateur final, une demande de publication).
Enregistrement	Action qui consiste pour une autorité d'enregistrement à éditer le profil d'un demandeur de certificat, conformément à une politique de certification.
Génération d'un certificat	Action réalisée par une AC et qui consiste à signer le gabarit d'un certificat édité par une AE, après avoir vérifié la signature de l'AE.
Journalisation	Fait d'enregistrer dans un fichier dédié à cet effet certains types d'événements provenant d'une application ou du système d'exploitation d'un poste informatique. Le fichier résultant rend possible la traçabilité et l'imputabilité des opérations effectuées.
Publication d'un certificat	Fait de mettre un certificat à disposition d'utilisateurs susceptibles d'avoir à vérifier une signature ou à chiffrer des informations.
Rapport facial	Action de se présenter en personne auprès d'une entité dans le but de prouver son identité ou son accord.
Renouvellement de certificat	Action effectuée à la demande d'un utilisateur final ou en fin de période de validité d'un certificat et qui consiste à générer un nouveau certificat pour un porteur. La re-génération de certificat après révocation n'est pas un renouvellement.

Révocation de certificat	Action demandée par une AC, une AE, une TPC, le porteur de certificat ou son autorité de sécurité, et dont le résultat est la suppression de la caution de l'AC sur un certificat donné, avant la fin de sa période de validité. Cette action peut être la conséquence de différents types d'événements tels que la compromission d'une clé, le changement d'informations contenues dans un certificat, etc. L'action de révocation peut consister soit à publier une liste des certificats révoqués, soit à mettre à la disposition des utilisateurs un serveur pouvant indiquer l'état révoqué ou non d'un certificat.
Signature numérique	Données ajoutées à une unité de données ou transformation cryptographique d'une unité de données permettant à un destinataire de prouver la source et l'intégrité de l'unité de données et protégeant contre la contrefaçon (par le destinataire, par exemple) [7498-2].
Suspension de certificat	Action demandée par une AC, une AE, une TPC, le porteur de certificat ou son autorité de sécurité et dont le résultat est la suspension de la validité d'un certificat pour une période donnée. Cette action peut être la conséquence de l'absence temporaire d'un porteur de certificat.
Validation de certificat	La procédure de vérification d'un certificat consiste en un ensemble d'opérations destinées à s'assurer que les informations contenues dans le certificat ont été validées par une autorité de confiance. La validation d'un certificat inclut entre autres la vérification de sa période validité, de son état (révoqué ou non), et la vérification de la signature de l'AC génératrice. Elle inclut également la validation du certificat de l'AC génératrice.
Vérification de signature	La vérification d'une signature consiste à déchiffrer la signature d'un message, en mettant en œuvre la clé publique de l'émetteur. Si le clair obtenu est identique au haché calculé à partir du message reçu, alors il est garanti que le message est intègre et qu'il a été signé par le porteur de la clé privée correspondante à la clé publique utilisée pour la vérification.

10.4Documents de références

Lois et Réglements	
[DES]	Directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques – (JOCE du 19 janvier 2000).
[L00-230]	Loi n 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique (JO du 14 mars 2000).
[L90-1170]	Article 28 de la loi n 90-1170 du 29 décembre 1990 sur la réglementation des télécommunications modifié par l'article 17 de la loi 96-659 du 26 Juillet 1996.
[LEN]	No 991 PROJET DE LOI modifié par le sénat pour la confiance dans l'économie numérique. Enregistré à la Présidence de l'Assemblée nationale le 26 juin 2003.
[L78-19]	Loi n 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (Art. 323-1 à 323-3 du Code pénal).
[D2002-535]	Décret du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.
[D2001-272]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316 du code civil et relatif à la signature électronique

