MINISTÈRE
DE L'ÉCONOMIE
DES FINANCES
ET DE LA RELANCE

Liberté
Égalité
Fraternité

Secrétariat général

Service d'émission de certificats qualifiés des ministères économiques et financiers

AC RACINE MEF QUALIFIEE (1.2.250.1.131.1.11.1.3.1.1)

Politique de Certification

AC Racine MEF Qualifiée

v1.1
Diffusion : publique

TABLE DES MATIERES

1 INTRODUCTION

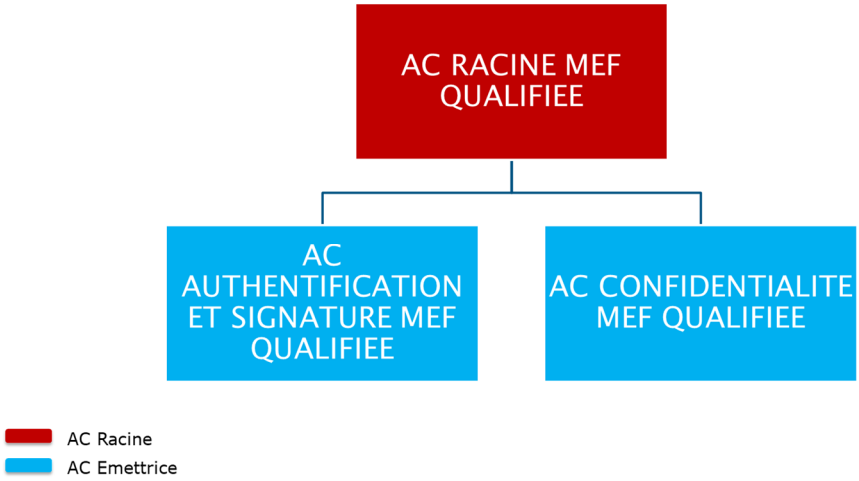
1.1 Présentation générale

Le Ministère de l'Economie, des Finances et de la Souveraineté Industrielle et Numérique (MEFSIN) met en œuvre un service d'émission de certificats électroniques afin de doter l'ensemble des personnels des différentes entités des Ministères économiques et financiers (MEF) de certificats qualifiés au sens du Référentiel Général de Sécurité (RGS** pour l'authentification-signature et RGS* pour la confidentialité) et de la règlementation européenne eIDAS.

Ces certificats sont délivrés à travers la nouvelle carte Rossignol destinée aux agents du MEFR et aux prestataires externes intervenant au sein des MEF. Cette carte est mise en œuvre sous deux formes (sans impact sur les caractéristiques des certificats) :

- Une carte agent, permanente, destinée aux agents des MEF connus dans les annuaires internes des MEF.
- Une carte temporaire (graphiquement différente) destinée aux agents et prestataires des MEF, qu'ils soient connus ou non des annuaires internes des MEF.

Le service d'émission de certificats des MEF s'appuie sur la hiérarchie d'Autorités de Certification qualifiées suivante pour délivrer des certificats pour les usages d'authentification, de signature électronique et de confidentialité :



Le présent document constitue la Politique de Certification (PC) de l'Autorité de Certification Racine « *AC RACINE MEF QUALIFIEE* » des MEF et contient les informations publiques de la Déclaration des Pratiques de Certification (DPC) associée.

La structure du présent document est basée sur les préconisations de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) relatives à l'application du Référentiel Général de sécurité (RGS).

Dans le cadre de la présente PC, l'AC « *AC RACINE MEF QUALIFIEE* » délivre exclusivement des certificats d'Autorités de Certification.

Cette Politique de Certification a vocation à être consultée et examinée par les organismes ou les personnes qui utiliseront ces certificats pour les aider à apprécier le degré de confiance qu'ils peuvent placer dans ces certificats.

1.2 Identification du document

La présente PC est identifiée par l'OID suivant : [1.2.250.1.131.1.11.1.3.1.1].

1.3 Définitions et acronymes

1.3.1 Acronymes

Les acronymes utilisés dans ce document sont présentés dans le tableau suivant :

AC	Autorité de certification
AE	Autorité d'enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ARL	Authority Revocation List, ou LAR
CS	Comité de Surveillance
CN	Common Name
CRL	Certificate Revocation List, ou LCR
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
LAR	Liste des certificats d'AC révoqués, ou ARL
LCR	Liste des Certificats Révoqués
OCSP	Online Certificate Status Protocol
OrgID	Organization Identifier
OID	Object Identifier
OU	Organizational Unit
PC	Politique de certification
PSCE	Prestataire de services de certification électronique
RGPD	Règlement Général sur la Protection des Données
RSA	Rivest Shamir Adelman
SHA256	Secure Hash Algorithm 256
SP	Service de publication
SSI	Sécurité des systèmes d'information
URL	Uniform Resource Locator

1.3.2 Définitions

Les termes utilisés dans ce document sont présentés dans le tableau suivant :

