

DATE : 06/04/2026 NB PAGES : 75

VERSION : 4.1

REFERENCE : IMAGE-IGC-PC04

Projet :

IMAGE

Titre :

POLITIQUE DE CERTIFICATION

AC PERSONNES-4

OID : 1.2.250.1.179.1.7.1.1.4

	Projet IMAGE AC Personnes-4 Sommaire	
---	---	--

Résumé exécutif

La présente Politique de Certification définit les règles, exigences organisationnelles et techniques applicables à l'Autorité de Certification AC Personnes-4 du projet IMAGE. Elle précise les responsabilités des acteurs, les conditions d'émission, de gestion et de révocation des certificats d'authentification délivrés à des personnes physiques.

L'AC Personnes-4 s'inscrit dans une chaîne de confiance reposant sur l'AC Racine-4 et s'appuie sur des mesures de sécurité conformes au RGSv2 niveau *. Elle met en œuvre des contrôles organisationnels et techniques destinés à garantir la confidentialité des clés privées, l'intégrité des certificats, la traçabilité des opérations et la continuité des services critiques.

Référence IMAGE-IGC-PC02	Version 4.1	Niveau : [Public]	Page 2/75
--	---------------------------	--------------------------	-------------------------

	Projet IMAGE AC Personnes-4 Sommaire	
---	---	--

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
----------------	----

1.6. USAGE DES CERTIFICATS	21
----------------------------	----

1.6.1. BI-CLES ET CERTIFICATS PORTEURS	21
--	----

1.6.2. BI-CLES ET CERTIFICATS DE L'AC PERSONNES-4 ET DE SES COMPOSANTES	22
---	----

1.7. GESTION DE LA PC	23
-----------------------	----

1.7.1. ENTITE GERANT LA POLITIQUE DE CERTIFICATION	23
--	----

1.7.2. POINT DE CONTACT	23
-------------------------	----

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		3/75

	Projet IMAGE AC Personnes-4 Sommaire	
---	---	--

1.7.3.	DECLARATION DES PRATIQUES DE CERTIFICATION (DPC)	23
--------	--	----

1.7.4.	PROCEDURE D'APPROBATION DE LA DPC	23
--------	-----------------------------------	----

2. RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS PUBLIEES **24**

2.1.	ENTITES CHARGEES DE LA MISE A DISPOSITION DES INFORMATIONS	24
------	--	----

2.2.	INFORMATIONS PUBLIEES	24
------	-----------------------	----

2.3.	DELAIS ET FREQUENCES DE PUBLICATION	25
------	-------------------------------------	----

2.4.	CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES	26
------	--	----

3. IDENTIFICATION ET AUTHENTIFICATION **27**

3.1.	NOMMAGE	27
------	---------	----

3.1.1.	TYPES DE NOMS	27
--------	---------------	----

3.1.2.	UTILISATION DE NOMS EXPLICITES	27
--------	--------------------------------	----

3.1.3.	UNICITE DES NOMS	27
--------	------------------	----

3.1.4.	NOMS ALTERNATIFS (SUBJECT ALT NAME)	27
--------	-------------------------------------	----

3.2.	VALIDATION INITIALE DE L'IDENTITE	28
------	-----------------------------------	----

3.2.1.	VALIDATION DE L'IDENTITE D'UN PORTEUR	28
--------	---------------------------------------	----

3.3.	IDENTIFICATION ET VALIDATION POUR LE RENOUVELLEMENT DES CLES	28
------	--	----

3.3.1.	IDENTIFICATION ET VALIDATION POUR UN RENOUVELLEMENT	28
--------	---	----

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS **29**

4.1.	ENREGISTREMENT INITIAL	29
------	------------------------	----

4.1.1.	ORIGINE DE L'ENREGISTREMENT INITIAL	29
--------	-------------------------------------	----

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		4/75

	Projet IMAGE AC Personnes-4 Sommaire	
---	---	--

4.1.2.	ORIGINE DE LA DEMANDE DE CERTIFICAT	29
4.2.	DELIVRANCE DU CERTIFICAT	30
4.2.1.	ACTIONS DE L'AC CONCERNANT LA DELIVRANCE DU CERTIFICAT	30
