




MINISTÈRE SOCIAUX


	DATE : 27/11/2018 NB PAGES : 79 VERSION : 1.0 REFERENCE : IMAGE-IGC-PC02 STATUT : Validé
Projet :	IMAGE
Titre :	POLITIQUE DE CERTIFICATION AC LOGICIELS-2 : AUTHENTIFICATION OID : 1.2.250.1.179.1.2.1.1.2

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>Sommaire</p>	
---	--	--

SOMMAIRE

HISTORIQUE DES VERSIONS	12
REFERENCES DOCUMENTAIRES	12
1. INTRODUCTION	13
1.1. PRESENTATION GENERALE	13
1.2. IDENTIFICATION DU DOCUMENT	14
1.3. NIVEAU DE CONFORMITE	14
1.4. DEFINITIONS ET ABREVIATIONS	15
1.4.1. DEFINITIONS	15
1.4.2. ABREVIATIONS	16
1.5. ENTITES INTERVENANT DANS L'IGC	18
1.5.1. AUTORITE ADMINISTRATIVE	18
1.5.2. AUTORITE DE CERTIFICATION	19
1.5.3. AUTORITE D'ENREGISTREMENT LOCALE	20
1.5.4. PORTEUR	21
1.5.5. TIERS UTILISATEURS DES CERTIFICATS	21
1.6. USAGE DES CERTIFICATS	22
1.6.1. BI-CLES ET CERTIFICATS PORTEURS	22
1.6.2. BI-CLES ET CERTIFICATS DE L'AC LOGICIELS-2 ET DE SES COMPOSANTES	22
1.7. GESTION DE LA PC	22

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		2/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>Sommaire</p>	
---	---	--

1.7.1.	ENTITE GERANT LA POLITIQUE DE CERTIFICATION	22
1.7.2.	POINT DE CONTACT	23
1.7.3.	DECLARATION DES PRATIQUES DE CERTIFICATION (DPC)	23
1.7.4.	PROCEDURE D'APPROBATION DE LA DPC	23
1.8.	CONDITIONS D'UTILISATION	24
2.	<u>RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS PUBLIEES</u>	25
2.1.	ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS	25
2.2.	INFORMATIONS PUBLIEES	25
2.3.	DELAIS ET FREQUENCES DE PUBLICATION	26
2.4.	CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES	27
3.	<u>IDENTIFICATION ET AUTHENTIFICATION</u>	28
3.1.	NOMMAGE	28
3.1.1.	TYPES DE NOMS	28
3.1.2.	UTILISATION DE NOMS EXPLICITES	28
3.1.3.	UNICITE DES NOMS	28
3.1.4.	IDENTIFIANTS ATTRIBUES AUX PERSONNES INTERNES ET AUX PERSONNES EXTERNES SUR SITE	29
3.2.	VALIDATION INITIALE DE L'IDENTITE	29
3.2.1.	VALIDATION DE L'IDENTITE D'UN PORTEUR	29
3.2.2.	VALIDATION DES AUTRES IDENTIFIANTS ATTRIBUES AUX PERSONNES INTERNES ET AUX « EXTERNES SUR SITE »	30
3.3.	IDENTIFICATION ET VALIDATION POUR LE RENOUVELLEMENT DES CLES	30

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		3/79



Projet IMAGE
AC Personnes : Authentification

[Sommaire](#)

3.3.1.	IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT COURANT	30
3.3.2.	IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT APRES REVOCATION	31
4.	EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	32
4.1.	ENREGISTREMENT INITIAL	32
4.1.1.	ORIGINE DE L'ENREGISTREMENT INITIAL ET DE LA DEMANDE DE CERTIFICAT	32
4.1.2.	PROCESSUS ET RESPONSABILITES POUR L'ETABLISSEMENT D'UNE DEMANDE DE CERTIFICAT	32
4.2.	DEROULEMENT DE L'ENREGISTREMENT	32
4.2.1.	PROCESSUS D'IDENTIFICATION ET DE VALIDATION	32
4.2.2.	ACCEPTATION OU REJET DE L'ENREGISTREMENT	33
4.2.3.	DUREE D'ETABLISSEMENT DU CERTIFICAT	33
4.3.	DELIVRANCE DU CERTIFICAT	34
4.3.1.	ACTIONS DE L'AC CONCERNANT LA DELIVRANCE DU CERTIFICAT	34
4.3.2.	MOT DE PASSE PKCS12	34
4.3.3.	NOTIFICATION PAR L'AC DE LA DELIVRANCE DU CERTIFICAT AU PORTEUR	34
4.4.	ACCEPTATION DU CERTIFICAT	35
4.4.1.	PUBLICATION DU CERTIFICAT	35
4.5.	USAGES DE LA BI-CLE ET DU CERTIFICAT	35
4.5.1.	UTILISATION DE LA CLE PRIVEE ET DU CERTIFICAT PAR LE PORTEUR	35
4.5.2.	UTILISATION DE LA CLE PUBLIQUE ET DU CERTIFICAT PAR UN TIERS UTILISATEUR	36
4.6.	RENOUVELLEMENT D'UN CERTIFICAT SANS CHANGEMENT DE BI-CLE	36
4.7.	RENOUVELLEMENT D'UN CERTIFICAT AVEC CHANGEMENT DE LA BI-CLE	36
4.7.1.	CAUSES POSSIBLES DE CHANGEMENT D'UNE BI-CLE	36

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		4/79



Projet IMAGE
AC Personnes : Authentification

Sommaire

4.7.2.	ORIGINE D'UNE DEMANDE DE RENOUVELLEMENT DE CERTIFICAT	37
4.7.3.	PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE RENOUVELLEMENT DE CERTIFICAT	37
4.7.4.	NOTIFICATION AU PORTEUR DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT	37
4.7.5.	DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT	37
4.7.6.	PUBLICATION DU NOUVEAU CERTIFICAT	37
4.8.	MODIFICATION DU CERTIFICAT	37
4.9.	REVOCACTION ET SUSPENSION DES CERTIFICATS	38
4.9.1.	CAUSES POSSIBLES D'UNE REVOCACTION	38
4.9.2.	ORIGINE D'UNE DEMANDE DE REVOCACTION	38
4.9.3.	PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE REVOCACTION FAITE PAR LE PORTEUR	39
4.9.4.	DELAJ ACCORDE AU PORTEUR POUR EFFECTUER LA REVOCACTION	39
4.9.5.	DELAJ DE TRAITEMENT PAR L'AC D'UNE DEMANDE DE REVOCACTION	40
4.9.6.	EXIGENCES DE VERIFICATION DE LA REVOCACTION PAR LES TIERS UTILISATEURS DE CERTIFICAT	40
4.9.7.	FREQUENCE D'ETABLISSEMENT DE LA LCR	40
4.9.8.	DELAJ MAXIMUM DE PUBLICATION D'UNE LCR	41
4.9.9.	DISPONIBILITE D'UN SYSTEME DE VERIFICATION EN LIGNE DE LA REVOCACTION ET DE L'ETAT DES CERTIFICATS	41
4.9.10.	AUTRES MOYENS DISPONIBLES D'INFORMATION SUR LES REVOICATIONS	41
4.9.11.	EXIGENCES SPECIFIQUES EN CAS DE COMPROMISSION DE LA CLE PRIVEE	41
4.9.12.	CAUSES POSSIBLES D'UNE SUSPENSION	41
4.10.	FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS	41
4.10.1.	CARACTERISTIQUES OPERATIONNELLES	41
4.10.2.	DISPONIBILITE DE LA FONCTION	42

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		5/79



Projet IMAGE
AC Personnes : Authentification


[Sommaire](#)

4.11. FIN DE RELATION ENTRE LE PORTEUR ET L'AC	42
4.12. SEQUESTRE DE CLE ET RECOUVREMENT	42
<u>5. MESURES DE SECURITE NON TECHNIQUES</u>	<u>43</u>
5.1. MESURES DE SECURITE PHYSIQUE	43
5.1.1. SITUATION GEOGRAPHIQUE ET CONSTRUCTION DES SITES	43
5.1.2. ACCES PHYSIQUE	43
5.1.3. ALIMENTATION ELECTRIQUE ET CLIMATISATION	43
5.1.4. VULNERABILITE AUX DEGATS DES EAUX	44
5.1.5. PREVENTION ET PROTECTION INCENDIE	44
5.1.6. CONSERVATION DES SUPPORTS	44
5.1.7. MISE HORS SERVICE DES SUPPORTS	44
5.1.8. SAUVEGARDES HORS SITE	45
5.2. MESURES DE SECURITE PROCEDURALES	45
5.2.1. ROLES DE CONFIANCE AUPRES DE L'AC	45
5.2.2. ROLES DE CONFIANCE MUTUALISES A D'AUTRES APPLICATIONS	46
5.2.3. NOMBRE DE PERSONNES REQUISES PAR TACHES	46
5.2.4. IDENTIFICATION ET AUTHENTIFICATION POUR CHAQUE ROLE	47
5.2.5. ROLES EXIGEANT UNE SEPARATION DES ATTRIBUTIONS	47
5.3. MESURES DE SECURITE VIS-A-VIS DU PERSONNEL	48
5.3.1. QUALIFICATIONS, COMPETENCES ET HABILITATIONS REQUISES	48
5.3.2. VERIFICATION DE L'ADEQUATION DES PROFILS	48
5.3.3. FORMATION INITIALE	49

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		6/79

5.3.4.	FORMATION CONTINUE	49
5.3.5.	FREQUENCE ET SEQUENCE DE ROTATION ENTRE DIFFERENTES ATTRIBUTIONS	49
5.3.6.	SANCTIONS EN CAS D' ACTIONS NON AUTORISEES	49
5.3.7.	EXIGENCES VIS-A-VIS DU PERSONNEL DES PRESTATAIRES EXTERNES	50
5.3.8.	DOCUMENTATION FOURNIE AU PERSONNEL	50
5.4.	PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT	50
5.4.1.	TYPES D'EVENEMENTS ENREGISTRES	50
5.4.2.	FREQUENCE DE TRAITEMENT DES JOURNAUX D'EVENEMENTS	52
5.4.3.	PERIODE DE CONSERVATION DES JOURNAUX D'EVENEMENTS SUR SITE	53
5.4.4.	PROTECTION DES JOURNAUX D'EVENEMENTS	53
5.4.5.	PROCEDURE DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS	54
5.4.6.	SYSTEME DE COLLECTE DES JOURNAUX D'EVENEMENTS	54
5.4.7.	NOTIFICATION DE L'ENREGISTREMENT D'UN EVENEMENT AU RESPONSABLE DE L'EVENEMENT	55
5.4.8.	EVALUATION DES VULNERABILITES	55
5.5.	ARCHIVAGE DES DONNEES	55
5.5.1.	TYPES DE DONNEES ARCHIVEES	55
5.5.2.	PERIODE DE CONSERVATION DES ARCHIVES	56
5.5.3.	PROTECTION DES ARCHIVES	57
5.5.4.	PROCEDURE DE SAUVEGARDE DES ARCHIVES	57
5.5.5.	DATATION DES DONNEES	57
5.5.6.	SYSTEME DE COLLECTE DES ARCHIVES	58
5.5.7.	PROCEDURES DE RECUPERATION ET DE VERIFICATION DES ARCHIVES	58
5.6.	CHANGEMENT DE CLE D'AC	58

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		7/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>Sommaire</p>	
---	---	--

5.7. REPRISE SUITE A COMPROMISSION ET SINISTRE	59
5.7.1. PROCEDURES DE REMONTEE ET DE TRAITEMENT DES INCIDENTS ET DES COMPROMISSIONS	59
5.7.2. PROCEDURES DE REPRISE EN CAS DE CORRUPTION DES RESSOURCES INFORMATIQUES (MATERIELS, LOGICIELS ET / OU DONNEES)	59
5.7.3. PROCEDURES DE REPRISE EN CAS DE COMPROMISSION DE LA CLE PRIVEE DE L'AC OU DE L'UNE DE SES COMPOSANTES	59
5.7.4. CAPACITES DE CONTINUITE D'ACTIVITE SUITE A UN SINISTRE	60
5.8. FIN DE VIE DE L'IGC	60
<u>6. MESURES DE SECURITE TECHNIQUES</u>	<u>62</u>
6.1. GENERATION DES BI-CLES	62
6.1.1. GENERATION DES BI-CLES DE L'AUTORITE	62
6.1.2. GENERATION DES BI-CLES DES PORTEURS	63
6.1.3. TRANSMISSION DE LA CLE PRIVEE A SON PROPRIETAIRE	63
6.1.4. TRANSMISSION DE LA CLE PUBLIQUE D'UN PORTEUR A L'AC	63
6.1.5. TRANSMISSION DE LA CLE PUBLIQUE DE L'AC AUX TIERS UTILISATEURS DE CERTIFICAT ET AUX PORTEURS	63
6.1.6. TAILLES DES CLES	63
6.1.7. VERIFICATION DE LA GENERATION DES PARAMETRES DES BI-CLES ET DE LEUR QUALITE	63
6.1.8. OBJECTIFS D'USAGE DE LA CLE	63
6.2. MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES	64
6.2.1. MODULES CRYPTOGRAPHIQUES DE L'AC	64
6.3. AUTRES ASPECTS DE LA GESTION DES BI-CLES	64