Entrée	Définition
Algorithme RSA	Inventé en 1978 par Ronald L. Rivest, Adi Shamir et Leonard M. Adleman. Il peut être utilisé pour chiffrer des informations et/ou pour les signer (signature numérique).
Autorité de certification (AC)	Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre 1.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.
Autorité de certification émettrice	Autorité de certification dont le certificat est signé par l'autorité de certification racine. Une autorité de certification émettrice signe les certificats des porteurs.
Autorité de certification Racine	Autorité de certification dont le certificat est auto-signé. L'autorité de certification racine signe les certificats des autorités de certification émettrices.
Autorité d'enregistrement (AE)	Cf. paragraphe 1.4.2.
Bi-clé	Ensemble constitué d'une clé publique et d'une clé privée, formant une paire indissociable utilisée par un algorithme cryptographique asymétrique.
Comité de Surveillance	Entité du MEFR en charge de la validation des politiques de certification.
Certificat électronique	Document sous forme électronique attestant du lien entre une clé publique et l'identité de son propriétaire. Cette attestation prend la forme d'une signature électronique réalisée par un prestataire PSCE. Il est délivré par une Autorité de Certification. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Les usages des certificats électroniques régis par le présent document sont le double usage signature électronique + authentification et la confidentialité.
Clé privée	Composant confidentiel d'une bi-clé, connu uniquement de son propriétaire et utilisé par lui seul pour déchiffrer une donnée dont il est destinataire ou pour signer des données dont il est l'auteur.

Entrée	Définition
Clé publique	Composant non confidentiel d'une bi-clé, pouvant être communiqué à tous les membres d'une population. Une clé publique permet de chiffrer des données à destination du porteur de la bi-clé. Elle permet également de vérifier une signature apposée par le porteur.
Composante	Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction du service d'émission de certificats.
Liste des certificats révoqués	Certificate Revocation List ou Liste de Certificats Révoqué (LCR) Liste des numéros de certificats ayant fait l'objet d'une révocation. La LCR est signée par l'autorité de certification pour assurer son intégrité et son authenticité.
Déclaration des pratiques de certification (DPC)	Ensemble des pratiques à mettre en œuvre pour satisfaire aux exigences de la PC.
Politique de certification (PC)	Ensemble de règles qui indique les conditions d'applicabilité d'un certificat pour une communauté donnée ou pour des applications ayant des besoins de sécurité communs.

1.4 Entités intervenant dans l'infrastructure de gestion de clés

Ce paragraphe présente les entités intervenant dans le service d'émission de certificats des MEF, ainsi que les obligations auxquelles elles sont soumises.

1.4.1 Autorités de certification

Dans le cadre de la présente Politique de Certification, le Ministère de l'Economie, des Finances et de la Relance endosse le rôle d'Autorité de Certification (*AC*).

L'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.
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.

L'AC s'appuie sur les services fonctionnels suivants :

- **Autorité d'enregistrement (AE)** (*aussi appelée « service d'enregistrement »*) - Cette fonction vérifie les informations d'identification de la future Autorité de Certification Subordonnée pour laquelle le certificat est émis, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate du service, en fonction des services rendus et de l'organisation du service.
- **Fonction de génération des certificats** - Cette fonction génère (*création du format, signature électronique avec la clé privée de l'AC*) les certificats de l'AC Racine, des AC Subordonnées à partir des informations transmises par l'Autorité d'Enregistrement.
- **Fonction de génération des éléments secrets** - Cette fonction génère les éléments secrets à destination de l'AC Racine, des AC Subordonnées.
- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées, les politiques et pratiques publiées par l'AC Racine, les certificats d'AC et toute autre information pertinente destinée aux AC Subordonnées et/ou aux utilisateurs de certificats, hors informations d'état des certificats.
- **Fonction de gestion des révocations** - Cette fonction 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 utilisateurs de certificats des informations sur l'état des certificats (*révoqués, suspendus, etc.).* Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (*LCR, LAR*) et éventuellement également selon un mode requête-réponse temps réel (*OCSP*).

Dans le cadre de ses fonctions opérationnelles, l'AC veille au respect des exigences suivantes en tant que responsable du service d'émission de certificats :

- Être une entité légale au sens de la loi française.
- Être en relation par voie contractuelle ou hiérarchique ou réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats des services applicatifs de cette entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux AC Subordonnées, aux porteurs finaux, aux utilisateurs de certificats, ceux qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes du service et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions obligatoires de la présente PC, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats.
- Élaborer, mettre en œuvre, contrôler et maintenir les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels.

- Mettre en œuvre ce qui est nécessaire pour respecter les engagements définis dans sa PC, notamment en termes de fiabilité, de qualité et de sécurité.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (*signature de certificats, de LAR*). Diffuser son certificat d'AC aux AC Subordonnées, aux porteurs finaux et aux utilisateurs de certificats.
- Suivre les demandes en capacité et réaliser des projections concernant les futurs besoins en capacité afin de garantir la disponibilité du service, notamment en matière de capacités de traitement et de stockage.

1.4.2 Autorité d'enregistrement

L'AE a pour rôle de vérifier les informations de la future AC Subordonnée. Pour cela, l'AE assure les tâches suivantes :

- La prise en compte et la vérification des informations de la future AC Subordonnée,
- La prise en compte et la vérification des informations des représentants légaux ou des représentants habilités de l'AC Subordonnée,
- L'établissement et la transmission des demandes afférentes à un certificat à la fonction adéquate du service d'émission de certificats,
- L'archivage des pièces du dossier d'enregistrement (*ou l'envoi vers la composante chargée de l'archivage*).

1.4.3 Autorité de Certification Subordonnée

Dans le cadre de la présente PC, le bénéficiaire de certificat ne peut être qu'une Autorité de Certification Subordonnée.
Un certificat d'AC Subordonnée ne peut être délivré qu'aux MEF.
La Politique de Certification et la Déclaration des Pratiques de Certification de l'AC Subordonnée doivent être fournies à l'AC Racine pour valider que les exigences sont cohérentes avec celles de la présente PC.