4.2.2.	INSTALLATION PAR L'AC DU CERTIFICAT AU PORTEUR	30
4.2.3.	DUREE D'ETABLISSEMENT DU CERTIFICAT	30
4.3.	ACCEPTATION DU CERTIFICAT	30
4.3.1.	PUBLICATION DU CERTIFICAT	30
4.4.	USAGES DE LA BI-CLE ET DU CERTIFICAT	31
4.4.1.	UTILISATION DE LA CLE PRIVEE ET DU CERTIFICAT PAR LE PORTEUR	31
4.4.2.	UTILISATION DE LA CLE PUBLIQUE ET DU CERTIFICAT PAR UN TIERS UTILISATEUR	31
4.5.	RENOUVELLEMENT D'UN CERTIFICAT SANS CHANGEMENT DE BI-CLE	31
4.6.	RENOUVELLEMENT D'UN CERTIFICAT AVEC CHANGEMENT DE LA BI-CLE	31
4.6.1.	CAUSES POSSIBLES DE CHANGEMENT D'UNE BI-CLE	32
4.6.2.	ORIGINE D'UNE DEMANDE DE RENOUVELLEMENT DE CERTIFICAT	32
4.6.3.	NOTIFICATION AU PORTEUR DE L'ETABLISSEMENT DU NOUVEAU CERTIFICAT	ERREUR ! SIGNET NON DEFINI.
4.6.4.	DEMARCHE D'ACCEPTATION DU NOUVEAU CERTIFICAT	32
4.6.5.	PUBLICATION DU NOUVEAU CERTIFICAT	32
4.7.	MODIFICATION DU CERTIFICAT	32
4.8.	REVOCATION ET SUSPENSION DES CERTIFICATS	33
4.8.1.	CAUSES POSSIBLES D'UNE REVOCATION	33
4.8.2.	ORIGINE D'UNE DEMANDE DE REVOCATION	33
4.8.3.	PROCEDURE DE TRAITEMENT D'UNE DEMANDE DE REVOCATION FAITE PAR LE PORTEUR	34

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		5/75

4.8.4.	DELAI ACCORDE AU PORTEUR POUR EFFECTUER LA REVOCATION	34
4.8.5.	DELAI DE TRAITEMENT PAR L'AC D'UNE DEMANDE DE REVOCATION	35
4.8.6.	EXIGENCES DE VERIFICATION DE LA REVOCATION PAR LES TIERS UTILISATEURS DE CERTIFICAT	35
4.8.7.	FREQUENCE D'ETABLISSEMENT DE LA LCR	35
4.8.8.	DELAI MAXIMUM DE PUBLICATION D'UNE LCR	36
4.8.9.	DISPONIBILITE D'UN SYSTEME DE VERIFICATION EN LIGNE DE LA REVOCATION ET DE L'ETAT DES CERTIFICATS	36
4.8.10.	AUTRES MOYENS DISPONIBLES D'INFORMATION SUR LES REVOCATIONS	36
4.8.11.	EXIGENCES SPECIFIQUES EN CAS DE COMPROMISSION DE LA CLE PRIVEE	36
4.8.12.	CAUSES POSSIBLES D'UNE SUSPENSION	36
4.9.	FONCTION D'INFORMATION SUR L'ETAT DES CERTIFICATS	37
4.9.1.	CARACTERISTIQUES OPERATIONNELLES	37
4.9.2.	DISPONIBILITE DE LA FONCTION	37
4.10.	FIN DE RELATION ENTRE LE PORTEUR ET L'AC	38
4.11.	SEQUESTRE DE CLE ET RECOUVREMENT	38
5.	MESURES DE SECURITE NON TECHNIQUES	39
5.1.	MESURES DE SECURITE PHYSIQUE	39
5.1.1.	SITUATION GEOGRAPHIQUE ET CONSTRUCTION DES SITES	39
5.1.2.	ACCES PHYSIQUE	39
5.1.3.	ALIMENTATION ELECTRIQUE ET CLIMATISATION	39
5.1.4.	VULNERABILITE AUX DEGATS DES EAUX	40
5.1.5.	PREVENTION ET PROTECTION INCENDIE	40

	Projet IMAGE AC Personnes-4 Sommaire	
---	---	--

5.1.6.	CONSERVATION DES SUPPORTS	40
5.1.7.	MISE HORS SERVICE DES SUPPORTS	40
5.1.8.	SAUVEGARDES HORS SITE	41
5.2.	MESURES DE SECURITE PROCEDURALES	41
5.2.1.	ROLES DE CONFIANCE AUPRES DE L'AC	41
5.2.2.	ROLES DE CONFIANCE MUTUALISES A D'AUTRES APPLICATIONS	42
5.2.3.	NOMBRE DE PERSONNES REQUISES PAR TACHES	42
5.2.4.	IDENTIFICATION ET AUTHENTIFICATION POUR CHAQUE ROLE	43
5.2.5.	ROLES EXIGEANT UNE SEPARATION DES ATTRIBUTIONS	43
5.3.	MESURES DE SECURITE VIS-A-VIS DU PERSONNEL	44
5.3.1.	QUALIFICATIONS, COMPETENCES ET HABILITATIONS REQUISES	44
5.3.2.	VERIFICATION DE L'ADEQUATION DES PROFILS	44
5.3.3.	FORMATION INITIALE	45
5.3.4.	FORMATION CONTINUE	45
5.3.5.	FREQUENCE ET SEQUENCE DE ROTATION ENTRE DIFFERENTES ATTRIBUTIONS	45
5.3.6.	SANCTIONS EN CAS D'ACTIONS NON AUTORISEES	45
5.3.7.	EXIGENCES VIS-A-VIS DU PERSONNEL DES PRESTATAIRES EXTERNES	45
5.3.8.	DOCUMENTATION FOURNIE AU PERSONNEL	46
5.4.	PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT	46
5.4.1.	TYPES D'EVENEMENTS ENREGISTRES	46
5.4.2.	FREQUENCE DE TRAITEMENT DES JOURNAUX D'EVENEMENTS	48
5.4.3.	PERIODE DE CONSERVATION DES JOURNAUX D'EVENEMENTS SUR SITE	49
5.4.4.	PROTECTION DES JOURNAUX D'EVENEMENTS	49