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		8/79



Projet IMAGE
AC Personnes : Authentification

Sommaire

6.3.1.	ARCHIVAGE DES CLES PUBLIQUES	64
6.3.2.	DUREES DE VIE DES BI-CLES ET DES CERTIFICATS	64
6.4.	DONNEES D'ACTIVATION DES CLES D'AC	65
6.4.1.	GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION	65
6.4.2.	PROTECTION DES DONNEES D'ACTIVATION	65
6.5.	MESURES DE SECURITE DES SYSTEMES INFORMATIQUES	65
6.6.	MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE	66
6.6.1.	MESURES DE SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES	66
6.6.2.	MESURES LIEES A LA GESTION DE LA SECURITE	66
6.7.	MESURES DE SECURITE RESEAU	67
6.8.	SYSTEME DE DATATION	67
7.	PROFILS DES CERTIFICATS, DE LA LCR ET DES REPONSES OCSP	68
8.	AUDITS INTERNES ET DE CONFORMITE	69
8.1.	FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS	69
8.2.	IDENTITES / QUALIFICATIONS DES EVALUATEURS	70
8.3.	RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES	70
8.4.	SUJETS COUVERTS PAR LES EVALUATIONS	70
8.5.	ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS	70
8.6.	COMMUNICATION DES RESULTATS	71
9.	AUTRES PROBLEMATIQUES METIERS ET LEGALES	72
9.1.	TARIFS	72

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		9/79



Projet IMAGE
AC Personnes : Authentification

Sommaire

9.2. RESPONSABILITE FINANCIERE	72
9.3. CONFIDENTIALITE DES DONNEES PROFESSIONNELLES	72
9.3.1. PERIMETRE DES INFORMATIONS CONFIDENTIELLES	72
9.3.2. RESPONSABILITES EN TERME DE PROTECTION DES INFORMATIONS CONFIDENTIELLES	72
9.4. PROTECTION DES DONNEES PERSONNELLES	72
9.4.1. POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES	72
9.4.2. INFORMATIONS A CARACTERE PERSONNEL	73
9.4.3. INFORMATIONS A CARACTERE NON PERSONNEL	73
9.4.4. RESPONSABILITE EN TERME DE PROTECTION DES DONNEES PERSONNELLES	73
9.4.5. NOTIFICATION ET CONSENTEMENT D'UTILISATION DES DONNEES PERSONNELLES	73
9.4.6. CONDITIONS DE DIVULGATION D'INFORMATIONS PERSONNELLES AUX AUTORITES JUDICIAIRES OU ADMINISTRATIVES	74
9.4.7. AUTRES CIRCONSTANCES DE DIVULGATION D'INFORMATIONS PERSONNELLES	74
9.5. DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE	74
9.6. INTERPRETATIONS CONTRACTUELLES ET GARANTIES	74
9.6.1. OBLIGATIONS APPLICABLES A L'AUTORITE DE CERTIFICATION	75
9.6.2. OBLIGATIONS APPLICABLES AUX OPERATEURS D'ENREGISTREMENT	75
9.6.3. OBLIGATIONS APPLICABLES AUX PORTEURS	76
9.6.4. OBLIGATIONS APPLICABLES AUX TIERS UTILISATEURS DE CERTIFICAT	76
9.7. LIMITE DE RESPONSABILITE	77
9.8. INDEMNITES	77
9.9. DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC	77
9.9.1. DUREE DE VALIDITE ET FIN DE VALIDITE DE LA PRESENTE PC	77

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		10/79




Projet IMAGE
AC Personnes : Authentification

[Sommaire](#)

9.9.2.	EFFETS DE LA FIN DE VALIDITE ET CLAUSES RESTANT APPLICABLES	78
9.10.	AMENDEMENTS A LA PC	78
9.10.1.	MECANISME ET PERIODE D'INFORMATION SUR LES AMENDEMENTS	78
9.10.2.	CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE	78
9.11.	DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS	79
9.12.	JURIDICTIONS COMPETENTES	79
9.13.	CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS	79

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		11/79

 <p>LIBERTÉ • ÉGALITÉ • FRATERNITÉ RÉPUBLIQUE FRANÇAISE</p> <hr/> <p>MINISTÈRE DE LA SANTÉ, DE LA JEUNESSE ET DES SPORTS</p>	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>Historique des versions</p>	
---	--	--

Historique des versions

Version	Date	Modification
0.94	17/09/2018	Version provisoire

Références documentaires

Référence	Titre
[PC-Profiles]	IMAGE : Profils de certificats AC Logiciels-2 Authentification
[DPC]	Déclaration des Pratiques de Certification, IGC IMAGE - AC Délégues
[PC-ACR]	Politique de Certification, IGC IMAGE - AC Racine-2

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		12/79

	Projet IMAGE AC Personnes : Authentification Introduction	
--	--	--

1. INTRODUCTION

1.1. Présentation générale

Présentation du projet IMAGE :

Le développement de l'administration électronique passe par la mise en place de moyens permettant d'apporter la confiance nécessaire à la dématérialisation des processus.

Le projet IMAGE (Infrastructure **M**inistérielle de gestion de clés, de services d'**A**uthentification et de services de confiance pour la **G**estion de la signature **E**lectronique et de la confidentialité) est un projet porté par la Direction des Systèmes d'Information assurant le support des MINISTÈRES SOCIAUX, dénommés « le Ministère ». Ce projet consiste à mettre en œuvre, d'une part, une Infrastructure de Gestion de Clés (IGC) permettant des services d'authentification forte, et d'autre part, une plate-forme de services de confiance.

Grâce à la mise en œuvre de l'IGC, le Ministère généralise au sein de son système d'information l'utilisation de services d'authentification forte pour l'accès à différents composants (postes de travail, applications sensibles).

Présentation de la Politique de Certification AC Logiciels-2 : Authentification :

Le présent document fait partie d'un ensemble de documents décrivant les politiques de certification utilisées dans le cadre du projet IMAGE.

Chaque document s'applique à un type de certificat émis par une autorité de certification, et définit les règles et les exigences auxquelles l'autorité se conforme dans la mise en place des prestations adaptées et appliquées à ce type de certificat.

Le présent document s'applique à l'autorité de certification « AC Logiciels-2 », ci-après dénommée « l'AC », et au type de certificat Authentification.

Le présent document spécifie les exigences concernant la politique mise en oeuvre par l'AC Logiciels-2 délivrant des certificats d'authentification et les clés privées associées.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		13/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>Introduction</p>	
--	---	--

Les certificats peuvent être attribués :

- 1) aux agents du Ministère travaillant sur le site du Ministère,
- 2) à des personnes extérieures au Ministère, mais travaillant sur le site du Ministère, par exemple des stagiaires ou des prestataires de service, et
- 3) à des personnes externes au Ministère ne travaillant pas sur le site du Ministère, mais utilisant certaines de ses applications pour lesquelles le niveau de sécurité est compatible avec un certificat logiciel.

Les certificats délivrés dans le cadre de ces exigences sont exclusivement utilisés pour :

- authentifier une personne physique agissant pour le compte de la personne morale de l'entité qu'elle représente auprès du système d'information du Ministère.

La présente Politique de Certification (PC) couvre la gestion et l'utilisation des clés et des certificats. La gestion d'un certificat comprend notamment l'ensemble des phases du cycle de vie d'un certificat, de la demande d'attribution d'un certificat, jusqu'à la fin de vie de ce certificat (fin de validité ou révocation). La politique est définie indépendamment des détails de l'environnement utilisé pour la mise en œuvre de l'infrastructure de gestion de clés (IGC) à laquelle elle s'applique.

Les porteurs et les tiers utilisateurs de certificat ont des obligations spécifiques qui sont définies dans cette politique de certification.

1.2. Identification du document

La présente PC dans sa version 1 est identifiée par l'OID : **1.2.250.1.179.1.2.1.1.2**

Le dernier chiffre permet de faire évoluer le numéro de version du document.

1.3. Niveau de conformité

Cette Politique de Certification se veut conforme aux exigences stipulées pour le niveau fort (niveau « 1 étoile » ou *) du RGSv2.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		14/79

	Projet IMAGE AC Personnes : Authentification Introduction	
--	--	--

1.4. Définitions et abréviations

1.4.1. Définitions

Pour les besoins du présent document, les termes et définitions suivants s'appliquent :

Administrateur central : Personne autorisée par l'AC à opérer les diverses fonctions de l'Autorité, et ayant notamment délégation des fonctions de l'AEL.

Autorité Administrative de l'AC : Personne responsable de l'AC sur le plan réglementaire et juridique.

Autorité de certification (AC) : Personne chargée de l'application de la présente Politique de Certification

Autorité de Certification Racine-2 : Autorité de Certification auto-signée, point de confiance de l'IGC, et certifiant les Autorités de Certification Délégées, dont l'AC Logiciels-2.

Autorité d'Enregistrement Locale : Autorité désignée par l'Autorité Administrative qui a pour rôle d'organiser l'enregistrement du porteur et la gestion des clés.

Certificat [électronique] : Certificat délivré à une personne physique et portant sur une bi-clé d'authentification, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, ...).

Cellules informatiques : Service fournissant des services de soutien technique de niveau 1 aux porteurs. Il s'agit, selon le cas, de soutien informatique, bureautique, ou réseau.

Composante de l'AC : Module technique ou plate-forme jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'AC.

Conditions d'Utilisation des certificats logiciels : Document reprenant les informations pertinentes de la présente PC (conditions d'usages des certificats logiciels, obligations et responsabilités, etc) et décliné suivant les catégories de porteurs auxquelles il s'adresse.

Déclaration des Pratiques de Certification : Enoncé des pratiques de certification effectivement mises en œuvre par l'AC pour l'émission, la gestion, la révocation, le renouvellement des certificats en

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		15/79

	Projet IMAGE AC Personnes : Authentification Introduction	
--	--	--

conformité avec la Politique de Certification qu'elle s'est engagée à respecter.

Identifiant d'objet (OID) : Liste d'entiers, globalement unique permettant d'identifier un objet.

Infrastructure de Gestion de Clés (IGC) : Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance.

Liste des Certificats Révoqués (LCR) : Liste signée indiquant un ensemble de certificats qui ne sont plus considérés comme valides par l'AC.

Opérateur d'enregistrement : Personne ayant délégation de fonctions de l'Autorité d'Enregistrement Locale.

Politique de Certification : Ensemble de règles, comportant un identifiant (OID) et définissant 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.

Porteur : Personne physique identifiée dans un certificat et détentrice de la clé privée correspondant à la clé publique présente dans ce certificat.

Réponse OCSP : Réponse par l'AC à une interrogation par un tiers utilisateur indiquant l'état révoqué ou non d'un certificat porteur.

Rôle de confiance : Rôle dévolu à un acteur intervenant dans la mise en œuvre ou l'exploitation de l'AC afin d'assurer, ou de maintenir en opération, une ou plusieurs de ses fonctions.

Tiers utilisateur : Utilisateur d'un certificat de porteur et qui fait confiance à ce certificat (maîtrise d'ouvrage d'application).

