Liberté • Égalité • Fraternité RÉPUBLIQUE FRANÇAISE	MINISTÈRES SOCIAUX	

	DATE : 24/06/2024 NB PAGES : **76** VERSION : 1.0 REFERENCE : IMAGE-IGC-PC01 STATUT : VALIDE
Projet :	**IMAGEv2**
Titre :	# POLITIQUE DE CERTIFICATION ## AC RACINE-4 ET COMPOSANTS D'INFRASTRUCTURE ## OID : 1.2.250.1.179.1.1.1.1.4

SOMMAIRE

Historique des versions

Version	Date	Modification
1.0	06/02/2024	Version initiale

Références documentaires

Référence	Titre
[RGSv2]	Référentiel Général de Sécurité - Version 2.0
[PC-profils]	IMAGE : Profils de certificats AC Racine-4
[DPC]	Déclaration des Pratiques de Certification : AC Racine-4

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 (**I**nfrastructure **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, d'une part, une Infrastructure de Gestion de Clés (IGC) permettant des services d'authentification forte et de signature.

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).

Présentation de la Politique de Certification AC Racine-4:

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

Il spécifie les exigences applicables :

- À l'AC Racine-4, pour :
  - La génération et le renouvellement de ses clés,
  - La certification des clés publiques des AC Déléguées et la révocation des certificats des AC Déléguées émis par l'Autorité Racine-4,
  - La génération, le renouvellement et la révocation de ses certificats d'administrateurs.
- Aux AC Déléguées, pour :
  - La génération et le renouvellement des clés des AC Déléguées ainsi que pour les demandes de certificats auprès de l'Autorité Racine-4,
- À l'AC Racine-4 et aux AC Déléguées, pour :
  - La protection des communications entre les composantes de chaque AC.

La politique est définie indépendamment des détails de l'environnement utilisé pour la mise en œuvre de l'IGC.

Les détenteurs de rôle de confiance de l'IGC et les tiers utilisateurs des certificats objets de cette Politique ont des obligations spécifiques définies dans cette Politique de Certification.

1.2. Identification du document

L'OID de la présente PC est : **1.2.250.1.179.1.1.1.1.4**

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

1.3. Relation avec la RGS

Cette Politique de Certification se veut cohérente avec les exigences stipulées pour le niveau « 1 étoile » ou * de la RGSv2.

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) : Dans le cadre du présent document, ce terme désigne, selon les cas :

- La personne ou l'Autorité chargée de l'application de la présente Politique de Certification,
- L'infrastructure technique réalisant les fonctions dévolues à l'AC. A cet effet, elle utilise notamment les clés de signature de l'AC.

Autorité de Certification Déléguée (ACD) : Autorité de Certification dont la bi-clé est certifiée par l'Autorité Racine-4.

Autorité de Certification Racine (ACR-4) : Autorité de Certification point de confiance de l'IGC IMAGE, et certifiant les Autorités de Certification Déléguées.

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 ou à une composante technique et portant sur une bi-clé détenue par celle-ci. L'usage de ce certificat est indiqué au sein de celui-ci (authentification client ou serveur, signature, signature de certificat ou de crl…)

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.

DNUM Direction du Numérique du Ministère

DO Département des Opérations

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

Infrastructure de Gestion de Clés (IGC) : Ensemble de composantes, fonctions et procédures dédiées à la génération et 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.

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 le certificat et détentrice de la clé privée correspondant à la clé publique présente dans ce certificat.

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

Tiers utilisateur : Utilisateur ou système faisant confiance à un certificat.

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

ACD Autorité de Certification Déléguée

ACR-4 Autorité de Certification Racine-4

AEL Autorité d'Enregistrement Locale

CN *Common name* ; nom commun

DN *Distinguished Name* ; nom distinctif

DPC Déclaration des Pratiques de Certification

EAL *Evaluation Assurance Level* ; 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

LCR Liste des Certificats Révoqués

LDAP *Light Directory Access Protocol* ; protocole d'interrogation et de modification de contenu d'annuaire

OID *Object Identifier* ; Identifiant d'objet

PIN *Personal Identification Number* ; nombre personnel d'identification

PC Politique de Certification

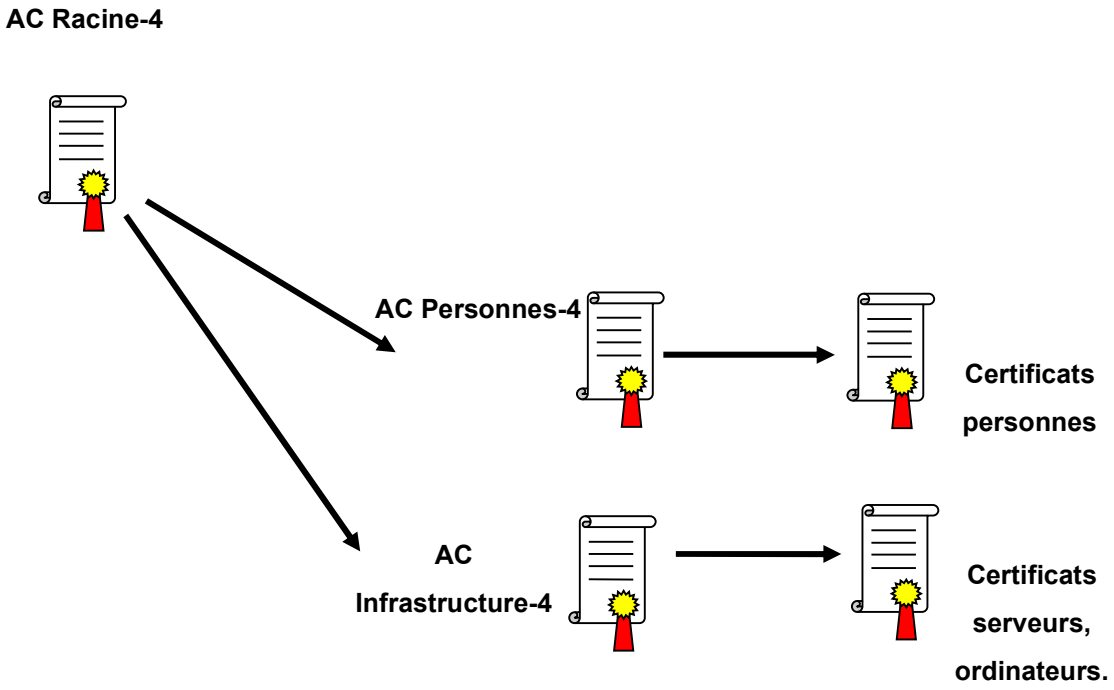
RSA *Rivest Shamir Adleman* ; algorithme de chiffrement asymétrique, du nom de leurs trois inventeurs.

1.5. Organisation hiérarchique de l'IGC IMAGE

L'AC Racine-4 du Ministère assure principalement les fonctions suivantes :

- La génération de ses certificats auto-signés.
- La certification des AC Déléguées placées sous l'autorité du Ministère.

Le schéma suivant illustre le schéma de certification :



1.6. Entités intervenant dans l'IGC

1.6.1. Autorité Administrative de l'AC Racine-4

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 demandeurs de certificats, aux Autorités Déléguées, 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.
- 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 de certificat, 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 Racine-4 et le certificat correspondant (signature de certificats, de LCR), puis diffuser son certificat d'AC aux tiers utilisateurs.

1.6.2. Autorité de Certification Racine-4

Le rôle d'Autorité de Certification Racine est assuré par la cheffe du Département Opérations de la DNUM.