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		7/75

	Projet IMAGE AC Personnes-4 Sommaire	
---	---	--

5.4.5.	PROCEDURE DE SAUVEGARDE DES JOURNAUX D'EVENEMENTS	50
5.4.6.	SYSTEME DE COLLECTE DES JOURNAUX D'EVENEMENTS	50
5.4.7.	NOTIFICATION DE L'ENREGISTREMENT D'UN EVENEMENT AU RESPONSABLE DE L'EVENEMENT	50
5.4.8.	EVALUATION DES VULNERABILITES	51
5.5.	ARCHIVAGE DES DONNEES	51
5.5.1.	TYPES DE DONNEES ARCHIVEES	51
5.5.2.	PERIODE DE CONSERVATION DES ARCHIVES	52
5.5.3.	PROTECTION DES ARCHIVES	52
5.5.4.	PROCEDURE DE SAUVEGARDE DES ARCHIVES	53
5.5.5.	DATATION DES DONNEES	53
5.5.6.	SYSTEME DE COLLECTE DES ARCHIVES	54
5.5.7.	PROCEDURES DE RECUPERATION ET DE VERIFICATION DES ARCHIVES	54
5.6.	CHANGEMENT DE CLE D'AC	54
5.7.	REPRISE A LA SUITE DE COMPROMISSION ET SINISTRE	55
5.7.1.	PROCEDURES DE REMONTEE ET DE TRAITEMENT DES INCIDENTS ET DES COMPROMISSIONS	55
5.7.2.	PROCEDURES DE REPRISE EN CAS DE CORRUPTION DES RESSOURCES INFORMATIQUES (MATERIELS, LOGICIELS ET / OU DONNEES)	55
5.7.3.	PROCEDURES DE REPRISE EN CAS DE COMPROMISSION DE LA CLE PRIVEE DE L'AC OU DE L'UNE DE SES COMPOSANTES	56
5.7.4.	CAPACITES DE CONTINUITE D'ACTIVITE A LA SUITE D'UN SINISTRE	56
5.8.	FIN DE VIE DE L'IGC	56
6.	MESURES DE SECURITE TECHNIQUES	58
6.1.	GENERATION DES BI-CLES	58

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		8/75

	Projet IMAGE AC Personnes-4 Sommaire	
---	---	--

6.1.1.	GENERATION DES BI-CLES DE L'AUTORITE	58
6.1.2.	GENERATION DES BI-CLES DES PORTEURS	59
6.1.3.	TRANSMISSION DE LA CLE PRIVEE A SON PROPRIETAIRE	59
6.1.4.	TRANSMISSION DE LA CLE PUBLIQUE D'UN PORTEUR A L'AC	59
6.1.5.	TRANSMISSION DE LA CLE PUBLIQUE DE L'AC AUX TIERS UTILISATEURS DE CERTIFICAT ET AUX PORTEURS	59
6.1.6.	TAILLES DES CLES ET ALGORITHMES UTILISES	59
6.1.7.	VERIFICATION DE LA GENERATION DES PARAMETRES DES BI-CLES ET DE LEUR QUALITE	59
6.1.8.	OBJECTIFS D'USAGE DE LA CLE	60
6.2.	MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES	60
6.2.1.	MODULES CRYPTOGRAPHIQUES DE L'AC	60
6.3.	AUTRES ASPECTS DE LA GESTION DES BI-CLES	60
6.3.1.	ARCHIVAGE DES CLES PUBLIQUES	60
6.3.2.	DUREES DE VIE DES BI-CLES ET DES CERTIFICATS	60
6.4.	DONNEES D'ACTIVATION DES CLES D'AC	61
6.4.1.	GENERATION ET INSTALLATION DES DONNEES D'ACTIVATION	61
6.4.2.	PROTECTION DES DONNEES D'ACTIVATION	61
6.5.	MESURES DE SECURITE DES SYSTEMES INFORMATIQUES	61
6.6.	MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE	62
6.6.1.	MESURES DE SECURITE LIEES AU DEVELOPPEMENT DES SYSTEMES	62
6.6.2.	MESURES LIEES A LA GESTION DE LA SECURITE	62
6.7.	MESURES DE SECURITE RESEAU	63