Format X.509 v3 : Format standard de certificat électronique

1.4.2. Abréviations

Pour les besoins du présent document, les abréviations suivantes s'appliquent :

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		16/79

	Projet IMAGE AC Personnes : Authentification Introduction	
--	--	--

AA	Autorité Administrative
AC	Autorité de Certification
AEL	Autorité d'Enregistrement Locale
BIMS	Annuaire Bureautique Infrastructure Messagerie Stockage
CN	<i>Common Name</i> ; Nom commun
CU	Conditions d'Utilisation
DN	<i>Distinguished Name</i> ; nom distinctif
DPC	Déclaration des Pratiques de Certification
EAL	<i>Evaluation Assurance Level</i> ; niveau d'assurance d'évaluation d'un objet de sécurité selon les Critères Communs. Par exemple : EAL 2+ (« niveau EAL 2 augmenté »), EAL 4+ (« niveau EAL4 augmenté »)
GUS	Guichet Unique des Services
IGC	Infrastructure de Gestion de Clés
IMAGE	Infrastructure Ministérielle de gestion de clés, de services d'Authentification et de services de confiance pour la Gestion de la signature Electronique et de la confidentialité
LCR	Liste des Certificats Révoqués
LDAP	<i>Light Directory Access Protocol</i> ; protocole d'interrogation et de modification de contenu d'annuaire
OCSP	<i>Online Certificate Status Protocol</i> ; protocole en-ligne de vérification de statut de certificat
OID	<i>Object Identifier</i> ; Identifiant d'objet
PIN	<i>Personal Identification Number</i> ; nombre personnel d'identification
PC	Politique de Certification
RSA	<i>Rivest Shamir Adleman</i> ; algorithme de chiffrement asymétrique, du nom de leurs trois

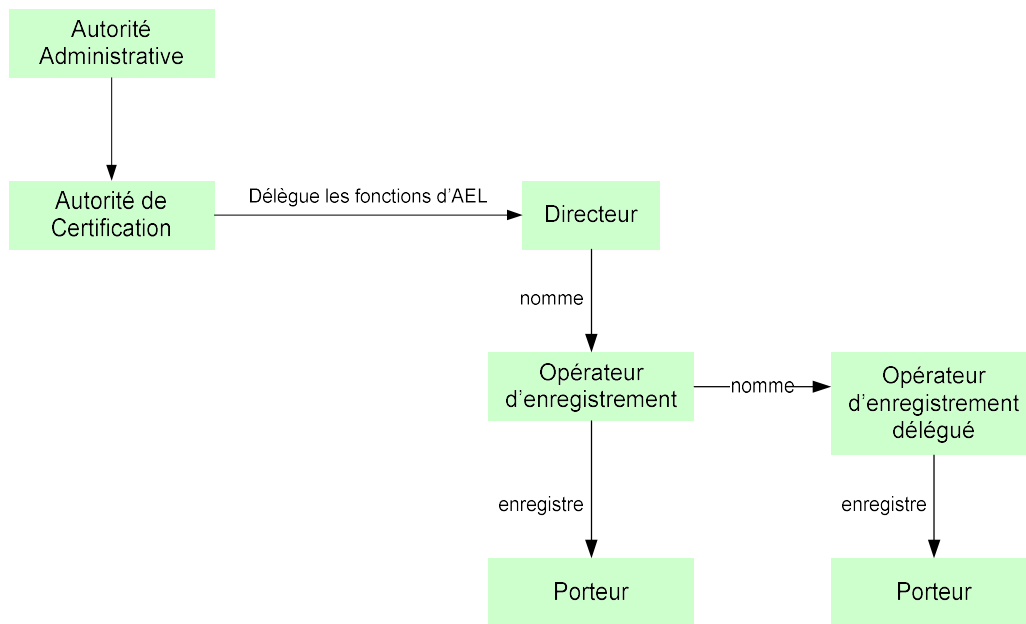
Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		17/79

inventeurs.

USB *Universal Serial Bus* ; bus série universel

UTC *Universal Time Coordinated* ; temps universel coordonné

1.5. Entités intervenant dans l'IGC



Le schéma ci-dessous ne constitue qu'une illustration synthétique des délégations de certains rôles de confiance auprès de l'IGC.

1.5.1. Autorité Administrative

Le rôle d'Autorité Administrative est assuré par le Directeur de la Direction des Systèmes d'Information (DSI) du Ministère.

Les fonctions assurées par l'Autorité Administrative en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- rendre accessible l'ensemble des prestations déclarées dans la PC aux porteurs et aux tiers utilisateurs.

	Projet IMAGE AC Personnes : Authentification Introduction	
--	--	--

- s'assurer que les exigences de la PC et les procédures de la DPC sont adéquates et conformes aux normes en vigueur.
- s'assurer que ces exigences et procédures sont appliquées par chacun des détenteurs de rôles auprès de l'IGC.
- mettre en œuvre les mesures de sécurité techniques et non techniques nécessaires pour couvrir les risques identifiés et assurer la continuité de l'activité de l'IGC en conformité avec les exigences de la présente PC.
- mettre en œuvre les différentes fonctions identifiées dans la PC, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats.
- mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans la présente PC, notamment en terme de fiabilité, de qualité et de sécurité.
- générer, et renouveler lorsque nécessaire, la bi-clé de l'AC et le certificat correspondant (signature de certificats, de LCR et de réponses OCSP). Diffuser son certificat d'AC aux porteurs et aux tiers utilisateurs de certificat.

1.5.2. Autorité de Certification

Le rôle d'Autorité de Certification est assuré par le Sous-Directeur de la sous direction infrastructures et support aux utilisateurs (SDISU).

L'Autorité de Certification (AC) a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) et s'appuie pour cela sur une infrastructure technique : une Infrastructure de Gestion de Clés (IGC).

Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats :

Fonction de génération des certificats : Cette fonction génère les certificats à partir des informations transmises par l'Autorité d'Enregistrement Locale.

Fonction de publication : Cette fonction met à disposition des

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		19/79

	Projet IMAGE AC Personnes : Authentification Introduction	
--	--	--

différentes parties concernées les différents documents établis par l'AC (Conditions d'Utilisation, Politiques et Pratiques...), les certificats d'AC et toute autre information pertinente destinée aux porteurs et aux tiers utilisateurs de certificat, hors informations d'état des certificats.

Fonction de gestion des révocations : Dans le cadre de cette fonction, l'AC traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

Fonction d'information sur l'état des certificats : Cette fonction fournit aux tiers utilisateurs de certificats des informations sur l'état des certificats (révoqués, non révoqués). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR) et également selon un mode requête / réponse temps réel au moyen d'un service OCSP.

1.5.3. Autorité d'Enregistrement Locale

Le rôle d'AEL est assuré par les différents AQSSI du Ministère.

Elle assure les fonctions suivantes :

Fonction d'enregistrement des porteurs : Cette fonction assure la vérification des informations d'identification, et l'enregistrement du futur porteur d'un certificat. La fonction inclut, lorsque cela est nécessaire, la re-vérification des informations du porteur lors du renouvellement du certificat de celui-ci.

Fonction de remise du certificat au porteur : Cette fonction importe le certificat généré.

Fonction de gestion des révocations : Dans le cadre de cette fonction, l'AEL enregistre dans certains cas les demandes de révocation pour transmission et traitement par l'AC.

Sur le plan opérationnel, ces fonctions sont déléguées aux opérateurs d'enregistrement.

L'AEL assure notamment à ce titre les tâches suivantes :

- la prise en compte et la vérification des informations du futur porteur, ainsi que la constitution du dossier d'enregistrement correspondant ;

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		20/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>Introduction</p>	
--	---	--

- l'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC;
- la conservation des pièces des dossiers d'enregistrement des porteurs ;
- la conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du porteur, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles),

L'AEL a aussi pour rôle d'assurer l'interface avec les porteurs disposant d'un certificat en cours de validité. Pour cela, l'AEL assure les tâches suivantes :

- la prise en compte des demandes de révocation,
- le renouvellement des certificats logiciels.

Pendant la phase de déploiement auprès des opérateurs d'enregistrement, ce rôle est assuré par les administrateurs centraux de l'AC.

1.5.4. Porteur

Le porteur utilise sa clé privée et le certificat correspondant dans le cadre de ses activités professionnelles.

Un porteur peut être :

- un agent du Ministère,
- une personne externe ne faisant pas partie des personnels du Ministère, mais travaillant pour un prestataire réalisant des missions au sein des locaux du ministère,

1.5.5. Tiers utilisateurs des certificats

Les certificats générés dans le cadre de la présente PC sont utilisés par les systèmes et applications informatiques faisant confiance à la l'IGC Image afin d'authentifier les porteurs de ces certificats.

Les systèmes et applications qui utilisent les certificats d'authentification émis par l'AC Personnes sont :

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		21/79

	Projet IMAGE AC Personnes : Authentification Introduction	
--	--	--

- Les applications et les services en ligne exigeant une authentification forte de l'utilisateur.

1.6. Usage des certificats

1.6.1. Bi-clés et certificats porteurs

La présente PC traite des bi-clés et des certificats à destination des porteurs, afin que ces porteurs puissent s'authentifier auprès des tiers utilisateurs de certificat.

L'utilisation de la clé privée du porteur et du certificat associé doit rester strictement limitée au service d'authentification.

L'AC décline toute responsabilité en ce qui concerne l'utilisation des certificats d'authentification pour des usages autres que ceux qui sont définis dans la présente PC et dans les documents « Conditions d'Utilisation des certificats logiciels » applicables.

1.6.2. Bi-clés et certificats de l'AC Logiciels-2 et de ses composantes

L'AC dispose de plusieurs clés et certificats décomposés de la manière suivante :

- la clé de signature de l'AC utilisée pour signer les certificats générés par l'AC ainsi que les informations sur l'état des certificats (LCR et réponses OCSP),
- les clés internes d'infrastructure, utilisées par les composantes de l'AC à des fins d'authentification et de chiffrement des données échangées ou stockées au sein de l'IGC, etc.

Le certificat de l'AC Logiciels-2, ainsi que les certificats des composantes et les engagements relatifs à ces certificats, font l'objet du document [PC-ACR].

1.7. Gestion de la PC

1.7.1. Entité gérant la Politique de Certification

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		22/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>Introduction</p>	
--	---	--

L'AC est responsable de l'établissement de la présente Politique de Certification en conformité avec le document RGS v2, de son application et de sa diffusion.

L'Autorité Administrative est responsable de la validation de la présente PC.

1.7.2. Point de contact

Pour toute information relative à la présente PC, il est possible de contacter :

<p>MINISTÈRES SOCIAUX</p> <p>Direction des Systèmes d'Information</p> <p>SDISU/ Bureau I3P Projet IMAGE</p> <p>Tour Mirabeau</p> <p>39-43 Quai André Citroën 75902 PARIS CEDEX 15</p> <p>dsi-sdisu-prod-image@sg.social.gouv.fr</p>

1.7.3. Déclaration des Pratiques de Certification (DPC)

L'AC s'engage à rédiger le document [DPC], décrivant les procédures et mesures mises en œuvre pour le respect des dispositions de la présente PC. Ce document n'est pas public.

Ce document est fourni à l'auditeur lors d'un audit interne ou d'un audit de conformité de la PC.

1.7.4. Procédure d'approbation de la DPC

Le document [DPC] est approuvé par l'AA.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		23/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>Introduction</p>	
--	---	--

1.8. Conditions d'Utilisation

Les Conditions d'Utilisation fournissent aux porteurs et aux tiers utilisateurs de certificat les informations pertinentes de la présente PC dont ils ont besoin. Elles sont divisées de la manière suivante :

- les « Conditions d'Utilisation des certificats logiciels applicables aux agents du Ministère »,
- les « Conditions d'Utilisation des certificats logiciels applicables aux personnes extérieures au personnel du Ministère »,

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		24/79

	Projet IMAGE AC Personnes : Authentification RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS PUBLIEES	
--	---	--

2. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS PUBLIEES

2.1. Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des porteurs et des tiers utilisateurs de certificat, l'AC met en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats.

2.2. Informations publiées

L'AC publie les informations suivantes à destination des tiers utilisateurs de certificat et des porteurs :

- les politiques de certification en cours de validité,
- les profils des certificats, de la LCR et des réponses OCSP,
- les différents documents « Conditions d'Utilisation des certificats logiciels IMAGE »
- la Liste des Certificats Révoqués en cours (LCR) ¹,
- les certificats de l'AC, en cours de validité (*),
- les certificats auto-signés de l'AC Racine-2 du Ministère à laquelle elle est subordonnée, ou les informations permettant aux tiers utilisateurs de certificats de s'assurer de l'origine de ces certificats (empreintes) (*),
- l'adresse permettant d'obtenir des informations concernant l'AC Racine-2 du Ministère (*),

¹ L'adresse de la LCR figure pour chaque certificat dans l'extension « CRLdistributionPoint ». Le protocole HTTP est utilisé.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		25/79

	Projet IMAGE AC Personnes : Authentification RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS PUBLIEES	
--	---	--

- l'adresse permettant d'obtenir des informations concernant l'IGC/A (*).

