Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

POLITIQUE DE CERTIFICATION
AC ACTEURS DE L'ADMINISTRATION DE L'ETAT

OID du document :	1.2.250.1.200.2.2.1.1 1.2.250.1.200.2.3.1.1	**Nombre total de pages :**	79
Statut du document :	☐ Projet	☒ Version finale	

Rédaction

Nom	**Fonction**
ANTS	-

Validation

Nom	**Fonction**	**Signature**
Cyril MURIE	Responsable Pôle Convergence – ANTS	
Jean-Baptiste VESPIERS	Chef de projet COMEDEC – ANTS	
Claudine LEVAGUERESSE	Responsable du programme Sécurité – ANTS	

Approbation

Nom	**Fonction**	**Signature**
Etienne GUÉPRATTE	Directeur de l'ANTS	

REVISION DOCUMENTAIRE

Date	Version	Commentaires
13/10/11	0.1	Création du document
18/10/11	0.2	Modifications suite à commentaires
09/01/12	0.3	Alignement avec la DPC et les CGU
27/08/12	1.0	Prise en compte des remarques de l'ANTS et mise à jour des processus
14/09/12	1.1	Prise en compte des remarques de l'ANTS et intégration des nouvelles URLs
01/10/12	1.2	Modification des gabarits de certificats - Corrections des adresses du SP - Mise en cohérence
05/10/12	1.3	La terminologie est adaptée. Introduction de la notion de Primo ACT - Les processus d'enregistrement sont précisés
08/10/12	1.4	Mise à jour des gabarits de certificats (AC Racine) - Ajustement de la définition de Primo ACT - Correction de mise en page.
15/10/12	1.5	Mise à jour des gabarits de certificats pour être cohérent avec l'AC Racine ANTS v2
23/11/12	1.6	Corrections – Mise à jour des adresses du SP
07/12/12	1.7	Mise à jour du document
13/12/12	1.8	Mise à jour de la partie « Vérification initiale de l'identité »
04/03/13	1.9	Corrections – Mise à jour concernant les attestations de validation
18/10/13	1.9.1	Corrections – Mise à jour du document

SOMMAIRE

1 INTRODUCTION

1.1 Généralités

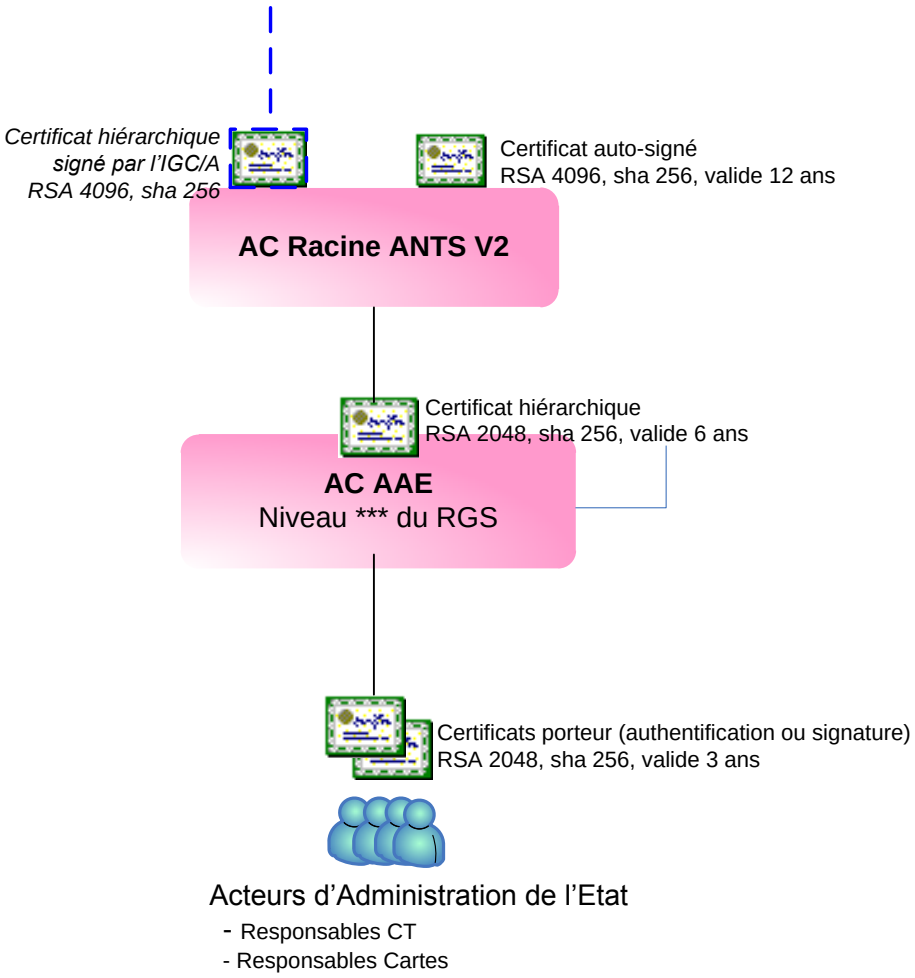
Dans la suite du document, le terme « Service de l'Etat » concernera soit la préfecture du département soit une sous-préfecture du département.

L'ANTS met en place et exploite une Infrastructure de Gestion de Clés (IGC) afin de gérer les certificats de clé publique des :

- acteurs de l'administration de l'état au sein des Services de l'Etat, émis par l'autorité de certification appelée « AC Acteurs de l'Administration de l'Etat » ou « AC AAE » ;
- acteurs des collectivités territoriales (officiers d'état-civil, maires, policiers municipaux), émis par l'autorité de certification appelée « AC Acteurs des Collectivités Territoriales » ou « AC ACT ».

Ces deux autorités de certification sont rattachées à une AC de niveau supérieur « AC ANTS V2 ». Cette dernière, ayant un certificat auto-signé qui peut être utilisée comme racine de confiance pour vérifier la validité d'un chemin de certification, est également gérée et exploitée par l'ANTS.

L'AC Racine ANTS V2 a vocation à être rattachée à l'IGC gouvernementale appelée IGC/A. Lorsque ce rattachement aura été effectué (illustré par la figure ci-dessous), il sera possible d'utiliser le certificat auto-signé de l'IGC/A en lieu et place ou en complément de celui de l'AC Racine ANTS V2.



Ce document constitue la Politique de Certification (PC) de l'AC AAE et a été établi sur la base de la Politique de Certification Type du RGS [RGS], en vue d'un référencement pour les profils Authentification et Signature, au niveau ***. Il a pour objet de décrire la gestion du cycle de vie des certificats des porteurs et des bi-clés associées.

On distingue deux types de porteurs de certificats émis par l'AC AAE :

- le Responsable CT qui est une personne d'un Service de l'Etat en charge des relations avec les collectivités territoriales. Celui-ci est nommé par le Secrétaire Général en préfecture. Il est porteur de la première carte AAE émise pour le Service de l'Etat concerné
- les Responsables Cartes qui sont des personnes d'un Service de l'Etat nommées par note de service, soit par le Responsable CT, soit par un autre Responsable de Cartes.

Ces porteurs peuvent procéder à :

- la demande et à la délivrance de certificats AAE à des Responsables Cartes de leur Service de l'Etat ;
- la demande et à la délivrance des certificats ACT pour des Primo ACT en Collectivité Territoriale rattachée à leur Service de l'Etat.

Comme complément à l'IGC, l'ANTS met en place et exploite :

- le référentiel des départements : un annuaire référençant, au fur et à mesure de déploiement de la dématérialisation, les Services de l'Etat ainsi que les collectivités territoriales (en particulier les communes) qui leur sont rattachées.
- le référentiel d'identité : un annuaire se basant sur le référentiel des départements, contenant les informations relatives aux différents porteurs.

Dans le cadre de la présente PC, les certificats mis à disposition des porteurs sont au nombre de deux :

- un certificat à usage d'authentification au niveau *** du RGS [RGS], et
- un certificat à usage de signature électronique au niveau *** du RGS [RGS].

L'AC AAE fournit au porteur un dispositif sécurisé de création de signature, intitulé « Carte AAE », qui contient ces certificats et les clés privées associées. Ces dispositifs sécurisés sont qualifiés au niveau renforcé, selon le processus décrit dans le RGS [RGS], et sont conformes aux exigences du chapitre XII.1 de la Politique de Certification Type Signature.

A chaque certificat correspond une clé privée qui est activable par la présentation d'un code spécifique appelé code PIN (Personal Identification Number).

Une signature électronique « présumée fiable » jusqu'à preuve du contraire, au sens de l'article 1316-4 du code civil, peut alors être obtenue en associant l'usage du certificat à usage de signature électronique au niveau *** du RGS, sur son dispositif sécurisé de signature électronique et l'usage d'un logiciel permettant de générer des signatures sécurisées.

De manière à faciliter l'identification des différences entre les certificats destinés à l'authentification et ceux destinés à la signature, les exigences spécifiques à un certificat sont encadrées, le titre du cadre précisant le type de certificat auquel l'exigence s'applique. Les exigences qui ne sont pas encadrées s'appliquent de manière identique pour les deux types de certificats.

La présente Politique de Certification est élaborée conformément :

- au RFC 3647 « X.509 Public Key Infrastructure Certificate Policy Certification Practise Statement Framework » de Internet Engineering Task Force (IETF) ;
- à la Politique de Certification Type Authentification, version 2.3 du Référentiel Général de Sécurité, OID 1.2.250.1.137.2.2.1.2.2.1
- à la Politique de Certification Type Signature, version 2.3 du Référentiel Général de Sécurité, OID 1.2.250.1.137.2.2.1.2.2.2.
- à la Politique de Certification ANTS v2, identifiée par le numéro d'identifiant d'objet (OID) 1.2.250.1.200.2.1.1.1.

1.2 Nom du document et identification

La présente PC appelée « PC AAE » est la propriété de l'ANTS.

Ce document couvre deux politiques de certification :

- la Politique de Certification Acteurs de l'Administration de l'Etat pour les certificats d'authentification, identifiée par le numéro d'identifiant d'objet (OID) **1.2.250.1.200.2.2.1.1**;
- la Politique de Certification Acteurs de l'Administration de l'Etat pour les certificats de signature électronique, identifiée par le numéro d'identifiant d'objet (OID) **1.2.250.1.200.2.3.1.1**

Les OID sont dans la branche suivante : iso(1) member-body(2) fr(250) type-org(1) ANTS(200).

Des éléments plus explicites comme le nom, le numéro de version, la date de mise à jour, permettent d'identifier la présente PC, néanmoins les seuls identifiants de la version applicable des PC sont les OID.

1.3 Entités intervenant dans l'IGC

L'AC s'appuie sur les composantes et sous-composantes suivantes :

- Service d'enregistrement: Ce service est aussi appelé « Autorité d'Enregistrement » (AE). On distingue deux types d'entités AE :
  - l'Autorité d'Enregistrement Centrale « AEC », assurée par des Agents de l'Opérateur de Services de Certification (OSC) pour gérer les demandes de certificats pour les Responsables CT.
  - des Autorités d'Enregistrement Déléguées « AED » au niveau des Services de l'Etat pour gérer les demandes de certificats pour les Responsables Cartes AAE et les Primo ACT.

  Toutes les demandes de certificats s'effectuent en ligne à l'adresse suivante :

  https://www.asscap.agents-ctae-sec.ants.gouv.fr/ par des personnes habilitées munies de leur carte AAE.
- Service de génération des certificats: Ce service est assuré par un Opérateur de Services de Certification (OSC) qui génère les certificats électroniques des porteurs à partir des informations transmises par le service d'enregistrement qui ont été préalablement vérifiées et validées par ledit service.
- Service de génération des éléments secrets du porteur : Ce service permet de personnaliser graphiquement et électriquement en générant les bi-clés dans la carte AAE puis en important dans cette carte les données fournies par le service de génération de certificats. Par ailleurs, ce service génère et insère un code d'activation temporaire dans chaque carte AAE. De plus, ce service génère aussi les deux codes de déblocage de carte AAE, appelé « Personal Unblocking Key » (PUK). Enfin, ce service communique aux porteurs les codes d'activation temporaire et les cartes AAE, acheminés par deux voies différentes.
- Service de remise au porteur : Ce service remet au porteur la carte AAE, contenant ses deux certificats : un certificat d'authentification et un certificat de signature électronique. La remise de la carte AAE est effectuée en face à face dans les locaux des Services de l'Etat :
  - au Responsable CT par une personne mandatée de l'AEC.
  - aux Responsables Cartes par le Responsable CT ou un autre Responsable Carte du même site.

  Les personnes affectées à ce service se connectent sur un portail dédié : https://www.asscap.agents-ctae-sec.ants.gouv.fr/ pour attester de la remise de la carte AAE au porteur après avoir vérifié son identité.

  Note : la remise de la carte AAE au porteur ne peut s'effectuer avant la réception par le porteur du code d'activation temporaire, envoyé au moyen d'une enveloppe sécurisée1.

[1] Il s'agit d'une enveloppe qui ne permet pas de voir par transparence le texte qu'elle contient et qui, si elle a été ouverte, ne peut pas être refermée sans que cela ne soit visible.

- Service de publication : Ce service met à disposition des utilisateurs de certificat (UC) au moyen de l'Internet les informations nécessaires à l'utilisation des certificats émis par l'AC (conditions générales, politiques de certification publiées par l'AC, certificats d'AC, …), ainsi que les informations de validité des certificats issues des traitements du service de gestion des révocations (LCR, avis d'information, …) ;
- Service de gestion des révocations : Ce service traite de la prise en compte des demandes de révocation des certificats des porteurs et détermine les actions à mener. Les résultats des traitements sont diffusés via le service d'information sur l'état des certificats;
- Service d'information sur l'état des certificats : Cette fonction fournit aux utilisateurs de certificats (UC) des informations sur l'état des certificats. Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers sous la forme de Listes de Certificats Révoqués (LCR).
- Service de journalisation : Ce service est mis en œuvre par l'ensemble des composantes techniques de l'IGC. Il est assuré par l'OSC. Il permet de collecter l'ensemble des données utilisées et ou générées dans le cadre de la mise en œuvre des services d'IGC afin d'obtenir des traces d'audits consultables.
- Service d'audit : Ce service est assuré par le Responsable en charge de la Sécurité des Systèmes d'information (RSSI) ou l'Officier de sécurité.
- Service d'assistance aux utilisateurs : Ce service est assuré par l'ANTS et fournit une assistance aux porteurs lorsqu'ils utilisent leur carte.

La présente PC définit les exigences de sécurité pour tous les services décrits ci-dessus afin de délivrer des certificats aux porteurs. La Déclaration des Pratiques de Certification (DPC) apporte des détails sur les pratiques de l'IGC dans cette perspective.

Les composantes de l'IGC mettent en œuvre leurs services conformément à la présente PC et à la DPC associée.

1.3.1 Autorité de Certification (AC)

L'Agence Nationale des Titres Sécurisés (ANTS) assure le rôle d'AC.

L'AC AAE garantit la cohérence et la gestion du référentiel de sécurité, ainsi que sa mise en application. Le référentiel de sécurité est composé de la présente PC, des Conditions Générales d'Utilisation (CGU) et de la DPC associée. L'AC AAE valide le référentiel de sécurité. Elle autorise et valide la création et l'utilisation des composantes des AC. Elle suit les audits et/ou contrôle de conformités effectués sur les composantes de l'IGC, décide des actions à mener et veille à leur mise en application.

L'AC AAE a pour responsabilité de garantir le lien (biunivoque) entre l'identifiant d'un porteur et une bi-clé cryptographique pour un usage donné. Cette garantie est apportée par des certificats de clé publique qui sont signés par une clé privée de l'AC.

En tant qu'autorité, l'AC :

- définit et valide l'organisation de l'IGC ;
- définit et contrôle la présente PC, les CGU et la DPC associée ;
- contrôle la mise en œuvre de la DPC ;
- arbitre les litiges.
- enregistre et prend en charge des demandes des certificats et les délivre dans des cartes AAE.

L'AC délègue ses services

- aux Responsables CT pour l'enregistrement des Responsables Cartes et la remise de leurs cartes AAE contenant les clés privées.
- aux Responsables Cartes pour l'enregistrement des Responsables Cartes et la remise des cartes AAE contenant les clés privées.
- à un prestataire postal pour la livraison des cartes AAE.
- à un prestataire postal pour la remise de la donnée d'activation de la carte AAE aux futurs porteurs.
- à l'Imprimerie Nationale (IN) le rôle du Centre de Personnalisation des Supports.

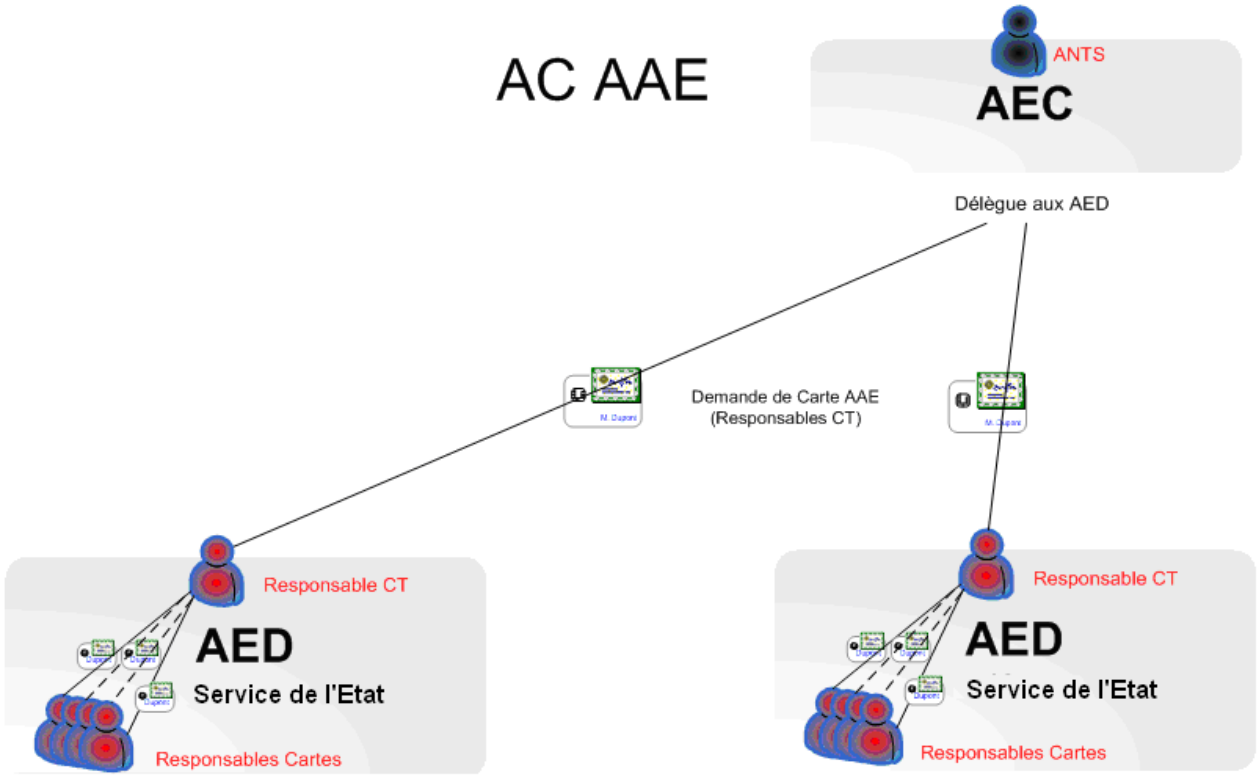
1.3.1.1 Certificats de test

Pour mener des tests, l'ANTS utilise des certificats de tests délivrés dans des cartes par l'AC AAE. La PC et la DPC donnent les détails de la gestion des certificats de test. Ces certificats ne peuvent servir qu'à des fins de tests dans le cadre d'une application clairement identifiée dans la demande de certificat ou le protocole de test défini entre le porteur et l'AC AAE. Les certificats de tests ne peuvent en aucun cas servir à engager le porteur et le responsable de l'application comme un certificat de production. Toutefois, les obligations de protection et d'utilisation du certificat pour le porteur et l'AC sont identiques à celles définies pour les certificats de production.