L'Autorité de Certification Racine-4 (ACR-4) a en charge la fourniture des prestations de gestion des certificats des ACD et de ses administrateurs 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 (Politiques et Pratiques…), les certificats d'AC et toute autre information pertinente destinée aux demandeurs, 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'ACR-4 traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

Fonction d'information sur l'état des certificats : Cette fonction fournit aux tiers utilisateurs de certificats des informations sur l'état des certificats (révoqués, non révoqués). Cette fonction est mise en œuvre selon un mode de publication d'informations au moyen de LCR.

1.6.3. Autorité d'Enregistrement Locale auprès de l'AC Racine-4

Le rôle d'AEL est assuré par les administrateurs centraux de l'AC Racine-4.

L'AEL de l'ACR-4 permet l'enregistrement des ACD et de ses administrateurs centraux, la remise des certificats et la prise en compte des demandes de révocation pour les certificats émis. Pour cela, elle assure les fonctions suivantes :

Fonction d'enregistrement des demandes de certificats : Cette fonction assure la vérification des données à mettre dans le certificat et des informations d'identification des demandeurs d'un certificat.

Fonction de remise du certificat aux demandeurs : Cette fonction remet le certificat à son ou à ses demandeurs une fois qu'il a été généré par l'ACR-4.

Fonction de gestion des révocations : Dans le cadre de cette fonction, l'AEL prend en compte les demandes de révocation pour transmission et traitement par l'AC Racine-4.

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

- La prise en compte et la vérification des informations concernant la future AC Déléguée ou le futur administrateur, ainsi que la constitution du dossier d'enregistrement correspondant ;
- L'établissement et la transmission de la demande de certificat à la fonction adéquate de l'AC Racine-4;
- La conservation des pièces des dossiers d'enregistrement.

L'AEL a aussi pour rôle d'assurer la prise en compte des demandes de révocation.

1.6.4. Autorité de Certification Déléguée

Chaque Autorité de Certification Déléguées (ACD) doit procéder à la génération de sa bi-clé et la faire certifier par l'ACR-4. Elle doit aussi demander la révocation de son certificat en cas de compromission réelle ou

suspectée de sa clé privée (vol ou perte), de changement de nom de l'AC ou de cessation d'activité.

Les responsabilités incombant à chaque ACD et relatives à la délivrance et à la gestion des certificats qu'elle émet sont décrites dans les Politiques de Certification de cette AC.

Ce document complète ces Politiques en décrivant les fonctions nécessaires à la création, au renouvellement et à la révocation des certificats de chaque ACD.

Les fonctions assurées par les Autorités Déléguées sont :

Fonction de création d'une demande de certificat d'une ACD : Cette fonction assure la génération initiale d'une bi-clé et la création d'un fichier de demande de certificat au format PKCS#10 pour une nouvelle Autorité Déléguée.

Fonction de demande de renouvellement du certificat d'une ACD : Cette fonction assure la génération d'une nouvelle bi-clé et la création d'un fichier de demande de certificat au format PKCS#10 pour une Autorité Déléguée existante.

Fonction de demande de révocation du certificat d'une ACD : Cette fonction assure la demande de révocation d'un certificat d'ACD.

1.6.5. Tiers utilisateurs de certificats

Les tiers utilisateurs concernent les utilisateurs des certificats émis selon la présente Politique de Certification :

- Certificat auto-signé de l'AC Racine-4 ;
- Certificats des Autorités Déléguées émis par l'AC Racine-4 ;
- Certificats de composantes de chaque AC ;
- Certificats d'authentification des administrateurs centraux de l'AC Racine-4.

Les tiers utilisateurs sont les systèmes et les applications informatiques :

- Soit utilisant des certificats porteurs ou serveurs émis par l'une des Autorités Déléguées rattachées à l'AC Racine-4, et à ce titre nécessitant les certificats du chemin de certification,
- Soit composantes de l'application IGC et à ce titre acceptant les certificats d'autres composantes

et/ou des administrateurs de l'AC Racine-4.

1.7. Gestion de la PC

1.7.1. Entité gérant la Politique de Certification

L'Autorité de Certification Racine est responsable de l'établissement de la présente Politique de Certification, ainsi que de son application et de sa diffusion.

L'Autorité Administrative afférente 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

Département opérations, Projet IMAGE

Tour Mirabeau

39-43 Quai André Citroën 75902 PARIS CEDEX 15

Dnum-do-image@sg.social.gouv.fr

1.7.3. Déclaration des Pratiques de Certification (DPC)

L'AC Racine-4 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.

1.7.4. Procédure d'approbation de la DPC

Le document [DPC] est approuvé par l'AA afférente. Responsabilités concernant la mise à disposition des informations publiées

1.8. Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des tiers utilisateurs de certificats, l'ACR-4 met en œuvre au sein de son IGC une fonction de publication des informations de statut des certificats.

1.9. Informations publiées

L'AC Racine-4 publie les informations suivantes à destination des tiers utilisateurs de certificats :

- La Politique de Certification de l'ACR-4 en cours de validité (le présent document),
- Les profils des certificats de l'ACR-4, des ACD, et des LCR émises par l'ACR-4,
- Les certificats auto-signés de l'ACR-4, en cours de validité et les informations permettant aux tiers utilisateurs de certificats de s'assurer de l'origine de ces certificats (empreintes),
- La LCR en cours de validité, en version V2 et accessible par le protocole http,
- L'adresse permettant d'obtenir des informations concernant l'AC Racine-4,

1.9.1. Délais de publication et disponibilité de l'information

Les délais de publication et la disponibilité de l'information 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 de l'ACR-4 et des ACD	
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 4 heures et une durée totale maximale d'indisponibilité par mois de 16 heures, ceci hors cas de force majeure.

Informations d'état des certificats	
Délais de publication :	Les exigences portant sur la fonction de publication de ces informations sont définies au chapitre 1.10.
Disponibilité de l'information :	

1.9.2. 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.

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

1.10.1. Caractéristiques opérationnelles

L'ACR-4 fournit aux tiers utilisateurs de certificats émis par l'AC Racine-4 les informations leur permettant de vérifier et de valider via la consultation libre de la LCR et préalablement à son utilisation, le statut d'un certificat, c'est-à-dire :

- De vérifier la signature d'un certificat par l'AC Racine-4,
- De vérifier la présence ou non d'un certificat d'ACD dans la LCR émise par l'AC Racine-4,
- De vérifier la signature de cette LCR par l'ACR-4.

La LCR émise par l'ACR-4 est au format V2 et est accessible au moyen du protocole HTTP depuis Internet.

1.10.2. Délais de publication et disponibilité de l'information

Les délais de publication et la disponibilité de l'information dépendent des informations concernées :

Information sur l'état des certificats	
Délais de publication :	La LCR est émise tous les 6 mois. Sa période de validité est de 18 mois.
Disponibilité de l'information :	L'infrastructure assurant cette fonction est disponible 7j/7, avec une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4 heures (jours ouvrés) et une durée totale maximale d'indisponibilité par mois de 16 heures, ceci hors cas de force majeure.

2. AC RACINE-4 : EXIGENCES RELATIVES AU CYCLE DE VIE DES CERTIFICATS

2.1. Dispositions générales

2.1.1. Mode de fonctionnement

L'AC Racine-4 doit fonctionner en mode « hors ligne ».

2.1.2. Garantie de fonctionnement

L'AC Racine-4 doit garantir son fonctionnement même en cas de sinistre majeur. Le délai de remise en service de l'AC Racine-4 en cas de besoin est inférieur à 24 heures.