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		9/75

 Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE	Projet IMAGE AC Personnes-4 Sommaire	
---	--	--

6.8. SYSTEME DE DATATION	63
<u>7. PROFILS DES CERTIFICATS, DE LA LCR ET DES REPONSES OCSP</u>	<u>64</u>
<u>8. AUDITS INTERNES ET DE CONFORMITE</u>	<u>65</u>
8.1. FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS	65
8.2. IDENTITES / QUALIFICATIONS DES EVALUATEURS	66
8.3. RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES	66
8.4. SUJETS COUVERTS PAR LES EVALUATIONS	66
8.5. ACTIONS PRISES A LA SUITE DES CONCLUSIONS DES EVALUATIONS	66
8.6. COMMUNICATION DES RESULTATS	67
<u>9. AUTRES PROBLEMATIQUES METIERS ET LEGALES</u>	<u>68</u>
9.1. TARIFS	68
9.2. RESPONSABILITE FINANCIERE	68
9.3. CONFIDENTIALITE DES DONNEES PROFESSIONNELLES	68
9.3.1. PERIMETRE DES INFORMATIONS CONFIDENTIELLES	68
9.3.2. RESPONSABILITES EN TERMES DE PROTECTION DES INFORMATIONS CONFIDENTIELLES	68
9.4. PROTECTION DES DONNEES PERSONNELLES	68
9.4.1. POLITIQUE DE PROTECTION DES DONNEES PERSONNELLES	68
9.4.2. INFORMATIONS A CARACTERE PERSONNEL	69
9.4.3. INFORMATIONS A CARACTERE NON PERSONNEL	ERREUR ! SIGNET NON DEFINI.
9.4.4. RESPONSABILITE EN TERMES DE PROTECTION DES DONNEES PERSONNELLES	69
9.4.5. NOTIFICATION ET CONSENTEMENT D'UTILISATION DES DONNEES PERSONNELLES	69

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		10/75

	Projet IMAGE AC Personnes-4 Sommaire	
---	---	--

9.4.6.	CONDITIONS DE DIVULGATION D'INFORMATIONS PERSONNELLES AUX AUTORITES JUDICIAIRES OU ADMINISTRATIVES	69
9.4.7.	AUTRES CIRCONSTANCES DE DIVULGATION D'INFORMATIONS PERSONNELLES	69
9.5.	DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE	70
9.6.	INTERPRETATIONS CONTRACTUELLES ET GARANTIES	70
9.6.1.	OBLIGATIONS APPLICABLES A L'AUTORITE DE CERTIFICATION	70
9.6.2.	OBLIGATIONS APPLICABLES AUX OPERATEURS D'ENREGISTREMENT	71
9.6.3.	OBLIGATIONS APPLICABLES AUX PORTEURS	71
9.6.4.	OBLIGATIONS APPLICABLES AUX TIERS UTILISATEURS DE CERTIFICAT	71
9.7.	LIMITE DE RESPONSABILITE	72
9.8.	INDEMNITES	73
9.9.	DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC	73
9.9.1.	DUREE DE VALIDITE ET FIN DE VALIDITE DE LA PRESENTE PC	73
9.9.2.	EFFETS DE LA FIN DE VALIDITE ET CLAUSES RESTANT APPLICABLES	73
9.10.	AMENDEMENTS A LA PC	73
9.10.1.	MECANISME ET PERIODE D'INFORMATION SUR LES AMENDEMENTS	73
9.10.2.	CIRCONSTANCES SELON LESQUELLES L'OID DOIT ETRE CHANGE	74
9.11.	DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS	74
9.12.	JURIDICTIONS COMPETENTES	74
9.13.	CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS	74

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		11/75

 Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE MINISTÈRE DE LA SANTÉ, DE LA JEUNESSE ET DES SPORTS	Projet IMAGE AC CERTIFICATS LOGICIEL-3 Historique des versions	
---	--	--

Historique des versions

Version	Date	Modification
1.0	24/02/2024	Première version
2.0	06/04/2026	Nouvelle organisation DNUM

Références documentaires

Référence	Titre
[PC-Profiles]	IMAGE : Profils de certificats AC Personnes-4
[DPC]	Déclaration des Pratiques de Certification, IGC IMAGE - AC Déléguées
[PC-ACR]	Politique de Certification, IGC IMAGE - AC Racine-4

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		12/75

	Projet IMAGE AC PERSONNES-4 Introduction	
--	--	--

1. INTRODUCTION

1.1. Présentation générale

Présentation du projet IMAGE :

La transformation numérique de l'Etat passe par la mise en place de moyens permettant d'apporter la confiance nécessaire à la dématérialisation des processus.