1.4.4 Utilisateurs de certificats

Sont appelés utilisateurs, les personnes physiques ou automates qui s'appuient sur les certificats d'AC délivrés par l'AC Racine pour vérifier l'origine et la validité des certificats d'utilisateurs finaux délivrés pour leurs propres besoins.

Les utilisateurs des AC Subordonnées sont précisés dans leurs PC respectives.

1.4.5 Autres participants

1.4.5.1 Composantes du service d'émission de certificats

Les composantes du service d'émission de certificats des MEF sont décrites dans le chapitre 1.4.1.

1.4.5.2 Opérateur de Service de Certification

Le MEFR s'appuie sur un acteur externe pour la mise à disposition et l'exploitation de du service d'émission de certificats. Cet acteur endosse le rôle d'Opérateur Technique (*OT*) et dispose de l'expertise nécessaire pour prendre en charge les services permettant d'assurer la génération et la révocation des certificats.

L'OT est en charge du bon fonctionnement du service d'émission de certificats, de la sécurité des moyens techniques ainsi que de la sécurité des personnels et des locaux.

1.5 Usage des certificats

1.5.1 Domaines d'utilisation applicables

1.5.1.1 Bi-clés et certificats des AC Subordonnées

Les bi-clés et certificats des AC Subordonnées émis dans le cadre de la présente PC couvrent les usages suivants :

- Signature des certificats qu'elles émettent,
- Signature des listes des AC révoquées (*LAR*) qu'elles émettent (*cas d'une AC Intermédiaire*),
- Signature des listes des certificats révoquées (*LCR*) qu'elles émettent (*cas d'une AC Emettrice*),
- Signature des certificats des répondeurs OCSP qu'elles émettent.

1.5.1.2 Bi-clés et certificats d'AC et de ses composantes

La bi-clé de l'AC« *AC RACINE MEF QUALIFIEE* » est utilisée uniquement pour :

- Signer les certificats des AC Subordonnées qu'elle émet,
- Signer les listes des AC révoquées (*LAR*) qu'elle émet,

1.5.2 Domaines d'utilisation interdits

Le MEFR décline toute responsabilité dans l'usage fait d'un certificat dans un cadre autre que l'usage prévu au paragraphe 1.5.1.1.

1.6 Gestion des politiques de certification

1.6.1 Entité gérant les politiques de certification

La présente PC est élaborée et mise à jour par le MEFR.

1.6.2 Point de contact de la politique de certification

Ci-dessous le point de contact pour toute question relative à la présente PC :

Ministère de l'économie, des finances et de la relance
Secrétariat général
139, rue de Bercy 75572 Paris Cedex 12

Contact-igc-mef@finances.gouv.fr

1.6.3 Entité gérant la conformité de la DPC avec les PC

Le Comité de Surveillance du service d'émission de certificats détermine la conformité de la DPC avec la présente PC.

1.6.4 Procédures d'approbation de la conformité de la DPC

L'AC met en place un processus d'approbation de la conformité de la DPC à la présente PC.

L'AC est responsable de la gestion (*mise à jour, révisions*) de la DPC. Toute demande de mise à jour de la DPC suit le processus d'approbation mis en place. Toute nouvelle version de la DPC est publiée, conformément aux exigences du paragraphe 2.2 sans délai.

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

2.1 Entités chargées de la mise à disposition des informations

L'AC met en œuvre une fonction de publication et une fonction d'information sur l'état des certificats afin de mettre à disposition des utilisateurs de certificats les informations devant être publiées.

Pour la mise à disposition de l'information sur l'état des certificats, l'AC s'appuie sur la publication d'une LAR (*Liste des Autorités Révoquées*).

Les méthodes d'accès ainsi que les URL correspondantes sont précisées au chapitre 2.2.

2.2 Informations publiées

Les informations de l'AC Racine sont publiées aux points de distribution suivants :

Information publiée	**Emplacement de publication**
PC de l'AC « *AC RACINE MEF QUALIFIEE* »	• https://igc.finances.gouv.fr/pc-ac-racine-mef-qualifiee.pdf • https://igc1.finances.gouv.fr/pc-ac-racine-mef-qualifiee.pdf • https://igc2.finances.gouv.fr/pc-ac-racine-mef-qualifiee.pdf
Certificat de la chaine de confiance	▪ https://igc.finances.gouv.fr/ac-racine-mef-qualifiee.cer ▪ https://igc1.finances.gouv.fr/ac-racine-mef-qualifiee.cer ▪ https://igc2.finances.gouv.fr/ac-racine-mef-qualifiee.cer
LAR	▪ http://crl.igc.finances.gouv.fr/ac-racine-mef-qualifiee.crl ▪ http://crl.igc1.finances.gouv.fr/ac-racine-mef-qualifiee.crl ▪ http://crl.igc2.finances.gouv.fr/ac-racine-mef-qualifiee.crl

L'intégrité des données publiées est assurée par la publication des empreintes numériques de ces données.

2.3 Délais et fréquence de publication

Les informations documentaires de l'AC (*nouvelle PC, ...*) sont publiées 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.

Le certificat de l'AC Racine est diffusé préalablement à toute diffusion de certificats et/ou de LAR correspondantes.

Le site de publication est disponible 24h/24 et 7j/7.