(*) Les adresses où ces informations sont disponibles sont indiquées dans les différents documents « Conditions d'Utilisation des certificats logiciels IMAGE ».

L'AC fournit en outre un service OCSP en accès libre sur internet, selon le protocole HTTP, à destination des tiers utilisateurs de certificat, leur permettant de connaître l'état révoqué/ non révoqué des certificats. L'adresse de ce service est indiquée dans l'extension « Authority Information Access » de chaque certificat.

2.3. Délais et fréquences de publication

Les délais et les fréquences de publication dépendent des informations concernées :

Informations liées à l'IGC (nouvelle version de la Politique de Certification, etc.) :	
Délais de publication :	L'information est publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.
Disponibilité de l'information :	L'infrastructure assurant cette fonction est disponible les jours ouvrés, avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 8 heures (jours ouvrés) et une durée totale maximale d'indisponibilité par mois de 32 heures, ceci hors cas de force majeure.
Certificats d'AC :	
Délais de publication :	Ceux-ci sont diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondants sous un délai de 24 heures.
Disponibilité de l'information :	L'infrastructure assurant cette fonction a une disponibilité de 24h/24 7j/7, avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2 heures et une durée totale

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		26/79

	Projet IMAGE AC Personnes : Authentification RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS PUBLIEES	
--	---	--

	maximale d'indisponibilité par mois de 8 heures, ceci hors cas de force majeure.
Informations d'état des certificats :	
Délais de publication :	Les exigences portant sur la fonction de publication de ces informations sont définies au chapitre 4.10.
Disponibilité de l'information :	

2.4. Contrôle d'accès aux informations publiées

L'information publiée est accessible avec accès en lecture seulement sur le site Internet du Ministère, à l'adresse suivante : <http://igc.sante.gouv.fr>

L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) est strictement limité aux rôles de confiance de l'IGC adéquats et identifiés, au travers d'un **contrôle d'accès fort** (basé sur une authentification au moins à deux facteurs).

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux rôles de confiance de l'IGC adéquats et identifiés, au travers d'un **contrôle d'accès de type mot de passe**, basée sur une politique de gestion stricte des mots de passe.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		27/79

	Projet IMAGE AC Personnes : Authentification IDENTIFICATION ET AUTHENTIFICATION	
--	--	--

3. IDENTIFICATION ET AUTHENTIFICATION

3.1. Nommage

3.1.1. Types de noms

Dans chaque certificat, émis au format X.509v3, l'AC émettrice et le porteur sont identifiés par un "Distinguished Name" (ou DN : nom distinctif ») de type X.501.

3.1.2. Utilisation de noms explicites

Les noms choisis pour désigner les porteurs de certificats sont explicites. Le DN du porteur est construit à partir des renseignements figurant dans des annuaires de référence du Ministère. Le nom commun du porteur (CN) est vérifié à partir des prénom et nom de son état civil tel que porté sur les documents d'identité présentés lors de son enregistrement auprès de l'opérateur d'enregistrement.

Dans le cas où le CN stocké dans l'annuaire présente un écart avec les prénom et nom portés sur le document d'identité présenté (emploi d'un diminutif, omission de l'un des prénoms, ajout d'un nom marital...), ces derniers sont conservés dans le dossier électronique d'enregistrement.

Dans le cas où le CN stocké dans l'annuaire diffère notablement des prénom et nom portés sur le document d'identité présenté, l'enregistrement n'est pas poursuivi.

3.1.3. Unicité des noms

Afin d'assurer l'identification unique du porteur au sein du domaine de l'AC dans ses certificats successifs (renouvellement) et pour éviter toute ambiguïté, le DN du sujet de chaque certificat de porteur identifie de façon unique le porteur correspondant au sein du domaine de l'AC.

Un nom distinctif (DN) de porteur est constitué des éléments suivants :

- C=FR

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		28/79

	Projet IMAGE AC Personnes : Authentification IDENTIFICATION ET AUTHENTIFICATION	
--	--	--

- O= Ministère en charge des affaires sanitaires et sociales
- OU=0002 110 036 035 00019
(Code SIRET du Ministère, précédé des quatre chiffres 0002 séparés par un espace)
- CN= *Prénom Nom*
- SerialNumber = numéro unique interne attribué au porteur.
Ce numéro permet de garantir l'unicité du DN pour chaque porteur. Il est choisi par l'AC.

Durant toute la durée de vie de l'AC, un DN attribué à un porteur ne peut être attribué à un autre porteur.

3.1.4. Identifiants attribués aux personnes internes et aux personnes externes sur site

Les personnes internes et les personnes externes sur site bénéficient de trois autres identifiants qui sont placés dans une extension « subject Alternative Name » du certificat :

- l'adresse de messagerie professionnelle,
- un identifiant applicatif pour accéder à certaines applications du Ministère,
- un identifiant UPN pour Windows.

3.2. Validation initiale de l'identité

L'enregistrement d'un porteur se fait directement auprès de l'opérateur d'enregistrement.

3.2.1. Validation de l'identité d'un porteur

L'authentification du porteur par l'opérateur d'enregistrement est réalisée lors d'un face-à-face physique, à partir d'une pièce d'identité², en cours de validité et comportant une photographie.

² Carte Professionnelle d'Identité du Ministère, Carte d'accès à l'un des sites du Ministère comportant nom et photographie, Carte Nationale d'Identité, Passeport, Permis de conduire, ou autre document officiel d'identité

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		29/79

	Projet IMAGE AC Personnes : Authentification IDENTIFICATION ET AUTHENTIFICATION	
--	--	--

Le dossier d'enregistrement, déposé auprès de l'opérateur d'enregistrement, comprend au moins :

- Pour toutes les catégories de porteurs : une acceptation des « Conditions d'Utilisation des certificats logiciels IMAGE » adéquates, signée par le porteur, datée du jour du face-à-face, comportant le prénom, nom, direction et service,

3.2.2. Validation des autres identifiants attribués aux personnes internes et aux « externes sur site »

Dans le cas des porteurs internes et externes sur site : l'opérateur d'enregistrement effectue un contrôle de cohérence entre le document d'identité présenté et les annuaires afin d'y trouver une entrée relative au porteur.

L'adresse de messagerie est également extraite des annuaires et placée dans l'extension subjectAlternativeName.

Dans le cas où l'adresse de messagerie n'est pas présente dans l'annuaire, l'opérateur d'enregistrement complète cette donnée dans le formulaire d'enregistrement.

3.3. Identification et validation pour le renouvellement des clés

Le renouvellement de la bi-clé d'un porteur entraîne la génération et la fourniture d'un nouveau certificat associé à la nouvelle bi-clé.

3.3.1. Identification et validation pour un renouvellement courant

L'opérateur identifie le porteur sur présentation de sa pièce d'identité, comme pour l'enregistrement initial.

(carte de séjour...)

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		30/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>IDENTIFICATION ET AUTHENTIFICATION</p>	
--	---	--

3.3.2. Identification et validation pour un renouvellement après révocation

Suite à la révocation d'un certificat, quelle qu'en soit la cause, la procédure d'identification et de validation du renouvellement est identique à la procédure d'enregistrement initial.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		31/79

	Projet IMAGE AC Personnes : Authentification EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	--	--

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1. Enregistrement initial

4.1.1. Origine de l'enregistrement initial et de la demande de certificat

C'est le porteur du certificat qui est à l'origine d'une demande de certificat et donc d'enregistrement.

Le porteur contacte l'AEL de sa structure.

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

Porteurs internes et externes sur site :

- L'enregistrement est effectué par l'opérateur d'enregistrement à partir des informations contenues dans les annuaires du ministère.

4.2. Déroulement de l'enregistrement

4.2.1. Processus d'identification et de validation

L'identité de la personne physique est vérifiée conformément aux exigences du chapitre précédent.

L'opérateur d'enregistrement effectue les opérations suivantes :

- consulte les annuaires de référence du ministère pour vérifier que le futur porteur fait bien partie des personnes éligibles pour l'obtention d'un certificat,

et dans tous les cas :

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		32/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS</p>	
--	--	--

- valide l'identité du futur porteur,
- s'assure que le futur porteur a pris connaissance des modalités applicables pour l'utilisation du certificat.

4.2.2. Acceptation ou rejet de l'enregistrement

Les données extraites de l'annuaire sont vérifiées par rapport à la pièce d'identité présentée.

En cas d'écart significatif, l'opérateur d'enregistrement informe le porteur de l'abandon de l'enregistrement.

4.2.3. Durée d'établissement du certificat

Les certificats sont valables pour une durée de trois ans.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		33/79

	Projet IMAGE AC Personnes : Authentification EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	--	--

4.3. Délivrance du 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'opérateur d'enregistrement, l'AC déclenche les processus de génération du certificat.

4.3.2. Mot de passe PKCS12

Lors de la génération du certificat par l'IGC, l'AEL est invité à saisir le mot de passe du fichier PKCS12.

Ce mot de passe complexe d'au moins 8 caractères est ensuite transmis au porteur par un autre moyen que le courriel (face à face, téléphone, SMS).

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

La remise du certificat se fait par l'envoi au porteur d'un lien de téléchargement du certificat, ce lien est à usage unique et valable 1 semaine.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		34/79

	Projet IMAGE AC Personnes : Authentification EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	--	--

4.4. Acceptation du certificat

Le porteur ne peut prendre possession du dispositif qu'après :

- La vérification de son identification personnelle, qui lui est présentée sur le poste de travail avant l'enregistrement. Cette identification renseigne l'attribut Nom commun (CN) contenu dans le champ « Subject » du certificat ainsi que l'adresse de messagerie contenue dans l'extension « SubjectAlternativeName » du certificat.
- La signature d'un exemplaire des « Conditions d'Utilisation des certificats logiciels IMAGE » adéquates. L'opérateur d'enregistrement conserve cet exemplaire et le joint au dossier d'enregistrement. Il en remet une copie au porteur.
- Le téléchargement du fichier PKCS12 et la saisie du mot de passe associé.
- L'installation du certificat marque l'acceptation de celui-ci.

4.4.1. Publication du certificat

Les certificats ne sont pas publiés.

4.5. Usages de la bi-clé et du certificat

4.5.1. Utilisation de la clé privée et du certificat par le porteur

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service d'authentification. Les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

Le personnel ayant le besoin d'accéder à certaines applications du Ministère dispose d'un identifiant contenu dans l'attribut « otherName » de l'extension « SubjectAlternativeName » du certificat.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		35/79

	Projet IMAGE AC Personnes : Authentification EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	--	--

Tous les porteurs peuvent utiliser leur certificat :

- pour réaliser une authentification client SSL. A cette fin, l'extension "extended key usage » du certificat contient la valeur de l'OID correspondant à l'usage « clientAuth »

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

Les tiers utilisateurs de certificat doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6. Renouvellement d'un certificat sans changement de bi-clé

Le simple renouvellement du certificat (changement des dates de validité du certificat, sans changement de la bi-clé) n'est pas supporté.

4.7. Renouvellement d'un certificat avec changement de la bi-clé

Les certificats et les bi-clés sont renouvelés tous les trois ans.

Nota - Par la suite, le terme « renouvellement du certificat » recouvre également le changement de bi-clé du porteur.

4.7.1. Causes possibles de changement d'une bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques.

Par ailleurs, une bi-clé et un certificat peuvent être fournis de nouveau à un porteur par anticipation, suite à la révocation du certificat du porteur. Ce cas suit alors le processus d'enregistrement initial, et non celui du renouvellement.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		36/79

	Projet IMAGE AC Personnes : Authentification EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	--	--

4.7.2. Origine d'une demande de renouvellement de certificat

Peu avant la date d'expiration de leur certificat, les porteurs internes sont invités à renouveler leur certificat. Ils en sont avertis par courriel.

Les demandes des porteurs externes sur site sont effectuées par le Directeur de leur direction d'accueil.

4.7.3. Procédure de traitement d'une demande de renouvellement de certificat

Le porteur interne se présente personnellement à l'opérateur d'enregistrement pour face-à-face.

4.7.4. Notification au porteur de l'établissement du nouveau certificat

La procédure de notification du nouveau certificat au porteur est identique à celle de l'enregistrement initial.

4.7.5. Démarche d'acceptation du nouveau certificat

L'installation du nouveau certificat vaut acceptation de celui-ci par le porteur.

Le certificat renouvelé contient les mêmes informations nominatives (CN, adresse de messagerie...).

4.7.6. Publication du nouveau certificat

Le certificat renouvelé n'est pas publié.