1.3.2 Les Autorité d'Enregistrement (AE)

L'autorité d'enregistrement (AE) est constituée de :

- l'autorité d'enregistrement centrale « AEC » ;
- des autorités d'enregistrement déléguées « AED » au niveau des Services de l'Etat.



Note : Le document [GUIDE_AE] recense l'ensemble des obligations et responsabilités qui incombent aux Autorités d'Enregistrement.

1.3.2.1 Autorité d'Enregistrement Centrale (AEC)

L'Agence Nationale des Titres Sécurisés (ANTS) assure le rôle d'AEC.

L'autorité d'enregistrement AEC est chargée de :

- l'enregistrement pour les demandes des Responsables CT,
- la révocation des certificats précédemment émis,
- la délivrance des cartes AAE aux Responsables CT lors d'un face à face.

Les opérations de demandes de certificat sont effectuées à la vue des données fournies par :

- les dossiers de demandes au format papier,
- le référentiel des départements,
- et éventuellement, le référentiel d'identités.

Les Responsables CT équipés de leur carte AAE activée, remplissent les fonctions des AED de leur Service de l'Etat. L'AEC délègue ainsi les services d'enregistrement et de délivrance de cartes à ces AED dans des domaines de responsabilités définis par le référentiel des départements.

1.3.2.2 Autorité d'Enregistrement Déléguée (AED)

Le Responsable CT et les Responsables Cartes assurent le rôle d'AED au niveau d'un Service de l'Etat.

L'AED des Services de l'Etat est initialement constituée du Responsable CT équipé de sa carte AAE activée. Ce dernier a la possibilité de désigner un ou plusieurs Responsables Cartes.

Les AED des Services de l'Etat sont chargées de :

- l'enregistrement des porteurs pour les demandes des Responsables Cartes et des Primo ACT,
- la révocation des certificats précédemment émis par la même AED,
- la délivrance des cartes AAE et cartes ACT lors d'un face à face.

Les services relatifs aux certificats et cartes ACT sont décrits dans [PC ACT].

Les opérations de demandes de certificat sont effectuées à la vue des données fournies par :

- le référentiel des départements,
- le référentiel d'identités,
- le portail dédié au service d'enregistrement et le système d'information associé.

1.3.3 Service de Publication (SP)

Le SP est une entité qui met à disposition des utilisateurs de certificat au moyen de l'Internet les informations nécessaires à l'utilisation des certificats émis par l'AC (conditions générales, politiques de certification publiées par l'AC, certificats d'AC, …). Ce service met aussi à disposition des utilisateurs de certificat les informations de validité des certificats issues des traitements du service de gestion des révocations (LCR, avis d'information, …). Le SP s'appuie sur les moyens de l'AC afin de réaliser ses services.

1.3.4 Centre de Personnalisation des Supports (CPS)

L'Imprimerie Nationale (IN) assure le rôle de Centre de Personnalisation des Supports. Le CPS dispose d'une plate-forme pour mettre en œuvre le service de personnalisation et de gestion des supports de bi-clé et la fourniture aux porteurs d'un code d'activation temporaire.

Le CPS met en œuvre un plan de continuité d'activité sur lequel s'appuie l'AC pour la continuité des services d'IGC. Une analyse de risques et ce plan de continuité couvrent le seul périmètre du CPS en tant qu'hébergeur de moyens qui permettent à l'AC de mettre en œuvre ses services d'IGC.

Le centre dispose en outre d'un service de journalisation et d'audit conformément à la présente PC et à la DPC applicable.

1.3.4.1 Opérateur de Service de Certification (OSC)

L'Agence Nationale des Titres Sécurisés (ANTS) assure le rôle d'Opérateur de Service de Certification.

L'Opérateur de Services certification assure des prestations techniques, en particulier des opérations cryptographiques, nécessaires au processus de certification, conformément à la présente PC et à la DPC associée. L'OSC est techniquement dépositaire des clés privées de l'AC utilisées pour la signature des certificats des porteurs et des LCR.

L'OSC possède un plan de continuité d'activité sur lequel s'appuie l'AC pour la continuité des services d'IGC. Une analyse de risques et ce plan de continuité couvrent le seul périmètre de l'OSC en tant qu'hébergeur de moyens qui permettent à l'AC de mettre en œuvre ses services d'IGC.

L'OSC met en place un service de journalisation et d'audit pour les composantes techniques qu'il opère.

Dans la présente PC, le rôle et les obligations de l'OSC ne sont pas toujours distingués de ceux de l'AC. Cette distinction est précisée dans la DPC.

1.3.5 Porteur de certificats

Un porteur de certificats est une personne physique qui fait nécessairement partie d'une des catégories suivantes :

- Responsable CT d'un Service de l'Etat,
- Responsable Carte d'un Service de l'Etat.

Un porteur de certificat dispose d'une carte AAE qui comporte deux couples (certificat et clé privée associée) :

- « Certificat d'authentification AAE » : certificat à usage d'authentification, généré par l'AC AAE dont les conditions de recevabilité sont décrites dans ce document,
- « Certificat de signature AAE » : certificat à usage de signature électronique, généré par l'AC AAE dont les conditions de recevabilité sont décrites dans ce document.

Chaque couple est activable / déverrouillable par l'usage d'un code PIN (Personal Identification Number) dédié.

Les cartes AAE sont utilisées pour s'authentifier auprès d'un serveur et ou signer électroniquement des documents.

1.3.6 Utilisateur de Certificats (UC)

L'UC est une application, une personne physique ou morale, un organisme administratif ou un système informatique matériel qui utilise un certificat de porteur conformément à la présente PC dans le cadre d'une authentification ou d'une signature électronique.

Dans le cadre de la présente PC, un UC, pour s'assurer de la validité d'un certificat d'un porteur, doit construire et valider un chemin de certification depuis le certificat du porteur jusqu'à une racine de confiance auto-signée qui en la circonstance peut être celle de l'ANTS ou celle de l'IGC/A et doit en outre contrôler les informations de révocation pour chaque élément du chemin de certification (LCR pour le certificat du porteur et LAR pour les certificats d'AC).

1.4 Usage des certificats

1.4.1 Utilisation appropriée des certificats

1.4.1.1 Certificat de l'AC

La bi-clé de l'AC sert à signer des certificats de porteurs et les Listes de Certificats Révoqués (LCR).

Pour cette AC, les chaînes de certificats issues de l'IGC possèdent la structure suivante :

- Certificat d'AC Racine (« AC ANTS V2 ») : certificat électronique auto-signé ;
- Certificat de l'AC AAE : certificat électronique délivré à l'AC AAE par l'AC ANTS V2 ;
- Certificat AAE de porteur : certificat électronique délivré à un porteur par l'AC AAE.

Note : l'AC racine de l'Agence Nationale des Titres sécurisés (« AC ANTS V2 ») a vocation à être signée par l'infrastructure de gestion de la confiance de l'administration « IGC/A ». Dans ce cas la chaîne de certification deviendra IGC/A → AC ANTS V2 → AC AAE → Certificat de porteur.

1.4.1.2 Certificats de porteur

Le porteur dispose de deux certificats :

- le certificat d'authentification sert à authentifier le porteur, typiquement lors d'une authentification du type « client SSL ».
- le certificat de signature électronique sert à signer les documents et vérifier qu'un document a été effectivement signé à l'aide d'une signature électronique sécurisée.

Ces certificats ne sont utilisables que dans le cadre des fonctions qui lui sont dévolues, uniquement sur des postes de travail des Services de l'Etat prévus à cet effet et uniquement sur les applications supportant les cartes AAE à microcircuit qui sont mises à disposition du personnel des Services de l'Etat.

Les certificats ne peuvent être utilisés que conformément aux lois en vigueur et à la règlementation applicable.

1.4.2 Utilisation interdite des certificats

Les utilisations de certificats émis par l'AC à d'autres fins que celles prévues au paragraphe ci-dessus et par la présente PC ne sont pas autorisées.

Dans le cas où cette interdiction serait outrepassée, l'AC ne peut être en aucun cas être tenue pour responsable d'une utilisation des certificats qu'elle émet.

1.5 Gestion de la PC

1.5.1 Organisme responsable de la présente politique

L'ANTS est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente PC.

A cette fin, l'ANTS met en œuvre et coordonne un comité dédié, qui statue à échéances régulières, sur la nécessité d'apporter des modifications à la PC.

1.5.2 Point de contact

La personne responsable est le Directeur de l'ANTS.

Fonction, titre de l'entité responsable	Téléphone	Adresse courrier
Directeur de l'Agence Nationale des Titres Sécurisés	01.77.93.52.10	102/116 rue Victor Hugo 92300 Levallois Perret.

1.5.3 Entité déterminant la conformité d'une DPC avec cette PC

L'ANTS commandite des analyses, des contrôles de conformité et/ou des audits qui aboutissent à l'autorisation ou non pour l'AC d'émettre des certificats. Ces opérations sont réalisés par une société extérieure à l'ANTS.

1.5.4 Procédures d'approbation de la conformité de la DPC

Les personnes ou les sociétés habilitées à déterminer la conformité de la DPC avec la présente PC sont choisies par l'ANTS sur la base, en particulier, de leur capacité à réaliser des évaluations de sécurité. Ces personnes ou ces sociétés sont rémunérées par l'ANTS, mais sont des personnes indépendantes de l'ANTS.

L'ANTS s'assure de la conformité de la DPC avec la présente PC pour la mise en œuvre opérationnelle des composantes de l'IGC.

1.6 Définitions et Acronymes

1.6.1 Acronymes

AA	Autorité Administrative
AC	Autorité de Certification
AC AAE	Autorité de Certification « Acteurs de l'Administration de l'Etat »
AC ACT	Autorité de Certification « Acteurs de Collectivité Territoriale »
ACT	Acteurs de Collectivité Territoriale
AE	Autorité d'Enregistrement
AEC	Autorité d'Enregistrement Centrale
AED	Autorité d'Enregistrement Déléguée
AAE	Acteurs de l'Administration d'Etat
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ANTS	Agence Nationale des Titres Sécurisés
ARL	Authority Revocation List
ARLDP	Authority Revocation List Distribution Point
CC	Critères Communs
CGU	Conditions Générales d'Utilisation
CN	Common Name
CNIL	Commission Nationale de l'Informatique et des Libertés
COMEDEC	Communication Electronique des Données d'Etat Civil
CPS	Centre de Personnalisation des Supports
CRL	Certificate Revocation List
CRLDP	Certificate Revocation List Distribution Point
DPC	Déclaration des Pratiques de Certification
DN	Distinguished Name
HTTPS	HyperText Transfer Protocol Secure
IAS	Identification Authentification Signature
IGC	Infrastructure de Gestion de Clés
IGC/A	Infrastructure de Gestion de Clés de l'Administration
IETF	Internet Engineering Task Force
IN	Imprimerie Nationale
ISO	International Organization for Standardization
LAR	Liste des Autorités Révoquées
LCR	Liste des Certificats Révoqués
NTP	Network Time Protocol
OID	Object Identifier

OC	Opérateur de Certification
OSC	Opérateur de Services de Certification
PC	Politique de Certification
PIN	Personal Identification Number
PUK	Personal Unblocking Key
PSCE	Prestataire de Services de Certification Electronique
PSCO	Prestataire de Services de Confiance
RCS	Registre du Commerce et des Sociétés
RFC	Request For Comments
RGRH	Responsable de Gestion des Ressources Humaines
RGS	Référentiel Général de Sécurité
RSA	Rivest Shamir Adleman
RSSI	Responsable de la Sécurité des Systèmes d'Information
SHA	Secure Hash Algorithm
SIREN	Système d'Identification du Répertoire des Entreprises
SP	Service de Publication
SSL	Secure Socket Layer
UC	Utilisateur de Certificats
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

1.6.2 Définitions

Audit : contrôle indépendant des enregistrements et activités d'un système afin d'évaluer la pertinence et l'efficacité des contrôles du système, de vérifier sa conformité avec les politiques et procédures opérationnelles établies, et de recommander les modifications nécessaires dans les contrôles, politiques, ou procédures.

Autorité de Certification (AC) : entité responsable de garantir le lien (infalsifiable et univoque) entre l'identifiant d'un porteur et une bi-clé cryptographique pour un usage donné. Cette garantie est apportée par des certificats de clé publique qui sont signés par une clé privée de l'AC.

Autorité d'Enregistrement (AE) : entité responsable de la délivrance des supports de clés et des certificats aux porteurs lors d'un face à face. L'AE effectue en outre, les opérations de demandes de certificat. L'AE est un terme générique utilisé pour désigner l'AEC ou une AED au niveau des Services de l'Etat.

Autorité d'Enregistrement Centrale (AEC) : l'autorité d'enregistrement centrale est assurée par l'ANTS. Elle est chargée des services d'enregistrement et de la délivrance des cartes AAE aux Responsables CT.

Autorité d'Enregistrement Déléguée (AED) : l'autorité d'enregistrement au niveau des Services de l'Etat est assurée par le Responsable CT et les Responsables Cartes locaux. Elle est chargée des services d'enregistrement et de la délivrance des cartes AAE et des cartes ACT (décrits dans la [PC ACT]).

Carte AAE : carte à microcircuit, contenant des certificats d'authentification et de signature émis par l'AC AAE, et les clés privées associées, délivrée aux Responsables CT et aux Responsables Cartes.

Carte ACT : carte à microcircuit, contenant des certificats d'authentification et de signature émis par l'AC ACT, et les clés privées associées.

Critères Communs : ensemble d'exigences de sécurité qui sont décrites suivant un formalisme internationalement reconnu. Les produits et logiciels sont évalués par un laboratoire afin de s'assurer qu'ils possèdent des

mécanismes qui permettent de mettent en œuvre les exigences de sécurité sélectionnées pour le produit ou le logiciel évalué.

Cérémonie de clés : Une procédure par laquelle une bi-clé d'AC est générée, sa clé privée transférée éventuellement sauvegardée, et/ou sa clé publique certifiée.

Certificat électronique: fichier électronique attestant qu'une clé publique appartient à la personne physique ou morale identifiée dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identifiant de la personne physique ou morale et la bi-clé. Le certificat est valide uniquement s'il est utilisé pendant une durée donnée précisée dans celui-ci.

Dans le cadre de la présente PC, le terme "certificat électronique" désigne un certificat délivré à une personne physique et portant sur une bi-clé d'authentification ou de signature, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

Certificat d'AC : certificat pour une AC émis par une autre AC. [X.509].

Certificat d'AC auto signé : certificat d'AC signé par la clé privée de cette même AC.

Chemin de certification : (ou chaîne de confiance, ou chaîne de certification) chaîne constituée de plusieurs certificats nécessaires pour valider un certificat vis-à-vis d'un certificat d'AC auto-signé.

Clé privée : clé de la bi-clé asymétrique d'une entité qui doit être uniquement utilisée par cette entité [ISO/IEC 9798-1].

Clé publique : clé de la bi-clé asymétrique d'une entité qui peut être rendue publique. [ISO/IEC 9798-1].

Composante : plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC.

Compromission : violation, avérée ou soupçonnée, d'une politique de sécurité, au cours de laquelle la divulgation non autorisée, ou la perte de contrôle d'informations sensibles, a pu se produire. En ce qui concerne les clés privées, une compromission est constituée par la perte, le vol, la divulgation, la modification, l'utilisation non autorisée, ou d'autres compromissions de cette clé privée.

Confidentialité : la propriété qu'a une information de n'être pas rendue disponible ou divulguée aux individus, entités, ou processus non autorisés.

Déclaration des Pratiques de Certification (DPC) : document qui identifie et référence les pratiques (organisation, procédures opérationnelles, moyens techniques et humains) que l'AC applique dans le cadre de la fourniture de ses services de certification électronique aux usagers et en conformité avec la ou les politiques de certification qu'elle s'est engagée à respecter.

Demande de certificat : message transmis par une entité AE à l'AC pour obtenir l'émission d'un certificat d'AC.

Disponibilité : propriété d'être accessible sur demande, à une entité autorisée [ISO/IEC 13335-1:2004].

Dispositif de création de signature : matériel et/ou logiciel utilisé par le porteur pour stocker et mettre en œuvre sa clé privée de signature.

Données d'activation : valeurs de données, autres que des clés, qui sont nécessaires pour exploiter les modules cryptographiques ou les éléments qu'ils protègent et qui doivent être protégées (par ex. un PIN, une phrase secrète, …).

Fonction de hachage : fonction qui lie des chaînes de bits à des chaînes de bits de longueur fixe, satisfaisant ainsi aux trois propriétés suivantes :

- Il est impossible, par un moyen de calcul, de trouver, pour une sortie donnée, une entrée qui corresponde à cette sortie;
- Il est impossible, par un moyen de calcul, de trouver, pour une entrée donnée, une seconde entrée qui corresponde à la même sortie [ISO/IEC 10118-1];
- Il est impossible par calcul, de trouver deux données d'entrées différentes qui correspondent à la même sortie.

Infrastructure de gestion de clés (IGC) : ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques utilisés par des services de confiance.

Infrastructure à Clé Publique (ICP) : IGC dédiée à la gestion de clés asymétriques. C'est l'infrastructure requise pour produire, distribuer, gérer des clés publiques et privées, des certificats et des Listes de Certificats Révoqués.

Intégrité : fait référence à l'exactitude de l'information, de la source de l'information, et au fonctionnement du système qui la traite.

Interopérabilité : implique que le matériel et les procédures utilisés par deux entités ou plus sont compatibles; et qu'en conséquence il leur est possible d'entreprendre des activités communes ou associées.

Liste de Certificats Révoqués (LCR) : liste signée numériquement par une AC et qui contient des identités de certificats qui ne sont plus valides. La liste contient l'identité de la LCR d'AC, la date de publication, la date de publication de la prochaine LCR et les numéros de série des certificats révoqués.

Module cryptographique : ensemble de composants logiciels et matériels utilisés pour mettre en œuvre une clé privée afin de permettre des opérations cryptographiques (signature, chiffrement, authentification, génération de clé …). Dans le cas d'une AC, le module cryptographique est une ressource cryptographique matérielle évaluée et certifiée (FIPS ou critères communs), utilisé pour conserver et mettre en œuvre la clé privée AC.

Période de validité d'un certificat : période pendant laquelle l'AC garantit qu'elle maintiendra les informations concernant l'état de validité du certificat. [RFC 2459].

PKCS #10 : (Public-Key Cryptography Standard #10) mis au point par RSA Security Inc., qui définit une structure pour une Requête de Signature de Certificat (en anglais: Certificate Signing Request: CSR).

Plan de secours (après sinistre) : plan défini par une AC pour remettre en place tout ou partie de ses services d'ICP après qu'ils aient été endommagés ou détruits à la suite d'un sinistre, ceci dans un délai défini dans l'ensemble PC/DPC.

Point de distribution de LCR *:* entrée de répertoire ou une autre source de diffusion des LCR; une LCR diffusée via un point de distribution de LCR peut inclure des entrées de révocation pour un sous-ensemble seulement de l'ensemble des certificats émis par une AC, ou peut contenir des entrées de révocations pour de multiples AC. [ISO/IEC 9594-8; ITU-T X.509].

Politique de Certification (PC) : ensemble de règles, identifié par un nom (OID), définissant (a) les exigences auxquelles une AC se conforme dans la mise en place et la fourniture de ses prestations et indiquant l'applicabilité d'un certificat à une communauté particulière et/ou à une classe d'applications avec des exigences de sécurité communes (b) les obligations et exigences portant sur les autres intervenants, notamment les porteurs et les utilisateurs de certificats.