[D98-102]	Décret 98-102 du 24 Février 1998 précisant l'article [L90-1170] relatif aux conditions dans lesquelles sont agréés les organismes gérant pour le compte d'autrui les conventions secrètes de cryptologie.
[A02]	Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation.
Documentations Internationales	
[TS 101 456]	ETSI TS 101 456 V1.2.1 (2002-04) - « Policy requirements for certification authorities issuing qualified certificates»
[SR 002 176]	ETSI SR 002 176 V1.1.1 (2003-03) - « Electronic Signatures and Infrastructures (ESI); Algorithms and Parameters for Secure Electronic Signatures»
[9594-1]	ISO/IEC 9594-1 (1995) - « Information Technology – Open Systems Interconnection : The Directory : Overview of concepts, Models and Services » (Egalement Recommandation ITU-T X.500).
[9594-8]	ISO/IEC 9594-8 (1995) - « Information Technology – Open Systems Interconnection : The Directory : Authentication Framework » (Egalement Recommandation ITU-T X.509 (1997)). NF ISO/CEI 9594-8 (1996) – « Technologies de l'information – Interconnexions de systèmes ouverts (OSI) – L'annuaire : Cadre d'authentification ».
[ISO/IEC 11770-1]	ISO/IEC 11770-1: 1996, *Information technology - Security techniques - Key management - Part 1: Framework.*
[ISO/IEC 9798-1]	ISO/IEC 9798-1 (2nd edition): 1997, « *Information technology - Security techniques - Entity authentication - Part 1: General* ».
[ALGO]	Algorithms and Parameters for Secure Electronic Signatures v2.1 (19 Octobre 2001)
[RFC 2527]	« Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practises Framework » (Mars 1999) - IETF - Network Working Group.
[RFC 3280]	« Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile » (avril 2002) - Internet Engineering Task Force (IETF) - Network Working Group.
[RFC 3039]	« Internet X.509 Public Key Infrastructure Qualified Certificates Profile » (Janvier 2001) - Internet Engineering Task Force (IETF) - Network Working Group.
[CWA 14169]	European Committee for Standardization CEN/ISS : Security Requirements of Secure Signature Creation Devices (SSCD) – SSCD-PP
[CWA 14167-1]	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements. November 2001
[CWA 14167-2]	Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations - Protection Profile (MCSO-PP). March 2002
[QCP]	Policy requirements for Certification Authorities issuing Qualified Certificates - ETSI TS 101 456 v1.2.1 (2002-04).

[GOC]	Digital Signature and Confidentiality - Certificate Policies - Government of Canada Public Key Infrastructure - Version 2.0 - Août 1998.
Documents Interministériels	
[IGI1300]	Instruction générale interministérielle sur la protection du secret et des informations concernant la défense nationale et la sûreté de l'état n 1300/SGDN/SSD du 12 mars 1982 (document en diffusion restreinte).
[IGI910]	Instruction interministérielle sur les articles contrôlés de la sécurité des systèmes d'information n 910/SGDN/SSD/DR, n 910/DISSI/SCSSI/DR du 19 décembre 1994 (document en diffusion restreinte).
[IGI900]	Instruction générale interministérielle sur la sécurité des systèmes d'information qui font l'objet d'une classification de défense pour eux-mêmes ou pour les informations traitées n 900/SGDN/SSD/DR n 900 /DISSI/SCSSI/DR du 20 juillet 1993 (document en diffusion restreinte).
[R901]	Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense n 901/DISSI/SCSSI du 2 mars 1994.
[CERTIFICAT_IGC]	Format des certificats utilisés dans les infrastructures de gestion de clés – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[SIG/P/01.1]	PROCEDURE SIG/P/01.1 "CERTIFICATION DE CONFORMITE DES DISPOSITIFS DE CREATION DE SIGNATURE ELECTRONIQUE" 7 avril 2003
[DECOUPAGE_IGC]	Découpage fonctionnel des autorités d'une IGC - Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[ROLES_IGC]	Rôles des exploitants d'une infrastructure de gestion de clés – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[PP_AC]	Profil de protection pour une autorité de certification – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[PP_AE]	Profil de protection autorité d'enregistrement – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[PP_IGC]	Profil de protection infrastructures de gestion des clés – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[PP_OSM]	Profil de protection sur les outils de sécurisation de message version 1.5 du 24 juin 1998 (PP/9804) – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[PP_RCIGC]	Profil de protection ressource cryptographique pour une infrastructure de gestion des clés – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.
[VAR_TEMPS]	Définition des variables de temps intervenant dans une infrastructure de gestion de clés – Groupe Ad Hoc Messagerie Sécurisée de la Sous-Commission Chiffre de la CISSI.

Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

Identification de la contribution
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

Remarques générales sur le document
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?

.....
.....

Remarques particulières sur le document

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

N°	Type	Référence	Énoncé de la remarque	Solution proposée
1				
2				
3				
4				
5				

Merci de votre contribution