2.2. Exigences relatives au cycle de vie des certificats auto-signés de l'AC Racine-4

2.2.1. Nommage

Dans chaque certificat X509v3 auto-signé d'ACR-4, les champs émetteur (« *issuer*") et sujet (« *subject* ») sont identiques et contiennent un nom distinctif (DN : « *Distinguished Name* ») de type X.501.

Le nom distinctif de l'AC Racine-4 est construit à partir des composants suivants :

CN = AC Racine-4
OU = 0002 130 006 802 00016
O = Ministeres Sociaux
C = FR

2.2.2. Génération d'une bi-clé et d'un certificat auto-signé de l'ACR-4

La génération des bi-clés de l'ACR-4 est réalisée dans le cadre d'une cérémonie des clés.

Le but de cette cérémonie est de générer un certificat racine auto-signé, de récupérer la valeur du certificat auto-signé à des fins de publication et de déclarer l'ACR-4 opérationnelle.

Cette cérémonie permet d'initialiser les modules de sécurité de l'infrastructure et de réaliser des copies de secours de la clé privée de l'AC Racine-4.

La cérémonie est conduite par le maître de cérémonie.

La cérémonie implique la présence d'au moins les personnes tenant les rôles de confiance suivants, outre le maître de cérémonie :

- Témoins de l'Autorité Administrative, garants du déroulement conforme de la cérémonie ;
- Opérateurs de l'IGC et des modules de sécurité, garants du fait que les systèmes (matériels, logiciels et modules de sécurité) sont correctement configurés et opérationnels ;
- Responsable sécurité pour la cérémonie, garant du bon déroulement de la cérémonie sur le plan de la sécurité ;

L'AC Racine-4 s'engage à établir le scénario complet de la cérémonie. Ce document n'est pas public, et précise la liste des personnes ayant accès au dit document, et détaille les mesures de protection mises en œuvre.

L'AC Racine-4 s'engage à émettre des procès-verbaux pour chaque étape importante de la Cérémonie. Ces documents ne sont pas publics.

La publication du certificat auto-signé de l'Autorité Racine par l'AC marque l'acceptation de ce certificat par celle-ci.

2.2.3. Renouvellement d'une bi-clé et d'un certificat auto-signé de l'ACR-4

Les exigences concernant cette cérémonie sont similaires à la cérémonie décrite ci-dessus, exception faite de l'initialisation des modules de sécurité non réalisée de nouveau.

2.2.4. Révocation d'un certificat auto-signé de l'ACR-4

Différentes circonstances peuvent être à l'origine de la révocation des certificats auto-signés de l'ACR-4:

- L'ACR-4 cesse son activité,
- L'un au moins des éléments servant à reconstituer la clé privée de l'AC Racine-4 a été perdu ou volé,
- Un module de sécurité de l'ACR-4 a été utilisé frauduleusement.

Lorsqu'une des circonstances ci-dessus se réalise et qu'un détenteur de rôle de confiance auprès de l'AC Racine-4 en a connaissance, des actions doivent être menées.

Le détail des procédures à mettre en œuvre est défini dans le Plan de Reprise d'Activité. Ce document n'est pas public.

2.3. Exigences relatives au cycle de vie des certificats d'AC Déléguées

2.3.1. Nommage

L'AC Déléguée en cours de certification choisit le contenu du champ « CN » (nom commun) qui sera présent dans son certificat établi par l'AC Racine-4.

Durant toute la durée de vie de l'AC, un DN attribué à une ACD ne peut être attribué à une autre ACD. L'AC Racine-4 vérifie l'unicité du CN demandé avant de valider la demande de certificat de l'AC Déléguée.

2.3.2. Génération d'un certificat pour une AC Déléguée

Toute demande de certification de la part d'une ACD doit recueillir l'accord de l'AA de l'ACR-4.

La demande de certification de la clé publique d'une AC Déléguée doit se faire lors d'un face-à-face, en la présence du responsable sécurité de l'AC Déléguée et d'au moins un témoin de l'Autorité Administrative signataire du procès-verbal de la cérémonie de génération de la clé de l'AC Déléguée et qui atteste par sa présence l'accord de l'AA.

Le dossier d'enregistrement, présenté à l'administrateur central de l'AC Racine-4, doit au moins comprendre :

- La copie de la section du procès-verbal signée et relative à la génération de la clé de l'AC Déléguée,
- Le fichier PKCS#10 signé, afin de prouver la possession de la clé privée. L'empreinte de la clé publique dont la certification est demandée figure dans le procès-verbal précédent,
- Pour le responsable sécurité de la Cérémonie et le témoin de l'Autorité Administrative présent, une pièce d'identité[1], en cours de validité et comportant une photographie.

L'opérateur de l'ACR-4 doit remettre au responsable sécurité de la Cérémonie le certificat une fois qu'il a été généré.

L'utilisation du certificat généré pour l'Autorité Délégué par le responsable Sécurité marque l'acceptation de celui-ci.

[1] Carte Professionnelle d'Identité du Ministère, Carte d'accès à l'un des sites du Ministère comportant nom et photographie, pièce d'identité officielle

2.3.3. Renouvellement d'un certificat d'une AC Déléguée

La demande de renouvellement d'un certificat de la clé publique d'une AC Déléguée est soumise aux mêmes exigences que la demande de certification initiale d'une AC Déléguée.

2.3.4. Révocation d'un certificat d'une AC Déléguée

En cas de compromission réelle ou suspectée d'une clé d'AC Déléguée (vol ou perte), la révocation doit être demandée auprès d'un administrateur de l'ACR-4 par l'AC Déléguée. La clé est compromise (ou suspectée d'être) si elle n'est plus considérée comme sûr : copiée ou diffusée par exemple.

Un administrateur de l'ACR-4 doit alors exécuter la procédure prévue dans le Plan de Reprise d'Activité qui comporte trois phases :

1) L'AC Déléguée doit avertir l'ACR-4 afin que l'un de ses administrateurs exécute la procédure prévue dans ce cas dans le Plan de Reprise d'Activité,
2) L'administrateur d'AC Déléguée doit demander la certification d'une nouvelle clé auprès de l'ACR-4. L'ACR-4 doit alors générer un nouveau certificat pour l'ACD concernée,
3) Lorsqu'un administrateur d'AC Déléguée a terminé l'exécution de la procédure prévue dans ce cas dans le Plan de Reprise d'Activité, alors il doit en informer l'ACR-4 pour que cette dernière termine la procédure décrite dans le plan.

2.4. Exigences relatives au cycle de vie des certificats d'administrateurs de l'AC Racine-4

L'AC Racine-4 est administrée par les administrateurs centraux. Ceux-ci disposent au moins d'un certificat d'authentification logiciel, permettant de s'authentifier de manière forte.

Ces certificats d'authentification sont émis par l'AC Racine-4. A ce titre, les administrateurs centraux sont des *porteurs* de certificats. Chaque porteur utilise son certificat et la privée correspondante dans le cadre de ses activités professionnelles liées aux fonctions d'administration de l'AC Racine-4.

2.4.1. Nommage

Le nommage utilisé au sein des certificats d'administrateur respecte les exigences du document [RGSv2], par le type de noms employés, la nécessité d'employer des noms explicites et l'exigence d'unicité des noms.

En particulier, 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'administrateur central réalisant l'enregistrement.