4.8. Modification du certificat

La modification de certificat n'est pas autorisée dans la présente PC.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		37/79

	Projet IMAGE AC Personnes : Authentification EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	--	--

4.9. Révocation et suspension des certificats

4.9.1. Causes possibles d'une révocation

Les circonstances suivantes peuvent être à l'origine de la révocation du certificat d'un porteur :

- l'une des informations nominatives du porteur figurant dans son certificat est périmée, ceci avant l'expiration normale du certificat³ ;
- une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du porteur ;
- L'équipement informatique (ordinateur, tablette, téléphone multifonction) ou est installé le certificat est perdu ou volé.
- le porteur ne fait plus partie du personnel du Ministère ;
- dans le cas d'un porteur externe sur site : le porteur quitte le Ministère ;
- le porteur est muté et ne dispose plus des mêmes droits, dans le cas où la mutation impose une révocation du certificat ;

Lorsque l'une des circonstances ci-dessus se réalise ; le certificat concerné doit être révoqué.

4.9.2. Origine d'une demande de révocation

Les personnes pouvant effectuer la révocation d'un certificat de porteur sont les suivantes :

- le porteur au nom duquel le certificat a été émis,
- l'opérateur d'enregistrement.

L'autorité hiérarchique d'un porteur peut également émettre une demande administrative de révocation d'un certificat de ce porteur à destination de l'opérateur d'enregistrement.

³ Il appartient au porteur de signaler tout changement dans celles-ci.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		38/79

	Projet IMAGE AC Personnes : Authentification EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	--	--

4.9.3. Procédure de traitement d'une demande de révocation faite par le porteur

Pour révoquer son certificat, le porteur peut :

- se rendre auprès de son opérateur d'enregistrement pour demander la révocation de son certificat.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque 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 et est aussi accessible au service OCSP.

L'opération est enregistrée dans les journaux d'évènements avec, le cas échéant, la cause ayant entraîné la révocation du certificat.

Les causes de la révocation ne sont pas publiées.

4.9.4. Délai accordé au porteur pour effectuer la révocation

Dès que le porteur a connaissance qu'une des causes possibles de révocation se vérifie, il doit effectuer sa demande de révocation sans délai.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		39/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS</p>	
--	--	--

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

La disponibilité de cette fonction de gestion des révocations en ligne est la suivante :

- disponibilité 24h / 24 7j / 7
- durée maximale d'indisponibilité par interruption de service
(panne ou maintenance) : une heure
- durée maximale totale d'indisponibilité par mois : 4 heures

Les opérateurs de révocation (les AEL), quant à eux, traitent les demandes dans les meilleurs délais.

4.9.6. Exigences de vérification de la révocation par les tiers utilisateurs de certificat

Les tiers utilisateurs de certificat sont tenus de vérifier, avant leur utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée, consultation de la LCR en cours de validité ou interrogation OCSP, ainsi que la fréquence des interrogations (liée à la durée de validité des informations éventuellement gardées dans un cache) est à l'appréciation des tiers utilisateurs de certificat selon les contraintes liées à leur application.

4.9.7. Fréquence d'établissement de la LCR

Une nouvelle LCR est publiée toutes les 12 heures. En outre, l'AC peut émettre une LCR mise à jour, sans attendre la publication faite toutes les douze heures.

Chaque LCR est émise avec une durée de validité de 8 jours.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		40/79

	Projet IMAGE AC Personnes : Authentification EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	--	--

4.9.8. Délai maximum de publication d'une LCR

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

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

Un service OCSP est mis en œuvre. L'adresse de ce service est spécifiée pour chaque certificat dans l'extension « authorityInformationAccess ». Ce service est disponible en accès libre depuis Internet.

4.9.10. Autres moyens disponibles d'information sur les révocations

L'opérateur d'enregistrement a la possibilité, après authentification, de vérifier l'état révoqué / non révoqué d'un certificat en interrogeant directement l'application de l'IGC.

4.9.11. Exigences spécifiques en cas de compromission de la clé privée

La clé privée peut être compromise dans les cas suivants en cas de vol ou de perte de l'équipement informatique où est installé le certificat (ordinateur, tablette, téléphone multifonction):

Le porteur est tenu d'effectuer une demande de révocation dans les meilleurs délais.

4.9.12. Causes possibles d'une suspension

La suspension de certificats n'est pas autorisée dans la présente PC.

4.10. Fonction d'information sur l'état des certificats

4.10.1. Caractéristiques opérationnelles

L'AC fournit aux tiers utilisateurs de certificat les informations leur permettant de vérifier et de valider,

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		41/79

	Projet IMAGE AC Personnes : Authentification EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	--	--

préalablement à son utilisation, le statut d'un certificat d'un porteur, c'est-à-dire :

- de vérifier la signature du certificat porteur par l'AC Logiciels-2,
- de vérifier la présence ou non du certificat porteur dans la LCR émise par l'AC Logiciels-2,
- de vérifier la signature de cette LCR par l'AC Logiciels-2.

via la consultation libre de la LCR.

La LCR émise par l'AC Logiciels-2 est au format V2 et est accessible au moyen du protocole HTTP depuis Internet.

Les informations nécessaires à la vérification du statut du certificat de l'AC Logiciels-2 relèvent de la responsabilité de l'AC Racine-2 et peuvent donc être obtenues auprès de celle-ci.

4.10.2. Disponibilité de la fonction

La disponibilité de la fonction d'information sur l'état des certificats est la suivante :

- disponibilité : 24h / 24 et 7j / 7.
- durée maximale d'indisponibilité par interruption de service (panne ou maintenance) : inférieure à 4 heures,
- durée maximale totale d'indisponibilité par mois : inférieure à 16 heures.

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

Si le porteur quitte le Ministère avant la fin de validité de son certificat, ce dernier est révoqué.

4.12. Séquestre de clé et recouvrement

Les clés privées des porteurs ne sont pas séquestrées.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		42/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

5. MESURES DE SECURITE NON TECHNIQUES

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

L'infrastructure de l'IGC est hébergée sur le site nominal dans un local sécurisé vis-à-vis des risques naturels.

Une infrastructure de secours est hébergée dans un local sécurisé vis-à-vis des risques naturels sur un autre site, distant du site nominal de plusieurs kilomètres.

5.1.2. Accès physique

Les zones hébergeant les systèmes informatiques de l'AC sont physiquement protégées. L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant un tel accès.

5.1.3. Alimentation électrique et climatisation

Les serveurs hébergeant l'IGC sur le site nominal bénéficient d'une double alimentation électrique. Les modules cryptographiques de l'IGC bénéficient d'une alimentation secourue.

Les locaux hébergeant l'IGC sont climatisés.

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'AC telles que fixées par leurs fournisseurs.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		43/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>MESURES DE SECURITE NON TECHNIQUES</p>	
--	---	--

5.1.4. Vulnérabilité aux dégâts des eaux

Les locaux hébergeant l'IGC sont protégés contre les dégâts des eaux :

- par un dispositif de détection d'eau,
- par le plan de prévention des inondations.

5.1.5. Prévention et protection incendie

Les locaux hébergeant l'IGC bénéficient des moyens de prévention et de lutte contre les incendies par des dispositifs de détection d'incendie et d'extinction.

Les alertes remontées par les dispositifs contre les dégâts des eaux et contre l'incendie sont remontées au PC Sécurité, dans le cadre de la GTC (Gestion Technique Centralisée).

5.1.6. Conservation des supports

Les sauvegardes des données et de l'application IGC sont conservées dans une enceinte sécurisée, accessible aux seules personnes autorisées.

Les supports papier de l'IGC sont également conservés avec des mesures de sécurité compatibles avec leur niveau de sensibilité.

La DPC identifie les différentes informations et données intervenant dans les activités de l'AC, ainsi que les mesures de sécurité qui leur sont appliquées, afin d'en garantir la confidentialité, l'intégrité et la disponibilité.

5.1.7. Mise hors service des supports

Les supports papier et électroniques de l'IGC en fin de vie sont systématiquement détruits par des moyens appropriés, permettant d'éviter toute perte de confidentialité.

Les matériels et supports informatiques de l'IGC ne sont pas utilisés à d'autres fins avant destruction complète des informations liées à l'IGC qu'ils sont susceptibles de contenir.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		44/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

5.1.8. Sauvegardes hors site

Les sauvegardes sont conservées sur un site externe selon la Politique de Sauvegarde.

5.2. Mesures de sécurité procédurales

5.2.1. Rôles de confiance auprès de l'AC

Les rôles de confiance définis au niveau de l'AC sont :

Administrateur central : Personne chargée de la configuration applicative et du maintien en conditions opérationnelles de l'application IGC, de l'habilitation des opérateurs d'enregistrement, ainsi que de l'analyse régulière des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc.

Auditeur : Personne désignée par l'Autorité Administrative et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par l'AC par rapport à la Politique de Certification et à la Déclaration des Pratiques de Certification de l'AC.

Autorité Qualifiée : Personne chargée de la Sécurité de l'application IGC pour le compte de l'Autorité Administrative.

Opérateur d'enregistrement : Personne ayant reçu délégation de l'AEL, de la part des administrateurs centraux et réalisant les différentes opérations de gestion des certificats des porteurs.

Opérateur d'enregistrement délégué : Personne ayant reçu délégation de l'AEL de la part d'un opérateur d'enregistrement, et assurant les mêmes fonctions que celui-ci.

Responsable de l'application IGC : Personne ayant reçu délégation par l'AC de la mise en œuvre de la Politique de Certification et de la Déclaration des Pratiques de Certification de l'AC, au niveau de l'application IGC. Sa responsabilité couvre l'ensemble des fonctions rendues par l'application IGC et des performances correspondantes.

Responsable Qualité : Personne ayant reçu délégation par l'AC de la vérification de

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		45/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

la cohérence des actions des différents rôles décrits précédemment et de la qualité des processus de l'IGC.

5.2.2. Rôles de confiance mutualisés à d'autres applications

Ci-dessous sont décrites les fonctions assurées par ces rôles dans le cadre de l'IGC ou ayant une incidence sur les processus de l'IGC :

Administrateur Sécurité : Personne chargée d'assurer la gestion de la sécurité au niveau des systèmes.

Administrateur système : Personne chargée d'assurer l'administration des systèmes, la mise en route et la configuration des équipements composant l'infrastructure. Elle réalise notamment le contrôle des fichiers d'audit du système, ainsi que de l'analyse courante des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

Cellules informatiques : Services chargés de fournir aux porteurs le support technique relatif à leur environnement informatique, bureautique et réseau..

Exploitant : Personne chargée d'assurer l'exploitation, la surveillance et la maintenance des systèmes et des réseaux.

Fonctionnaire de Sécurité des Systèmes d'Informations (FSSI) : Personne chargée de la Politique de Sécurité du SI du Ministère.

Responsable de production : Personne chargée du maintien en conditions opérationnelles du système d'information du Ministère.

Responsable de salle : Personne chargée de la gestion des accès physiques aux salles informatiques hébergeant l'infrastructure et aux équipements.

5.2.3. Nombre de personnes requises par tâches

Les rôles liés à la gestion des systèmes sont distincts des rôles de gestion de l'application IGC, ainsi que des rôles intervenants sur les données enregistrées au niveau de l'application.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		46/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

Ces différents rôles sont assurés par des personnes distinctes.

Par ailleurs, toute opération impliquant les secrets principaux de l'IGC nécessite l'intervention de trois personnes.

La DPC de l'AC précise les opérations nécessitant l'intervention de plusieurs personnes ainsi que les contraintes que ces personnes doivent respecter.

5.2.4. Identification et authentification pour chaque rôle

Tout accès à l'application IGC est soumis à authentification forte, les droits d'accès étant définis en fonction des rôles. Notamment, toute personne susceptible d'intervenir auprès de l'application IGC, et ainsi de modifier des données ou des informations de configuration, doit être préalablement enregistré dans l'IGC et disposer d'un certificat d'authentification.

Pour les autres rôles en relation avec l'IGC, l'Autorité Administrative fait vérifier l'identité et les autorisations du personnel concerné avant :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux hébergeant la plate-forme de l'IGC ;
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans ces systèmes.

Ces contrôles sont décrits dans la DPC associée à cette PC

Chaque attribution de rôle dans l'IGC est notifiée par écrit.

5.2.5. Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre, et dans le respect des règles de non-cumul

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		47/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

définis dans la section 5.2.3. Les attributions associées à chaque rôle sont décrites dans la DPC de l'AC.

Les règles de non-cumul des rôles de confiance sont décrites au sein de la DPC.