Politique de sécurité : ensemble de règles édictées par une autorité de sécurité et relatives à l'utilisation, la fourniture de services et d'installations de sécurité [ISO/IEC 9594-8; ITU-T X.509].

Porteur : personne physique qui est un fonctionnaire de l'Etat, un acteur d'une Collectivité Territoriale, un contractant de l'ANTS ou d'un Service de l'Etat, qui dispose d'une carte AAE comportant deux couples clé privée/certificat, l'un à usage d'authentification et l'autre à usage de signature électronique.

Porteur de secret : personne qui détient une donnée d'activation liée à la mise en œuvre de la clé privée d'une AC à l'aide d'un module cryptographique.

Prestataire de services de confiance (PSCO) : personne offrant des services tendant à la mise en œuvre de fonctions qui contribuent à la sécurité des informations échangées par voie électronique [Ordonnance n°2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives].

Prestataire de services de certification électronique (PSCE) : un PSCE se définit comme toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE est un type de PSCO particulier.

Primo ACT : personne désignée par la convention signée par une collectivité territoriale pour être le porteur de la première carte ACT émise pour cette collectivité territoriale par l'AED du Service de l'Etat de rattachement selon le référentiel des départements.

Qualificateur de politique : informations concernant la politique qui accompagnent un identifiant de politique de certification (OID) dans un certificat X.509. [RFC 3647]

Qualification d'un prestataire de services de certification électronique : le [DécretRGS] décrit la procédure de qualification des PSCO. Un PSCE étant un PSCO particulier, la qualification d'un PSCE est un acte par lequel un

organisme de certification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) à certaines exigences d'une PC Type pour un niveau de sécurité donné et correspondant au service visé par les certificats.

Qualification d'un produit de sécurité : acte par lequel l'ANSSI atteste de la capacité d'un produit à assurer, avec un niveau de robustesse donné, les fonctions de sécurité objet de la qualification. L'attestation de qualification indique le cas échéant l'aptitude du produit à participer à la réalisation, à un niveau de sécurité donné, d'une ou plusieurs fonctions traitées dans le [RGS]. La procédure de qualification des produits de sécurité est décrite dans le [DécretRGS].

Responsable Carte : porteur de carte AAE, disposant par défaut des droits nécessaires pour effectuer les demandes d'enregistrement et la délivrance des cartes AAE aux Responsables Cartes, et des cartes ACT aux Primo ACT des collectivités territoriales rattachées au domaine de responsabilités des Services de l'Etat selon les données fournies par le référentiel des départements.

Responsable CT : personne chargée des relations avec les collectivités territoriales, nommée par le Secrétaire Général de la préfecture. Il est à ce titre le porteur de la première carte AAE émise par l'ANTS pour le Service de l'Etat concerné. Il est chargé, dans son rôle d'AED d'effectuer les demandes d'enregistrement et la délivrance des cartes AAE aux Responsables Cartes locaux, et des cartes ACT aux Primo ACT des collectivités territoriales rattachées au domaine de responsabilités du Services de l'Etat.

RSA : algorithme de cryptographie à clé publique inventé par Rivest, Shamir, et Adleman.

Service de l'Etat : désigne soit la préfecture du département soit une sous-préfecture du département.

Signature électronique: 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.

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.

Signature numérique : somme de contrôle cryptographique générée en utilisant une fonction de hachage et une clé privée et vérifiable en utilisant une clé publique.

Utilisateur de Certificats (UC) : application, personne physique ou morale, organisme administratif ou système informatique matériel qui utilise un certificat de porteur conformément à la présente PC dans le cadre d'une authentification ou d'une signature électronique.

Validation d'un certificat électronique : opération de contrôle permettant d'avoir l'assurance que les informations contenues dans le certificat ont été vérifiées par une ou des autorités de certification (AC) et sont toujours valides. La validation d'un certificat inclut entre autres la vérification de sa période de validité, de son état (révoqué ou non), de l'identité des AC et la vérification de la signature électronique de l'ensemble des AC contenues dans le chemin de certification. Elle inclut également la validation du certificat de l'ensemble des AC du chemin de certification. La validation d'un certificat électronique nécessite au préalable de choisir le certificat auto-signé qui sera pris comme référence.

2 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

2.1 Entités chargées de la mise à disposition des informations

Le service de publication est le service en charge de la publication du présent document et des autres documents ou informations dont la publication est nécessaire afin d'assurer la bonne utilisation des certificats délivrés au titre de la présente PC.

Le SP est chargé de mettre à disposition les informations, citées ci-après, au niveau de l'Internet. La DPC précise les différentes interfaces du SP en fonction des informations à publier.

2.2 Informations devant être publiées

L'AC s'assure que les termes et conditions applicables à l'usage des certificats qu'elle délivre sont mis à la disposition des porteurs et des UC.

L'AC, via le SP, rend disponibles les informations suivantes via l'URL https://sp.ants.gouv.fr/antsv2/index.html :

- La PC ;
- Les certificats de l'AC AAE et les autres certificats utiles;
- Les conditions générales d'utilisation [CGU] ;
- Les guides pour les porteurs et pour les utilisateurs de certificats :

Les LCR sont publiées aux points de distribution des LCR (CRL Distribution Points). Chaque certificat comporte l'adresse du point de distribution de la LCR le concernant.

Nota : A partir du moment où l'AC ANTS V2 sera rattachée à l'IGC/A, le SP indiquera les liens permettant de vérifier un chemin de certification jusqu'au niveau de l'IGC/A.

2.3 Délais et fréquences de publication

La PC de l'AC et les documentations relatives aux demandes de certificat et de révocation sont accessibles 24 heures sur 24, 7 jours sur 7.

Le certificat de l'AC Racine ANTS V2 à laquelle est rattachée l'AC AAE est publié préalablement à toute diffusion de certificats porteurs ou de LCR avec une disponibilité de 24h/24 7j/7.

2.4 Contrôle d'accès aux informations publiées

Le SP s'assure que les informations sont disponibles, protégées contre les modifications non autorisées et sont accessibles en lecture uniquement pour les porteurs et les utilisateurs de certificats (UC).

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).

L'AC s'assure que toute information conservée dans une base documentaire de son IGC et dont la diffusion est publique ou la modification n'est pas autorisée est protégée.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Dans chaque certificat X 509, le fournisseur (Issuer) et le porteur (Subject) sont identifiés par un nom distinctif, en anglais « Distinguished Name » (DN). Les identifiants utilisés dans un certificat sont conforme à la norme X.501.

3.1.1.1 Certificat de l'AC Acteurs de l'Administration de l'Etat

Les identifiants utilisés dans le certificat de l'AC AAE sont les suivants :

Champ de base	Valeur
Issuer DN	C=FR O=Gouv OU=0002 130003262 CN=Autorité de certification ANTS V2
Subject DN	C=FR O=Agence Nationale des Titres Sécurisés OU=0002 130003262 CN=Autorité de certification porteur AAE 3 étoiles

3.1.1.2 Certificat de porteur

L'identité du porteur dans le certificat du porteur est la suivante :

Champ de base	Valeur
Issuer DN	C=FR O=Agence Nationale des Titres Sécurisés OU=0002 130003262 CN=Autorité de certification porteur AAE 3 étoiles
Subject DN	C=FR O=<nom du Service de l'Etat > OU=0002 <espace> <Numéro SIREN du Service de l'Etat> CN= <prénom nom identifiant> (le séparateur est le caractère « espace »)

L'identifiant est un nombre de dix chiffres suivi de deux caractères. L'unicité de cet identifiant est assurée par le référentiel des identités.

Pour des raisons de test des certificats de porteurs de test peuvent être émis par l'AC AAE. Le certificat de porteur comporte alors la valeur « TEST » apposé dans le CN avant le <prénom nom identifiant>.

3.1.2 Nécessité d'utilisation de noms explicites

Les identités incluses dans les certificats émis conformément à la présente PC sont toujours explicites et nominatives. Le nom de famille ou le nom d'usage et le premier prénom du porteur sont ceux qui correspondent à l'identité du porteur (personne physique).

3.1.3 Pseudonymisation des porteurs

L'identité utilisée dans les certificats de porteurs n'est ni un pseudonyme ni un nom anonyme.

3.1.4 Règles d'interprétations des différentes formes de noms

Les UC (applications, réseaux, machines, organisme extérieurs, …) et les porteurs peuvent se servir des certificats d'AC et de porteurs pour mettre en œuvre et valider des fonctions de sécurité, en vérifiant entre autres les identifiants (DN) des porteurs et des AC contenues respectivement dans les certificats de porteur et d'AC.

3.1.5 Unicité des noms

Les DN des certificats porteurs sont uniques au sein du domaine de certification de l'AC qui émet le certificat. Durant toute la durée de vie de l'AC AAE, un DN attribué à un porteur ne peut être attribuée à un autre porteur.

3.1.6 Identification, authentification et rôle des marques déposées

Sans objet pour les marques déposées.

3.2 Vérification initiale d'identité

L'enregistrement d'un futur porteur peut se faire soit directement auprès de l'AEC, soit via un mandataire de certification, en la circonstance une personne d'une AED.

La vérification initiale de l'identité d'un futur porteur et de son rattachement à un Service de l'Etat est réalisée, selon le type de porteur, de la manière suivante :

pour l'enregistrement d'un Responsable CT: la validation est effectuée par l'AEC.

pour l'enregistrement d'un Responsable Carte: la validation est effectuée par le Responsable CT ou par un autre Responsable Carte du même site déjà en possession de sa carte AAE.

3.2.1 Méthode pour prouver la possession de la clé privée

Les clés privées initiales sont générées par l'AC. Seule la personne possédant à la fois la carte AAE et un code d'activation initial est en mesure d'utiliser les clés privées.

Lors d'un premier renouvellement des clés privées, les bi-clés sont générées par la carte AAE. Il est alors vérifié que les clés privées ont bien été générées dans le support initialement en possession du porteur. De ce fait, seul le porteur original est en mesure d'utiliser les nouvelles clés privées.

3.2.2 Validation de l'identité d'un organisme

Sans objet.

3.2.3 Validation de l'identité des porteurs

Le processus de validation de l'identité des porteurs diffère selon le type du porteur.

Pour les certificats de test, la demande de certificat doit référencer un protocole de test ou indiquer de manière explicite dans le dossier de souscription que le certificat est délivré à titre de test.

Pour un Responsable CT

Le dossier d'enregistrement du Responsable CT déposé au format papier auprès de l'AEC (ANTS) comprend :

- un formulaire d'enregistrement (identification des interlocuteurs en préfecture) rempli avec :
    - les informations sur le site de rattachement,
    - les éléments inscrits sur le document officiel d'identité :
        - **le nom complet** équivalent à un des noms inscrit sur le document officiel d'identité (*nom de famille* ou *nom d'usage*) ;

- **le premier prénom (**Le premier prénom figure en début de liste, et peut ainsi être un prénom composé (deux prénoms séparés par un tiret) ;
- **la date de naissance**.

- une adresse de messagerie et un numéro de téléphone permettant de contacter le futur porteur. Cette adresse de messagerie permet à l'ANTS d'informer le Responsable CT des mises à jour relatives aux procédures d'enregistrements.
- une adresse nominative dans un Service de l'Etat pour l'expédition du code d'activation temporaire du porteur.

Après avoir vérifié le contenu du dossier fourni, les personnes chargées des opérations d'AEC saisissent d'abord les informations du futur porteur dans le référentiel d'identité. Ces personnes doivent s'assurer de l'intégrité des éléments enregistrés. Ensuite, elles effectuent la demande via le portail dédié à l'adresse https://www.asscap.agents-ctae-sec.ants.gouv.fr/. Enfin, elles procèdent à l'archivage du dossier papier.

L'authentification du Responsable CT est réalisée dans le Service de l'Etat concerné lors de la remise de la carte AAE en face-à-face physique, par une personne mandatée par l'ANTS qui s'assure de l'identité du Responsable CT à l'aide d'un document officiel d'identité en cours de validité comportant une photographie d'identité (une carte d'identité, un passeport ou un titre de séjour).

La personne mandatée par l'ANTS procède, lors de cette authentification, à une copie du document officiel d'identité du futur Responsable CT. Cette copie est signée par la personne mandatée par l'ANTS qui effectue la remise et le futur Responsable CT. Ces signatures sont précédées par la mention « *Copie certifiée conforme à l'original* ». Cette copie, tout comme le reste du « dossier papier », est conservée par l'AEC et tenue à disposition de l'AC.

Ces dispositions permettent d'être conforme au niveau (***).

Pour un Responsable Carte

Les demandes de certificats pour les Responsables Cartes sont effectuées soit par le Responsable CT, soit par un autre Responsable Carte du même site.

Le dossier d'enregistrement des Responsables Cartes, est constitué de deux parties :

- le « dossier papier » composé d'une fiche d'identification désignant le Responsable Carte.
- les informations contenues dans le référentiel des identités :
  - les éléments inscrits sur le document officiel d'identité :
    - **le nom complet** équivalent à un des noms inscrit sur le document officiel d'identité (*nom de famille* ou *nom d'usage*) ;
    - **le premier prénom** (Le premier prénom figure en début de liste, et peut ainsi être un prénom composé (deux prénoms séparés par un tiret) ;
    - **la date de naissance**.
  - une adresse de messagerie et un numéro de téléphone permettant de contacter le futur porteur. Cette adresse de messagerie permet à l'ANTS d'informer le Responsable Carte des mises à jour relatives aux procédures d'enregistrements.
  - une adresse nominative du futur porteur dans un Service de l'Etat pour l'expédition du code d'activation temporaire du porteur,
  - une adresse nominative du demandeur dans un Service de l'Etat pour l'expédition de la carte AAE du porteur.

Le Responsable CT ou un Responsable Carte du Service de l'Etat saisit d'abord les informations du futur porteur dans le référentiel d'identité. Les données recueillies dans le dossier d'enregistrement doivent être rigoureusement retranscrites dans le référentiel d'identité. Le Responsable CT ou le Responsable Carte, en charge de la saisie, doit s'assurer de l'intégrité des éléments enregistrés.

Ensuite, il effectue la demande via un portail dédié. Après avoir effectué l'opération de la demande, le dossier est archivé sur le site.

L'authentification d'un Responsable Carte est réalisée lors d'un face à face physique lors de la remise de la carte AAE par le Responsable CT ou un autre Responsable Carte. Ce dernier s'assure de l'identité du porteur à l'aide d'un document officiel d'identité en cours de validité comportant une photographie d'identité (une carte d'identité, un passeport ou un titre de séjour).

Le Responsable CT ou un autre Responsable Carte procède, lors de cette authentification, à une copie du document officiel d'identité du nouveau Responsable Carte. Cette copie est signée par le Responsable CT ou le Responsable Carte qui effectue la remise et le nouveau Responsable Carte. Ces signatures sont précédées par la mention « *Copie certifiée conforme à l'original* ». Cette copie, tout comme le reste du « dossier papier », est conservée par l'AED et tenue à disposition de l'AC.

Ces dispositions permettent d'être conforme au niveau (***).

3.2.4 Informations non vérifiées du porteur

Aucune information non vérifiée n'est introduite dans les certificats.

3.2.5 Validation de l'autorité du demandeur

Cette étape est effectuée lors de la validation de l'identité de la personne physique directement par l'AE.

3.2.6 Certification croisée d'AC

L'AC AAE est uniquement rattachée à l'AC ANTS V2. Tout autre rattachement n'est pas autorisé.

3.3 Identification et validation d'une demande de renouvellement des clés

3.3.1 Identification et validation pour un renouvellement courant

On distingue deux types de renouvellement : le renouvellement de certificats avec ou sans changement de carte AAE.

Le premier renouvellement est un renouvellement de certificats. Lors de ce renouvellement, le porteur est invité par un courriel à se connecter à un portail qui lui permet de renouveler à la fois ses deux clés privées et ses certificats. Dans ce cas, les bi-clés sont générées par la carte AAE.

Avant l'envoi du courriel, l'AC s'assure que les informations du dossier d'enregistrement initial sont toujours valides et que le certificat à renouveler existe, et est toujours valide. Cette disposition permet d'être conforme au niveau (***).

Le renouvellement suivant est un renouvellement de carte AAE. Il suit le même processus que celui de la première demande de carte AAE : le porteur reçoit un courrier postal contenant le code d'activation et qui l'invite à retirer sa carte AAE auprès de l'AED de rattachement. Dans ce cas, les bi-clés sont générées par l'AC.

Si lors du premier renouvellement l'un des certificats à renouveler a été révoqué, alors les conditions de la section § 3.2.3 s'appliquent.

3.3.2 Identification et validation pour un renouvellement après révocation

Les vérifications aux fins de renouvellement de clés après révocation du certificat sont identiques à celles prévues pour un renouvellement de carte (Cf. § 3.3.1).

3.4 Identification et validation d'une demande de révocation

La révocation d'un certificat porteur entraine la révocation du deuxième certificat hébergé sur la même carte AAE.

Un certificat porteur peut être révoqué par :

- le porteur au nom duquel le certificat a été émis,
- le Responsable CT ou un Responsable Carte du site du porteur,

- un agent de l'ANTS dans son rôle d'AEC.

Un service en ligne à l'adresse https://www.asscap.agents-ctae.ants.gouv.fr/ accessible sur internet en mode HTTPS, est mis à disposition des porteurs pour effectuer les demandes de révocation. Les utilisateurs de ce service sont formellement authentifiés sur la base d'un mot de passe personnel[1] et d'une série de trois questions. Cette disposition permet d'être conforme au niveau (***).

Si le porteur n'est pas en mesure de présenter les quatre bonnes réponses, il doit alors s'adresser au personnel de l'AED qui lui a remis sa carte AAE. Les Responsables Cartes assurant leur rôle d'AED, après s'être authentifié à l'aide de leur carte AAE, sont en mesure de révoquer toute personne appartenant aux sites rattachés à l'AED.

En dernier recours, l'AEC (ANTS) peut également prendre en charge toute demande de révocation issue des porteurs de n'importe quel site.

[1] Ce mot de passe a été choisi par le porteur lors de l'activation de son support.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Les personnes habilitées à enregistrer une demande de certificats sont :

- les agents de l'ANTS (rôle d'AEC) ;
- les Responsables CT (rôle d'AED) ;
- les Responsables Cartes (rôle d'AED).

4.1.2 Processus et responsabilités pour l'établissement d'une demande de certificat

Le contenu des dossiers de demande de certificat est décrit au § 3.2.3.

Une validation des demandes de certificat est effectuée par le service d'enregistrement avant sa transmission à l'AC pour y être traitée.

Pour une demande de certificat, l'AE (AEC ou AED) en charge de la validation de la demande doit signer une attestation de validation incorporant également une acceptation de son rôle de confiance.

4.2 Traitement d'une demande de certificat

4.2.1 Exécution des processus d'identification et de validation de la demande

L'autorité d'enregistrement (AEC ou AED) procède pour chaque demande à un contrôle et à une validation du dossier d'enregistrement comme décrit dans § 3.2.3.

Des photocopies des justificatifs d'identité et des notes de services sont conservées et archivées soit à l'ANTS pour les Responsables CT, soit à l'ANTS ou/et sur le site de porteur pour les Responsables Cartes.

4.2.2 Acceptation ou rejet de la demande

Un rejet peut intervenir au moment de la demande de certificats par l'AE. A titre d'exemple, il n'est pas possible de demander des certificats si une demande est déjà en cours.

4.2.3 Durée d'établissement d'un certificat

La durée d'établissement d'un certificat est d'au plus quelques jours.

4.3 Délivrance d'un certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AEC ou de l'AED, l'AC déclenche les processus de génération de la carte AAE, des certificats du porteur et du code d'activation temporaire. Les conditions de génération des bi-clés et des certificats et les mesures de sécurité sont précisées aux sections § 5 et 6.