2.4.2. Génération d'un certificat

L'authentification du nouvel administrateur par l'administrateur assurant l'enregistrement est réalisé lors d'un face-à-face physique, à partir d'une pièce d'identité[2], en cours de validité et comportant une photographie.

L'utilisation du certificat généré par le nouvel administrateur marque l'acceptation de celui-ci.

2.4.1. Mot de passe PKCS12

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

Ce mot de passe complexe d'au moins 12 caractères est ensuite transmis au porteur par un moyen hors ligne (face à face).

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

La remise du certificat se fait par transmission sur clé usb.

2.4.2. Renouvellement d'un certificat

[2] Carte Professionnelle d'Identité du Ministère, Carte d'accès à l'un des sites du Ministère comportant nom et photographie, pièce d'identité officielle

Le renouvellement de la bi-clé d'un porteur entraîne le renouvellement de la bi-clé correspondante ainsi que la génération et la fourniture d'un nouveau certificat.

2.4.3. Révocation d’un certificat

La demande de révocation se fait auprès d’un administrateur central de l’AC Racine-4.

3. MESURES DE SECURITE NON TECHNIQUES

3.1. Mesures de sécurité physique

3.1.1. 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.

3.1.2. 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.

3.1.3. Alimentation électrique et climatisation

Le serveur hébergeant l'ACR-4 sur le site nominal ainsi que son module cryptographique sont arrêtés électriquement lorsque non utilisés.

Les locaux hébergeant l'ACR-4 sont climatisés.

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'ACR-4 telles que fixées par leurs fournisseurs.

3.1.4. Vulnérabilité aux dégâts des eaux

Les locaux hébergeant l'ACR-4 sont protégés contre les dégâts des eaux :

- Par un dispositif de détection d'eau,

- Par le plan de prévention des inondations.

3.1.5. Prévention et protection incendie

Les locaux hébergeant l'ACR-4 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).

3.1.6. Conservation des supports

Les sauvegardes des données et de l'application opérant l'ACR-4 sont conservées dans une enceinte sécurisée, accessible aux seules personnes autorisées.

Les supports papier de l'ACR-4 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'ACR-4, ainsi que les mesures de sécurité qui leur sont appliquées, afin d'en garantir la confidentialité, l'intégrité et la disponibilité.

3.1.7. Mise hors service des supports

Les supports papier et électroniques de l'ACR-4 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'ACR-4 ne sont pas utilisés à d'autres fins avant destruction complète des informations liées à l'ACR-4 qu'ils sont susceptibles de contenir.

3.1.8. Sauvegardes hors site

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

3.2. Mesures de sécurité procédurales

3.2.1. Rôles de confiance relatifs aux Cérémonies des Clés

Les rôles de confiance spécifiques aux Cérémonies des Clés sont décrits dans le document de Cérémonie des Clés. Ce document n'est pas public. Ce document décrit les personnes ayant accès au dit document, ainsi que les mesures de protection mises en œuvre.

3.2.2. Rôles de confiance auprès de l'ACR-4

Les rôles de confiance définis au niveau de l'ACR-4 sont :

Administrateur central : Personne chargée de la configuration applicative et du maintien en conditions opérationnelles de l'application IGC, de l'habilitation des administrateurs centraux, ainsi que de l'analyse régulière des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission. Elle assure également le rôle d'AEL et réalise à ce titre les opérations de gestion des certificats émis par l'AC Racine-4.

Auditeur : Personne désignée par l'Autorité Administrative dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par l'ACR-4 par rapport à la Politique de Certification et à la Déclaration des Pratiques de Certification de l'ACR-4.

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

Responsable de l'application IGC : Personne ayant reçu délégation par l'ACR-4 de la mise en œuvre de la Politique de Certification et de la Déclaration des Pratiques de Certification de l'ACR-4, 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'ACR-4 de la vérification de la

cohérence des actions des différents rôles décrits précédemment et de la qualité des processus de l'ACR-4.

3.2.3. Rôles de confiance mutualisés

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.

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.

3.2.4. 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.

Par ailleurs, toute opération impliquant les secrets principaux de l'ACR-4 nécessite l'intervention de deux administrateurs parmi trois.

La DPC précise les opérations nécessitant l'intervention de plusieurs personnes ainsi que les contraintes que

ces personnes doivent respecter.

3.2.5. 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'application 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.

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

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

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

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

3.3.1. 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.

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 Racine-4.

L'Autorité Administrative de l'AC Racine-4 informe toute personne intervenant dans des rôles de confiance de l'AC :

- De ses responsabilités relatives aux services de l'AC Racine-4,
- Des procédures liées à la sécurité du système et au contrôle du personnel.

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

3.3.2. Vérification de l'adéquation des profils

Le personnel amené à assurer un rôle de confiance vis-à-vis de l'AC Racine-4 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 personnels ne doivent notamment pas avoir 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. Ceci doit être écrit dans leur fiche de poste. Ils reportent au FSSI tout incident sur ce sujet.

3.3.3. Formation initiale

En préalable à leur entrée en fonction, les administrateurs centraux 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.

3.3.4. 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.

3.3.5. Fréquence et séquence de rotation entre différentes attributions

Aucune rotation programmée des attributions n'est prévue.

3.3.6. Sanctions en cas d'actions non autorisées

En cas d'actions non autorisées par le personnel, sont applicables les actions disciplinaires s'il y a lieu.

3.3.7. 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. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

3.3.8. 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.

3.4. Procédures de constitution des données d'audit

Cette section s'applique exclusivement aux événements liés aux certificats objets de la présente Politique.

3.4.1. Types d'évènements enregistrés

3.4.1.1 Enregistrements sur papier ou bureautique

Sont enregistrés sur papier :

- Les opérations et événements survenant à l'occasion des Cérémonies des Clés. Ces enregistrements sont décrits dans le document de Cérémonie des Clés. Ce document n'est pas public.

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 ;
- Mises à jour de la présente PC, au sein du présent document.

3.4.1.2 Enregistrements électroniques par l'application IGC

Toute action sur un dossier lié à un certificat émis par l'ACR-4 est enregistrée, et un historique complet du dossier est conservé dans la base de données de l'ACR-4.

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 ;
- Demande de certificat lors d'une demande initiale ainsi que l'éventuel acceptation ou refus de la demande ;

- Demande de renouvellement de certificat, ainsi que l'éventuelle acceptation ou refus de la demande ;
- Génération des certificats ;
- Demande de révocation ;
- Révocation de certificat ;
- Génération puis publication de la LCR ;
- Modification des droits des personnels autorisés à intervenir auprès de l'application IGC ;
- Modification des paramètres de configuration de l'IGC.

3.4.1.3 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 pour donner suite à une défaillance de la fonction de journalisation ;
- Connexion / déconnexion des détenteurs des rôles de confiance, et les tentatives non réussies correspondantes.

3.4.1.4 Caractéristiques communes

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’événement 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.

3.4.2. Fréquence de traitement des journaux d'évènements

3.4.2.1 Enregistrements sur papier ou bureautique

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

3.4.2.2 Enregistrements électroniques par l’application IGC

L’AC Racine-4 étant arrêtée en dehors des périodes ponctuelles d’utilisation, il n’y a pas lieu de prévoir le contrôle régulier des journaux d’événements.

Le contenu du journal électronique d’événements applicatifs de l’application IGC peut être éventuellement contrôlé avant toute utilisation de la plate-forme afin de vérifier l’absence d’utilisation non autorisée de l’AC Racine-4.