5.3. Mesures de sécurité vis-à-vis du personnel

Au sein de la présente section ; le terme « personnel » désigne les détenteurs de rôles de confiance.

5.3.1. Qualifications, compétences et habilitations requises

Tous les personnels intervenant sur l'IGC sont soumis à un devoir de réserve.

Le responsable de l'application IGC s'assure que les attributions des personnels détenteurs de rôle de confiance correspondent à leurs compétences professionnelles et tient à jour la liste des personnels intervenants sur l'IGC, exception faite des opérateurs d'enregistrement.

Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'AC.

L'Autorité Administrative de l'AC informe toute personne intervenant dans des rôles de confiance de l'AC :

- de ses responsabilités relatives aux services de l'AC,
- des procédures liées à la sécurité du système et au contrôle du personnel.

par une lettre de mission signée par l'Autorité Administrative.

Les opérateurs d'enregistrement sont informés de leurs responsabilités et des procédures en vigueur par une lettre de mission signée par l'AEL.

5.3.2. Vérification de l'adéquation des profils

Le personnel amené à assurer un rôle de confiance vis-à-vis de l'AC a fait l'objet lors de son entrée en fonction, d'une vérification de l'adéquation de son profil par les services du Ministère.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		48/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>MESURES DE SECURITE NON TECHNIQUES</p>	
--	---	--

Ces personnes ne doivent pas notamment avoir fait l'objet de condamnation incompatible 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. En particulier, les porteurs de secrets permettant la reconstitution de la clé privée de l'AC ne doivent pas subir de pression hiérarchique les incitant à se dessaisir de leur secret. Ceci doit être écrit dans leur fiche de poste. Ils reportent au FSSI tout incident sur ce sujet.

5.3.3. Formation initiale

En préalable à leur entrée en fonction, les opérateurs d'enregistrement ainsi que le personnel des cellules informatiques sont formés aux concepts et objectifs de l'IGC IMAGE, ainsi qu'aux procédures à mettre en œuvre.

Les exploitants et administrateurs système sont formés aux concepts et objectifs de l'IGC IMAGE, ainsi qu'aux logiciels, matériels et procédures d'exploitation applicables.

Les administrateurs centraux sont formés aux concepts et objectifs de l'IGC IMAGE, aux diverses procédures à mettre en œuvre au niveau de l'IGC, notamment en terme de gestion des secrets et de délégation des droits.

5.3.4. Formation continue

Avant toute évolution majeure de l'infrastructure de l'IGC ou des procédures, une étude d'impact est réalisée par l'AC, avec élaboration d'un plan de formation le cas échéant.

5.3.5. Fréquence et séquence de rotation entre différentes attributions

Aucune rotation programmée des attributions n'est prévue.

5.3.6. Sanctions en cas d'actions non autorisées

Sont applicables les sanctions disciplinaires s'il y a lieu.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		49/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

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

Le personnel des prestataires externes intervenant dans les locaux et/ou sur la plate-forme hébergeant l'IGC doit également respecter les exigences du présent chapitre..

5.3.8. Documentation fournie au personnel

Le personnel dispose de la documentation relative aux procédures opérationnelles ou organisationnelles et aux outils spécifiques qu'il met en œuvre.

5.4. Procédures de constitution des données d'audit

5.4.1. Types d'évènements enregistrés

5.4.1.1 Enregistrements sur papier ou bureautique

Sont enregistrés sur outil bureautique :

- Les actions de maintenance et de changements de configuration des systèmes de l'infrastructure ; suivant les procédures d'exploitation ;
- Les changements apportés au personnel détenteur de rôle de confiance, exception faite des opérateurs d'enregistrement ;
- Mises à jour de la présente PC, au sein du présent document.

5.4.1.2 Enregistrements électroniques par l'application IGC

Toute action sur un dossier porteur est enregistrée, et un historique complet du dossier est conservé dans la base de données de l'AC.

De plus, les événements suivants font l'objet d'un enregistrement électronique de type log par l'application IGC :

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		50/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

- acceptation ou refus de connexion à l'application IGC ;
- demande de certificat lors de l'enregistrement initial,
- demande de renouvellement de certificat ;
- génération des certificats ;
- demande de révocation ;
- révocation de certificat ;
- génération puis publication de la LCR ;
- requête et réponse concernant la validité d'un certificat (OCSP) ;
- modification des droits des personnels autorisés à intervenir auprès de l'application IGC, dont les opérateurs d'enregistrement ;
- modification des paramètres de configuration de l'IGC.

5.4.1.3 Autres enregistrements électroniques

Les accès physiques aux locaux hébergeant l'infrastructure matérielle font l'objet d'un enregistrement électronique automatique.

Les événements suivants font l'objet d'un enregistrement électronique au niveau des systèmes d'exploitation de la plate-forme hébergeant l'IGC, dès le démarrage de ceux-ci :

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation ;
- modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des détenteurs des rôles de confiance, et les tentatives non réussies correspondantes.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		51/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

5.4.1.4 Caractéristiques communes

Pour tous les types d'enregistrements présentés ci-dessus : chaque enregistrement d'évènement contient au minimum les informations suivantes :

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

La personne, le service ou le système ayant exécuté l'évènement est responsable de sa journalisation.

Les opérations de journalisation électronique sont effectuées au cours du processus ou à la fin de celui-ci.

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

5.4.2. Fréquence de traitement des journaux d'évènements

5.4.2.1 Enregistrements sur papier ou bureautique

Les journaux enregistrés sous forme papier ou bureautique sont éventuellement revus lors des différents audits.

5.4.2.2 Enregistrements électroniques par l'application IGC

Le contenu du journal électronique d'évènements applicatifs de l'application IGC est surveillé quotidiennement afin de vérifier le fonctionnement normal de l'AC, et de mettre en évidence les tentatives d'intrusion au niveau de l'application.

Son contenu est également surveillé chaque semaine afin de vérifier le fonctionnement normal de l'AC, et la cohérence entre les différents types d'évènement au niveau de l'infrastructure d'IGC.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		52/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

5.4.2.3 Autres enregistrements électroniques

Les autres journaux enregistrés sous forme électronique sont éventuellement revus lors des opérations de corrélation avec les journaux de l'application IGC.

5.4.3. Période de conservation des journaux d'évènements sur site

5.4.3.1 Enregistrements sur papier ou bureautique

Les enregistrements papier sont conservés sur site et par leur dépositaire pendant 5 ans.

5.4.3.2 Enregistrements électroniques par l'application IGC

Les enregistrements des journaux sont conservés au sein de l'application IGC pendant toute la durée de vie de l'AC.

5.4.3.3 Autres enregistrements électroniques

Les autres journaux d'enregistrement sous forme électronique sont sauvegardés puis purgés chaque début de mois.

5.4.4. Protection des journaux d'évènements

5.4.4.1 Enregistrements sur papier ou bureautique

Les journaux sous forme papier sont conservés en lieu sûr par leur dépositaire.

Les journaux sous forme de document bureautique sont soumis à contrôle d'accès en écriture. Ces contrôles d'accès sont gérés par le rédacteur du document.

5.4.4.2 Enregistrements électroniques par l'application IGC

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		53/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

Les journaux d'événements conservés par l'application IGC sont protégés en intégrité.
 Ils ne sont accessibles qu'en lecture et exclusivement pour les administrateurs centraux.

5.4.4.3 Autres enregistrements électroniques

Les droits en modification/suppression/écriture des journaux d'événements des systèmes d'exploitation sont réservés aux utilisateurs avec droits avancés (« compte administrateur »).

5.4.5. Procédure de sauvegarde des journaux d'évènements

5.4.5.1 Enregistrements sur papier ou bureautique

Les enregistrements papier ne sont pas sauvegardés.

Les enregistrements sous forme de documents bureautiques sont sauvegardés selon les procédures applicables à ce type de documents.

5.4.5.2 Enregistrements électroniques par l'application IGC

Les journaux d'événements de l'application IGC sont sauvegardés selon la procédure de sauvegarde des données de l'application IGC. Les journaux sauvegardés sont protégés en intégrité par le même mécanisme qu'au sein de l'application IGC.

5.4.5.3 Autres enregistrements électroniques

Les autres journaux sous forme électroniques sont sauvegardés par un système centralisé de sauvegardes.

5.4.6. Système de collecte des journaux d'évènements

Dans tous les cas, il n'est pas prévu de système de collecte des journaux d'événements.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		54/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>MESURES DE SECURITE NON TECHNIQUES</p>	
--	---	--

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

Dans tous les cas, il n'est pas prévu de notification de l'enregistrement d'un événement à son responsable.

5.4.8. Evaluation des vulnérabilités

L'Autorité de Certification est en mesure de détecter toute tentative de violation de son intégrité ; les accès à l'application IGC étant soumis à authentification forte et journalisés.

Les anomalies liées à des tentatives d'accès en échec peuvent être consultées à tout moment par consultation des journaux d'évènements.

La mise en relation des différents journaux d'évènements est réalisée en cas de détection de compromission ou de suspicion de tentative de compromission de l'application IGC.

5.5. Archivage des données

5.5.1. Types de données archivées

5.5.1.1 Données sous forme papier ou bureautique

Les données conservées sous forme papier et archivées par leur dépositaire sont :

- Les journaux d'évènements tels qu'identifiés dans la section ci-dessus.

Les données conservées sous forme de document bureautique et archivées sont :

- les journaux d'évènements tels qu'identifiés dans la section ci-dessus, archivés selon la procédure d'archivage applicable à ce type de document. L'archivage est sous la responsabilité de leurs rédacteurs ;
- l'ensemble des documents référencés applicables à l'AC (i.e. la présente Politique de Certification, la DPC et ses annexes, les « Conditions d'Utilisation des certificats logiciels IMAGE »...). L'archivage est sous la responsabilité du responsable de l'application IGC.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		55/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

5.5.1.2 Données de l'application IGC (sous forme électronique)

L'ensemble des données créées et/ou utilisées par l'application IGC est archivé, y compris les LCR.

5.5.1.3 Autres données sous forme électronique

Les logiciels et fichiers de configuration sont sauvegardés périodiquement mais non archivés.

Les journaux d'événements autres que ceux de l'application IGC et tels que définis dans la section précédente sont sauvegardés mais non archivés.

5.5.2. Période de conservation des archives

Dossiers d'enregistrement et certificats

Les dossiers électroniques d'enregistrement et les certificats attachés sont conservés par l'application IGC pendant toute la vie de l'IGC sans être purgés.

Les dossiers d'enregistrements et les certificats attachés peuvent être présentés par l'AC lors de toute sollicitation par les autorités habilitées.

Ces dossiers permettent de retrouver l'identité des personnes physiques désignées dans les certificats émis par l'AC.

LCR émis par l'AC

Les LCR successives produites sont archivées sans limitation de durée par l'application IGC.

Journaux d'évènements

Les journaux d'événements de l'application IGC sont conservés par celle-ci pendant la durée de vie de l'AC. Leur intégrité est garantie par les mécanismes mis en œuvre lors de leur constitution.

Données sous forme papier et bureautique

Les données sont archivées durant au moins 5 ans ; hormis l'ensemble des documents référencés applicables à l'AC archivés sans limitation de durée.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		56/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

5.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives :

- sont protégées en intégrité selon les mécanismes mis en œuvre lors de la constitution des données qu'elles contiennent ;
- sont accessibles uniquement aux personnes autorisées ;
- peuvent être relues et exploitées.

Les moyens mis en oeuvre pour archiver les pièces en toute sécurité sont indiqués dans la DPC.

5.5.4. Procédure de sauvegarde des archives

5.5.4.1 Données sous forme papier ou bureautique

Les archives des données sous forme papier ou bureautique ne sont pas sauvegardées.

5.5.4.2 Données de l'application IGC (sous forme électronique)

Les données de l'application IGC sont archivées par l'application IGC elle-même et font donc l'objet de sauvegardes régulières selon les modalités définies dans la section 5.4.5.

5.5.5. Datation des données

5.5.5.1 Données sous forme papier ou bureautique

La datation des données enregistrées est réalisée à partir d'une source de temps d'utilisation courante supposée correcte avec une précision inférieure à 5 minutes.

5.5.5.2 Données de l'application IGC (sous forme électronique) :

La datation des données est réalisée selon les modalités définies au 6.8.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		57/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

5.5.6. Système de collecte des archives

5.5.6.1 Données sous forme papier ou bureautique

Les archives des données sous forme papier ou bureautique ne sont pas collectées mais conservées par leur rédacteur ou dépositaire.