4.3.2 Notification par l'AC de la délivrance du certificat au porteur

Le futur porteur est informé par un courrier postal sécurisé que sa carte AAE est à sa disposition. Ce courrier postal contient un code d'activation temporaire qu'il aura à présenter pour pouvoir activer sa carte AAE.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

4.4.1.1 Remise de la carte AAE

Seule l'autorité d'enregistrement (AEC, AED) qui a fait la demande peut faire la remise de carte AAE.

Selon le type de porteur, le processus de remise d'une carte AAE est diffèrent :

Remise de carte pour un Responsable CT

Le processus de remise de la carte AAE au Responsable CT se déroule comme suit :

- une personne mandatée par l'AEC se rend dans le Service de l'Etat concerné ;
- elle vérifie l'identité du futur porteur à l'aide d'un document officiel d'identité ;
- elle effectue une copie du document officiel d'identité ;
- elle signe avec le futur Responsable CT le document officiel d'identité avec la mention « Copie certifiée conforme à l'original » ;
- elle remet la carte AAE au porteur ;
- elle enregistre la remise de carte dans l'application de gestion de cartes;
- le porteur active sa carte AAE comme décrit dans 4.4.1.2 ;
- il signe électroniquement l'attestation d'acceptation au moyen de sa clé privée de signature ;
- la personne mandatée de l'AEC appose sa signature électronique sur l'attestation d'acceptation.

Remise de carte pour un Responsable Carte

Un Responsable CT ou un Responsable Carte

- le Responsable CT ou un Responsable Carte dans le rôle d'AED vis-à-vis du futur porteur, vérifie l'identité du futur porteur à l'aide d'un document officiel d'identité s'il ne le connait pas et en effectue une copie ;
- il signe avec le futur Responsable Carte le document officiel d'identité avec la mention « Copie certifiée conforme à l'original » ;
- il lui remet la carte AAE ;
- il enregistre la remise de carte dans l'application de gestion de cartes ;
- le porteur active sa carte AAE comme décrit dans 4.4.1.2 ;
- il signe électroniquement l'attestation d'acceptation au moyen de sa clé privée de signature ;
- le Responsable CT ou un Responsable Carte appose sa signature électronique sur l'attestation d'acceptation.

Ces dispositions permettent d'être conforme au niveau (***).

4.4.1.2 Activation de la carte AAE

L'activation d'une carte AAE par son porteur n'est possible qu'une fois qu'une attestation électronique de remise de carte AAE a été signée par une personne de l'entité AE (AEC ou AED). Pour activer sa carte AAE, le porteur doit se connecter au portail dédié https://www.asscap.agents-ctae.ants.gouv.fr/ en utilisant un poste de travail professionnel équipé d'un lecteur de carte à microcircuit.

Le porteur doit alors contrôler l'identifiant (DN) qui figure dans ses certificats. Il doit ensuite utiliser son code d'activation temporaire et choisir ensuite ses codes PIN (l'un pour l'authentification et l'autre pour la signature électronique), définir un mot de passe personnel et les réponses à trois questions qui lui seront demandées s'il doit révoquer ou débloquer ses certificats plus tard, puis signer l'attestation d'acceptation au moyen de sa clé privée de signature.

Le porteur ne pourra utiliser sa carte AAE, dans le cadre des fonctions qui lui sont dévolues, qu'à partir du moment où l'attestation d'acceptation de carte AAE aura été signée à son tour par l'entité AE concernée (AEC ou l'AED). Cette opération de double-signature peut porter sur un ou plusieurs porteurs.

4.4.1.3 Renouvellement des certificats

Le porteur est invité à renouveler ses certificats une seule fois en utilisant la même carte AAE. Pour cela, il doit se connecter l'application de gestion de cartes, s'authentifier à l'aide de son code PIN d'authentification.

Le renouvellement suivant des certificats s'effectue avec la génération d'une nouvelle carte AAE.

4.4.2 Publication du certificat

Après l'acceptation de la carte AAE par le porteur, ses certificats sont enregistrés dans le référentiel des identités sous la responsabilité de l'ANTS.

Nota : les certificats des porteurs ne sont pas publiés par le SP.

4.4.3 Notification par l'AC aux autres entités de la délivrance du certificat

L'ensemble des composantes de l'IGC, à l'exception du SP, est informé de la délivrance du certificat.

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisations de la clé privée et du certificat par le porteur

Les usages autorisés des bi-clés et des certificats sont définis au § 1.4.1.2 ci-dessus.

Le porteur dispose de deux clés privées :

- une clé privée pour l'authentification ;
- une clé privée pour les signatures électroniques.

L'usage d'une bi-clé et du certificat associé est indiqué dans le certificat lui-même, via les extensions concernant les usages des bi-clés (voir § 6.1.7).

Certificats d'authentification

Les bi-clés et les certificats générés dans le cadre de la PC pour les certificats d'authentification sont uniquement destinés à l'authentification des porteurs.

Certificats de signature

Les bi-clés et les certificats générés dans le cadre de la PC pour les certificats de signature sont uniquement destinés à la génération ou à la vérification de signatures électroniques sécurisées.

Cet usage est également explicité dans les conditions générales d'utilisation qui sont fournies au porteur lors de la remise de la carte AAE. Le porteur est tenu de les respecter.

4.5.2 Utilisation de la clé publique et du certificat par un utilisateur du certificat

Un utilisateur de certificat doit utiliser des logiciels qui sont à même de vérifier que le certificat d'un porteur est effectivement utilisé selon l'usage prescrit dans le certificat (authentification ou signature électronique). S'il n'utilise pas les logiciels prévus à cet effet, sa responsabilité pourrait être engagée.

Un utilisateur de certificat (UC) doit utiliser un logiciel qui vérifie que le certificat est valide. La vérification que doit effectuer le logiciel est différente selon qu'il s'agit de la vérification en temps-réel d'un échange d'authentification ou de la vérification en temps réel ou en temps différé d'une signature électronique.

Pour la vérification en temps-réel d'un échange d'authentification, le logiciel doit construire un chemin de certification entre le certificat du porteur et le certificat auto-signé de l'AC ANTS V2 (ou ultérieurement le certificat auto-signé de l'IGC/A), et s'assurer qu'au moment de l'échange, aucun des certificats du chemin n'est révoqué ou en dehors de sa période de validité.

Pour la vérification en temps différé d'une signature électronique, le logiciel doit construire un chemin de certification entre le certificat du porteur et le certificat auto-signé de l'AC ANTS V2 (ou ultérieurement le certificat auto-signé de l'IGC/A), et s'assurer qu'au moment où la signature numérique a été horodatée par une unité d'horodatage de confiance qu'aucun des certificats du chemin n'était en dehors de sa période de validité ou révoqué. Il doit en outre s'assurer que le certificat de l'unité d'horodatage était valide à la date où le tampon d'horodatage a été apposé.

4.6 Renouvellement d'un certificat

Nota - Conformément au [RFC3647], la notion de "renouvellement de certificat" correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique).

Dans la cadre de la présente PC, il ne peut pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé correspondante. La délivrance d'un nouveau certificat suite à changement de la bi-clé est traitée à la section 4.7.

4.6.1 Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification au porteur de l'établissement du nouveau certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6 Publication du nouveau certificat

Sans objet.

4.6.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat

Sans objet.

4.7 Délivrance d'un nouveau certificat suite à changement de la bi-clé

Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat au porteur liée à la génération d'une nouvelle bi-clé.

4.7.1 Causes possibles de changement d'une bi-clé

Une bi-clé et un certificat peuvent être renouvelés parce que le certificat est sur le point d'expirer ou suite à la révocation du certificat du porteur (cf. § 4.9, notamment le § 4.9.1 pour les différentes causes possibles de révocation) ou pour anticiper un renouvellement massif de certificats.

4.7.2 Origine d'une demande d'un nouveau certificat

En temps normal, le certificat est renouvelé peu de temps avant son expiration:

- la première fois, puis une fois sur deux seuls les certificats sont renouvelés (la carte est conservée). Dans ce cas, le renouvellement des bi-clés et des certificats s'effectue en ligne.
- la fois suivante, puis une fois sur deux, une nouvelle carte AAE est générée et les certificats sont renouvelés.

4.7.3 Procédure de traitement d'une demande d'un nouveau certificat

Quelques semaines avant la fin de validité d'un certificat, l'AC ajoute automatiquement à la liste des demandes initiales de certificats à valider, les demandes de renouvellement de certificats à valider. Ces demandes sont ventilées auprès des personnes ayant le rôle d'AED.

Ces personnes vérifient que les personnes pour lesquelles le renouvellement est demandé font toujours partie de leurs effectifs et, si cela est le cas, valident la demande de renouvellement.

Pour une demande de renouvellement, l'AE (AEC ou AED) en charge de la validation de la demande doit signer une attestation de validation de renouvellement incorporant également une acceptation de son rôle de confiance.

4.7.4 Notification au porteur de l'établissement du nouveau certificat

Lorsque la carte AAE est conservée, le porteur est invité par la réception d'un courriel à effectuer le renouvellement des bi-clés et des certificats en se connectant à un portail dont l'adresse est spécifiée dans ce courriel.

Lorsque la carte AAE est changée et une fois que la nouvelle carte AAE a été fabriquée, le porteur est invité par la réception d'un courrier postal à retirer sa nouvelle carte. La procédure est alors analogue à un retrait de carte initial.

Lorsque les certificats d'une carte AAE ont été révoqués, le porteur est invité par la réception d'un courrier postal à retirer sa nouvelle carte AAE. La procédure est alors analogue à un retrait de carte initial.

Lors d'un renouvellement anticipé, le porteur peut recevoir, selon le cas, un courriel ou un courrier postal avant la date anniversaire.

4.7.5 Démarche d'acceptation du nouveau certificat

Lorsqu'il s'agit de la délivrance d'une nouvelle carte AAE, se reporter à la section § 4.4.1.

Lorsqu'il s'agit d'un renouvellement des bi-clés et des certificats sans changement de carte, le porteur se connecte à un portail en utilisant sa carte AAE. Il doit alors suivre les instructions données par le portail.

4.7.6 Publication du nouveau certificat

Après l'acceptation des certificats par le porteur, ceux-ci sont enregistrés dans le référentiel des identités sous la responsabilité de l'ANTS.

4.7.7 Notification par l'AC aux autres entités de la délivrance du nouveau certificat

L'ensemble des composantes de l'IGC, à l'exception du SP, est informé de la délivrance du certificat.

4.8 Modification du certificat

Dans la cadre de la présente PC, la modification de certificat n'est pas autorisée. Toute demande de modification se traduit par une demande de nouveau certificat, détaillée dans les sections 4.1 et 4.2.

4.8.1 Causes possibles de modification d'un certificat

Sans objet.

4.8.2 Origine d'une demande de modification d'un certificat

Sans objet.

4.8.3 Procédure de traitement d'une demande de modification d'un certificat

Sans objet.

4.8.4 Notification au porteur de l'établissement du certificat modifié

Sans objet.

4.8.5 Démarche d'acceptation du certificat modifié

Sans objet.

4.8.6 Publication du certificat modifié

Sans objet.

4.8.7 Notification par l'AC aux autres entités de la délivrance du certificat modifié

Sans objet.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificats de porteurs

Un certificat porteur est révoqué quand l'association entre ce certificat, la clé publique et le porteur qu'il certifie n'est plus considérée comme valide. Les motifs qui invalident cette association peuvent être :

- le changement d'affectation du porteur ;
- le décès du porteur ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur ;
- l'information contenue dans le DN du certificat n'est plus valide (par exemple, changement de nom) ;
- le porteur n'a pas respecté les modalités applicables à l'utilisation du certificat ;
- le support de clés du porteur a été perdu ou volé ;
- le support de clés du porteur a été endommagé ;
- l'un des PIN a été compromis ou est suspecté d'avoir été compromis ;
- le support de clés du porteur est bloqué et ne peut être débloqué ;
- le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- le porteur n'a pas respecté ses obligations découlant de cette PC;
- la modification de la taille des clés imposée par des institutions nationales compétentes ;
- la perte de l'autorisation de possession d'un certificat.

Lorsque l'une quelconque de ces occurrences se produit, le certificat du porteur en question doit être révoqué.

4.9.1.2 Certificats d'une composante de l'IGC

Une composante de l'IGC est une plate-forme jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC. Les composantes de l'IGC disposant d'un certificat et visibles depuis l'extérieur sont :

- l'AC elle-même, qui utilise la même clé et donc le même certificat que l'émetteur de LCR.
- les sites web et les référentiels accessibles en mode HTTPS aux utilisateurs pour effectuer les fonctions d'enregistrement, de révocation, de déblocage de PIN ou de changement de PIN.

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats ou de LCR) :

- suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- cessation d'activité de l'entité opérant la composante.

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'un site web accessible en mode HTTPS et utilisé par l'AC:

- suspicion de compromission, compromission, perte ou vol de la clé privée du site web ;
- cessation d'activité du site web.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats de porteurs

Les personnes / entités qui peuvent demander la révocation d'un certificat porteur sont les suivantes :

- le porteur au nom duquel le certificat a été émis, ou
- une personne de l'ANTS dans le rôle d'AEC, ou
- une personne ayant le rôle d'AED vis à vis du porteur.

4.9.2.2 Certificats d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Révocation d'un certificat de porteur

Une demande de révocation peut être effectuée par le porteur sur le portail à l'adresse https://www.asscap.agents-ctae.ants.gouv.fr/ 24h / 24 et 7j / 7.

Les demandes de révocation sont authentifiées, dans ce cas, à l'aide du mot de passe personnel du porteur et les trois réponses aux questions secrètes.

Une demande de révocation peut également être réalisée, 24h / 24 et 7 j/ 7, sur le portail à l'adresse https://www.asscap.agents-ctae-sec.ants.gouv.fr/ par toute personne habilitée dans son rôle d'AEC ou d'AED vis-à-vis du porteur. L'authentification se fait alors à l'aide de la carte AAE du demandeur.

Les informations suivantes figurent dans la demande de révocation de certificat :

- l'identifiant (DN) du porteur du certificat ;
- le nom du demandeur de la révocation et ses contacts (téléphone, email) ;
- la cause de révocation.

Dans le cas où la demande de révocation est faite par un AE (AEC ou AED) autre que le porteur, une fois la demande authentifiée et contrôlée, l'AE doit signer une attestation de validation de révocation incorporant également une acceptation de son rôle de confiance. Cette attestation n'est pas présente dans le cas où le porteur révoque lui-même sa carte AAE.

La fonction de gestion des révocations révoque alors le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée via une LCR signée par l'AC.

Les causes de révocation ne sont pas publiées dans les Listes de Certificats Révoqués (LCR).

Le demandeur de la révocation est informé du bon déroulement de l'opération et de la révocation effective du certificat.

4.9.3.2 Révocation d'un certificat d'une composante de l'IGC

L'AC précise dans sa DPC les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des porteurs et des utilisateurs de certificats concernés. Pour cela, l'IGC utilise les moyens d'information à destination des Responsables Cartes qui sont à sa disposition (intranet, communiqués,…).

Conformément à la section IV.9.3.2 de la PC Type (Révocation d'un certificat d'une composante de l'IGC), l'ANSSI doit être informée et se réserve le droit de diffuser cette information par tout moyen.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

Dès que le porteur (ou une personne autorisée) a connaissance qu'une des causes possibles de révocation, de son ressort, est effective, il doit formuler sa demande de révocation sans délai.

4.9.5 Délai de traitement par l'AC d'une demande de révocation

4.9.5.1 Révocation d'un certificat de porteur

La fonction de gestion des révocations est disponible 24h / 24 et 7j / 7. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 1 heure et une durée maximale totale d'indisponibilité par mois de 4 heures.

Toute demande de révocation d'un certificat porteur est traitée dans un délai inférieur ou égal à 24 heures. Il s'agit du délai entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

4.9.5.2 Révocation d'un certificat d'une composante de l'IGC

La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans une LCR de l'AC qui a émis le certificat. La révocation d'un certificat d'AC (signature de certificats et de LCR) est effectuée après accord ou sur demande de l'ANTS.

4.9.6 Exigences de vérification de révocation par les utilisateurs de certificats

L'utilisateur d'un certificat (UC) de porteur est tenu de vérifier, l'état des certificats de l'ensemble du chemin de certification correspondant, en utilisant une LCR pour chaque certificat faisant partie du chemin.

4.9.7 Fréquence d'établissement des LCR

Une nouvelle LCR est émise au minimum toutes les 24 heures.

Il n'est pas mis en place de mécanisme de delta LCR.

4.9.8 Délai maximum de publication d'une LCR

Une LCR est publiée dans un délai maximum de 30 minutes après sa génération.

4.9.9 Disponibilité d'un système de vérification en ligne de la révocation et de l'état des certificats

Sans objet.

4.9.10 Exigences de vérification en ligne de la révocation des certificats par les utilisateurs de certificats

Sans objet.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission d'une clé privée

La compromission d'une clé privée peut survenir, au cas où deux événements distincts se produisent simultanément :

- l'emprunt temporaire de la carte du porteur à son insu ou le vol de la carte d'un porteur, et
- la connaissance par des moyens détournés d'un PIN associé à cette carte.

En cas de compromission d'une clé privée ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le porteur s'oblige à interrompre immédiatement et définitivement l'usage de ses deux clés privées et les certificats associés.

Les entités autorisées à effectuer des demandes de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

4.9.13 Causes possibles d'une suspension

Dans le cadre de la présente PC, la suspension de certificats n'est pas supportée.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LAR / LCR au format v2. De ce fait, les LAR / LCR comportent la date au plus tard de leur prochaine publication.

Les LAR sont publiées aux points de distribution des LAR (CRL Distribution Point). Chaque certificat d'AC comporte l'adresse du point de distribution de la LAR le concernant.

Les LCR sont publiées aux points de distribution des LCR (CRL Distribution Point). Chaque certificat d'un porteur comporte l'adresse du point de distribution de la LCR le concernant.

Il n'y a pas de service d'état de validité des certificats autre que la publication de LCR et de LAR.

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h / 24 et 7j / 7. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2 heures et une durée maximale totale d'indisponibilité par mois de 8 heures.

4.10.3 Dispositifs optionnels

Sans objet.

4.11 Fin de la relation entre le porteur et l'AC

En cas de fin de relation contractuelle, hiérarchique ou réglementaire entre l'AC et le porteur avant la fin de validité de ses certificats, pour une raison ou pour une autre, les certificats de porteur doivent être révoqués.

4.12 Séquestre de clé et recouvrement

Le séquestre des clés privées des porteurs est interdit par la présente PC.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

4.12.2 Politique et pratiques de recouvrement par encapsulation des clés de session

Sans objet.

5 MESURES DE SECURITE NON TECHNIQUES

5.1 Mesures de sécurité physique

La section § 1.3 définit les différentes entités intervenant dans l'IGC.

- service d'enregistrement,
- service de génération des certificats,
- service de génération des éléments secrets du porteur,
- service de remise au porteur,
- service de publication,
- service de gestion des révocations,
- service d'information sur l'état des certificats, et
- service de journalisation.

Les services de génération des certificats, de publication, d'informations sur l'état des certificats, de gestion des révocations sont assurés par l'OSC.

Le service de génération des éléments secrets du porteur est assuré par le CPS.

Le service d'enregistrement et le service de remise au porteur sont des services décentralisés.

Pour le service d'enregistrement :

- l'enregistrement des Responsables CT est réalisé par l'ANTS.
- l'enregistrement des Responsables Cartes est réalisé, soit par le Responsable CT, soit par un autre Responsable Carte du même site.

Pour le service de remise au porteur :

- la remise des cartes AAE aux Responsables CT est réalisée dans un Service de l'Etat par une personne mandatée par l'AEC de l'ANTS.
- la remise des cartes AAE aux Responsables Cartes est effectuée, soit par le Responsable CT, soit par un Responsable Carte du même site.