La LAR est mise à jour chaque mois et est publiée.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est en accès libre et gratuit en lecture.

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

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées du service d'émission de certificats, au moins au travers d'un contrôle d'accès de type mots de passe basé sur une politique de gestion stricte des mots de passe.

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Les noms utilisés sont conformes aux spécifications de la norme [X.500] de l'ITU (Union Internationale des Télécommunications).
Dans chaque certificat, l'AC Subordonnée et l'AC Racine sont identifiés par un « Distinguished Name » (*au sens de la norme [X.501] de l'ITU*) aussi appelé DN dans la suite du document.

3.1.2 Nécessité d'utilisation de noms explicites

3.1.2.1 Identités de l'AC Racine

L'AC Racine est identifiée par son DN, comme suit :

Attribut du DN	Valeur
country (C)	FR
organisationName (O)	MINISTERES ECONOMIQUES ET FINANCIERS
organizationUnitName (OU)	0002 130013345
organizationIdentifier (OrgID)	NTRFR-130013345
commonName (CN)	AC RACINE MEF QUALIFIEE

3.1.2.2 Identités des AC Subordonnées

L'identification des AC Subordonnées se fait en utilisant le DN dont la composition est décrite ci-dessous :

Attribut du DN	Valeur
country (C)	FR
organisationName (O)	MINISTERES ECONOMIQUES ET FINANCIERS
organizationUnitName (OU)	0002 130013345
organizationIdentifier (OrgID)	NTRFR-130013345
commonName (CN)	[NOM SIGNIFICATIF DE L'AC SUBORDONNEE]

3.1.3 Anonymisation et pseudonymisation des services applicatifs

L'anonymisation ou l'utilisation des pseudonymes dans les certificats émis n'est pas autorisée par l'AC.

3.1.4 Règles d'interprétation des différentes formes de noms

Tous les caractères sont au format UTF8String ou PrintableString.

3.1.5 Unicité des noms

Le DN du champ « *subject* » identifie une AC Subordonnée de façon unique au sein du domaine du service d'émission de certificats des MEF.

3.1.6 Rôle des marques déposées

L'AC est responsable de l'unicité des noms des AC Subordonnées et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.
L'utilisation de marque déposée appartient au propriétaire légitime de cette marque de fabrique.
L'AC ne peut voir sa responsabilité engagée en cas d'utilisation illicite par les porteurs des marques déposées.

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

Pour un certificat d'AC Subordonnée, la bi-clé est générée sous le contrôle de l'OT. Le demandeur prouve la possession de la clé privée en transmettant à l'AC Racine une requête signée avec la clé privée générée.

3.2.2 Validation de l'identité d'un organisme

Les certificats des AC Subordonnées sont délivrés exclusivement aux MEF.
L'AE vérifie toutefois l'identification de l'organisme, de son représentant légal et de toutes personnes désignées par ce dernier, directement ou indirectement, pour le représenter vis-à-vis de l'AC Racine ou de l'AE.
Le cas échéant, les informations d'enregistrement sont archivées par l'AC Racine ou par l'AE.

3.2.3 Validation de l'identité d'un individu

Sans objet.

3.2.4 Informations non vérifiées

Sans objet.

3.2.5 Validation de l'autorité du demandeur

Une demande de certificat d'AC Subordonnée ne peut être réalisée que par un personnel habilité, du MEFR, à demander un certificat d'AC Subordonnée sur le service d'émission de certificats du MEFR pour le compte du demandeur.

3.2.6 Critères d'interopérabilité, certification croisée d'AC

Dans le cadre de la présente PC, l'AC ne dispose d'aucun accord de reconnaissance avec des AC extérieures au domaine de sécurité auquel l'AC appartient.

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

Le renouvellement de la bi-clé d'une AC Subordonnée entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne

peut pas être fourni à une AC Subordonnée sans renouvellement de la bi-clé correspondante (cf. chapitre 4.6).

3.3.1 Identification et validation pour un renouvellement courant

La procédure d'identification et de validation de toute demande de renouvellement est identique à la procédure d'enregistrement initiale.

3.3.2 Identification et validation pour un renouvellement des clés après révocation

Suite à la révocation définitive d'un certificat d'AC Subordonnée, quelle qu'en soit la cause, la procédure d'identification et de validation de la demande de renouvellement est identique à la procédure d'enregistrement initiale.

3.4 Identification et validation d'une demande de révocation

Pour des raisons précisées au chapitre 4.9.1, les certificats des AC Subordonnées peuvent être révoqués.
La demande de révocation ne peut être effectuée que par l'entité ayant demandé initialement le certificat (*par l'intermédiaire du responsable de l'AC concernée*) auprès de l'AE de l'AC Racine.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DE CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Une demande de certificat d'AC Subordonnée ne peut être effectuée que par un représentant légal du MEFR ou toute personne habilitée et désignée par celui-ci pour le compte du MEFR.

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

Une demande de certificat d'AC Subordonnée est établie par le représentant légal de l'entité responsable de l'AC ou par la personne désignée par celui-ci.
La demande est spécifiée auprès de l'AC Racine qui sera en charge d'établir un document de cérémonie des clés décrivant les conditions de génération et d'émission du certificat d'AC Subordonnée.

4.2 Traitement d'une demande de certificat

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

L'AE contrôle l'identité et le pouvoir de la personne désignée par le représentant légal de l'entité responsable de l'AC.