3.4.2.3 Autres enregistrements électroniques

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

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

3.4.3.1 Enregistrements sur papier ou bureautique

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

3.4.3.2 Enregistrements électroniques par l'application IGC

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

.

3.4.3.3 Autres enregistrements électroniques

Les autres journaux d'enregistrement sous forme électronique sont sauvegardés puis purgés chaque début de mois, hormis ceux situés sur la plate-forme de l'ACR-4, non purgés.

3.4.4. Protection des journaux d'évènements

3.4.4.1 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.

3.4.4.2 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.

3.4.4.3 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 »).

3.4.5. Procédure de sauvegarde des journaux d'évènements

3.4.5.1 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.

3.4.5.2 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.

3.4.5.3 Autres enregistrements électroniques

Les autres journaux sous forme électroniques sont sauvegardés par un système centralisé de sauvegardes, hormis ceux hébergés sur la plate-forme de l'ACR-4, non sauvegardés.

3.4.6. Système de collecte des journaux d'évènements

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

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

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

3.4.8. 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'événements est réalisée en cas de détection de compromission ou de suspicion de tentative de compromission de l'application IGC.

3.5. Archivage des données

3.5.1. Types de données archivées

3.5.1.1 Données sous forme papier ou bureautique :

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

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

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

- Les journaux d'événements 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 Racine-4 (i.e. la présente Politique de Certification, la DPC et ses annexes…). L'archivage est sous la responsabilité du responsable de l'application IGC.

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

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

3.5.1.3 Autres données sous forme électronique :

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

Les journaux d'événements autres que ceux de l'application IGC et tels que définis dans la section précédente sont éventuellement sauvegardés selon la procédure définie ci-dessus, mais non archivés.

3.5.2. Période de conservation des archives

3.5.2.1 Dossiers d'enregistrement et certificats

Certificats d'Autorités Déléguées et certificats d'administrateurs de l'ACR-4, émis par l'ACR-4 :

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'ACR-4 lors de toute sollicitation par les autorités habilitées.

Ces dossiers permettent de retrouver :

- L'identité des personnes physiques désignées dans le certificat émis, dans le cas de certificat de personne,
- La dénomination de l'Autorité pour laquelle le certificat a été émis, dans le cas de certificat d'Autorité.

Certificats de composantes :

Les certificats de composantes sont générés ou renouvelés parallèlement à la génération ou au renouvellement de la clé de l'Autorité correspondante. Il n'est donc pas constitué de dossiers d'enregistrement relatifs à ces certificats.

Certificat auto-signé de l'ACR-4 :

Le certificat auto-signé de l'ACR-4 est émis sitôt la génération de la clé de l'Autorité Racine-4. Il n'est donc pas constitué de dossiers d'enregistrement relatifs à ces certificats.

3.5.2.2 LCR émis par l'AC

Les LCR successives produites sont conservées pendant la durée de vie de l'AC.

3.5.2.3 Journaux d'évènements

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

3.5.2.4 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.

3.5.3. Protection des archives

Pendant tout le temps de leur conservation, les archives :

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

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

3.5.4. Procédure de sauvegarde des archives

3.5.4.1 Données sous forme papier ou bureautique

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

3.5.4.2 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 3.4.5.

3.5.5. Datation des données

3.5.5.1 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 minute.

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

La datation des données est réalisée selon les modalités définies au 4.7.

3.5.6. Système de collecte des archives

3.5.6.1 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 pendant 5 ans.

3.5.6.2 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.

3.5.7. 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.

3.5.7.1 Données sous forme papier ou bureautique

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

3.5.7.2 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.

3.6. Changement de clé d'ACR-4

Le renouvellement du certificat d'ACR-4 et de sa bi-clé privée sera planifié de façon que le certificat auto-signé de l'ACR-4 soit valide au plus tard lors de la fin de validité de tous les certificats qu'elle a émis et de façon à pouvoir émettre des certificats sans discontinuité.

La nouvelle bi-clé générée servira à signer les nouveaux certificats 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.

3.7. Reprise à la suite de compromission et sinistre

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

L'infrastructure hébergeant l'AC Racine-4 est hors-ligne et arrêtée entre chaque période ponctuelle d'utilisation. Il n'est donc pas mis en œuvre dans ce cadre de dispositif de remontée des incidents.

Ponctuellement, les administrateurs centraux de l'AC Racine-4 peuvent mettre 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, par exemple avant utilisation de l'AC Racine-4.

Les procédures de traitement des incidents et des compromissions font l'objet du Plan de Reprise d'Activité de l'IGC. Ce document n'est pas public.

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.

3.7.2. 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.

3.7.3. 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 la compromission de sa clé privée (vol ou perte), l'AC Racine-4 procède à sa cessation d'activité, et en informe selon tout moyen à sa disposition, les Autorités Déléguées rattachées, les porteurs et tiers utilisateurs des certificats de l'IGC.

3.7.4. Capacités de continuité d'activité à la suite d'un sinistre

En cas d'incident impactant l'infrastructure de l'AC Racine-4, les services de l'AC Racine-4 peuvent être restaurés sur une infrastructure semblable dans un délai inférieur à 8 jours en période ouvrée, permettant le respect des exigences de la présente PC en matière de disponibilité des fonctions de l'IGC, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

3.8. Fin de vie de l'ACR-4

Dans l'hypothèse d'une cessation d'activité totale, l'ACR-4 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'ACR-4 :

1) S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats ;
2) Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;

3) Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;

4) Publie cette information sur le site web igc.social.gouv.fr.

4. MESURES DE SECURITE TECHNIQUES

4.1. Génération des bi-clés

4.1.1. Génération des bi-clés des Autorités

La génération des clés de signature des Autorités est effectuée dans un environnement sécurisé.

Les clés de signature d'ACR-4 sont générées et mises en œuvre dans un module cryptographique conforme aux exigences de la RGS v2.

La génération de la clé de signature de l'ACR-4 est effectuée dans des circonstances contrôlées, par des personnels dans des rôles de confiance, dans le cadre de « Cérémonies de Clés ». Ces Cérémonies se déroulent suivant des scripts préalablement définis. Ces documents ne sont pas publics.

L'initialisation de l'IGC et/ou des boitiers HSM s'accompagne 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'AA. Un même porteur ne peut détenir plus d'une part de secrets d'un 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 DPC.

4.1.2. Transmission de la clé publique d'une ACD à l'ACR-4

Lors de la transmission de la clé publique d'une ACD vers l'ACR-4 en vue de sa certification, son origine est authentifiée.

4.1.3. Transmission des clés publiques des ACD et de l'ACR-4 aux utilisateurs de certificat

La clé publique de l'ACR-4 est contenue dans un certificat signé par l'AC Racine-4 (certificat auto-signé). La clé publique d'une ACD est diffusée dans un certificat signé par l'AC Racine-4.

Ces clés publiques sont notamment disponibles depuis le site web igc.social.gouv.fr.

4.1.4. Tailles des clés

Les clés des certificats suivants respectent les exigences de caractéristiques (tailles, algorithmes, etc.) de la RGSv2 B1 et sont de type :

RSA de 4096 bits.

- Certificat auto-signé de l'AC Racine-4,
- Certificats des Autorités Déléguées,
- Certificats des composantes,

RSA de 2048 bits.

- Certificats des administrateurs de l'AC Racine-4.

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

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

4.1.6. Objectifs d'usage des clés

L'utilisation des clés privées des différentes Autorités et des certificats associés est strictement limitée à la signature de certificats et de LCRs.

L'utilisation des clés privées et des certificats des composantes associés est strictement limitée à la sécurisation des échanges entre composantes.