Le projet IMAGEv2 (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 du Numérique du Secrétariat Général assurant le support des MINISTÈRES SOCIAUX, ci-après dénommés « le Ministère ». Ce projet consiste à mettre en œuvre une Infrastructure de Gestion de Clés (IGC) permettant des services d'authentification forte, de signature et de chiffrement.

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 (accès distants, applications sensibles), de signature et de chiffrement.

Présentation de la Politique de Certification AC Personnes-4 :

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 Personnes-4 », ci-après dénommée « l'AC », et au type de certificat authentification.

Il spécifie les exigences concernant la politique mise en œuvre par l'AC Personnes-4 délivrant des certificats d'authentification et les clés privées associées.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		13/75

	Projet IMAGE AC PERSONNES-4 Introduction	
--	--	--

Les certificats peuvent être attribués :

- 1) Aux agents du Ministère travaillant sur l'un des sites du Ministère, ou des directions clientes,
- 2) Aux personnes extérieures au Ministère, mais travaillant sur le site du Ministère, par exemple des stagiaires ou des prestataires de service,
- 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 personne.

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, ou auprès du système d'information d'autres ministères ou partenaires.

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 4 est identifiée par l'OID : **1.2.250.1.179.1.7.1.1.4**

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 « 1 étoile » ou * du RGSv2.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		14/75

	Projet IMAGE AC PERSONNES-4 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-4 : Autorité de Certification auto-signée, point de confiance de l'IGC, et certifiant les Autorités de Certification Délégées, dont l'AC Personnes-4.

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, ou de signature ou de chiffrement, 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.

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 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.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		15/75

	Projet IMAGE AC PERSONNES-4 Introduction	
--	---	--

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 :

AA	Autorité Administrative
AC	Autorité de Certification
AEL	Autorité d'Enregistrement Locale

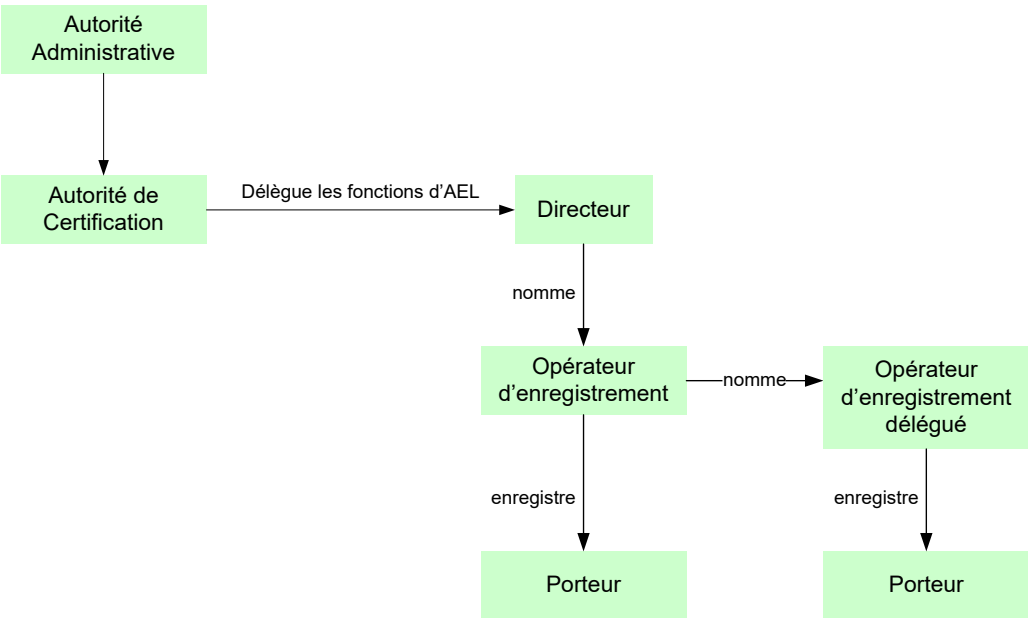
Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		16/75

	Projet IMAGE AC PERSONNES-4 Introduction	
--	---	--

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 »)
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
PC	Politique de Certification
RSA	<i>Rivest Shamir Adleman</i> ; algorithme de chiffrement asymétrique, du nom de leurs trois inventeurs.
UTC	<i>Universal Time Coordinated</i> ; temps universel coordonné

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		17/75

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 la directrice de la direction du numérique (DNUM) du secrétariat général des ministères sociaux.