5.1.1 Situation géographique et construction des sites

Le site d'exploitation de l'IGC est installé dans les locaux de l'OSC. La construction des sites respecte les règlements et normes en vigueur, ainsi que les recommandations de l'ANSSI. Les caractéristiques ont été définies selon les résultats de l'analyse de risques précisée dans la DPC. Les opérations cryptographiques sur l'AC sont réalisées au sein des locaux de l'OSC qui sont à plus de 20 mètres à l'intérieur d'une zone réservée au sens de l'Instruction Générale Interministérielle n° 1300 [IGI 1300] approuvée par l'arrêté du 23 juillet 2010.

Le site de mise à disposition des informations est installé dans les locaux de l'ANTS.

Les personnes ayant le rôle d'AED sont localisées dans un Service de l'Etat

5.1.2 Accès physique

Les moyens et informations du site d'exploitation de l'IGC utilisés dans le cadre de la mise en œuvre opérationnelle de l'IGC sont installés dans une enceinte des locaux d'exploitation de l'OSC dont les accès sont contrôlés et réservés aux personnels habilités.

L'OSC met en œuvre un système de contrôle des accès qui permet de garantir la traçabilité des accès aux zones en question. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique. Si des personnes non habilitées doivent pénétrer dans les installations, elles font l'objet d'une prise en charge par une personne habilitée qui en assure la surveillance. Ces personnes doivent en permanence être accompagnées par des personnels habilités.

L'OSC a défini un périmètre de sécurité physique où sont installées ces machines. La mise en œuvre de ce périmètre permet de respecter la séparation des rôles de confiance telle que prévue dans la présente PC. Ce périmètre de sécurité garantit, en cas de mise en œuvre dans des locaux en commun, que les fonctions et informations hébergées sur les machines ne sont accessibles qu'aux seules personnes ayant des rôles de confiance reconnus et autorisées. Ces points sont précisés dans la DPC. Ces dispositions permettent d'être conforme au niveau (***).

5.1.3 Alimentation électrique et climatisation

Afin d'assurer la disponibilité des systèmes informatiques du site d'exploitation de l'IGC, des systèmes de génération et de protection des installations électriques sont mis en œuvre par l'OSC. Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements du site d'exploitation de l'IGC telles que fixées par l'ANTS et leurs fournisseurs.

5.1.4 Vulnérabilité aux dégâts des eaux

Les mesures de protection contre les dégâts des eaux mis en œuvre par l'OSC permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC, notamment en matière de disponibilité de ses fonctions de gestion des révocations de publication et d'information sur l'état de validité des certificats.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies mis en œuvre par l'OSC permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC, notamment en matière de disponibilité de ses fonctions de gestion des révocations, de publication et d'information sur l'état de validité des certificats.

5.1.6 Conservation des supports

Les mesures et moyens de conservation des supports d'information mis en œuvre par l'OSC permettent de respecter les exigences et les engagements pris par l'AC dans la présente PC. En particulier la disponibilité, la confidentialité et l'intégrité des données conservées dans les journaux, les archives et les logiciels utilisées par l'AC est assurée.

5.1.7 Mise hors service des supports

Le site d'exploitation de l'IGC utilise des mécanismes de destruction des supports papiers (tels que des broyeurs) et des supports magnétiques d'information. Les matériels réformés ayant servi à supporter l'IGC font l'objet de mesures préalables de neutralisation. En fin de vie, les supports sont détruits.

En fin de vie (Révocation, dysfonctionnement, fin de validité,…), toute carte AAE doit impérativement être détruite :

- Dans le cas où le Responsable CT, un Responsable Carte ou l'AEC sont à l'origine d'une révocation, si la carte est en leur possession, ils se chargent de la destruction de cette dernière selon ses propres moyens.
- Dans le cas où les porteurs sont à l'origine de la révocation de leur carte, si la carte est en leur possession, ils se chargent de la destruction de cette dernière selon leurs propres moyens.
- Dans le cas où les Responsable CT, un Responsable Carte ou l'AEC sont à l'origine d'une révocation mais que la carte n'est pas à leur disposition, ils se chargent de prévenir par courriel (disponible dans l'annuaire) le porteur afin qu'il se charge de la destruction de sa carte.
- Dans les autres cas (carte défectueuse, en fin de vie,…), tant que le porteur est en possession de sa carte, celui-ci doit procéder à la destruction de la carte selon ses propres moyens.

L'ensemble des porteurs, en possession d'une carte dont la fin de vie est effective, doit s'assurer de la destruction du composant électronique.

5.1.8 Sauvegardes hors site

Le site d'exploitation de l'IGC réalise des sauvegardes placées hors site en s'appuyant majoritairement sur les procédures d'exploitation interne existantes de l'OSC, ajustées en fonction des particularités de cette IGC. Celles-ci sont de nature à permettre une reprise rapide des fonctions de gestion des révocations, de publication et

d'information sur l'état des certificats, suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ces fonctions.

Le site de mise à disposition des informations de l'ANTS, met en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un évènement affectant gravement et de manière durable la réalisation de ces prestations (destruction du site, etc.). Cette disposition permet d'être conforme au niveau (***).

5.2 Mesures de sécurité procédurales

L'ensemble de ce chapitre est respecté par les entités intervenant dans la gestion du cycle de vie des certificats émis par l'AC. En particulier, l'OSC s'assure de la mise en œuvre effective des mesures de sécurité procédurales pour l'utilisation opérationnelle des certificats d'AC au sein de ses locaux.

5.2.1 Rôles de confiance

Les personnes auxquelles sont attribués des rôles de confiance de l'IGC sont toutes des personnes habilitées de l'OSC et l'IN.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité des opérations au sein de l'IGC. Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

Les rôles de confiance sont classés en cinq groupes :

- « Responsable de sécurité » - il est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission,… etc.
- « Responsable d'application » - il est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
- « Ingénieur système » - il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
- « Opérateur » - Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante
- « Contrôleur » - personnel, dont la responsabilité est de réaliser les opérations de vérification de la bonne application des mesures et de la cohérence de fonctionnement de l'AC AAE de l'ANTS. Ce personnel est désigné par le RSSI ou l'Officier de sécurité de l'ANTS, ou par le responsable d'application de l'OSC (avec dans ce dernier cas une portée des opérations de vérification limitées aux prestations opérées par l'OSC).

Les attributions détaillées de chaque rôle de l'IGC sont données dans l'annexe « Rôles » de la DPC.

5.2.2 Nombre de personnes requises par tâche

Selon le type d'opérations effectuées, le nombre et le type de rôles et de personnes devant nécessairement être présentes (en tant qu'acteurs ou témoins) peuvent être différents. L'annexe "Rôles" de la DPC définit le nombre d'exploitants nécessaires à chaque opération.

5.2.3 Identification et authentification pour chaque rôle

L'OSC procède à la vérification de l'identité et des autorisations de tout membre de son personnel amené à travailler au sein de l'IGC avant de lui attribuer un rôle et les droits correspondants.

Les contrôles effectués sont décrits dans la DPC de l'AC et sont conformes à la politique de sécurité applicable.

5.2.4 Rôles exigeant une séparation des attributions

Les attributions de chaque rôle de l'IGC sont données dans l'annexe « Rôles » de la DPC qui précise comment et sous quelles conditions ces rôles peuvent être cumulés par un même exploitant.

La séparation de ces rôles reposent sur :

- la notion de séparation des rôles dits « d'administration », des rôles dits « opérationnel » : une personne qui peut assigner des fonctions et/ou un rôle sur une composante d'IGC pour la mise en œuvre d'un service ne met pas en œuvre le service correspondant ;
- la notion de double contrôle sur un service de l'IGC : une double validation est nécessaire sur les opérations dites « sensibles » (cérémonie des clés, demande et génération d'un certificat, …).

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur,
- contrôleur et tout autre rôle,
- ingénieur système et opérateur.

Ces dispositions permettent d'être conforme au niveau (***).

La mise en œuvre de cette séparation repose sur des mécanismes organisationnels et/ou techniques.

5.3 Mesures de sécurité vis-à-vis du personnel

L'ensemble des mesures décrites dans ce chapitre est respecté par les entités intervenant dans la gestion du cycle de vie des certificats émis par l'AC. En particulier, l'OSC s'assure de la mise en œuvre effective des mesures de sécurité du personnel lors de la mise en œuvre opérationnelle des certificats d'AC au sein de ses locaux.

5.3.1 Qualifications, compétences et habilitations requises

Tout le personnel opérant pour le compte de l'AC de l'ANTS est formé pour comprendre les rôles qui leur sont attribués. Le nom et la fonction de tout le personnel intervenant pour le compte de l'AC AAE de l'ANTS sont répertoriés. L'OSC fait en sorte que les compétences professionnelles des personnes placées sous leur responsabilité soient cohérentes à leurs attributions.

Le Responsable CT ou les Responsables Cartes s'assurent que le statut d'un futur porteur est en adéquation avec ses futures responsabilités. Toute attribution d'une carte AAE à une personne occupant une fonction à courte durée est proscrite (Stagiaire, intérimaire,…).

5.3.2 Procédures de vérification des antécédents

Chaque entité opérant une composante de l'IGC s'assure de l'honnêteté de ses personnels amenés à travailler au sein de la composante.

Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions. Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflits d'intérêts préjudiciables à l'impartialité de leurs tâches. Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues au minimum tous les 3 ans.

5.3.3 Exigences en matière de formation initiale

Le personnel a été préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, au sein de l'entité dans laquelle il opère.

Le personnel a eu connaissance et est réputé avoir compris les implications des opérations dont il a la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures et dans l'organisation, en fonction de la nature de ces évolutions.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Aucune rotation n'est imposée dans le cadre de la présente PC.

5.3.6 Sanctions en cas d'actions non autorisées

Le responsable de l'AC AAE décide des sanctions à appliquer lorsqu'un Responsable Carte sous la responsabilité de l'OSC abuse de ses droits ou effectue une opération non conforme à ses attributions, selon les modalités applicables.

Lorsque le manquement est commis par un Responsable Carte de l'OSC, le responsable de l'AC demande au responsable de l'OSC de prendre les sanctions appropriées et de lui en rendre compte. Les modalités d'application et de délégation sont précisées dans la DPC.

5.3.7 Exigences vis-à-vis du personnel des prestataires externes

Les éventuels personnels contractants doivent respecter les mêmes conditions que celles énoncées dans le § 5.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

5.3.8 Documentation fournie au personnel

Chaque personnel dispose de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille, en particulier en termes de sécurité.

5.4 Procédures de constitution des données d'audit

L'ensemble de ce chapitre est respecté par les entités intervenant dans la gestion du cycle de vie des certificats émis par l'AC. En particulier, l'OSC s'assure de la mise en œuvre effective des mesures de constitution des données d'audit dans la mise en œuvre opérationnelle des certificats, des supports de clé et des données d'activation au sein de ses locaux.

5.4.1 Type d'évènements à enregistrer

L'IGC enregistre les évènements liés aux services et à la protection de l'AC (accès physique, …) qu'elle met en œuvre.

Chaque enregistrement d'un évènement dans un journal contient au minimum les informations suivantes :

- le type d'évènement ;
- le nom de l'exécutant ou la référence du système déclenchant l'évènement ;
- la date et l'heure de l'évènement ;
- le résultat de l'évènement (échec ou réussite).

Pour les types d'évènements pour lesquels ces informations existent, les enregistrements comporteront également les champs suivants :

- le destinataire de l'opération ;
- le nom du demandeur de l'opération ou la référence du système effectuant la demande ;
- le nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- la cause de l'évènement ;
- toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Les opérations de journalisation sont effectuées en tâche de fond tout au long de la vie de l'IGC. L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée.

En cas de saisie manuelle, l'écriture est effectuée, sauf exception, le même jour ouvré que l'évènement.

5.4.2 Fréquence de traitement des journaux d'évènements

Les journaux d'évènements sont contrôlés et analysés sur une base hebdomadaire par un responsable de sécurité de l'OSC afin d'identifier les anomalies liées à des tentatives en échec. Cette analyse donne lieu à un résumé qui fait apparaître les anomalies constatées.

5.4.3 Période de conservation des journaux d'évènements

Les journaux d'évènements sont conservés pendant 10 ans après leur génération. Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous 1 mois. Ils restent sur le site au moins un mois.

5.4.4 Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Le système interne de datation de l'IGC associe à toutes les archives une date UTC.

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations contenues. Elle peut entraîner un besoin de protection en confidentialité.

5.4.5 Procédure de sauvegarde des journaux d'évènements

Chaque entité intervenant pour le compte de l'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité de ses journaux d'évènements, conformément aux exigences de la présente PC.

5.4.6 Système de collecte des journaux d'évènements

Le système de collecte des journaux assure la collecte des archives en respectant le niveau de sécurité relatif à l'intégrité, la disponibilité et la confidentialité des données.

5.4.7 Notification de l'enregistrement d'un évènement au responsable de l'évènement

Le journal d'événements permet d'imputer chaque opération sensible à toute personne, organisme ou système ayant un rôle identifié dans la présente PC.

5.4.8 Evaluation des vulnérabilités

Chaque entité intervenant pour le compte de l'IGC est en mesure de détecter toute tentative de violation de l'intégrité de son fonctionnement.

Les journaux sont analysés dans leur totalité chaque jour ouvré par un responsable de sécurité de l'OSC.

Un rapprochement entre les journaux d'évènements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, par exemple) est effectué sur une base hebdomadaire par un responsable de sécurité de l'OSC afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

Les procédures sont détaillées dans la DPC.

5.5 Archivage des données

5.5.1 Types de données à archiver

L'archivage permet d'assurer la pérennité des données numériques constituées lors des opérations effectuées au profit de l'IGC. Il permet également la conservation de pièces papier, ainsi que leur disponibilité en cas de nécessité.

- Les informations archivées sont au minimum les suivantes :
- les PC ;

- les DPC ;
- les Conditions Générales d'Utilisation (CGU) ;
- la déclaration à la CNIL de la base de données personnelles gérée par l'IGC ;
- les certificats et LCR tels qu'émis ou publiés ;
- les demandes d'enregistrement signées électroniquement par le personnel ayant le rôle d'AEC ou d'AED ;
- les attestations de remise de cartes signées électroniquement ;
- les attestations d'acceptation de cartes signées électroniquement avec une double signature ;
- les dossiers papiers des Responsables CT reçus des Services de l'Etat ;
- les dossiers papiers des Responsables Cartes reçus des Services de l'Etat ;
- les accords contractuels avec les sous-traitants ;
- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les journaux d'événements des différentes entités de l'IGC.

5.5.2 Période de conservation des archives

Dossiers de demande de certificats

Tout dossier de demandes de certificats accepté et reçu est archivé durant au moins 10 ans. L'archivage des dossiers de demandes de certificats pour les Responsables CT est effectué par l'ANTS. Les dossiers des demandes de certificats pour les Responsables Cartes sont conservés sur site.

Documents d'identité

Une photocopie d'un document d'identité du porteur est archivée dans le dossier de demandes de certificats pour une durée minimum de 10 ans.

Au cours de cette durée, les dossiers de demande de certificats et les photocopies des documents d'identité sont en mesure d'être présentés par l'AC lors de toute sollicitation par les autorités habilitées. Ces dossiers permettent de retrouver l'identité réelle des personnes physiques désignées dans le certificat émis par l'AC.

Noms Distinctifs

Le nom distinctif comprend le prénom et le nom. Tout DN (Distinguished Name) est unique. L'unicité des DN s'appuie sur l'unicité de l'identifiant unique contenu dans l'attribut CN (CommonName). Un nom distinctif attribué à une personne physique donnée ne peut jamais être utilisé par une autre personne que le premier titulaire du DN.

Certificats et LCR émis par l'AC

La période de conservation des certificats et des LCR est de 5 ans après leur expiration.

Journaux d'évènements

Les journaux d'évènements sont archivés pendant au moins 5 ans après leur génération. Les moyens mis en œuvre par l'AC pour leur archivage offrent le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des journaux est assurée tout au long de leur cycle de vie.

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives et leurs sauvegardes :

- sont protégées en intégrité ;
- ne sont accessibles qu'aux personnes autorisées ;
- peuvent être relues et exploitées.

5.5.4 Procédure de sauvegarde des archives

Le responsable de l'AC et l'OSC ont la responsabilité de mettre en place et maintenir les mesures requises afin d'assurer l'intégrité et la disponibilité de leurs archives, conformément aux exigences de la présente PC.

5.5.5 Exigences d'horodatage des données

Tous les composants de l'AC sont régulièrement synchronisés avec un serveur Network Time Protocol (NTP).

5.5.6 Système de collecte des archives

Le système assure la collecte des archives en respectant le niveau de sécurité relatif à la protection des données (voir § 5.5.3).

5.5.7 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) sont accessibles aux personnes autorisées dans un délai maximum de deux jours ouvrés.

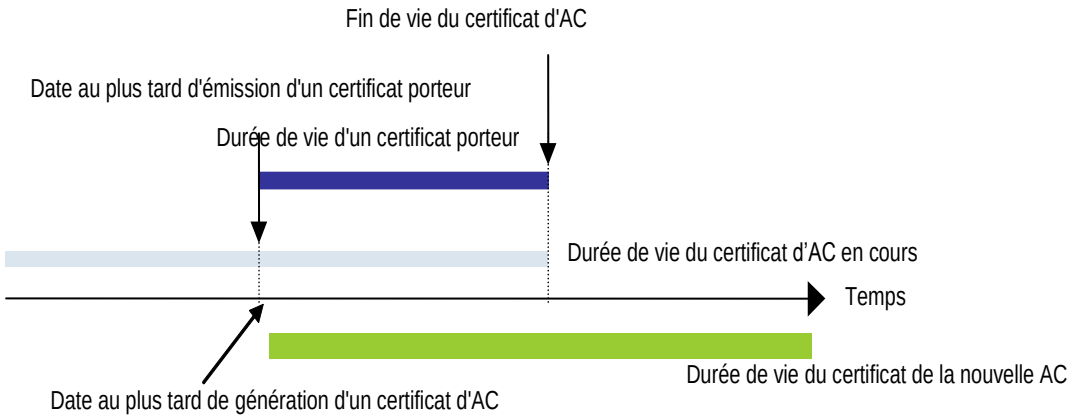
5.6 Changement de clé d'AC

5.6.1 Certificat d'AC

La durée de vie d'un certificat d'AC est de 6 ans et déterminée selon la période de validité de la clé privée associée, en conformité avec les recommandations cryptographiques de sécurité relatives aux longueurs de clés, notamment conformément aux recommandations des autorités nationales compétentes en la matière.

Une AC ne peut pas générer de certificats porteurs dont la durée de vie dépasse la période de validité de son certificat d'AC. C'est pourquoi, une bi-clé d'AC est renouvelée au plus tard à la date d'expiration du dernier certificat en cours de validité de l'AC moins la durée de vie garantie des certificats des porteurs. Le nom de l'AC (DN) est inchangé et un nouveau certificat d'AC est demandé à l'AC de niveau supérieur, en la circonstance à l'AC Racine ANTS V2.

A partir du moment où une nouvelle clé privée d'AC a été générée pour l'AC et qu'un certificat d'AC a été obtenu par l'AC de niveau supérieur, celle-ci est utilisée dès le début de la période de validité de ce certificat pour générer de nouveaux certificats de porteurs et les LCR de l'AC pour ces nouveaux certificats. Le précédent certificat d'AC reste valable pour valider le chemin de certification des anciens certificats porteurs émis par la précédente clé privée d'AC, jusqu'à l'expiration de tous les certificats porteurs émis à l'aide de cette bi-clé. L'ancienne clé de l'AC sert alors à signer les LCR pour les certificats émis sous cette ancienne clé d'AC.



Par ailleurs, l'AC change sa bi-clé et le certificat correspondant quand la bi-clé cesse d'être conforme aux recommandations de sécurité cryptographique concernant la taille des clés ou si celle-ci est soupçonnée de compromission ou compromise.