5.5.6.2 Données de l'application IGC (sous forme électronique)

Les données électroniques sont collectées et conservées en ligne dans la base de données de l'AC.

5.5.7. Procédures de récupération et de vérification des archives

Les modalités d'accès aux différentes archives papier, bureautique et électroniques sont définies au sein de la DPC.

5.5.7.1 Données sous forme papier ou bureautique

Les archives sous format papier et bureautique peuvent être récupérées dans un délai inférieur à deux jours ouvrés.

5.5.7.2 Données de l'application IGC (sous forme électronique)

Les archives électroniques sont disponibles en ligne via l'application IGC pour les personnes autorisées à y accéder. En particulier, chaque opérateur d'enregistrement accède à ses données d'enregistrement.

5.6. Changement de clé d'AC

Le renouvellement du certificat d'AC et de sa bi-clé privée sera planifié de façon à ce que le certificat de l'AC soit valide au plus tard lors de la fin de validité de tous les certificats porteurs qu'elle a émis et de façon à pouvoir émettre des certificats porteurs sans discontinuité.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		58/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

La nouvelle bi-clé générée servira à signer les nouveaux certificats porteurs émis ainsi que la LCR relative à ces nouveaux certificats.

Le certificat précédent restera utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7. Reprise suite à compromission et sinistre

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

Le fonctionnement des systèmes composants l'IGC et leur environnement technique, sont surveillés par les exploitants de l'IGC, qui traitent et remontent les incidents.

Les administrateurs centraux de l'AC mettent en œuvre des procédures et des moyens de remontée et de traitement des compromissions, notamment au travers de l'analyse des différents journaux d'évènements.

Les procédures de traitement des incidents et des compromissions font l'objet d'un Plan de Reprise d'Activité dédié.

En particulier, l'AC s'engage à prévenir dans les meilleurs délais les porteurs et tiers utilisateurs de certificat en utilisant tout moyen à sa convenance (messagerie, appel téléphonique, affichage, site Web, ...) en cas d'incident impactant durablement ses services.

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

L'IGC dispose d'un Plan de Reprise d'Activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'AC découlant de la présente PC et identifiées comme critiques.

Ce plan est testé au minimum une fois tous les deux ans.

5.7.3. Procédures de reprise en cas de compromission de la clé privée de l'AC ou de l'une de ses composantes

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		59/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

Dans le cas de compromission de la clé de l'AC Logiciels-2, l'AC demandera la révocation de son certificat auprès de l'AC Racine-2 ; ceci après avoir demandé le renouvellement de son certificat et assuré la continuité de ses services critiques, conformément au Plan de Reprise d'Activité.

La compromission des clés des composantes techniques de l'IGC fait l'objet du document [PC-ACR].

5.7.4. Capacités de continuité d'activité suite à un sinistre

En cas d'incident sur le site nominal, l'exploitation de l'IGC est transférée sur le site de secours en moins de 24 heures, permettant le respect des exigences de la présente PC en matière de disponibilité des fonctions de l'IGC, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

En particulier, en complément des sauvegardes sur site, les données créées par l'application IGC sont répliquées par le réseau interne sécurisé du Ministère à des intervalles réguliers sur le site de secours.

5.8. Fin de vie de l'IGC

Transfert d'activité ou cession d'activité affectant l'AEL

La mise en oeuvre des services de révocation, de mise à disposition des informations de révocation et d'archivage étant de la responsabilité de l'AC, le transfert ou la cessation d'activité d'opérateurs d'enregistrement est sans incidence sur ces fonctions et sur la validité des certificats émis antérieurement.

Cessation d'activité affectant l'AC

Dans l'hypothèse d'une cessation d'activité totale, l'AC s'engage à assurer la continuité des fonctions de révocation des certificats et la publication de la LCR, dans la limite de ses propres possibilités.

En particulier, lors de l'arrêt du service, l'AC :

- 1) s'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- 2) prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- 3) demande la révocation de son certificat auprès des autorités ayant certifié sa clé ;

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		60/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE NON TECHNIQUES	
--	--	--

- 4) révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- 5) informe tous les porteurs des certificats révoqués ou à révoquer.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		61/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE TECHNIQUES	
--	--	--

6. MESURES DE SECURITE TECHNIQUES

6.1. Génération des bi-clés

6.1.1. Génération des bi-clés de l'Autorité

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé.

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique conforme aux exigences de la RGSv2.

La génération de la clé de signature de l'AC Logiciels-2 est effectuée dans des circonstances contrôlées, par des personnels dans des rôles de confiance, dans le cadre de "Cérémonies de Clés". Ces Cérémonies se déroulent suivant des scripts préalablement définis.

L'initialisation de l'IGC et/ou la génération des clés de signature d'AC s'accompagnent de la génération de parts de secrets. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC.

Suite à leur génération, les parts de secrets sont remises à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets est mise en œuvre par son porteur.

Les détails de la méthode utilisée pour la génération des parts de secrets sont fournis dans la [PC-ACR].

Les Cérémonies de Clés se déroulent sous le contrôle de deux témoins impartiaux et de confiance désignés par l'Autorité Administrative, qui attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		62/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE TECHNIQUES	
--	--	--

6.1.2. Génération des bi-clés des porteurs

La génération de la bi-clé du porteur est effectuée dans un dispositif répondant aux exigences du RGSv2.

6.1.3. Transmission de la clé privée à son propriétaire

La clé privée est transmise au format PKCS12.

6.1.4. Transmission de la clé publique d'un porteur à l'AC

Lors de la transmission de la clé publique du porteur vers l'AC, la clé est protégée en intégrité et son origine est authentifiée.

6.1.5. Transmission de la clé publique de l'AC aux tiers utilisateurs de certificat et aux porteurs

La clé publique de l'AC est diffusée dans son certificat, signé par l'AC Racine-2.

6.1.6. Tailles des clés

Les clés d'AC et de porteurs respectent les exigences de caractéristiques (tailles, algorithmes, etc.) du document [RGSv2]. Les clés d'AC sont des clés RSA de 4096 bits. Les clés des porteurs sont des clés RSA de 2048 bits.

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

Les équipements de génération de bi-clés, (les boîtiers cryptographiques), utilisent des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

6.1.8. Objectifs d'usage de la clé

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		63/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE TECHNIQUES	
--	--	--

L'utilisation de la clé privée de l'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR, et des réponses OCSP.

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service d'authentification tel que décrit dans la présente PC.

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

6.2.1. Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC pour la génération et la mise en œuvre de ses clés de signature, répondent au minimum aux exigences du document [RGSv2]. Les cartes cryptographiques utilisées ont été évaluées selon les Critères Communs au niveau EAL4+.

Ni les clés privées d'AC, ni les clés privées des porteurs ne sont séquestrées ou archivées. Les clés privées des porteurs sont archivés pendant 8 jours par l'AC.

6.3. Autres aspects de la gestion des bi-clés

6.3.1. Archivage des clés publiques

Les clés publiques de l'AC et des porteurs sont archivées dans le cadre de l'archivage des certificats correspondants.

6.3.2. Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des porteurs couverts par la présente PC ont une durée de validité de trois ans.

La durée de validité des clés de signature d'AC et des certificats correspondants est de dix ans. Les certificats d'AC sont renouvelés après une période de 7 ans maximum, afin que toute la période de

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		64/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE TECHNIQUES	
--	--	--

validité des certificats émis pour les porteurs soit couverte.

6.4. Données d'activation des clés d'AC

6.4.1. Génération et installation des données d'activation

La génération et l'installation des données d'activation des modules cryptographiques de l'IGC se font lors de la phase d'initialisation et de personnalisation de ce module, pendant la Cérémonie des Clés. Les données d'activation sont choisies et saisies par les porteurs de secret responsables de ces données.

6.4.2. Protection des données d'activation

Les données d'activation ne sont connues que par les porteurs de secret nommément identifiés dans le cadre des rôles qui leurs sont attribués.

Elles sont scellées et conservées en coffre-fort par les responsables de ces données eux-mêmes, de manière à les protéger en intégrité et en confidentialité.

6.5. Mesures de sécurité des systèmes informatiques

Les mesures de sécurité mises en place au niveau des systèmes informatiques couvrent les objectifs de sécurité suivants :

- identification et authentification forte des détenteurs de rôles de confiance pour l'accès à la plate-forme de l'IGC,
- identification et authentification forte des opérateurs d'enregistrement et administrateurs centraux pour l'accès à l'application IGC,
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels,
- gestion des comptes des opérateurs d'enregistrement et des administrateurs centraux au

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		65/79

	Projet IMAGE AC Personnes : Authentification MESURES DE SECURITE TECHNIQUES	
--	--	--

niveau de l'application IGC,

- gestion des comptes des détenteurs de rôles de confiance au niveau des systèmes de la plate-forme de l'IGC,
- 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 transitent entre les composantes de l'IGC,
- fonctions d'audits (non-répudiation et nature des actions effectuées),
- gestion des incidents,
- protection en confidentialité, en intégrité et en disponibilité des clés nécessaires au fonctionnement de l'AC.

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.

6.6. Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1. Mesures de sécurité liées au développement des systèmes

La configuration des systèmes de la plate-forme d'IGC (systèmes d'exploitation, application IGC...), ainsi que toute modification et mise à niveau, sont documentées et contrôlées.

6.6.2. Mesures liées à la gestion de la sécurité

L'Autorité Qualifiée est tenue informée de toute évolution majeure sur les systèmes de la plate-forme d'IGC.

Celle-ci est documentée et apparaît dans les procédures d'exploitation de l'AC.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		66/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>MESURES DE SECURITE TECHNIQUES</p>	
--	---	--

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 bon fonctionnement de l'application IGC.

De plus, les échanges au sein de l'application IGC mettent en œuvre systématiquement des services d'intégrité et de confidentialité.

6.8. Système de datation

La datation des événements enregistrés par les différentes fonctions de l'AC dans les journaux est basée sur l'heure système de la plate-forme hébergeant l'AC, après synchronisation par rapport à une source fiable de temps UTC, au minimum à la seconde près.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		67/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>Profils des certificats, de la LCR et des réponses OCSP</p>	
--	--	--

7. PROFILS DES CERTIFICATS, DE LA LCR ET DES REPONSES OCSP

Les profils des certificats d'authentification émis par l'AC Logiciels-2, ainsi que les profils de la LCR et des réponses OCSP correspondantes figurent dans le document [PC-Profils].

Ce document est référencé selon l'OID de la présente PC et fait partie intégrante du présent document. Toute modification majeure de ce document entraîne une évolution de l'OID de la présente PC, et vice-versa.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		68/79

	Projet IMAGE AC Personnes : Authentification AUDITS INTERNES ET DE CONFORMITE	
--	--	--

8. AUDITS INTERNES ET DE CONFORMITE

L'Autorité Administrative de l'AC Logiciels-2 fait contrôler la conformité de son AC avec les exigences du RGSv2 (niveau *) ».

Les audits internes ont notamment pour but de vérifier que l'AC respecte ce qui est écrit dans la présente PC et dans la DPC associée.

Les audits de conformité, ou audits « externes », ont notamment pour but de vérifier la conformité de la PC et de la DPC vis-à-vis des exigences du RGSv2 au même niveau. Pour ces audits externes :

- La reconnaissance du respect par l'AC des exigences du RGSv2 est effectuée par un organisme de qualification de services de confiance choisi parmi les organismes accrédités par le COFRAC selon la norme EN NF 45012 (ou ISO 17021) et le programme CEPE REF 21 (Exigences spécifiques pour la qualification des prestataires de services de confiance).
- Les résultats de l'audit de conformité sont communiqués par l'auditeur à l'Autorité Administrative de l'AC. Suite au résultat de l'audit de conformité, l'auditeur rend un avis à l'Autorité Administrative. Suivant les résultats, celle-ci met éventuellement en place des actions correctives et peut demander ensuite un nouvel audit de conformité auprès de l'auditeur.
- En cas de changement de toute nature intervenant dans la composition de l'IGC, l'AC devra :
 - au plus tard un mois avant le début de l'opération, 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'AC et de ses différentes composantes.
 - au plus tard un mois après la fin de l'opération, en informer l'organisme accrédité.

La suite du présent chapitre ne concerne que les audits et évaluation *internes* de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son AC.