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.
- 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.

	Projet IMAGE AC PERSONNES-4 Introduction	
--	--	--

- 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 termes 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 de la Confiance, de l'Infrastructure et des Données de la DNUM.

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 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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		19/75

	Projet IMAGE AC PERSONNES-4 Introduction	
--	--	--

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;
- L'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC;
- 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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		20/75

	Projet IMAGE AC PERSONNES-4 Introduction	
--	---	--

personnelles),

- La désignation des autres AEL de sa direction.

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.

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 ou d'une direction cliente (ARS, DREETS...),
- 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, où ayant besoin d'un accès à certaines applications « extranet ».

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 suivant le type de certificat :

- s'authentifier auprès des tiers utilisateurs de certificat.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		21/75

	Projet IMAGE AC PERSONNES-4 Introduction	
--	---	--

- Signer électroniquement
- Chiffrer

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 pour des usages autres que ceux qui sont définis dans la présente PC.

1.6.2. Bi-clés et certificats de l'AC Personnes-4 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 Personnes-4, ainsi que les certificats des composantes et les engagements relatifs à ces certificats, font l'objet du document [PC-ACR].

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		22/75

	Projet IMAGE AC PERSONNES-4 Introduction	
--	---	--

1.7. Gestion de la PC

1.7.1. Entité gérant la Politique de Certification

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 :

MINISTÈRES SOCIAUX Direction du numérique / Sous-direction de la Confiance, de l'Infrastructure et des Données , projet Image 9, Rue Louis Lejeune – 92120 Montrouge (dnum-do-image@sg.social.gouv.fr)

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	4.1		23/75

	Projet IMAGE AC PERSONNES-4 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-4 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-4 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	4.1		24/75

	Projet IMAGE AC PERSONNES-4 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS PUBLIEES	
--	--	--

(*) 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 maximale d'indisponibilité par mois de 8 heures, ceci hors cas de force majeure.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		25/75

	Projet IMAGE AC PERSONNES-4 RESPONSABILITES CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS PUBLIEES	
--	--	--

Informations d'état des certificats :	
Délais de publication :	Les exigences portant sur la fonction de publication de ces informations sont définies au chapitre 4.9.
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.social.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 basé sur une authentification par certificat.

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	4.1		26/75

	Projet IMAGE AC PERSONNES-4 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 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

Elle est réalisée en amont dans le peuplement des annuaires.

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

- CN = NOM, Prenom
- OU = direction
- OUs suivants d'après la hiérarchie dans l'annuaire
- DC=FR

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. Noms alternatifs (subject alt name)

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		27/75

	Projet IMAGE AC PERSONNES-4 IDENTIFICATION ET AUTHENTIFICATION	
--	---	--

Un identifiant est placé dans une extension « subject Alternative Name » du certificat :

- 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.

Cette étape est réalisée en amont lors de la création du compte dans l'annuaire de référence.

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

Tant que le compte AD de référence existe, le renouvellement est automatique sans nouvelle vérification d'identité.

À la suite de 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.

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	4.1		28/75

	Projet IMAGE AC PERSONNES-4 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

La vérification de l'identité est effectuée par l'opérateur en amont lors de la création des comptes dans les annuaires du ministère.

L'enregistrement des porteurs est réalisé automatiquement par synchronisation avec les annuaires de référence.

4.1.2. Origine de la demande de certificat

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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		29/75

	Projet IMAGE AC PERSONNES-4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	---	--

4.2. Délivrance du certificat

4.2.1. Actions de l'AC concernant la délivrance du certificat

À la suite de 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.

4.2.2. Installation par l'AC du certificat au porteur

L'installation du certificat d'authentification se fait automatiquement par les outils en place, dans le magasin personnel Windows de l'utilisateur.

4.2.3. Durée d'établissement du certificat

Les certificats sont valables pour une durée de trois ans.

4.3. 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'UPN contenue dans l'extension « SubjectAlternativeName » du certificat.

4.3.1. Publication du certificat

Les certificats ne sont pas publiés.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		30/75

	Projet IMAGE AC PERSONNES-4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	---	--

4.4. Usages de la bi-clé et du certificat

4.4.1. 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, conformément aux profils de certificats définis dans le document « profils relatifs à la PC Infrastructure authentification ».

. Les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

Tous les porteurs peuvent utiliser leur certificat, suivant le type :

- 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 »

4.4.2. 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.

4.5. 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.

4.6. 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.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		31/75

	Projet IMAGE AC PERSONNES-4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	---	--

4.6.1. 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, par suite de la révocation du certificat du porteur. Ce cas suit alors le processus d'enregistrement initial, et non celui du renouvellement.