5.6.2 Certificat de Porteur

La durée de vie des certificats des porteurs est définie dans le RGS [RGS_A_13]. Au moment où cette PC est publiée, la durée de vie maximale d'une bi-clé et d'un certificat porteur (T_PORT_MAX) est spécifiée à 3 ans. Si une nouvelle version du RGS [RGS_A_13] était publiée, la durée de vie des certificats des porteurs pourrait être augmentée en conséquence, sans remettre en cause l'identifiant de cette PC.

5.7 Reprise suite à compromission et sinistre

5.7.1 Procédures de remontée et de traitement des incidents et des compromissions

Notamment chaque entité agissant pour le compte de l'IGC met en œuvre des procédures et des moyens de remontée et de traitement des incidents, Ce plan est régulièrement testé. L'IGC dispose d'un plan de reprise d'activité en cas de sinistre. La référence au plan anti-sinistre, ses modalités de déclenchement et les personnes responsables de ce plan sont identifiées dans la DPC. Le plan de reprise d'activité en cas de sinistre prend en compte les paramètres suivants :

- priorisation des actions à mener et délais maximums de recouvrement pour la continuité des services ;
- politique de sécurité et de protection des secrets ;
- procédures de secours ;
- tests pratiques, formation et entraînement des personnels ;
- procédure de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données) ;
- procédure de reprise en cas de compromission de clés.

Ces procédures sont établies en cohérence avec la politique de sécurité des systèmes d'information de l'OSC.

5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Chaque composante de l'IGC dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la présente PC, des engagements de l'AC dans sa propre PC notamment en ce qui concerne les fonctions liées à la publication et à la révocation des certificats.

Ce plan de continuité est testé au minimum une fois par an.

Si le matériel de l'AC est endommagé ou hors service alors que les clés privées de signature ne sont pas détruites, l'exploitation est rétablie dans les plus brefs délais, en donnant la priorité à la capacité de fourniture des services de révocation et de publication d'état de validité des certificats, conformément au plan de reprise d'activité de l'AC.

5.7.3 Procédures de reprise en cas de compromission de la clé privée d'une composante

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité de la composante (voir § 5.7.2) en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat de l'AC sera immédiatement révoqué (voir § 4.9).

Si la clé de signature de l'AC est compromise, perdue, détruite, ou soupçonnée d'être compromise :

- le responsable de l'AC, après enquête sur l'évènement décide de demander à l'AC de niveau supérieur (l'AC ANTS V2) de révoquer le certificat de l'AC ;
- les personnes ayant le rôle d'AE ou AED et tous les porteurs dont les certificats ont été émis par l'AC compromise, sont avisés dans les plus brefs délais que le certificat d'AC a été révoqué ;
- une nouvelle bi-clé AC est générée et un nouveau certificat d'AC est émis ;
- le responsable de l'AC demande à l'AC de niveau supérieur (l'AC ANTS V2) de générer un nouveau certificat d'AC ;
- les personnes ayant le rôle d'AE ou d'AED et les porteurs sont informées de la capacité retrouvée de l'AC de générer des certificats ;

5.7.4 Capacités de continuité d'activité suite à un sinistre

Le plan de reprise d'activité après sinistre traite de la continuité d'activité telle qu'elle est décrite au § 5.7.1. Le SP est installé afin d'être disponible 24 heures sur 24 et 7 jours sur 7.

5.8 Fin de vie d'AC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité.

Le transfert d'activité est défini comme la fin d'activité d'une entité agissant pour le compte de l'IGC qui n'induit pas d'incidence sur la validité des certificats antérieurement émis. La reprise de cette activité est organisée par l'AC.

La cessation d'activité est définie comme la fin d'activité de l'autorité responsable d'une entité agissant pour le compte de l'IGC, qui induit une incidence sur la validité des certificats antérieurement émis, autres que les certificats de l'AC.

5.8.1 Transfert d'activité

Dans le cas d'un transfert d'activité d'une entité œuvrant pour le compte de l'IGC, l'AC s'engage à:

- mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats) ;
- assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC ;
- informer ses partenaires du transfert d'activité et de sa réalisation.

L'entité œuvrant pour le compte de l'IGC et procédant au transfert de son activité s'engage à:

- avertir l'AC de son intention de transférer son activité avec un préavis d'au moins un mois ;
- remettre ses archives à l'autorité responsable de l'AC ;
- mettre à disposition de l'entité à laquelle son activité est transférée les informations et moyens nécessaires au maintien ou la reprise de l'activité ;
- communiquer au RSSI ou Officier de sécurité. les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à la cessation d'activité ou au transfert d'activité de la composante ;
- communiquer à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus ;
- tenir informées l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

5.8.2 Cessation d'activité

La cessation d'activité peut être totale ou partielle, typiquement, la cessation d'émission de nouveaux certificats sous cette PC.

En cas de cessation partielle d'activité et dans le cadre d'une cessation de l'émission de nouveaux certificats sous cette PC, l'AC :

1) en informe à l'avance, via le SP, les porteurs et les utilisateurs de certificats ;
2) continue à assurer la révocation des certificats et la publication des LCR conformément aux engagements pris dans sa PC, le temps que les porteurs soient équipés de nouveaux certificats, et au plus tard jusqu'à la fin de validité du dernier certificat émis.

Dans l'hypothèse d'une cessation partielle d'activité et dans le cadre d'une cessation de gestion totale des certificats émis sous cette PC, l'AC :

1) en informe à l'avance, via le SP, les porteurs et les utilisateurs de certificats ;
2) cesse d'émettre des LCRs, ce qui a pour conséquence d'empêcher la validation des chemins de certification ;

Dans l'hypothèse d'une cessation totale d'activité de l'AC, c'est-à-dire pour tous les certificats émis sous cette clé d'AC (toutes PC confondues), l'AC :

1) s'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats ;
2) prend toutes les mesures nécessaires pour détruire la clé privée lui ayant permis d'émettre des certificats (y compris les copies de sauvegarde) ou la rendre inopérante ;
3) demande la révocation de son certificat par l'AC de niveau supérieur (AC ANTS V2) ;
4) informe via le SP les porteurs et les utilisateurs de certificats.

6 MESURES DE SECURITE TECHNIQUES

6.1 Génération et installation des bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'AC

Les bi-clés de signature d'AC sont générées lors d'une cérémonie de clé à l'aide d'une ressource cryptographique matérielle.

Les cérémonies de clés se déroulent sous le contrôle d'au moins trois personnes dans des rôles de confiance (maître de cérémonie et témoins). Elle se déroule dans les locaux de l'OSC. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement approuvé par l'ANTS. Les rôles des personnels impliqués dans les cérémonies de clés sont précisés dans la DPC.

Les manipulations de données secrètes en clair (clés privées d'AC, clés privées des porteurs, parts de secrets d'IGC) sont effectuées dans un environnement protégé contre les rayonnements parasites compromettant : matériels protégés, cage de Faraday et locaux limitant les risques de fuites d'information par observation visuelle ou rayonnements électromagnétiques. Ces dispositions permettent d'être conforme au niveau (***).

6.1.1.2 Clés porteurs générées par l'AC

Ce paragraphe ne s'applique que lorsque la bi-clé d'un porteur est générée par l'AC.

La génération des clés des porteurs est effectuée dans un environnement sécurisé (voir § 6.4.1). L'OSC génère, pour les bi-clés ainsi qu'un code d'activation de la carte AAE (voir § 6.4.1).

Les bi-clés des porteurs sont générées dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré, puis la clé privée est transférée de manière sécurisée dans le support de clés destiné au porteur, sans que l'AC n'en garde aucune copie, tandis que la clé publique est incorporée à la demande de certificat afin d'obtenir un certificat.

Les clés privées sont protégées à la fois en intégrité et en confidentialité et protégées contre un usage abusif à l'aide d'un code d'activation de la carte AAE au sein de leur support de clés de telle sorte qu'elles ne soient utilisables que par le détenteur du code d'activation.

6.1.1.3 Clés porteurs générées par le porteur

Ce paragraphe ne s'applique que lorsque la bi-clé d'un porteur est générée par le support de clés.

Dans le cas où le porteur génère sa bi-clé, cette génération est effectuée dans un dispositif répondant aux exigences du chapitre 12 ci-dessous pour le niveau de sécurité considéré. L'AC s'en assure en mettant en œuvre un canal sécurisé (secure channel) entre l'AC et la carte AAE pour récupérer la valeur de la clé publique.

Les clés privées sont protégées à la fois en intégrité et en confidentialité et protégées contre un usage abusif à l'aide des codes PIN courants au sein de leur support de clés de telle sorte qu'elles ne soient utilisables que par le détenteur des codes PIN.

6.1.2 Transmission de la clé privée à son propriétaire

6.1.2.1 Clé privée de l'AC

La clé privée de l'AC reste et est mise en œuvre dans les locaux sécurisés de l'OSC.

6.1.2.2 Clés privées du porteur générées par l'AC

La délivrance du support de bi-clés au porteur s'effectue via l'AEC ou l'AED de manière à garantir la confidentialité et l'intégrité de la clé privée et à ne la délivrer qu'au seul porteur. La bi-clé est protégée dans son support de bi-clé à l'aide d'un code d'activation temporaire. L'AEC et l'AED ne gardent aucune donnée permettant de récupérer tout ou partie de la bi-clé qu'elle a transmise au porteur (bi-clé dont la clé publique est certifiée). La DPC précise les mesures techniques mises en œuvre.

La vérification de l'identité du porteur par l'AE ou l'AED est effectuée via un face-à-face physique lors de la remise de la bi-clé générée par l'AC en présence du porteur.

L'envoi du support est effectué de manière séparée dans l'espace et le temps de l'envoi du code d'activation. Ces dispositions permettent d'être conforme au niveau (***).

6.1.2.3 Clés privées du porteur générées par la carte AAE du porteur

Lors du renouvellement des certificats sur la carte AAE, les clés privées sont générées directement par la carte AAE lors d'une connexion à un site web. La carte reste constamment sous le contrôle de son propriétaire.

6.1.3 Transmission de la clé publique à l'AC

6.1.3.1 Bi-clés générées par l'AC

Lorsque l'AC génère la bi-clé d'un porteur (cf. chapitre 6.1.1.2), la clé publique est protégée en intégrité et son origine authentifiée lorsqu'elle est extraite du module cryptographique. Le système de gestion des clés de l'OSC permet lors de la génération en central de la bi-clé, d'assurer l'intégrité et l'origine de la demande. Les mécanismes mis en œuvre sont décrits dans la DPC.

6.1.3.2 Bi-clés générées par le support du porteur

Lorsque la bi-clé d'un porteur est générée par le support de clés, la clé publique est protégée en intégrité et son origine authentifiée lorsqu'elle est extraite du support de clés. Un canal sécurisé (secure channel) est mis en œuvre entre l'AC et la carte AAE. Ces mécanismes sont décrits dans la DPC.

6.1.4 Transmission de la clé publique de l'AC aux utilisateurs de certificats

Les informations suivantes sont disponibles via l'URL https://sp.ants.gouv.fr/antsv2/index.html :

- Les certificats de l'AC AAE ;
- Les certificats auto-signés de l'AC Racine ANTS v2 ;
- Les Conditions Générales d'Utilisation.

Elles reprennent ces informations et indiquent les valeurs des empreintes des certificats auto-signés de l'AC Racine ANTS v2 ainsi que l'URL où ces certificats auto-signés sont disponibles.

6.1.5 Taille des clés

Les clés d'AC et de porteurs respectent les exigences de caractéristiques (longueurs, algorithmes, etc.) du document [RGS_A_14].

6.1.5.1 Certificat AC

Les recommandations des organismes nationaux et internationaux compétents (relatives aux longueurs de clés, algorithmes de signature, algorithme de hachage…) sont périodiquement consultées afin de déterminer si les paramètres utilisés dans l'émission de certificats d'AC doivent ou ne doivent pas être modifiés.

L'algorithme RSA avec la fonction de hachage SHA-256 est utilisé. La taille des bi-clés de l'AC AAE est de 2048 bits.

6.1.5.2 Certificat Porteur

Les recommandations des organismes nationaux et internationaux compétents (relatives aux longueurs de clés, algorithmes de signature, algorithme de hachage…) sont périodiquement consultées afin de déterminer si les paramètres utilisés dans l'émission de certificats porteurs doivent ou ne doivent pas être modifiés.

L'algorithme RSA avec la fonction de hachage SHA-256 est utilisé pour les certificats de porteur. La taille des bi-clés est de 2048 bits.

6.1.6 Vérification de la génération des paramètres des bi-clés et de leur qualité

Les équipements utilisés pour la génération des bi-clés d'AC sont des ressources cryptographiques matérielles qualifiées au niveau renforcé par l'ANSSI et respectent donc les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

6.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée de l'AC et du certificat associé est strictement limitée à la signature de certificats et de LCR (voir § 1.4.1.1).

Certificat d'authentification

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service d'authentification (voir § 1.4.1.2 et § 4.5). L'utilisation du champ "keyUsage" dans le certificat porteur est : « digitalSignature » tel qu'appelé dans le RFC 5280 de l'IETF et dans la recommandation ITU-T X.509.

Certificat de signature

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de signature (cf. § 1.4.1.2 et § 4.5). L'utilisation du champ "keyUsage" dans le certificat porteur est «nonRepudiation» tel qu'appelé dans le RFC 5280 de l'IETF ou « content Commitment » tel qu'appelé dans la recommandation ITU-T X.509.

6.2 Mesures de sécurité pour la protection des clés privées et pour les modules cryptographiques

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'AC

Les ressources cryptographiques de l'AC sont qualifiées au niveau renforcé par l'ANSSI.

La ressource cryptographique matérielle de l'AC utilise des générateurs d'aléas qui sont conformes à l'état de l'art, et aux standards en vigueur. Les algorithmes utilisés pour générer l'aléa de départ sont conformes aux standards en vigueur.

6.2.1.2 Dispositifs d'authentification et de signature des porteurs

L'AC fournit aux utilisateurs le dispositif d'authentification et de signature (carte AAE). Ce dispositif est qualifié au niveau renforcé par l'ANSSI et respecte les exigences du chapitre § 12.

Le renouvellement des bi-clés se fait par la mise en place d'un « secure messaging » entre la carte AAE et l'AC permettant de s'assurer que le porteur utilise bien le dispositif fourni originellement.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC est assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets.

Cette disposition permet d'être conforme au niveau (***).

6.2.3 Séquestre de clé privée

Les clés privées d'AC et des porteurs ne font jamais l'objet de séquestre.

6.2.4 Copie de secours de la clé privée

6.2.4.1 Clé privée d'AC

La bi-clé d'AC est sauvegardée sous le contrôle de plusieurs personnes à des fins de disponibilité. Les copies de secours des clés privées sont réalisées à l'aide de ressources cryptographiques matérielles. Les sauvegardes sont rapidement transférées sur site sécurisé de sauvegarde délocalisé afin de fournir et maintenir la capacité de reprise d'activité de l'AC. Les sauvegardes de clés privées d'AC sont stockées dans des ressources cryptographiques matérielles ou sous forme chiffrée.

6.2.4.2 Clés privées des porteurs

Les clés privées des porteurs générées par l'AC ne font l'objet d'aucune copie de secours par l'AC. Les clés privées générées par les cartes ne peuvent pas être exportées.

6.2.5 Archivage des clés privées

Les clés privées de l'AC AAE et des porteurs ne sont pas archivées.

6.2.6 Transfert de la clé privée vers ou depuis le module cryptographique

6.2.6.1 Clé privées de l'AC

Les clés d'AC sont générées et stockées dans des modules de sécurité matériels (HSM) et sauvegardées afin de pouvoir être restaurées. Les clés privées d'AC ne peuvent être sauvegardées que sous forme chiffrée et ne peuvent être restaurées que sur un module de sécurité matériel (HSM) avec le concours d'au mois trois personnes dans les rôles de confiance.

6.2.6.2 Clés privées des porteurs

Lorsque les clés privées des porteurs sont générées dans des modules de sécurité matériels (HSM), elles sont transférées dans les cartes AAE pour être finalement détruites au niveau des modules qui les ont générées.

6.2.7 Stockage des clés privées de l'AC dans un module cryptographique

Les clés privées d'AC stockées dans des ressources cryptographique matérielles sont protégées avec le même niveau de sécurité que celui dans lequel elles ont été générées.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'AC

L'activation des clés privées d'AC dans les modules cryptographiques est contrôlée via des données d'activation (cf. chapitre 6.4) et doit faire intervenir au moins trois personnes dans des rôles de confiance. Cette disposition permet d'être conforme au niveau (***).

6.2.8.2 Clés privées des porteurs

Chaque clé privée est activable à l'aide d'un code PIN.

La présentation du code PIN d'authentification est demandée lors de la première authentification. La présentation du code PIN d'authentification n'est pas demandée pour les authentifications suivantes, et ce tant que la carte n'est pas retirée du lecteur.

La présentation du code PIN de signature électronique est nécessaire pour chaque signature.

La carte AAE est configurée de telle sorte que suite à la saisie de trois mauvaises valeurs d'un code PIN, les présentations de ce code ne sont plus possibles. Selon le code concerné, la fonction d'authentification ou la fonction de signature est bloquée. Une procédure particulière permet de débloquer l'une ou l'autre fonction.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'AC

La désactivation des clés privées d'AC dans le module cryptographique est automatique dès qu'il y a arrêt ou déconnexion du module. Les ressources cryptographiques sont stockées dans une zone sécurisée pour éviter toute manipulation non autorisée par des rôles non fortement authentifiés.

6.2.9.2 Clés privées des porteurs

Les conditions de désactivation de la clé privée d'un porteur répondent aux exigences du chapitre § 12. Toute mise hors tension de la carte désactive les clés privées.

Pour la fonction d'authentification, la clé privée à usage d'authentification est utilisable tant que la carte demeure dans son lecteur.

Pour la fonction de signature électronique, la clé privée à usage de signature est utilisable une seule fois. L'utilisation du code PIN de signature électronique est nécessaire pour chaque signature.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées d'AC

Les clés privées d'AC sont détruites quand les certificats auxquels elles correspondent sont expirés ou révoqués. La destruction d'une clé privée implique la destruction des copies de sauvegarde, et l'effacement de cette clé sur la ressource cryptographique qui la contient, de manière à ce qu'aucune information ne puisse être utilisée pour la recouvrer.

6.2.10.2 Clés privées des porteurs

Lors d'un renouvellement de clé et de certificat, la clé privée précédente et le certificat précédent sont automatiquement détruits.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs

Les ressources cryptographiques de l'AC AAE et des dispositifs des porteurs sont qualifiées au niveau renforcé par l'ANSSI conformément aux exigences du chapitre § 11.

6.2.11.1 Niveau de qualification du module cryptographique et des dispositifs d'authentification

Les dispositifs d'authentification des porteurs sont évalués conformément aux exigences du chapitre § 12.

6.2.11.2 Niveau de qualification du module cryptographique et des dispositifs de création de signature

Les dispositifs de création de signature des porteurs sont évalués conformément aux exigences du chapitre § 12.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques sont archivées par archivage des certificats (Voir § 5.5.2).

6.3.2 Durées de vie des bi-clés et des certificats

La durée de vie opérationnelle d'un certificat est limitée par son expiration ou sa révocation. La durée de vie opérationnelle d'une bi-clé est équivalente à celle du certificat auquel elle correspond.

L'AC AAE ne peut pas émettre des certificats porteur dont la durée de vie est supérieure à celle de son certificat, cf. § 5.6.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

6.4.1.1 Génération et installation des données d'activation correspondant à la clé privée de l'AC

Les données d'activation des clés privées de l'AC AAE sont générées durant les cérémonies de clés (Voir § 5.2.1). Les données d'activation sont générées automatiquement selon un schéma de type m parmi n. Dans tous les cas les données d'activation sont remises à leurs porteurs immédiatement après leur génération. Les porteurs de données d'activation sont des personnes habilitées pour ce rôle de confiance.