L'utilisation des clés privées et des certificats des administrateurs centraux de l'AC Racine-4 associés est strictement limitée au service d'authentification auprès des services de l'AC Racine-4.

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

4.2.1. Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'ACR-4 pour la génération et la mise en œuvre de ses clés de signature, répondent au minimum aux exigences de l'annexe B2 du document [RGSv2]. Les cartes cryptographiques utilisées ont été évaluées selon les Critères Communs au niveau EAL4+.

Les clés privées d'AC ne sont ni séquestrées, ni archivées.

4.2.2. Dispositifs d'authentification des administrateurs centraux de l'AC Racine-4

Les clés et certificats des administrateurs centraux de l'ACR-4 sont stockés au sein de leurs magasins respectifs de certificats Windows, fournies aux administrateurs centraux lors de leur enregistrement.

L'accès à ce certificat nécessite un mot de passe de 12 caractères minimum.

En dehors des temps d'opérations sur l'AC Racine 4, les clés et certificats des administrateurs centraux de l'ACR-4 sont conservés au format p12 sur clé USB, elle-même stockée en lieu sûr.

4.3. Autres aspects de la gestion des bi-clés

4.3.1. Archivage des clés publiques

Les clés publiques de l'ACR-4 et des ACD sont archivées dans le cadre de l'archivage des certificats correspondants.

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

Les certificats de l'ACR-4 couverts par la présente PC ont une durée de validité de vingt ans.

La durée de validité des certificats des ACD et de leurs composantes est de dix ans.

La durée de validité des certificats des administrateurs centraux de l'AC Racine-4 est de huit ans.

4.4. Données d'activation des clés d'AC

4.4.1. 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.

4.4.2. 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.

4.5. Mesures de sécurité des systèmes informatiques

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

- Identification et authentification forte des détenteurs de rôles de confiance pour l'accès à la plate-forme de l'IGC,
- Identification et authentification forte des administrateurs centraux pour l'accès à l'application IGC,
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels,
- Gestion des comptes des 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 (imputabilité des actions effectuées),
- Gestion des incidents,
- Protection en confidentialité, en intégrité et en disponibilité des clés nécessaires au fonctionnement de l'AC Racine-4.

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

4.6.1. 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.

4.6.2. 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.

4.7. Système de datation

La datation des évènements enregistrés par les différentes fonctions de l'AC dans les journaux est basée sur l'heure système de la plate-forme hébergeant l'AC et vérifiée avant toute utilisation avec une précision inférieure à 1 minute. Il n'est pas mis en œuvre de mécanisme de synchronisation.

5. PROFILS DES CERTIFICATS EMIS PAR L'AC RACINE-4

Les profils :

- Du certificat auto-signé de l'AC Racine-4,
- Des certificats des Autorités Déléguées émis par l'AC Racine-4,
- Des LCR émises par l'AC Racine-4,
- Des certificats d'authentification des administrateurs centraux de l'AC Racine-4,
- Des certificats de composantes des Autorités figurent dans le document séparé [PC-profils].

Ce document fait référence à 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.

6. AC RACINE-4 : AUDITS INTERNES ET DE CONFORMITE

L'Autorité Administrative de l'AC Racine-4 fait contrôler la conformité de son AC avec les exigences de la présente PC.

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.

6.1. Audits internes

Le présent chapitre ne concerne que les audits et évaluation *internes* de la responsabilité de l'AC Racine-4 afin de s'assurer du bon fonctionnement de son AC.

6.1.1. Fréquences et / ou circonstances des évaluations

À la suite de la première mise en service de l'application IGC ou à la suite de toute modification significative de celle-ci ou des procédures fonctionnelles applicables, l'Autorité Administrative de l'AC Racine-4 fait procéder à un audit interne global ou limité au périmètre de l'impact de la modification.

L'Autorité Administrative de l'AC Racine-4 fait aussi procéder régulièrement à un audit interne de l'ensemble de son AC, une fois tous les deux ans.

6.1.2. 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 Racine-4 à une équipe d'auditeurs, compétents en sécurité des systèmes d'information et dans le domaine couvert par le périmètre à auditer.

6.1.3. Relations entre évaluateurs et entités évaluées

L'auditeur ne doit pas posséder de rôle de confiance auprès de l'AC Racine-4 autre que le présent rôle et doit être dûment autorisé à pratiquer les contrôles visés.

6.1.4. Sujets couverts par les évaluations

Les audit internes portent sur un rôle, une procédure, une fonction de l'AC Racine-4 ou sur l'application IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans la présente PC et dans la DPC associée, ainsi que des éléments qui en découlent (procédures opérationnelles, ressources déployées, etc.).

6.1.5. 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 Racine-4 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 Racine-4 et doit respecter ses politiques de sécurité internes.
- En cas de résultat « A confirmer », l'auditeur remet à l'Autorité Administrative de l'AC Racine-4 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 Racine-4 la conformité aux exigences de la présente PC et la DPC associée.

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.

6.1.6. Communication des résultats

Les résultats des audits internes ne sont communiqués qu'à la discrétion de l'Autorité Administrative de l'AC Racine-4.

7. AUTRES PROBLEMATIQUES METIERS ET LEGALES

7.1. Confidentialité des données professionnelles

7.1.1. 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.

7.1.2. Responsabilités en termes de protection des informations confidentielles

La présente PC ne formule pas d'exigence supplémentaire au respect de la législation et de la réglementation en vigueur sur le territoire français relatives à la protection des informations confidentielles.

7.1.3. Politique de protection des données personnelles

Toute collecte et tout usage de données à caractère personnel par l'AC et les rôles de confiance de l'AC sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.

En particulier, l'IGC 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 Libertés ».

Le récépissé de cette déclaration porte le numéro : 1245693.

7.1.4. Informations à caractère personnel

Les informations considérées comme personnelles sont les suivantes :

- Les causes de révocation des certificats des administrateurs centraux de l'AC Racine-4 ;
- Le dossier d'enregistrement des administrateurs centraux de l'AC Racine-4.

7.1.5. Informations à caractère non personnel

Sont considérées comme non personnelles l'ensemble des informations n'étant pas identifiées comme personnelles.

7.1.6. Responsabilité en termes de protection des données personnelles

La présente PC ne formule pas d'exigence supplémentaire au respect de la législation et de la réglementation en vigueur sur le territoire français relatives à la protection des données personnelles.

7.1.7. Notification et consentement d'utilisation des données personnelles

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

7.1.8. 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.

7.1.9. Autres circonstances de divulgation d'informations personnelles

Le dossier d'enregistrement d'un administrateur central peut faire l'objet d'une divulgation auprès de la hiérarchie de cet administrateur.

7.2. Droits sur la propriété intellectuelle et industrielle

La présente PC ne formule pas d'exigence supplémentaire au respect de la législation et la réglementation en vigueur sur le territoire français.

7.3. Limite de responsabilité

L'objectif de l'AC Racine-4 est d'émettre des certificats à destination des Autorités Déléguées composant l'IGC IMAGE.

L'AC est responsable en cas de négligence ou de faute intentionnelle des préjudices causés à une personne physique ou morale qui s'est fiée raisonnablement à ses certificats. La responsabilité de l'AC pourra être mise en jeu si un des rôles de confiance 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 évènement irrésistible, insurmontable et imprévisible.

7.4. Indemnités

Les indemnités sont à l'appréciation des tribunaux compétents.

7.5. Durée et fin anticipée de validité de la PC

7.5.1. 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.