4.6.2. Origine d'une demande de renouvellement de certificat

Peu avant la date d'expiration de leur certificat, les certificats sont renouvelés automatiquement par les mêmes mécanismes que la création initiale.

4.6.3. 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, UPN...).

4.6.4. Publication du nouveau certificat

Le certificat renouvelé n'est pas publié.

4.7. Modification du certificat

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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		32/75

	Projet IMAGE AC PERSONNES-4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	---	--

4.8. Révocation et suspension des certificats

4.8.1. 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) où 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 compte de l'utilisateur est supprimé de l'annuaire source, où il est déplacé dans une autre direction : dans ce cas la révocation est automatique après un délai de grâce de 24h.
- Le porteur est muté dans une autre direction : dans ce cas la révocation du certificat s'impose;

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

4.8.2. 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,

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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		33/75

	Projet IMAGE AC PERSONNES-4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	---	--

- 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.

4.8.3. 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, où fait sa demande par messagerie électronique, où par un outil de gestion de ticket.

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.

4.8.4. 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	4.1		34/75

	Projet IMAGE AC PERSONNES-4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	---	--

4.8.5. 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.

4.8.6. 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.

4.8.7. Fréquence d'établissement de la LCR

Une nouvelle LCR est publiée toutes les 12 heures. En outre, en cas de révocation d'un certificat, l'AC émet une LCR mise à jour, sans attendre la publication faite toutes les 12 heures,

Chaque LCR est émise avec une durée de validité de 15 jours.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		35/75

	Projet IMAGE AC PERSONNES-4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	---	--

4.8.8. Délai maximum de publication d'une LCR

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

4.8.9. 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.

4.8.10. 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.

4.8.11. 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 ou est installé le certificat (ordinateur, tablette, téléphone multifonction):

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

4.8.12. Causes possibles d'une suspension

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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		36/75

	Projet IMAGE AC PERSONNES-4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	---	--

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

4.9.1. Caractéristiques opérationnelles

L'AC fournit aux tiers utilisateurs de certificat les informations leur permettant de vérifier et de valider, 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 Personnes-4,
- De vérifier la présence ou non du certificat porteur dans la LCR émise par l'AC Personnes-4,
- De vérifier la signature de cette LCR par l'AC Personnes-4.

via la consultation libre de la LCR.

La LCR émise par l'AC Personnes-4 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 Personnes-4 relèvent de la responsabilité de l'AC Racine-4 et peuvent donc être obtenues auprès de celle-ci.

4.9.2. 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.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		37/75

	Projet IMAGE AC PERSONNES-4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	
--	---	--

4.10.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.

4.11.Séquestre de clé et recouvrement

Les clés privées des porteurs ne sont pas séquestrées.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		38/75

	Projet IMAGE AC PERSONNES-4 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.

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	4.1		39/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	---	--

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	4.1		40/75

	Projet IMAGE AC PERSONNES-4 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 la

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		41/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	---	--

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.

Ces différents rôles sont assurés par des personnes distinctes.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		42/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	--	--

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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		43/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	---	--

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.

Les opérateurs d'enregistrement sont informés de leurs responsabilités et des procédures en vigueur.

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.

Ces personnes ne doivent pas notamment avoir fait l'objet de condamnation incompatible avec leurs attributions.

Les personnes jouant 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.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		44/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	--	--

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 termes 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.

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.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		45/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	---	--

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 :

- Acceptation ou refus de connexion à l'application IGC ;

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		46/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	--	--

- 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 par suite d'une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des détenteurs des rôles de confiance, et les tentatives non réussies correspondantes.

5.4.1.4 Caractéristiques communes

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		47/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	--	--

Pour tous les types d'enregistrements présentés ci-dessus : chaque enregistrement d'événement 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'événements applicatifs de l'application IGC est surveillé régulièrement 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 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.

5.4.2.3 Autres enregistrements électroniques

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		48/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	---	--

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 sans limitation de durée.

5.4.3.3 Autres enregistrements électroniques

Les autres journaux d'enregistrement sous forme électronique sont conservés pendant une durée de 1 an.

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

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.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		49/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	---	--

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.

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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		50/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	--	--

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.

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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		51/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	--	--

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.

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 ne sont pas archivées.

Journaux d'évènements

Les journaux d'événements de l'application IGC sont conservés par celle-ci pendant une durée de 1 an.

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.

5.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives :

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		52/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	--	--

- 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 œuvre 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 1 seconde.

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	4.1		53/75

	Projet IMAGE AC PERSONNES-4 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 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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		54/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	---	--

pouvoir émettre des certificats porteurs sans discontinuité.

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 à la suite de 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.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		55/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	---	--

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

Dans le cas de compromission de la clé de l'AC Personnes-4, l'AC demandera la révocation de son certificat auprès de l'AC Racine-4 ; 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 à la suite d'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 5 jours.