6.4.1.2 Génération et installation des données d'activation correspondant à une clé privée du porteur

Chaque donnée d'activation d'une clé privée, appelée « code PIN », est choisie par le porteur lors de l'activation de sa carte AAE.

L'OSC transmet pour courrier à chaque porteur, protégé en intégrité et en confidentialité, un code d'activation temporaire de la carte. Ce code est à usage unique. L'envoi du code d'activation de la carte est séparé dans le temps et dans l'espace de l'envoi de la carte.

Pour un support de bi-clé, après avoir présenté le bon code d'activation, le porteur doit choisir deux codes PIN qui sont :

- un code PIN pour l'usage de la fonction authentification : donnée d'activation utilisée par le porteur pour s'authentifier.
- un code PIN pour l'usage de la fonction signature : donnée d'activation utilisée par le porteur pour signer électroniquement un ou plusieurs documents.

L'OCS conserve le code d'activation temporaire de la carte jusqu'au moment où le porteur a pris possession de son support, après quoi le code d'activation de la carte ne peut plus être communiqué.

6.4.2 Protection des données d'activation

6.4.2.1 Protection des données d'activation correspondant aux clés privées de l'AC

Les données d'activation sont protégées de la divulgation par une combinaison de mécanismes cryptographiques et de contrôle d'accès physique. Les porteurs de secret sont responsables de la gestion et de la protection des parts de secrets dont ils sont porteurs. Un porteur de secret ne peut détenir plus d'une donnée d'activation d'une même clé d'AC à un même instant.

6.4.2.2 Protection des données d'activation correspondant aux clés privées des porteurs

Le code d'activation temporaire est communiqué au porteur au moyen d'un courrier postal sécurisé envoyé à son attention. Si le courrier est illisible ou non reçu, il peut être réémis.

Les codes PIN créés par le porteur doivent être mémorisés par le porteur.

6.4.3 Autres aspects liés aux données d'activation

6.4.3.1 Déblocage d'un code PIN

La présentation d'un code PIN peut être bloquée, suite à la présentation successive de trois codes PIN erronés. Le service de déblocage permettant de réactiver les codes PIN bloqués, est proposé aux porteurs sur internet en mode HTTPS via l'URL https://www.asscap.agents-ctae.ants.gouv.fr/. Une authentification des porteurs au moyen du mot de passe personnel et les réponses aux questions secrètes, est exigée.

6.4.3.2 Changement d'un code PIN

Le changement d'un code PIN peut être effectué via le même service.

6.5 Mesures de sécurité des systèmes informatiques

Pour revendiquer le niveau ***, l'AC doit mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre.

L'AC a effectué une telle analyse. Les mesures de sécurité relatives aux systèmes informatiques satisfont aux objectifs de sécurité qui découlent de cette analyse de risque. La DPC a été élaborée en fonction de cette analyse. Ces dispositions permettent d'être conforme au niveau (***).

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est défini dans la DPC. Il répond aux objectifs de sécurité suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) ;
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels ;
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- protection du réseau contre toute intrusion d'une personne non autorisée ;
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- éventuellement, gestion des reprises sur erreur.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle (voir § 1.4.1.1) fait l'objet de mesures particulières, découlant de l'analyse de risque.

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) sont mis en place.

6.5.2 Niveau de qualification des systèmes informatiques

Les systèmes informatiques de l'IGC mettant en œuvre le module cryptographique ont fait l'objet d'une qualification conformément à l'[ORDONNANCE], au niveau standard défini par le [RGS] et en respectant les exigences du [CWA 14167-1].

La qualification d'un produit de sécurité est prévue par l'article 9 de l'ordonnance n° 2005-1516 du 8 décembre 2005 [ORDONNANCE]. Elle atteste de sa conformité à un niveau de sécurité du RGGS. Elle est délivrée par l'ANSSI.

L'AC utilise pour les fonctions propres à l'AC (génération des certificats et service d'enregistrement) un logiciel qui a reçu une qualification au niveau standard délivrée par l'ANSSI.

L'AC utilise des RCM qui ont obtenu une certification Critères Communs au niveau EAL4+ vis-à-vis du profil de protection PP/0308 ou d'un profil similaire.

En application de l'article 23 du décret n° 2010-112 du 2 février 2010 [Décret_RGS], les autorités administratives doivent obtenir la validation de leurs certificats électroniques et de ceux de leurs Responsables Cartes au plus tard dans les trois ans à compter de la publication de l'arrêté du 6 mai 2010. L'AC s'engage à se conformer à ces exigences dans le délai imparti.

Nota : en application de l'article 21 du décret n°2010-112 du 2 février 2010, l'ANSSI a mis en place une procédure de validation des certificats électroniques délivrés aux autorités administratives ou à leurs Responsables Cartes.

6.6 Mesures de sécurité liées au développement des systèmes

Le contrôle des développements des systèmes s'effectue comme suit :

- les matériels et les logiciels sont achetés de manière à réduire les possibilités qu'un composant particulier soit altéré ;
- les applications nécessaires à l'exécution des activités de l'AC sont acquises auprès de sources autorisées ;
- les applications nécessaires à l'exécution des activités de l'AC sont mises au point dans un environnement contrôlé, et le processus de mise au point est défini et documenté ;
- les matériels et logiciels sont dédiés aux activités de l'AC. Il n'y a pas d'autre application, matériel, ou composant logiciel installé qui ne soit pas dédiés aux activités de l'AC ;
- les logiciels de l'AC font l'objet d'une recherche de codes malveillants avant leur première utilisation et périodiquement par la suite ;
- les mises à jour des matériels et logiciels sont installés par des personnels de confiance et formés selon les procédures en vigueur.

6.6.1 Mesures liées à la gestion de la sécurité

La configuration du système d'AC, ainsi que toute modification ou évolution, est documentée et contrôlée par l'AC. Des mécanismes permettant de détecter toute modification non autorisée du logiciel ou de la configuration de l'AC sont mis en œuvre. Une méthode formelle de gestion de configuration est utilisée pour l'installation et la maintenance subséquente du système d'AC. Lors de son premier chargement, il est vérifie que le logiciel de l'AC est bien celui livré par le vendeur, qu'il n'a pas été modifié avant d'être installé, et qu'il correspond bien à la version voulue.

Toute évolution significative d'un système d'une composante de l'AC AAE est signalée au responsable de l'AC pour validation.

6.6.2 Niveau d'évaluation sécurité du cycle de vie des systèmes

En ce qui concerne les logiciels et matériels évalués, l'AC poursuit sa surveillance des exigences du processus de maintenance pour maintenir le niveau de confiance.

Nota : La PC Type ne formule aucune exigence. Il n'existe pas encore à l'heure actuelle de métrique pour mesurer le niveau de sécurité du cycle de vie des systèmes.

6.7 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

L'AC utilise des composants de réseau local (routeurs, par exemple) qui sont maintenus dans un environnement physiquement sécurisé et leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par l'AC.

Les échanges entre composantes au sein de l'IGC utilisent des mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

6.8 Horodatage/Système de datation

Il n'y a pas d'horodatage au sens du RFC 3161 de l'IETF utilisé par l'AC mais une datation sûre. Tous les composants de l'AC sont régulièrement synchronisés au moyen d'un serveur NTP (Network Time Protocol). Le temps fourni par ce serveur de temps est utilisé en particulier pour établir:

- la date du début de validité d'un certificat porteur ;
- la date du début de l'instant de révocation d'un certificat porteur ;
- les dates utilisées dans les journaux.

Des procédures automatiques ou manuelles peuvent être utilisées pour maintenir l'heure du système. Les réglages de l'horloge sont des événements susceptibles d'être audités.

7 PROFILS DES CERTIFICATS ET DES LCR

7.1 Profil de Certificats

Les certificats émis par l'AC sont des certificats au format X.509 v3. Les champs des certificats de l'AC et des porteurs sont définis par le RFC 5280.

7.1.1 Extensions de Certificats

7.1.1.1 Certificat AC

Les informations principales contenues dans le certificat de l'AC AAE sont :

Champ de base	**Valeur**
version	2 (= version 3)
serialNumber	défini par l'outil de cérémonie des clés
issuer	C=FR O=Gouv OU=0002 130003262 CN=Autorité de certification ANTS V2
notBefore	début de la période de validité du certificat
notAfter	fin de la période de validité du certificat
subject	C=FR O=Agence Nationale des Titres Sécurisés OU=0002 130003262 CN=Autorité de certification porteur AAE 3 étoiles
subjectPublicKey	clé publique de l'AC
signatureAlgorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

Nota : Les certificats de test incluent dans le DN un composant OU supplémentaire :

OU = POUR QUALIF UNIQUEMENT

Extensions

Champ de base	**Criticité**	**Valeur**
authorityKeyIdentifier	non critique	identique au champ « Subject Key Identifier » du certificat de l'AC ANTS V2
subjectKeyIdentifier	non critique	identifiant de la clé publique
keyUsage	critique	Certificate Sign et CRL Sign
certificatePolicies	non critique	Any Policy
basicConstraints	critique	CA:TRUE, pathlen:0
crlDistributionPoints	non critique	Indique l'adresse HTTP où est publiée la LAR pour ce certificat

Autres caractéristiques :

Taille des clés	2048 bits
Durée de validité	6 ans

7.1.1.2 Certificat de porteur

Les informations principales contenues dans le certificat du porteur sont :

Champ de base	**Valeur**
version	2 (=version 3)
serialNumber	défini par l'outil
issuer	C=FR O=Agence Nationale des Titres Sécurisés OU=0002 130003262 CN=Autorité de certification porteur AAE 3 étoiles
notBefore	début de la période de validité du certificat
notAfter	fin de la période de validité du certificat
subject	C=FR O=<nom du Service de l'Etat> OU=0002 <espace> Numéro SIREN du Service de l'Etat CN= <prénom nom identifiant> (le séparateur est le caractère « espace »)
subjectPublicKey	clé publique du porteur
signatureAlgorithm	sha256WithRSAEncryption (1.2.840.113549.1.1.11)

Nota : Pour des raisons de test des certificats porteurs de test peuvent être émis par l'AC AAE. Le certificat porteur comporte alors la valeur « TEST » apposé dans le CN avant le <prénom nom identifiant>.

Extensions

Champ de base	**Criticité**	**Valeur**	
authorityKeyIdentifier	non critique	identique au champ « subject key identifier » du certificat de l'AC	
subjectKeyIdentifier	non critique	identifiant de la clé publique	
keyUsage	critique	utilisations autorisées de la clé privée. Selon le type de certificat, l'usage est différent :	
		certificat d'authentification	digital Signature
		certificat de signature	Content Commitment
certificatePolicies	non critique	OID de la politique de certification sous laquelle le certificat a été émis. Selon le type de certificat, le champ contient un OID différent :	
		certificat d'authentification	1.2.250.1.200.2.2.1.1

		certificat de signature	1.2.250.1.200.2.3.1.1
basicConstraints	non critique	CA:FALSE	
crlDistributionPoints	non critique	Indique l'adresse HTTP où est publiée la LCR pour ce certificat	
QcStatements	non critique	N'est présente que dans les certificats de signature. Elle indique : a) que le certificat est qualifié, et b) que la clé privée réside dans un dispositif de création de signature électronique (SSCD) Se référer aux explications ci-après	

Autres caractéristiques :

taille des clés	2048 bits
durée de validité	3 ans

Explications complémentaires :

L'identifiant contenu dans l'attribut CN du DN dans le champ subject est unique. Son unicité est gérée dans un annuaire de confiance externe.

- Pour la fonction de signature uniquement, le certificat contient une extension QcStatements {iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) pkix(7) privateExtension(1) qcStatements(3)} qui contient deux identifiants d'objet (OID), l'un indiquant qu'il s'agit d'un certificat qualifié {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcCompliance(1)}, et l'autre indiquant que la clé privée réside dans un dispositif sécurisé de création de signature (SSCD) {itu-t(0) identified-organization(4) etsi(0) qc-profile(1862) qcs(1) qcs-QcSSCD(4)}.

Pour plus d'informations, consulter le [RFC 5280].

7.2 Profil des LCR

Les caractéristiques des LCR sont :

Champ de base	**Valeur**
version	1 (= version 2)
signature	sha256WithRSAEncryption OID: 1.2.840.113549.1.1.11
issuer	C=FR O=Agence Nationale des Titres Sécurisés OU=0002 130003262 CN=Autorité de certification porteur AAE 3 étoiles
thisUpdate	date et heure UTC
nextUpdate	date et heure UTC
revokedCertificates	Liste de tuples: UserCertificate (numéro de série) RevocationDate (date de révocation)

Extensions

Champ de base	**Criticité**	**Valeur**
authorityKeyIdentifier	Extension non critique	identique au champ « Subject Key Identifier » du certificat de l'AC
crlNumber	Extension non critique	nombre entier
issuingDistributionPoint	Extension critique	le champ distributionPoint contient une URI avec la méthode d'accès (scheme) HTTP. La valeur correspond aux valeurs qui sont présentes dans les extensions cRLDistributionPoints des certificats.

Autres caractéristiques :

Caractéristiques d'une LCR :	Durée de validité : 48 heures Périodicité de mise à jour : 24 heures.

Pour plus d'informations, consulter le [RFC 5280].

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Ainsi que le précise l'article 8 de l'[Ordonnance], lorsqu'une autorité administrative (AA) met en place un système d'information, elle détermine les fonctions de sécurité nécessaires pour protéger ce système. Pour les fonctions de sécurité traitées par le [RGS], elle fixe le niveau de sécurité requis parmi les niveaux prévus et respecte les règles correspondantes.

Dans le cadre de la présente PC, le niveau de sécurité choisi par l'ANTS est le niveau ***.

Ainsi que le précise l'article 8 de l'[Ordonnance], les actes des autorités administratives qui font l'objet d'une signature électronique doivent être signés au moyen d'un procédé, conforme aux règles du [RGS] mentionné au I de l'article 9, qui permette l'identification du signataire, garantisse le lien de la signature avec l'acte auquel elle s'attache et assure l'intégrité de cet acte.

Dans le cadre de la présente PC, des certificats à usage de signature sont délivrés pour signer et vérifier des actes. Le niveau de sécurité choisi par l'ANTS pour ces certificats est le niveau ***.

Le [RGS] liste les règles que les prestataires de service de certification électronique (PSCE) délivrant des certificats électroniques de type signature électronique ou authentification doivent respecter. Les documents de référence du RGS, pour ce qui concerne les certificats objets de cette PC, sont au nombre de quatre :

- RGS_A_7 : RGS_PC-Type_Authentification_V2_3.pdf
- RGS_A_8 : RGS_PC-Type_Signature_V2_3.pdf
- RGS_A_13 : RGS_Variables_de_temps_V2_3.pdf
- RGS_A_14 : RGS_Profils_Certificat_LCR_OCSP_V2-3.pdf

Le RGS 1.0 a été approuvé par l'arrêté du Premier Ministre du 6 mai 2010 [Arrêté060510].

L'article 23 du décret du décret n° 2010-112 du 2 février 2010 [DécretRGS] précise que les autorités administratives doivent obtenir la validation de leurs certificats électroniques et de ceux de leurs Responsables Cartes au plus tard dans les trois ans à compter de la publication de l'arrêté du 6 mai 2010.

Le présent chapitre ne traite pas des audits effectués par les organismes qui procèdent à la qualification des prestataires de services de confiance dans le but d'obtenir la validation des certificats électroniques des agents de l'ANTS. La compétence de ces organismes est appréciée par l'ANSSI à partir d'un audit des moyens, des ressources et de l'expérience de l'organisme, c.f. [DécretRGS].

Le présent chapitre traite uniquement des audits et des évaluations de la responsabilité de l'AC afin de s'assurer que l'ensemble de son IGC est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

8.1 Fréquences et / ou circonstances des évaluations

Le responsable de l'exploitation des composantes de l'AC demande l'approbation de l'AA pour toute modification jugée comme étant une perte de la conformité avec la présente PC et la DPC qu'il met en œuvre.

L'AA se doit de prévenir les IGC avec lesquelles des accords sont conclus dans la mesure où ces modifications peuvent affecter ces accords ou le niveau de sécurité offert par l'IGC.

Le responsable de l'exploitation des composantes d'IGC demande l'approbation du responsable de l'AC AAE pour toute modification jugée comme étant une perte de la conformité avec la présente PC et la DPC qu'il met en œuvre.

L'AC AAE procède à un contrôle de conformité de l'ensemble de son IGC tous les ans.

8.2 Identités / qualifications des évaluateurs

Le contrôle d'une composante est effectué par une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée.

8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit n'appartient pas à l'entité opérant la composante contrôlée, quelle que soit cette composante, elle est dûment autorisée à pratiquer les contrôles visés.

8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définis dans la présente PC et dans la DPC associée, ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5 Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend un avis au responsable d'exploitation et à l'AC AAE 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, l'équipe d'audit émet des recommandations au responsable d'exploitation qui peuvent être la cessation (temporaire ou définitive) d'activité, 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 mesure à appliquer est effectué par le responsable d'exploitation et doit respecter ses politiques de sécurité internes.
- En cas de résultat "A confirmer", le responsable d'exploitation 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, le responsable d'exploitation confirme à la composante contrôlée la conformité aux exigences de la présente PC et la DPC.

8.6 Communication des résultats

Les résultats des contrôles de conformité sont communiqués à la composante contrôlée ainsi qu'à l'AC AAE.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

Sans objet.

9.2 Responsabilité financière

L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences de la présente PC, par elle-même ou l'une de ses composantes. De fait, en cas de dommage subi par une entité utilisatrice du fait d'un manquement par l'AC à ses obligations, l'AC pourra être amené à dédommager l'entité utilisatrice dans la limite de la responsabilité de l'AC définie dans les conditions générales d'utilisation et aux présentes.

L'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

L'ETAT est financièrement responsable pour le compte de l'AC.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations suivantes (liste non exhaustive) sont considérées comme confidentielles :

- les clés privées des certificats d'AC ;
- les données d'activation associées à une bi-clé cryptographique ;
- les journaux d'événements des composantes d'IGC ;
- les rapports d'audits ;
- les informations techniques relatives à la sécurité des fonctionnements des modules cryptographiques ;
- les informations techniques relatives à la sécurité des fonctionnements de certaines composantes d'IGC ;
- la DPC et les procédures associées ;
- les causes de révocation.

9.3.2 Informations hors du périmètre des informations confidentielles

Les informations concernant l'IGC publiées par le SP sont considérées comme non confidentielles, elles sont communiquées selon le principe du besoin d'en connaître.

9.3.3 Responsabilités en termes de protection des informations confidentielles

L'IGC respecte la législation et la réglementation en vigueur sur le territoire français.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

Il est entendu que toute collecte et tout usage de données à caractère personnel qui est effectuée par l'AC AAE est réalisée dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier de la loi informatique et libertés [CNIL].

9.4.2 Informations à caractère personnel

L'AC considère que les informations suivantes sont des informations à caractère personnel :

- données d'identification du porteur (hors celles figurant dans le certificat) ;
- le mot de passe et les réponses aux questions secrètes utilisées en particulier pour la révocation ;
- demande (renseignée) de certificat ;
- demande (renseignée) de révocation ;
- motif de la révocation.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

L'AE, l'AED, le CPS et l'AC traitent et protègent toutes les données à caractère personnel de manière à ce que seuls des personnels dans des rôles de confiance (internes ou autorités judiciaires) y aient accès, selon la présente PC.

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés [CNIL] et la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique [LCEN] s'applique au contenu de tous les documents collectés, détenus ou transmis par l'AC dans le cadre de la délivrance d'un certificat.