4.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le représentant de l'AC Subordonnée en indiquant les raisons du rejet.
En cas d'acceptation de la demande, une cérémonie des clés est organisée pour l'émission du certificat d'AC Subordonnée.

4.2.3 Durée d'établissement du certificat

Le certificat d'une AC Subordonnée est émis durant la cérémonie des clés.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Pour toute demande de certificat d'AC Subordonnée, l'AC Racine effectue les opérations suivantes :

- Vérification de la conformité entre les informations de l'AC Subordonnée du futur certificat et le document de cérémonie des clés,

- Activation de la clé privée de l'AC Racine pour signature du certificat de l'AC Subordonnée,
- Signature du certificat de l'AC Subordonnée,
- Vérification du contenu du certificat généré,
- Désactivation de la clé privée de l'AC Racine.

4.3.2 Notification par l'AC de la délivrance du certificat

Le certificat de l'AC Subordonnée est remis à son représentant au cours de la cérémonie des clés. La signature du procès-verbal (PV) de cérémonie des clés atteste de la remise du certificat.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

La signature du PV de cérémonie des clés vaut acceptation du certificat.

4.4.2 Publication du certificat

Les certificats des AC Subordonnées des MEF sont publiés.

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

Sans objet.

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par l'AC Subordonnée

L'utilisation de la clé privée et du certificat associé est décrite au chapitre 1.5.1, de façon limitative. Les usages décrits doivent être respectés. Dans le cas contraire, la responsabilité de l'AC pourrait être engagée, et le certificat associé pourrait être révoqué.

L'usage autorisé de la bi-clé et du certificat associé sont par ailleurs indiqués dans le certificat lui-même, via les extensions concernant les usages des clés et limités à :

- « *keyCertSign* » et « *cRLsign* » pour la signature de certificats et de LCR,

4.5.2 Utilisation de la clé publique et du certificat par l'utilisateur du certificat

Les utilisateurs de certificats ne doivent les utiliser que dans les domaines d'utilisation spécifiés au chapitre 1.5.1. Les utilisateurs s'engagent à respecter strictement ces domaines d'utilisation. Dans le cas contraire, leur responsabilité pourrait être engagée. L'usage autorisé du certificat est indiqué dans le certificat dans les extensions concernant les usages des clés.

4.6 Renouvellement (au sens RFC 3647) d'un certificat

Nota -Conformément au [RFC3647], la notion de « *renouvellement de certificat* » correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de

validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (*y compris la clé publique*).

La présente PC impose que les certificats et les bi-clés correspondantes aient la même durée de vie, il ne peut donc pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé.

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

4.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés des AC Subordonnées ainsi que les certificats correspondants sont renouvelées au minimum tous les 7 ans.
Par ailleurs, une bi-clé et un certificat peuvent être renouvelés :

- Par anticipation (*ex : pour minimiser les possibilités d'attaques cryptographiques*),
- Ou suite à la révocation du certificat d'une AC Subordonnée (*cf. chapitre 4.9*).

Nota – Dans la suite du présent chapitre, le terme « *fourniture d'un nouveau certificat* » couvre également la fourniture d'une nouveau bi-clé à l'AC Subordonnée.

4.7.2 Origine d'une demande d'un nouveau certificat

Le traitement d'un nouveau certificat est identique à celui d'une demande initiale (*cf. chapitre 4.1.1*).

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

La procédure de traitement d'une demande d'un nouveau certificat est identique à la procédure d'une demande initiale (*cf. chapitre 4.2*).
L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont régies par les dispositions du chapitre 4.3.1.

4.7.4 Notification de l'établissement du nouveau certificat

Cf. chapitre 4.3.2.

4.7.5 Démarche d'acceptation du nouveau certificat

Cf. chapitre 4.4.1.

4.7.6 Publication du nouveau certificat

Cf. chapitre 4.4.2.

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

Cf. chapitre 4.4.3.

4.8 Modification d'un certificat

La présente PC ne recommande pas la modification de certificat.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificat d'AC Subordonnée

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

- Les informations figurant dans le certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat,
- L'AC Subordonnée n'a pas respecté les modalités applicables d'utilisation du certificat,
- L'AC Subordonnée n'a pas respecté ses obligations découlant de la PC dont le certificat dépend,
- Une erreur (*intentionnelle ou non*) a été détectée dans le dossier de l'AC Subordonnée,
- La clé privée associée au certificat de l'AC Subordonnée est suspectée de compromission, est compromise, est perdue ou est volée (*éventuellement les données d'activation associées*),
- Le représentant légal de l'AC Subordonnée ou un représentant habilité demande la révocation du certificat,
- La cessation d'activité de l'entité de l'AC Subordonnée.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC Racine en a connaissance, le certificat concerné est révoqué.

4.9.1.2 Certificat d'une composante du service

Non-applicable.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificat d'AC Subordonnée

Les personnes et entités habilitées à demander une révocation de certificat sont :

- Un représentant légal (RL) ou un représentant habilité de l'entité responsable de l'AC Subordonnée,
- L'AC Racine,
- L'AE rattachée à l'AC Racine.

4.9.2.2 Certificat d'une composante du service

Non-applicable.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Certificat d'AC Subordonnée

À la réception d'une demande de révocation, l'AE vérifie l'identité du demandeur et la validité de la demande, selon les exigences décrites au paragraphe 3.4.
La demande de révocation doit au moins comporter les informations suivantes :

- L'identité de l'AC Subordonnée figurant dans le certificat,
- Le nom de l'entité responsable de l'AC Subordonnée,
- Le nom du demandeur de la révocation (*représentant légal ou représentant habilité*),
- Une information permettant de retrouver rapidement et sans erreur le certificat à révoquer (*par défaut le n° de série*).