7.5.2. 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.

7.6. Amendements à la PC

7.6.1. Procédures d'amendements

La procédure d'amendement à la PC est initiée par l'Autorité Administrative ou par l'AC.

En cas de changement important, l'AC s'engage à faire appel à un auditeur pour en contrôler l'impact.

7.6.2. Mécanisme et période d'information sur les amendements

Les tiers utilisateurs de certificat peuvent prendre connaissance des amendements au moyen du site web igc.sante.gouv.fr.

7.6.3. 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, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) ou du document décrivant les profils associés se traduira par une évolution de l'OID. Ainsi, les tiers utilisateurs de certificat pourront clairement distinguer quels certificats correspondent à quelles exigences.

7.7. Dispositions concernant la résolution de conflits

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

7.8. Juridictions compétentes

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

7.9. 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).

8. AC DELEGUEES : EXIGENCES RELATIVES AU CYCLE DE VIE DES CERTIFICATS D'AUTORITES DELEGUEES

8.1. Génération des clés, demande et installation des certificats d'Autorités Déléguées

L'AC Déléguée doit s'assurer auprès de l'AA de l'ACR-4 que le nom qu'elle propose d'utiliser pour s'identifier, et qui est contenu dans le champ CN de son certificat, n'est pas déjà réservé pour un autre AC Déléguée.

Les opérations suivantes :

- génération des bi-clés d'une ACD et émission de la demande de certificat correspondante,

- installation du certificat à la suite de sa génération par l'AC Racine-4

s'inscrivent dans le cadre d'une cérémonie des clés. Le but de cette cérémonie est de générer une bi-clé ainsi qu'un fichier de demande de certificat, et de créer un procès-verbal de demande de certificat.

Le résultat de la première opération est constitué :

- D'un procès-verbal signé de la cérémonie de génération de la clé de l'AC Déléguée et incluant l'empreinte de la clé publique dont la certification est demandée à l'AC Racine-4,
- D'un fichier PKCS#10 signé.

Le résultat de la seconde étape donne lieu à l'établissement d'un procès-verbal signé.

La cérémonie permet de réaliser des copies de secours des clés privées et des certificats des Autorités Déléguées, ainsi que d'initialiser les modules de sécurité de l'infrastructure.

La cérémonie est conduite par un maître de cérémonie.

La cérémonie implique la présence d'au moins les personnes tenant les rôles suivants :

- Témoins de l'Autorité Administrative, garants du déroulement conforme de la cérémonie ;

- Opérateurs de l'IGC et des modules de sécurité, garants du fait que les systèmes (matériels, logiciels et modules de sécurité) sont correctement configurés et opérationnels ;
- Responsable sécurité pour la cérémonie, garant du bon déroulement de la cérémonie sur le plan de la sécurité.
- Détenteurs de secrets et de supports sensibles.

L'ACD s'engage à établir un descriptif complet de chaque cérémonie. Ce document n'est pas public.

L'ACD s'engage à émettre des procès-verbaux pour chaque étape importante du processus. Ces documents ne sont pas publics.

8.2. Renouvellement des clés, demande et installation des certificats

Les exigences concernant cette cérémonie sont identiques à la cérémonie décrite ci-dessus.

La valeur du champ qui identifie l'ACD, le champ DN du certificat, doit être identique à la valeur du champ DN utilisée précédemment.

8.3. Révocation du certificat d'une ACD

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

1) Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
2) Au moins l'un des éléments permettant de reconstituer la clé secrète a été perdu ou volé ;
3) Un module de sécurité a été utilisé frauduleusement.

Lorsqu'une des circonstances ci-dessus se réalise et qu'un détenteur de rôle de confiance auprès de l'ACD en a connaissance, il doit immédiatement en informer l'ACR-4 et une nouvelle bi-clé doit être créée. Une cérémonie des clés doit être organisée par l'ACR-4 pour créer le nouveau certificat d'ACD.

L'ACD doit ensuite suivre une procédure spécifique selon la nature des certificats qu'elle génère, aboutissant à la révocation de son certificat par l'AC Racine-4.

Le détail des procédures à suivre est défini, d'une part dans le Plan de Reprise d'Activité de l'IGC. Ce document n'est pas public.

8.4. Mise à disposition des informations publiées

Dans le cadre de cette PC, l'ACD ne met à disposition aucune information. Les informations qui la concernent sont mises à disposition par l'ACR-4.

9. TOUTES AC : EXIGENCES RELATIVES AU CYCLE DE VIE DES CERTIFICATS DE COMPOSANTES DE L'IGC

9.1. Introduction : Architecture générale de l'infrastructure technique de l'IGC

L'infrastructure technique de l'IGC est composée de deux plates-formes indépendantes :

- L'une dédiée à l'AC Racine-4, et
- L'autre dédiée aux AC Déléguées.

9.1.1. Composantes internes pour chaque AC

Chaque AC (ACR-4 ou AC Personnes-3) comporte les composants internes suivants :

- Des composantes assurant les services d'AEL. Elles permettent d'effectuer des demandes de création de certificat, de renouvellement de certificat ou de révocation de certificat.
- Une composante assurant les services de certification et de signature de LCR, ainsi que de signature des réponses OCSP dans le cas des Autorités Déléguées.
- Une composante de publication des certificats émis.
- Une composante d'administration (gestion des droits auprès des composantes de l'Autorité concernée).
- Une composante permettant l'accès à la journalisation d'événements de l'Autorité concernée.

L'ensemble de ces composantes est disponible par service https et après authentification par certificat émis par l'Autorité à laquelle est liée la composante.

9.1.2. Architecture de l'AC Racine-4

L'infrastructure de l'AC Racine-4 est « hors-ligne ».

9.1.3. Architecture des AC Déléguées

Chaque serveur web hébergeant une ou plusieurs composantes d'AC Déléguées dispose d'un certificat SSL émis selon les conditions de la PC Infrastructure Authentification.

9.2. Exigences sur les échanges de données entre composantes

Les échanges de données entre composantes au sein de l'IGC répondent aux exigences présentées ci-après. Des précisions sont apportées dans la DPC.

9.2.1. Protection des données échangées entre composantes

Les échanges entre les différentes composantes de chaque AC doivent être protégés :

- En intégrité,
- En confidentialité,
- Avec garantie de l'origine.

De même, les échanges entre les utilisateurs « humains » d'une composante (administrateurs centraux) et cette composante doivent être protégés selon les mêmes dispositions.

Les certificats d'authentification et de chiffrement SSL des composantes de chaque AC sont émis par l'Autorité concernée.

Les certificats d'authentification et de chiffrement TLS des serveurs Web sont émis par :

- L'AC Infrastructure-4 pour les serveurs Web utilisés par les AC Déléguées ; selon la Politique de Certification de l'AC Infrastructure - Service Authentification, d'OID : 1.2.250.1.179.1.3.1.1.4 ;
- L'AC Racine-4 pour les serveurs Web utilisés par l'AC Racine-4, selon la présente PC.

9.2.2. Dispositions applicables aux certificats de composantes

Ces dispositions s'appliquent à chaque Autorité pour ses propres composantes :

Génération : Lors de l'installation, les certificats d'authentification SSL des composantes sont générés lors de l'installation de l'Autorité concernée et sont signés par la clé privée de cette Autorité.

Renouvellement : Le renouvellement de l'ensemble de ces certificats d'authentification est effectué simultanément à chaque changement de clé de l'Autorité concernée.