Les porteurs disposent d'un droit d'accès et de rectification des données collectées par l'AC ou l'AED pour l'émission du certificat et la gestion de son cycle de vie. Ce droit peut s'exercer auprès de l'ANTS.

Toutes les données collectées et détenues par l'AC sont considérées comme confidentielles, hormis les données figurant dans le certificat.

En vertu des articles 323-1 à 323-7 du Code pénal applicable lorsqu'une infraction est commise sur le territoire français, les atteintes et les tentatives d'atteintes aux systèmes de traitement automatisé de données sont sanctionnées, notamment l'accès et le maintien frauduleux, les modifications, les altérations et le piratage de données, etc. Les peines encourues varient de 1 à 3 ans d'emprisonnements assortis d'une amende allant de 15.000 à 225.000 euros pour les personnes morales.

9.4.5 Notification et consentement d'utilisation des données personnelles

Aucune des données à caractère personnel fournies par un porteur ne peut être utilisée par l'AC, pour une autre utilisation autre que celle définie dans le cadre de la présente PC, sans consentement exprès et préalable de la part du porteur.

Les composantes d'IGC et les porteurs disposent d'un droit d'accès et de rectification des données collectées par l'IGC. Ce droit peut s'exercer auprès de l'AC AAE. Les opérations demandées par l'AC ne doivent pas porter atteinte à l'intégrité de l'ensemble des données propres aux opérations mise en œuvre pour la gestion de son certificat.

9.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

L'AC agit conformément aux réglementations européenne et française et dispose de procédures pour permettre l'accès des autorités judiciaires aux données à caractère personnel.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Les informations relatives à une personne définies comme confidentielles au § 9.4.2 ne peuvent être divulguées qu'à leur propriétaire ou à un tiers habilité au niveau adéquat.

L'AC s'oblige à obtenir l'accord de l'ANTS pour transférer ses données à caractère personnel dans le cas d'un transfert d'activité tel qu'il est décrit au § 5.8.

9.5 Droits relatifs à la propriété intellectuelle et industrielle

La législation et la réglementation en vigueur sur le territoire français sont applicables.

9.6 Interprétations contractuelles et garanties

L'AC a pour obligation de :

- respecter et appliquer la PC et la DPC,
- se soumettre aux contrôles de conformité effectués, d'une part par l'équipe d'audit mandatée par l'AC et, d'autre part par l'organisme de qualification,
- respecter les clauses qui la lient aux porteurs et aux utilisateurs de certificats,
- documenter les procédures internes de fonctionnement,
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elle s'engage dans des conditions garantissant qualité et sécurité.

9.6.1 Autorités de Certification

L'AC s'assure que toutes les exigences détaillées dans la présente PC et la DPC associée, sont satisfaites en ce qui concerne l'émission et la gestion de certificats.

L'AC est responsable du maintien de la conformité aux procédures prescrites dans la présente PC. L'AC fournit tous les services de certification en accord avec sa DPC. Les obligations communes aux composantes de l'AC sont:

- de protéger les clés privées et leurs données d'activation en intégrité et confidentialité ;
- de n'utiliser ses clés cryptographiques et certificats qu'aux seules fins pour lesquelles ils ont été générés et avec les moyens appropriés, comme spécifié dans la DPC ;
- de respecter et appliquer les dispositions de la partie de la PC/DPC qui les concerne ;
- de documenter ses procédures internes de fonctionnement afin de compléter la DPC générale ;
- de mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC ;
- de faire certifier la clé publique, correspondante à sa clé privée, par l'AC ANTS V2 ;
- d'assurer l'information des Responsables Cartes auxquelles elle délègue, concernant leurs rôles et responsabilités, et le traitement des informations à caractère personnel ou confidentielles, conformément à la présente PC ;
- d'apporter les mesures nécessaires et suffisantes à la correction des non-conformités détectées dans les audits, dans les délais préconisés par les auditeurs ;
- de communiquer toutes les informations utiles, d'une part à l'équipe d'audit mandatée par l'AC et, d'autre part à l'organisme de qualification.

9.6.2 Service d'enregistrement

Les obligations découlent des obligations pertinentes de l'AC du chapitre § 9.6.1 en se restreignant aux services qu'elle met en œuvre dans le cadre de la présente PC. Les obligations communes aux composantes de l'AE sont:

- de respecter et appliquer les dispositions décrites dans les documents [GUIDE_AE] et [CGU] ;
- de documenter ses procédures internes de fonctionnement afin de compléter la PC/DPC générale ;
- de mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la mise en place et la réalisation des prestations auxquelles elle s'engage dans la PC/DPC ;
- d'assurer l'information des Responsables Cartes auxquelles elle délègue, concernant leurs rôles et responsabilités, et le traitement des informations à caractère personnel ou confidentielles, conformément à la présente PC ;
- d'apporter les mesures nécessaires et suffisantes à la correction des non-conformités détectées dans les audits, dans les délais préconisés par les auditeurs ;
- de communiquer toutes les informations utiles, d'une part à l'équipe d'audit mandatée par l'AC et, d'autre part à l'organisme de qualification.

9.6.3 Porteurs de certificats

Les porteurs :

- reconnaissent être informés que leur carte est personnelle ;
- s'engagent à ne pas la prêter et à la conserver constamment sous leur garde ;
- s'engagent à rendre leur carte au Service de l'Etat concerné ou l'ANTS en cas de cessation d'activité ou à la demande de leur hiérarchie ;
- s'engagent à retirer leur carte du lecteur de carte dès qu'ils quittent leur poste de travail ;
- reconnaissent que les codes d'activation d'authentification et de signature sont confidentiels et s'engagent à prendre toutes les précautions pour qu'ils ne soient pas divulgués ;
- reconnaissent que les accès effectués au moyen du code d'authentification sont journalisés et que le contenu de ces journaux pourra être utilisé en tant que preuve d'accès ;
- s'engagent à respecter l'usage (authentification ou signature électronique) pour lequel la clé privée associée à un certificat peut être utilisée ;
- s'engagent à n'utiliser leur carte qu'avec les matériels et les logiciels mis à leur disposition par la mairie, soit sous leur propre responsabilité en utilisant des matériels ou des logiciels donnant les mêmes garanties. Dans le cas contraire, leur responsabilité pourrait être engagée ;
- en cas de perte ou vol de leur carte et dès la découverte du vol ou de la perte s'engagent à demander la révocation des certificats contenus dans la carte dans les plus brefs délais ;
- en cas de divulgation d'un code PIN et dès la découverte la divulgation d'un code PIN, s'engagent à en changer dans les plus brefs délais.

La relation entre le porteur et l'AC est formalisée dans les Conditions Générales d'Utilisation.

9.6.4 Utilisateurs de certificats

Un utilisateur de certificats doit utiliser des logiciels qui sont à même de vérifier que le certificat est effectivement utilisé selon l'usage prescrit dans le certificat (authentification ou signature électronique).

Chaque certificat contient l'identifiant de la politique de certification sous lequel le certificat a été émis. La présence de cet identifiant doit être vérifiée.

Pour cela, il doit, soit utiliser les logiciels mis à sa disposition par le Service de l'Etat, soit sous sa propre responsabilité utiliser des logiciels donnant les mêmes garanties. Dans le cas contraire, sa responsabilité pourrait être engagée.

Un utilisateur de certificat doit utiliser un logiciel qui vérifie que le certificat est valide. La vérification que doit effectuer le logiciel est différente selon qu'il s'agit de la vérification d'un certificat à usage d'authentification ou de la vérification d'un certificat à usage de signature électronique.

Pour la vérification d'un certificat à usage d'authentification, le logiciel doit construire un chemin de certification entre le certificat du porteur et le certificat auto-signé de l'AC ANTS V2, et s'assurer qu'au moment de l'échange d'authentification aucun des certificats du chemin n'est en dehors de sa période de validité ou révoqué.

Pour la vérification d'un certificat à usage de signature électronique, le logiciel doit construire un chemin de certification entre le certificat du porteur et le certificat auto-signé de l'AC ANTS V2, et s'assurer qu'au moment où la signature numérique a été horodatée par une unité d'horodatage de confiance qu'aucun des certificats du chemin n'était en dehors de sa période de validité ou révoqué. Il doit en outre s'assurer que le certificat de l'unité d'horodatage est valide.

La relation entre le porteur et l'AC est formalisée dans la section « Conditions pour les utilisateurs de certificats »

9.6.5 Autres participants

La DPC précisera les exigences si besoin est.

9.7 Limite de garantie

L'AC garantit au travers de ses services d'IGC :

- L'identification et l'authentification de l'ACR avec son certificat auto signé ;
- l'identification et l'authentification des porteurs avec les certificats générés par l'AC ;
- la gestion des certificats correspondant et des informations de validité des certificats selon la DPC/PC.

Aucune autre garantie ne peut-être mise en avant par l'AC, les porteurs et les UC dans leurs accords contractuels (s'il en est).

9.8 Limites de responsabilité

Seule la responsabilité de l'ETAT peut être mise en cause en cas de non-respect des dispositions prévues par les présentes.

L'AC décline toute responsabilité à l'égard de l'usage des certificats émis par elle ou des bi-clés publiques/privées associées dans des conditions et à des fins autres que celles prévues dans la présente PC.

L'AC décline toute responsabilité à l'égard de l'usage qui est fait des certificats d'AC qu'elle a émis dans des conditions et à des fins autres que celles prévues dans la présente politique de certification ainsi que dans tout autre document contractuel applicable associé.

L'AC décline toute responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, et quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication.

L'AC ne saurait être tenue responsable, et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'Article 1148 du Code civil.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, outre ceux habituellement retenus par la jurisprudence des cours et tribunaux français, les conflits sociaux, la défaillance du réseau ou des installations ou réseaux de télécommunications externes.

L'AC n'est en aucun cas responsable des préjudices indirects subis par les entités utilisatrices, ceux-ci n'étant pas préqualifiés par les présentes.

En cas de prononcé d'une quelconque responsabilité de l'AC, les dommages, intérêts et indemnités à sa charge toutes causes confondues, et quel que soit le fondement de sa responsabilité, sont limités par certificat à la somme prévue au titre de limite de responsabilité dans les conditions générales d'utilisation applicable audit certificat.

Pour les certificats de signature, l'AC est responsable du préjudice causé aux personnes qui se sont fiées raisonnablement aux certificats présentés par eux comme qualifiés dans chacun des cas précisé par l'article 33 de la [LCEN].

9.9 Indemnités

Les parties conviennent qu'en cas de prononcé d'une quelconque responsabilité de l'AC vis-à-vis d'un tiers utilisateur, les dommages, intérêts et indemnités à sa charge seront déterminés lors de la procédure prévue à l'article 9.2 des présentes.

En cas de préjudice causé aux personnes qui se seraient fiées raisonnablement aux certificats de signature et uniquement selon les conditions précisées à l'article 33 de la LCEN, la responsabilité financière de l'ETAT pourra être engagée.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

La présente PC devient effective une fois signée par le directeur de l'ANTS. La PC reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Fin anticipée de validité

La publication d'une nouvelle version de la présente PC peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer la PC qu'elle met en œuvre.

En fonction de la nature et de l'importance des évolutions apportées à la PC, le délai de mise en conformité sera arrêté conformément aux modalités prévues par la réglementation en vigueur.

De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié aux modifications des exigences de sécurité contenu dans la présente PC.

9.10.3 Effets de la fin de validité et clauses restant applicables

Les clauses restant applicables au-delà de la fin d'utilisation de la PC, sont celles concernant l'archivage des données. Toutes les autres obligations deviennent caduques et sont remplacées par celles décrites dans la ou les PC encore en vigueur.

9.11 Notifications individuelles et communications entre les participants

En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC s'engage :

- au plus tard un mois avant le début de l'opération, à faire valider ce changement au travers d'une expertise technique, afin d'évaluer les impacts sur le niveau de qualité et de sécurité des fonctions de l'ACR et de ses différentes composantes.
- au plus tard un mois après la fin de l'opération, à en informer l'organisme de qualification.

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

L'AC s'engage à contrôler que tout projet de modification de sa PC reste conforme aux exigences de la présente PC Type et des éventuels documents complémentaires du [RGS]. L'AC pourra réviser sa PC et/ou sa DPC chaque fois qu'une évolution remarquable de l'état de l'art le justifie.

9.12.2 Mécanisme et période d'information sur les amendements

L'ANTS donne un préavis de deux mois au moins aux composantes de l'AC de son intention de modifier sa PC/DPC avant de procéder aux changements et en fonction de l'objet de la modification.

9.12.3 Circonstances selon lesquelles un OID doit être changé

L'OID de la PC est inscrit dans les certificats émis. Toute évolution d'une PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) se traduira par un changement de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

9.13 Dispositions concernant la résolution de conflits

Les conflits entre des personnes appartenant aux mairies ou aux Services de l'Etat sont traités respectivement au niveau des Services de l'Etat ou du Ministère de l'Intérieur. A défaut, ils sont du ressort du Tribunal Administratif.

9.14 Juridictions compétentes

Le Tribunal Administratif compétent est soit celui du plaignant soit celui du défendant.

9.15 Conformité aux législations et réglementations

La présente PC est sujette aux lois, règles, règlements, ordonnances, décrets et ordres nationaux, d'état, locaux et étrangers concernant les IGC, mais non limités aux IGC, restrictions à l'importation et à l'exportation de logiciels ou de matériels cryptographiques ou encore d'informations techniques.

L'environnement législatif pour la mise en œuvre de l'AC AAE est notamment constitué des textes de lois et règlements suivants :

- la directive 1999/93/CE du Parlement européen et du Conseil en date du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques [Directive] ;
- les articles 1316 et suivants du Code Civil relatif à la signature électronique [CC1316] ;
- le décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique [SIG] ;
- l'article 801-1 du CPP [CPP801] ;
- la loi n° 2004-575 du 21 juin 2004 modifiée, pour la confiance dans l'économie numérique, et en particulier l'article 33 [LCEN] ;
- la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés [LCNIL] ;
- l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives [Ordonnance] ;
- le décret n° 2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique [DEC2001-272] ;
- l'arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation [Arrêté260704] ;
- le décret n°2010-112 du 2 février 2010 pris pour application des articles 9 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives [DécretRGS] ;
- l'arrêté du 10 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques [Arrêté060510].

9.16 Dispositions diverses

9.16.1 Accord global

Les éventuels accords passés avec les partenaires doivent être validés par l'ANTS.

9.16.2 Transfert d'activités

Voir § 5.8.

9.16.3 Conséquences d'une clause non valide

Les conséquences, le cas échéant, seront traitées en fonction de la législation en vigueur.

9.16.4 Application et renonciation

La présente PC ne formule pas d'exigence spécifique sur le sujet.

9.16.5 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un évènement irrésistible, insurmontable et imprévisible.

9.17 Autres dispositions

Le cas échéant, la DPC en fournira les détails.

10 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 Réglementation

Renvoi	Document
[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.
[Directive]	Directive 1999/93/CE du Parlement européen et du Conseil en date du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques
[Ordonnance]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives (Journal Officiel du 9 décembre 2005). Disponible en ligne : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000636232&dateTexte=vig
[CPP801]	Article 801-1 du code de procédure pénale
[CC1316]	Articles 1316 et suivants du Code Civil relatif à la signature électronique [CC1316
[DécretRGS]	Décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'[Ordonnance]. Disponible en ligne : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000021779444&dateTexte=vig
[Décret2001-272]	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. Disponible en ligne : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=vig
[Arrêté260704]	Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation. Disponible en ligne : http://www.legifrance.gouv.fr/./affichTexte.do?cidTexte=JORFTEXT000000441678&dateTexte=vig
[Arrêté060510]	Arrêté du 6 mai 2010 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques. Disponible en ligne : http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000022220429&fastPos=1&fastReqId=1704766824&categorieLien=id&oldAction=rechTexte
[LCEN]	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
[SIG]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.

10.2 Documents techniques

Renvoi	Document
[RGS]	Référentiel Général de Sécurité – Version 1.0
[RGS_A2]	RGS – Fonction de sécurité « Authentification » – Version 2.3
[RGS_A3]	RGS – Fonction de sécurité « Signature électronique » – Version 2.3
[RGS_A7]	RGS – Politique de Certification Type Authentification – Version 2.3
[RGS_A8]	RGS – Politique de Certification Type Signature – Version 2.3
[RGS_A_13]	RGS – Politiques de Certification Types - Variables de Temps - Version 2.3
[RGS_A_14]	RGS – Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3
[RGS_B_1]	RGS – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques - Version 1.20
[X.509]	Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks. 6 th Edition. Version de novembre 2008. Disponible à l'adresse : http://www.x500standard.com/index.php?n=Ig.LatestAvail.
[RFC3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003. Disponible à l'adresse : http://www.ietf.org/rfc/rfc3647.txt
[GUIDE_AE]	ANTS – Guide de procédure pour les operateurs de l'AE
[CGU]	Conditions Générales d'Utilisation des cartes AAE et des cartes ACT

11 ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC

11.1 Exigences sur les objectifs de sécurité

Le module cryptographique (HSM), utilisé par l'AC pour générer et mettre en œuvre ses clés d'authentification (pour la génération des certificats électroniques, des LCR) et ses clés de signature (pour la génération des certificats électroniques, des LCR) répond aux exigences de sécurité suivantes :

- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie,
- être capable d'identifier et d'authentifier ses utilisateurs,
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné,
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur,
- permettre de signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance des clés privées,
- créer des enregistrements d'audit pour chaque modification concernant la sécurité,
- dans le cadre des fonctions de sauvegarde et de restauration des clés privée de l'AC, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

11.2 Exigences sur la qualification

Le module cryptographique utilisé par l'AC fait l'objet d'une qualification au niveau renforcé, selon le processus décrit dans le [RGS], et est conforme aux exigences du chapitre 11.1 ci-dessus.

12 ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF DE CREATION DE SIGNATURE

12.1 Exigences sur les objectifs de sécurité

12.1.1 Authentification

Le dispositif d'authentification, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée répond aux exigences de sécurité suivantes :

- lorsque la bi-clé de signature du porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération,
- disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- générer une signature numérique qui ne peut être falsifiée sans la connaissance de la clé privée (dans la mesure où la fonction de hachage utilisée à l'extérieur du dispositif soit exempte de collisions et que le protocole d'authentification soit exempt de faiblesses et de possibilités de rejeu) ;
- assurer la fonction d'authentification pour le porteur légitime uniquement en utilisant un code d'activation personnel et spécifique pour mettre en œuvre la fonction.

12.1.2 Signature

Le dispositif de création de signature, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, répond aux exigences de sécurité suivantes :

- lorsque la bi-clé de signature du porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- assurer la correspondance entre la clé privée et la clé publique ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.
- détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération,
- disposer de techniques sûres d'invalidation de la clé privée précédente en cas de re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- générer une signature numérique qui ne peut être falsifiée sans la connaissance de la clé privée (dans la mesure où la fonction de hachage utilisée à l'extérieur du dispositif soit exempte de collisions et que le format de signature électronique soit exempt de faiblesses et de possibilités d'anti-datation) ;
- assurer la fonction de signature électronique pour le porteur légitime uniquement en utilisant un code d'activation personnel et spécifique pour mettre en œuvre la fonction.

Les dispositifs d'authentification des porteurs sont des cartes à puce respectant le socle commun IAS (Identification, Authentification, Signature) et permettent de répondre à l'ensemble de ces exigences de sécurité.

12.2 Exigences sur la qualification

12.2.1 Authentification

Le dispositif d'authentification utilisé par le porteur fait l'objet d'une qualification au niveau renforcé, selon le processus décrit dans le [RGS], et est conforme aux exigences du chapitre 12.1.1 ci-dessus.

12.2.2 Signature

Le dispositif de création de signature utilisé par le porteur fait l'objet d'une qualification au niveau renforcé, selon le processus décrit dans le [RGS], et est conforme aux exigences du chapitre 12.1.2 ci-dessus.