Si la demande est recevable, l'AC Racine organise une cérémonie des clés pour :

- Activer la clé privée de l'AC Racine,
- Signer une nouvelle LAR contenant le numéro de série du certificat de l'AC Subordonnée révoquée,
- Détruire les clés de l'AC Subordonnée révoquée.

Si la demande n'est pas recevable, le demandeur en est informé.
L'opération de révocation est enregistrée dans les journaux d'événements de l'AC « *AC RACINE MEF QUALIFIEE* ». Les demandes de révocation sont enregistrées et archivées.
Les causes de révocation définitive des certificats ne sont pas publiées.

4.9.3.2 Certificat d'une composante du service

Non-applicable.

4.9.4 Délai accordé à l'AC Subordonnée pour formuler la demande de révocation

Dès que le représentant habilité a connaissance de la survenance d'une des causes possibles de révocation, de son ressort, il doit formuler sa demande de révocation sans délai.

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

4.9.5.1 Certificat d'AC Subordonnée

Dès lors qu'une demande de révocation d'AC Subordonnée est authentifiée et validée, l'AC Racine met tous les moyens en œuvre pour organiser une cérémonie des clés dans les meilleurs délais.

4.9.5.2 Disponibilité du système de traitement des demandes de révocation

La fonction de gestion des révocations est disponible 24h/24 7j/7.

4.9.5.3 Certificat d'une composante du service

Non-applicable.

4.9.6 Exigences de vérification de la révocation par les utilisateurs de certificats

L'AC Racine met à disposition des utilisateurs de certificats des listes de certificats révoqués (LCR) et des listes d'autorités révoquées (LAR) tous précisés au chapitre 2.2.
L'utilisateur d'un certificat est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. Le choix de la méthode utilisée (LCR) est à l'appréciation de l'utilisateur.

4.9.7 Fréquence d'établissement des LCR

La fréquence de publication de la LAR est de 1 fois par an.

4.9.8 Délai maximum de publication d'une LCR

La LAR est publiée dans un délai maximum de 24 heures.

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

L'AC Racine ne met pas à disposition de service de vérification en ligne du statut des certificats (OCSP).

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

Cf. chapitre 4.9.6.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

En cas de compromission de clé privée, les actions suivantes sont entreprises :

- Cas des certificats d'AC Subordonnées :
  - Les entités (*cf. chapitre 4.9.2*) autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.
- Cas du certificat de l'AC Racine :
  - la révocation suite à une compromission de la clé privée fait l'objet d'une information clairement diffusée sur le site du MEFR.

Une information est diffusée auprès du point de contact identifié de l'ANSSI.

4.9.13 Causes possibles d'une suspension

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

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

L'AC fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante (*jusqu'à et y compris l'AC Racine*), c'est à dire de vérifier également les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LCR / LAR et l'état du certificat de l'AC Racine.

Ces LCR / LAR sont des LCR au format V2, publiées sur un serveur web accessible en protocole HTTP(s).

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24h/24 7j/7.

Cette fonction a une durée maximale d'indisponibilité par interruption de service (*panne ou maintenance*) de 4h et une durée maximale totale d'indisponibilité par mois de 16h.

4.10.3 Dispositifs optionnels

Sans objet.

4.11 Fin de la relation entre l'AC Subordonnée et l'AC Racine

En cas de fin de relation contractuelle entre l'AC Racine et l'AC Subordonnée, avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier est révoqué.

4.12 Séquestre de clé et recouvrement

Sans objet.

4.12.1 Politiques et pratiques de recouvrement par séquestre des clés

Sans objet.

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

Sans objet.

5 MESURES DE SECURITE NON TECHNIQUES

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

Les sites d'exploitation du service d'émission de certificats des MEF sont situés en France et respectent les règlements et normes en vigueur ainsi qu'éventuellement des exigences spécifiques face à des risques de type tremblement de terre ou explosion (*proximité d'une zone d'usines ou d'entrepôts de produits chimiques, ...*).

5.1.2 Accès physiques

Afin d'éviter toute perte, dommage et compromission des ressources du service d'émission de certificats et l'interruption des services de l'AC, les accès aux locaux des différentes composantes du service d'émission de certificats sont contrôlés.
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 (*ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisés pour la mise en œuvre de ces fonctions*) est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

5.1.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements du service d'émission de certificats telles que fixées par leurs fournisseurs, ainsi que les engagements en matière de disponibilité des différentes fonctions de l'AC, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.4 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences de la présente PC, ainsi que les engagements en matière de disponibilité des différentes fonctions de l'AC, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences de la présente PC, ainsi que les engagements en matière de disponibilité des différentes fonctions de l'AC, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.6 Conservation des supports

Les différentes informations intervenant dans les activités du service d'émission de certificats ont été identifiées dans le cadre de l'analyse de risque, et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).
Les supports (*papier, disque dur, disquette, CD, etc.*) correspondant à ces informations sont traités et conservés conformément à ces besoins de sécurité.

5.1.7 Mise hors service des supports

En fin de vie, les supports sont soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.
Les procédures et moyens de destruction et de réinitialisation sont conformes aux différents niveaux de confidentialité.