8.1. Fréquences et / ou circonstances des évaluations

Suite à la première mise en service de l'application IGC ou suite à toute modification significative de

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		69/79

	Projet IMAGE AC Personnes : Authentification AUDITS INTERNES ET DE CONFORMITE	
--	--	--

celle-ci ou des procédures fonctionnelles applicables, l'Autorité Administrative de l'AC fait procéder à un audit interne global ou limité au périmètre de l'impact de la modification.

L'Autorité Administrative de l'AC fait aussi procéder régulièrement à un audit interne de l'ensemble de son AC, une fois tous les deux ans.

8.2. Identités / qualifications des évaluateurs

Le contrôle d'un périmètre particulier de l'IGC (procédure, application, fonction, rôle) est assigné par l'Autorité Administrative de l'AC à une équipe d'auditeurs, compétents en sécurité des systèmes d'information et dans le domaine couvert par le périmètre à auditer.

8.3. Relations entre évaluateurs et entités évaluées

L'auditeur ne doit pas posséder de rôle de confiance auprès de l'AC, autre que le présent rôle et doit être dûment autorisé à pratiquer les contrôles visés.

8.4. Sujets couverts par les évaluations

Les audits internes portent sur un rôle, une procédure, une fonction de l'AC ou sur l'application IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'AC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la présente PC et dans la DPC associée, ainsi que des éléments qui en découlent (procédures opérationnelles, ressources déployées, etc.).

8.5. Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle, l'auditeur rend à l'Autorité Administrative, un avis parmi les suivants : "réussite", "échec", "à confirmer".

Selon l'avis rendu, les conséquences du contrôle sont les suivantes :

- en cas d'échec, et selon l'importance des non-conformités, l'auditeur émet des recommandations à l'Autorité Administrative de l'AC pouvant être la cessation (temporaire ou définitive) d'activité, la suppression du rôle de confiance, la modification de la procédure, la

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		70/79

	Projet IMAGE AC Personnes : Authentification AUDITS INTERNES ET DE CONFORMITE	
--	--	--

révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'Autorité Administrative de l'AC et doit respecter ses politiques de sécurité internes, pour les références de ces politiques voir le document interne [DPC-AD].

- en cas de résultat "A confirmer", l'auditeur remet à l'Autorité Administrative de l'AC un avis précisant sous quel délai les non-conformités doivent être réparées. Puis, un contrôle de «confirmation» permettra de vérifier que tous les points critiques ont bien été résolus.
- en cas de réussite, l'auditeur confirme à l'Autorité Administrative de l'AC la conformité aux exigences de la PC et la DPC.

En cas d'échec ou de résultat « à confirmer », l'Autorité Administrative informe, selon un moyen à sa convenance, les tiers utilisateurs de ce résultat.

8.6. Communication des résultats

Les résultats des audits internes sont tenus à la disposition de l'organisme de qualification de services de confiance accrédité.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		71/79

	Projet IMAGE AC Personnes : Authentification AUTRES PROBLEMATIQUES METIERS ET LEGALES	
--	--	--

9. AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1. Tarifs

Sans objet.

9.2. Responsabilité financière

Sans objet.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations et données à caractère confidentiel sont listées et classifiées au sein de la DPC. La DPC détaille les mesures de sécurité applicables à chaque niveau de sécurité identifié.

9.3.2. Responsabilités en terme de protection des informations confidentielles

La présente PC ne formule pas d'exigences supplémentaires autres que celles prévues par la législation et la réglementation en vigueur sur le territoire français relatives à la protection des informations confidentielles.

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

Toute collecte et tout usage de données à caractère personnel par l'AC et les rôles de confiance de l'AC sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		72/79

	Projet IMAGE AC Personnes : Authentification AUTRES PROBLEMATIQUES METIERS ET LEGALES	
--	--	--

aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.

En particulier, l'AC en tant qu'infrastructure de stockage et de gestion de données nominatives contenues dans les certificats électroniques, est déclarée et soumise à l'avis de la CNIL selon les termes de la Loi n° 78-17 du 6 janvier 1978 « informatique et les libertés ».

Le récépissé de cette déclaration porte le numéro : 1245693.

9.4.2. Informations à caractère personnel

Les informations considérées comme personnelles sont les suivantes :

- les causes de révocation des certificats des porteurs ;
- le dossier d'enregistrement du porteur.

9.4.3. Informations à caractère non personnel

Les informations considérées comme non personnelles sont au moins les suivantes :

- les adresses de messagerie professionnelles des porteurs.

9.4.4. Responsabilité en terme de protection des données personnelles

La présente PC ne formule pas d'exigences supplémentaires autres que celles prévues par la législation et la réglementation en vigueur sur le territoire français relatives à la protection des données personnelles.

9.4.5. Notification et consentement d'utilisation des données personnelles

La présente PC ne formule pas d'exigence particulière sur ce point

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		73/79

	Projet IMAGE AC Personnes : Authentification AUTRES PROBLEMATIQUES METIERS ET LEGALES	
--	--	--

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

La communication aux autorités judiciaires des données personnelles sera effectuée en cas de demande de leur part.

9.4.7. Autres circonstances de divulgation d'informations personnelles

Le dossier d'enregistrement du porteur peut faire l'objet d'une divulgation auprès de la hiérarchie du porteur ou du service du personnel dont dépend le porteur.

9.5. Droits sur la propriété intellectuelle et industrielle

La présente PC ne formule pas d'exigences supplémentaires autres que celles prévues par la législation et la réglementation en vigueur sur le territoire français.

9.6. Interprétations contractuelles et garanties

Les obligations communes aux rôles de confiance de l'AC sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques et privées) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la présente PC et les documents applicables,
- respecter et appliquer la partie de la DPC leur incombant (cette partie étant communiquée aux rôles de confiance correspondants),
- se soumettre aux contrôles de conformité effectués par l'auditeur mandaté par l'AC et l'organisme de qualification accrédité,
- mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		74/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>AUTRES PROBLEMATIQUES METIERS ET LEGALES</p>	
--	---	--

9.6.1. Obligations applicables à l'Autorité de Certification

L'AC s'oblige à :

- pouvoir démontrer aux tiers utilisateurs de certificat qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, conformément aux exigences de la présente PC.
- garantir et maintenir la cohérence de sa DPC avec la présente PC.
- prendre toutes les mesures raisonnables pour s'assurer que les porteurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation des certificats. La relation entre un porteur et l'AC est formalisée par l'acceptation par le porteur des « Conditions d'Utilisation des certificats logiciels IMAGE » le concernant.
- Prendre toutes les mesures raisonnables pour s'assurer que les détenteurs de rôle de confiance auprès de l'AC ont connaissance de leurs droits et obligations conférés de par l'attribution de ce rôle.

L'AC assume toute conséquence dommageable résultant du non-respect de la présente PC par elle-même ou l'un de ses rôles de confiance.

De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou d'une personne assurant un rôle de confiance auprès de l'AC, 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.

Par ailleurs, l'AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même.

9.6.2. Obligations applicables aux opérateurs d'enregistrement

Les opérateurs d'enregistrement ont pour obligation :

- d'assurer leur rôle dans le respect de la présente PC, et notamment d'assurer les fonctions dévolues à l'AEL telles que précisées dans la présente PC,

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		75/79

	<p>Projet IMAGE</p> <p>AC Personnes : Authentification</p> <p>AUTRES PROBLEMATIQUES METIERS ET LEGALES</p>	
--	---	--

- de contrôler et vérifier l'identité des futurs porteurs,
- de conserver une copie des « Conditions d'Utilisation des certificats logiciels IMAGE » applicables signées par le porteur.

9.6.3. Obligations applicables aux porteurs

Les porteurs ont le devoir de respecter les exigences décrites dans les documents applicables :

- pour les porteurs internes : « Conditions d'Utilisation des certificats logiciels IMAGE applicables aux agents du Ministère »,

9.6.4. Obligations applicables aux tiers utilisateurs de certificat

Les tiers utilisateurs de certificat doivent :

- vérifier et respecter les conditions d'utilisation pour lesquelles un certificat a été émis et décrites dans le document « Conditions d'Utilisation des certificats logiciels IMAGE applicables aux tiers utilisateurs »),
- Contrôler la validité du certificat de l'Autorité de Certification « Logiciels-2 » :
 - par contrôle de la signature par l'Autorité de Certification « Racine-2 » du ministère en charge des affaires sanitaires et sociales ;
 - par contrôle des dates de validité ;
 - par contrôle de l'absence de révocation, d'après la dernière Liste de Révocation de Certificats en cours de validité émis par l'Autorité de Certification « Racine-2 » ;
- Contrôler la validité de chaque certificat porteur :
 - par contrôle de la signature par l'Autorité de Certification « Logiciels-2 » ;
 - par contrôle des dates de validité ;
 - par contrôle de l'absence de révocation, d'après la dernière Liste de Révocation de Certificats en cours de validité émis par l'Autorité de Certification « Logiciels-2 ».
- vérifier et respecter les obligations des tiers utilisateurs de certificats exprimées dans la présente PC,

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		76/79

	Projet IMAGE AC Personnes : Authentification AUTRES PROBLEMATIQUES METIERS ET LEGALES	
--	--	--

- contrôler que le certificat émis par l'AC Logiciels-2 est référencé au niveau de sécurité requis par l'application.

Les « Conditions d'Utilisation des certificats logiciels IMAGE applicables aux tiers utilisateurs » constituent un document public auquel les tiers utilisateurs de certificat ont accès.

9.7. Limite de responsabilité

L'objectif de l'AC est d'émettre des certificats qui soient acceptés par le système d'information du Ministère, par ses applications, et par les applications d'autres ministères ou d'autres partenaires, auxquelles le personnel du Ministère pourrait être amené à accéder.

L'AC est responsable en cas de négligence ou de faute intentionnelle des préjudices causés à une personne physique ou morale qui s'est fiée raisonnablement à ses certificats. La responsabilité de l'AC pourra être mise en jeu si une personne assurant un rôle de confiance auprès de l'AC a commis une erreur accidentelle ou volontaire, ou bien une négligence.

L'AC ne pourra pas être tenue pour responsable d'un fait dommageable qui relèverait de sa compétence en cas de force majeure. Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un événement irrésistible, insurmontable et imprévisible.

9.8. Indemnités

Les indemnités sont à l'appréciation des tribunaux compétents.

9.9. Durée et fin anticipée de validité de la PC

9.9.1. Durée de validité et fin de validité de la présente PC

La présente PC de l'AC est valide jusqu'à :

- émission d'une mise à jour majeure du présent document, avec évolution du numéro de version,

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		77/79

	Projet IMAGE AC Personnes : Authentification AUTRES PROBLEMATIQUES METIERS ET LEGALES	
--	--	--

- information publique de la part de l'Autorité Administrative, de l'invalidité de la présente PC. Dans ce cas, les certificats publiés selon la présente PC seront également révoqués.

9.9.2. Effets de la fin de validité et clauses restant applicables

Les traces d'audit enregistrées avant la fin de validité de la PC restent valables.

9.10. Amendements à la PC

9.10.1. Mécanisme et période d'information sur les amendements

Le cas échéant, les porteurs seront avertis des amendements au moyen de leur adresse de messagerie et/ou sur l'Intranet du Ministère.

Les amendements applicables seront également reportés sur la version mise à jour des différents documents « Conditions d'Utilisation des certificats logiciels IMAGE » applicables aux porteurs et aux tiers utilisateurs de certificat.

Les porteurs et les tiers utilisateurs de certificat peuvent prendre connaissance des amendements au moyen des sites web de publication.

9.10.2. Circonstances selon lesquelles l'OID doit être changé

L'OID de la présente PC étant inscrit dans les certificats qu'elle émet, toute évolution de cette 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) ou du document décrivant les profils associés (cf. 7 Profils des certificats, de la LCR et des réponses OCSP) se traduira par une évolution de l'OID. Ainsi, les porteurs et tiers utilisateurs de certificat pourront clairement distinguer quels certificats correspondent à quelles exigences.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		78/79

	Projet IMAGE AC Personnes : Authentification AUTRES PROBLEMATIQUES METIERS ET LEGALES	
--	--	--

9.11. Dispositions concernant la résolution de conflits

A défaut d'une résolution à l'amiable, les conflits sont résolus par les tribunaux compétents.

9.12. Juridictions compétentes

En cas de litige, ces derniers seront soumis à l'appréciation des tribunaux compétents.

9.13. Conformité aux législations et réglementations

L'AC s'engage à respecter les textes de lois et décrets d'application relatifs aux moyens de cryptologie, selon l'article 28 de la loi n°90-1170 du 29 décembre 1990 (Loi de Réforme des Télécommunications).

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	2.1		79/79