Révocation : La suspicion de compromission d'un certificat de composante entraîne la mise en œuvre des procédures détaillées dans le Plan de Reprise d'Activité de l'IGC. Ce document n'est pas public.

9.2.3. Protection des données échangées avec la base de données

Les communications entre les composantes et la base de données doivent protégées en intégrité et en confidentialité.

9.2.4. Protection des données échangées entre sites

Les informations de la base de données sont répliquées en mode quasi-temps réel entre sites. Les informations échangées doivent être protégées en intégrité et en confidentialité.

10. OBLIGATIONS RESPECTIVES

10.1. Obligations applicables à l'AA de l'AC Racine-4

Les obligations de l'AA de l'IGC IMAGE sont :

- Approuver la PC de l'ACR-4 et des composantes de l'IGC IMAGE (le présent document) ;
- Approuver la DPC de l'ACR-4 et des composantes de l'IGC IMAGE.
- Définir les exigences minimales applicables aux AC Déléguées souhaitant obtenir un certificat de l'ACR-4 de l'IGC IMAGE ;
- Décider des sanctions à appliquer lorsqu'un détenteur de rôle de confiance auprès de l'AC Racine-4 abuse de ses droits ou effectue une opération non conforme à ses attributions ;
- Prononcer si nécessaire la décision de révocation de l'ACR-4 ou/et de ses composantes ;
- Déclarer si nécessaire la cessation d'activité de l'ACR-4.

10.2. Obligations applicables à l'AC Racine-4

L'ACR-4 de l'IGC IMAGE s'oblige à :

- Elaborer et respecter les exigences définies dans la présente PC et la DPC afférente ;
- Elaborer la DPC relative à la présente PC, et garantir et maintenir la cohérence entre cette DPC et la présente PC ;
- Demander l'autorisation à l'AA pour toute évolution de son système ;
- Protéger ses clés privées et leurs moyens d'activation en intégrité et en confidentialité ;
- Utiliser ses clés publiques et privées, et ses certificats, aux seules fins pour lesquelles ils ont été émis et avec les outils spécifiés, conformément à la présente PC ;
- Assurer la disponibilité de son certificat auto-signé ;

- Mettre à la disposition d'un utilisateur de certificat la présente PC afin de lui permettre d'apprécier la confiance à accorder à un certificat ;
- Procéder à un changement de certificat auto-signé en cas de compromission, suspicion de compromission, vol, perte des moyens de reconstitution de la clé privée de l'ACR-4 (perte du secret principal, perte du code d'activation et perte de plus de deux secrets partagés) ;
- Documenter les schémas de certification qu'elle entretient avec les AC Déléguées ;
- Vérifier la complémentarité des clés publique et privée d'une AC Déléguée souhaitant être certifiées par l'AC Racine-4 ;
- Générer le certificat d'une AC Déléguée dès lors que les conditions de certification posées dans la PC sont remplies par l'AC Déléguée ;
- Renouveler le certificat d'une AC Déléguée dès lors que les conditions de renouvellement du certificat posées dans la PC sont remplies par l'AC Déléguée ;
- Obtenir confirmation de l'acceptation du certificat par l'AC Déléguée sous la forme d'un accord signé ;
- Révoquer le certificat d'un AC Déléguée selon les conditions posées et dans le respect des procédures déterminées dans la présente PC ;
- Enregistrer et archiver les informations pertinentes ;
- Respecter les impératifs des contrôles ;
- Respecter les conditions de disponibilité définies dans la présente PC et la DPC afférente ;
- Publier des informations authentiques et intègres.

10.3. Obligations des administrateurs centraux de l'AC Racine-4

Les administrateurs centraux de l'AC Racine-4 IMAGE, dans le cadre de leur rôle d'AEL, 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 vérifier l'identité du demandeur de demande de génération de certificat,

- De vérifier l'identité du demandeur de demande de révocation de certificat,
- D'assister les demandeurs de certificats dans l'utilisation et la gestion des certificats,
- De respecter les exigences décrites dans les documents de cérémonies des clés,
- De conserver et protéger en confidentialité et en intégrité les données d'identification transmises pour l'enregistrement,
- Enregistrer et archiver ces informations conformément à la présente PC, et notamment les demandes de certificats d'AC Déléguées.

Note : les administrateurs centraux de l'AC Racine-4 IMAGE, dans leur rôle d'AEL, assurent l'enregistrement des Autorités Déléguées et des nouveaux administrateurs centraux de l'AC Racine-4 IMAGE.

10.4. Obligations applicables aux AC Déléguées

La présente section définit les obligations applicables à chaque Autorité Déléguée dans le cadre de la présente PC, et donc relatives à :

- Sa qualité d'Autorité subordonnée à l'Autorité Racine-4,
- La gestion de ses certificats de composantes.

Chaque AC Déléguée s'oblige donc, dans le cadre de la présente PC, à :

- Respecter les exigences définies dans la présente PC et la DPC afférente ;
- Protéger ses clés privées et leurs moyens d'activation en intégrité et en confidentialité ;
- Utiliser ses clés publiques et privées, et ses certificats, aux seules fins pour lesquelles ils ont été émis et avec les outils spécifiés, conformément à la présente PC ;
- Contrôler les accès physiques aux locaux hébergeant les composantes de l'IGC IMAGE et les limiter aux personnels autorisés ;
- Enregistrer et archiver les informations pertinentes ;
- Demander la révocation de son certificat en cas de compromission, suspicion de compromission, vol,

perte des moyens de reconstitution de la clé privée de l'ACD (perte du secret principal, perte du code d'activation et perte de plus de deux secrets partagés) ;

- Prendre toutes les mesures raisonnables pour s'assurer que les détenteurs de rôle de confiance auprès de l'AC ont connaissance de leurs droits et obligations conférés de par l'attribution de ce rôle.

Les obligations applicables à chaque Autorité Déléguée relatives à son propre rôle d'Autorité sont définies au sein des Politiques de Certifications émises par l'Autorité Déléguée elle-même.

10.5. Obligations applicables aux demandeurs de certificats d'ACD

Les demandeurs de certificats d'ACD ont le devoir de respecter les exigences décrites dans les documents de cérémonies des clés. Ces documents ne sont pas publics.

10.6. Obligations applicables aux porteurs de certificats

Les porteurs de certificats sont les administrateurs centraux de l'AC Racine-4.

En tant que porteurs de certificats d'authentification émis par l'AC Racine-4, ils ont le devoir de respecter les obligations suivantes :

- Conserver de façon sûre leur certificat d'authentification
- Signaler sans délai toute suspicion de vol, perte ou tentative de compromission de leur certificat logiciel d'authentification,
- Suivre les procédures et directives du responsable de l'application IGC, notamment pour le renouvellement du certificat d'authentification.

10.7. Obligations applicables aux tiers utilisateurs

Les tiers utilisateurs tels que définis dans la présente PC doivent :

- Vérifier et respecter les usages pour lesquelles un certificat a été émis,
- Contrôler la validité du certificat utilisé :
  - Par contrôle de la signature par l'AC émettrice,
  - Par contrôle des dates de validité du certificat,
  - Par contrôle de l'absence de révocation, d'après la dernière LCR en cours de validité émis par l'AC émettrice,
- Contrôler de la même façon chaque certificat de la chaîne de certification, jusqu'au certificat auto-signé Racine-4.

La fréquence des interrogations de la LCR (liée à la durée de validité des informations éventuellement gardées dans un cache) est à l'appréciation des tiers utilisateurs de certificats selon les contraintes liées à leur application.