5.1.8 Sauvegardes hors site

En complément de sauvegardes sur sites, les composantes du service d'émission de certificats mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes sont organisées de façon à assurer une reprise des fonctions du service d'émission de certificats après incident le plus rapidement possible, et conforme aux exigences et aux engagements de la présente PC.

Les informations sauvegardées hors site respectent les exigences de la présente PC en matière de protection en confidentialité et en intégrité de ces informations.

Les composantes du service d'émission de certificats en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, mettent en œuvre des sauvegardes hors site permettant une reprise rapide de ces fonctions suite à la survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ces prestations (*destruction du site, etc.*).

Les fonctions de sauvegarde et de restauration sont effectuées par les rôles de confiance appropriés et conformément aux mesures de sécurité procédurales.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Chaque composante du service d'émission de certificats distingue au moins les cinq rôles fonctionnels de confiance suivants :

- **Responsable de sécurité** - Le responsable de sécurité est chargé de la mise en œuvre et du contrôle de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et des journaux d'évènements.
- **Responsable d'application** - Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification du service d'émission de certificats au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.

- **Ingénieur système** - Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
- **Opérateur** - Un opérateur au sein d'une composante du service d'émission de certificats réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
- **Contrôleur** - Personne autorisée à accéder et en charge de l'analyse régulière des archives et de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

En fonction de son organisation, chaque composante du service d'émission de certificats peut être amenée à répartir tout ou partie des rôles principaux listés ci-dessus sur plusieurs rôles complémentaires.

En plus de ces rôles de confiance au sein de chaque composante du service d'émission de certificats, et en fonction de l'organisation du service d'émission de certificats et des outils mis en œuvre, l'AC peut être amenée à distinguer également en tant que rôle de confiance, les rôles de porteur de parts de secrets de l'AC : cf. chapitres 6.1et 6.2.

Ces porteurs de parts de secrets ont la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui leur sont confiés.

5.2.2 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

5.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante du service d'émission de certificats fait vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

- Que leur nom soit ajouté à la liste d'accès aux locaux de l'AC, ou
- Que leur nom soit ajouté à la liste des personnes autorisées à accéder physiquement au système de l'AC.
- Le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- Eventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans le service d'émission de certificats.

Chaque attribution d'un rôle à un membre du personnel du service d'émission de certificats de MEF est notifiée par écrit.

5.2.4 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.
Concernant les rôles de confiance, les cumuls suivants sont interdits :

- Responsable de sécurité et ingénieur système / opérateur / contrôleur
- Ingénieur système, opérateur et contrôleur

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Toute personne amenée à travailler au sein du service d'émission de certificats est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles.
Toute personne intervenant au sein de l'AC est informée de ses responsabilités relatives au sein du service d'émission de certificats et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2 Procédures de vérification des antécédents

L'AC s'assure de l'honnêteté des personnels amenés à travailler au sein des composantes du service d'émission de certificats. A ce titre, les personnels ne doivent pas avoir de condamnation de justice en contradiction avec leurs attributions.
L'AC s'assure que les personnes ayant un rôle de confiance ne souffrent pas de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.
Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (*a minima tous les 3 ans*).

5.3.3 Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité correspondants à la composante au sein de laquelle il opère.

5.3.4 Exigences et fréquence en matière de formation continue

En fonction de la nature des évolutions (*liées aux systèmes, aux procédures, à l'organisation,* …), le personnel concerné reçoit une formation appropriée préalablement à toute évolution.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

L'AC peut prendre toutes sanctions adéquates envers un personnel ayant un rôle de confiance au sein du service d'émission de certificats en cas d'action non-autorisée soupçonnée ou avérée de sa part. Elle peut notamment lui interdire l'accès aux systèmes de l'AC.

5.3.7 Exigences vis-à-vis du personnel des prestataires

L'AC s'assure que le personnel des prestataires intervenant sur les composantes du service d'émission de certificats respecte les exigences de l'AC du chapitre 5.3.
Ces exigences sont traduites en clauses adéquates dans les contrats avec ces prestataires.

5.3.8 Documentation fournie au personnel

Le personnel de chaque composante du service d'émission de certificats dispose au minimum de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques applicables à la composante (*notamment la PC*) et pratiques générales.

5.4 Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer de façon manuelle ou automatique.
Les fichiers résultants, sous forme papier ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Type d'évènements à enregistrer

Chaque entité opérant une composante du service d'émission de certificats journalise, au minimum, les événements tels que décrit ci-dessous sous forme électronique. La journalisation est automatique depuis le démarrage du système et sans interruption jusqu'à son arrêt.

- 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,
- Traces d'activité (logs) des pare-feux et des routeurs,
- Evénements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à la défaillance de la fonction de journalisation, pannes logicielles et matérielles,
- Connexion / déconnexion des Utilisateurs ayant des rôles de confiance, et des tentatives non réussies correspondantes,

D'autres évènements sont aussi recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- Les accès physiques,
- Les actions de maintenance et de changements de la configuration des systèmes,
- Les changements apportés au personnel,
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles.