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 œuvre 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 ;

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		56/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE NON TECHNIQUES	
--	---	--

- 3) Demande la révocation de son certificat auprès des autorités ayant certifié sa clé ;
- 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	4.1		57/75

	Projet IMAGE AC PERSONNES-4 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 Personnes-4 est effectuée dans des circonstances contrôlées, par des personnels dans des rôles de confiance.

L'initialisation de l'IGC et/ou des boîtiers HSM 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.

À la suite de 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	4.1		58/75

	Projet IMAGE AC PERSONNES-4 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-4.

6.1.6. Tailles des clés et algorithmes utilisés

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, avec algorithme de hachage SHA-256.

Les clés des porteurs sont des clés RSA de 2048 bits, avec algorithme de hachage SHA-256.

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.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		59/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE TECHNIQUES	
--	---	--

6.1.8. Objectifs d'usage de la clé

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

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.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		60/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE TECHNIQUES	
--	---	--

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 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 plateforme 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,

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		61/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE TECHNIQUES	
--	---	--

- Gestion des comptes des opérateurs d'enregistrement et des administrateurs centraux au 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	4.1		62/75

	Projet IMAGE AC PERSONNES-4 MESURES DE SECURITE TECHNIQUES	
--	---	--

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 minute près.

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		63/75

	Projet IMAGE AC PERSONNES-4 Profils des certificats, de la LCR et des réponses OCSP	
--	--	--

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

Les profils des certificats d'authentification émis par l'AC Personnes-4, ainsi que les profils de la LCR et des réponses OCSP correspondantes figurent dans le document « profils relatifs à la PC Personnes authentification 4 ».

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	4.1		64/75

	Projet IMAGE AC PERSONNES-4 AUDITS INTERNES ET DE CONFORMITE	
--	---	--

8. AUDITS INTERNES ET DE CONFORMITE

L'Autorité Administrative de l'AC Personnes-4 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.
- Les résultats de l'audit de conformité sont communiqués par l'auditeur à l'Autorité Administrative de l'AC. À la suite du 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

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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		65/75

	Projet IMAGE AC PERSONNES-4 AUDITS INTERNES ET DE CONFORMITE	
--	---	--

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 audit 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 à la suite des 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 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 voire le document interne [DPC-AD].

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		66/75

	Projet IMAGE AC PERSONNES-4 AUDITS INTERNES ET DE CONFORMITE	
--	---	--

- 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	4.1		67/75

	Projet IMAGE AC PERSONNES-4 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 termes 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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		68/75

	Projet IMAGE AC PERSONNES-4 AUTRES PROBLEMATIQUES METIERS ET LEGALES	
--	---	--

français, en particulier le règlement général sur la protection des données – RGPD.

En outre, 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 ;

9.4.3. Responsabilité en termes 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.

9.4.4. Notification et consentement d'utilisation des données personnelles

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

9.4.5. 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.

9.4.6. Autres circonstances de divulgation d'informations personnelles

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		69/75

	Projet IMAGE AC PERSONNES-4 AUTRES PROBLEMATIQUES METIERS ET LEGALES	
--	---	--

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.

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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		70/75

	Projet IMAGE AC PERSONNES-4 AUTRES PROBLEMATIQUES METIERS ET LEGALES	
--	--	--

droits et obligations en ce qui concerne l'utilisation des certificats. La relation entre un porteur et l'AC est formalisée par « 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 du fait de 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,
- De contrôler et vérifier l'identité des futurs porteurs,

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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		71/75

	Projet IMAGE AC PERSONNES-4 AUTRES PROBLEMATIQUES METIERS ET LEGALES	
--	--	--

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 « Personnes-4 » :
 - Par contrôle de la signature par l'Autorité de Certification « Racine-4 » 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-4 » ;
- Contrôler la validité de chaque certificat porteur :
 - Par contrôle de la signature par l'Autorité de Certification « Personnes-4 » ;
 - 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 « Personnes-4 ».
- Vérifier et respecter les obligations des tiers utilisateurs de certificats exprimées dans la présente PC,
- Contrôler que le certificat émis par l'AC Personnes-4 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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		72/75

	Projet IMAGE AC PERSONNES-4 AUTRES PROBLEMATIQUES METIERS ET LEGALES	
--	--	--

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,
- 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

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		73/75

	Projet IMAGE AC PERSONNES-4 AUTRES PROBLEMATIQUES METIERS ET LEGALES	
--	---	--

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 présent 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.

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).

*** Fin du document ****

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		74/75

	Projet IMAGE AC PERSONNES-4 AUTRES PROBLEMATIQUES METIERS ET LEGALES	
--	--	--

Référence	Version	Niveau : [Public]	Page
IMAGE-IGC-PC02	4.1		75/75