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions du service d'émission de certificats, des évènements spécifiques aux différentes fonctions du service d'émission de certificats sont journalisés, notamment :

- Réception d'une demande de certificat (initiale et renouvellement),
- Validation / rejet d'une demande de certificat,
- Transmission du certificat à l'entité responsable de l'AC Subordonnée,
- Accusé de réception de l'entité responsable de l'AC Subordonnée
- Acceptation ou rejet explicite par l'entité responsable de l'AC Subordonnée,

- Evénements liés aux clés de signature et aux certificats d'AC (*génération, sauvegarde / récupération, destruction, …*),
- Génération des bi-clés d'AC Subordonnée,
- Génération des certificats d'AC Subordonnée,
- Publication et mise à jour des informations liées aux AC (*PC/DPC, certificats d'AC, …*)
- Réception d'une demande de révocation,
- Validation / rejet d'une demande de révocation,
- Génération puis publication des LAR,

Chaque enregistrement d'un évènement dans un journal contient au minimum les champs suivants :

- Type de l'évènement,
- Nom de l'exécutant ou référence du système déclenchant l'évènement,
- Date et heure de l'évènement,
- Résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'événements.
Suivant le type d'événement concerné, les champs suivants peuvent être enregistrés :

- Destinataire de l'opération,
- Nom ou identifiant du demandeur de l'opération ou référence du système effectuant la demande,
- Nom des personnes présentes (*s'il s'agit d'une opération nécessitant plusieurs personnes*),
- Cause de l'événement,
- Toute information caractérisant l'événement (*par exemple pour la génération d'un certificat, son numéro de série*).

Les opérations de journalisation sont effectuées au cours du processus concerné. En cas de saisie manuelle, l'écriture s'effectue, sauf exception, le même jour ouvré que l'événement.

5.4.2 Fréquence de traitement des journaux d'évènements

Voir chapitre 5.4.8.

5.4.3 Période de conservation des journaux d'évènements

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

5.4.4 Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.
Les journaux d'évènements sont protégés en disponibilité (*contre la perte et la destruction partielle ou totale, volontaire ou non*).

Les systèmes générant les journaux d'événements sont synchronisés sur une source fiable de temps détaillée au chapitre 6.8.

5.4.5 Procédure de sauvegarde des journaux d'évènements

Chaque entité opérant une composante du service d'émission de certificats met en œuvre des mesures afin d'assurer l'intégrité et la disponibilité des journaux d'évènements.

5.4.6 Système de collecte des journaux d'évènements

Un système de collecte des journaux d'événements est mis en place au sein du service d'émission de certificats.

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

Lorsqu'un événement est consigné par le système de collecte des données de vérification, il n'est pas requis d'en aviser la personne, l'organisation, le dispositif ou l'application qui en est la cause.

5.4.8 Évaluation des vulnérabilités

Chaque entité opérant une composante du service d'émission de certificats est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.
Les journaux d'évènements sont contrôlés au moins 1 fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.
Les journaux sont analysés dans leur totalité 1 fois par semaine et dès la détection d'une anomalie. Cette analyse donne lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.
Un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (*AE et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.)* est effectué au moins 1 fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

5.5 Archivage des données

5.5.1 Types de données à archiver

Des dispositions en matière d'archivage sont également prises par l'AC. Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes du service d'émission de certificats.
Il permet également la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.
Les données archivées sont les suivantes :

- Les logiciels (*exécutables*) et les fichiers de configuration des équipements informatiques,
- Les PC,
- Les DPC,
- Les accords contractuels avec d'autres AC ;

- Les certificats,
- Les récépissés ou notifications (*à titre informatif*),
- Les justificatifs d'identité du représentant légal ou du représentant habilité et, le cas échéant, de leur entité de rattachement,
- Les journaux d'évènements des différentes entités du service d'émission de certificats.

5.5.2 Période de conservation des archives

Dossier de demande de certificat

Les dossiers et les pièces justificatives de la génération des AC émettrices (documents projet de décision de création d'AC Emettrices, documents de création des AC Emettrices) sont archivés pendant au moins sept (7) ans après l'expiration de l'AC Subordonnée.

A l'issue de la période d'archivage, le dossier et les pièces justificatives font l'objet d'une destruction.

Certificats, LAR émis par l'AC

Les certificats ainsi que les LAR émises par l'AC Racine sont archivés pendant au moins sept (7) ans après l'expiration de l'AC Racine.

A l'expiration de la durée d'archivage, les LAR font l'objet d'une destruction.

Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 sont archivés pendant sept (7) années après leur génération.

A l'expiration de la durée d'archivage, les journaux d'événements font l'objet d'une destruction.

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives :

- Sont protégées en intégrité,
- Sont accessibles aux seules personnes autorisées,
- Peuvent être relues ou exploitées,
- Lisibles et exploitables sur l'ensemble de leur cycle de vie.

5.5.4 Procédure de sauvegarde des archives

Le niveau de protection des sauvegardes est équivalent au niveau de protection des archives.

5.5.5 Exigences d'horodatage des données

Cf. chapitre 5.4.4 pour la datation des journaux d'évènements.

Le chapitre 6.8 précise les exigences en matière de datation et d'horodatage.

5.5.6 Système de collecte des archives

Le système de collecte des archives respecte les exigences de protection des archives concernées.

5.5.7 Procédures de récupération et de vérification des archives

Les archives (*papier et électroniques*) sont récupérables dans un délai inférieur à 2 jours ouvrés par l'AC.

5.6 Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC.
Pour cela la période de validité de ce certificat de l'AC est supérieure à celle des certificats qu'elle signe.
Au regard de la date de fin de validité de ce certificat, son renouvellement est demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.
Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats.
Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7 Reprise suite à compromission ou sinistre

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

Chaque entité agissant pour le compte du service d'émission de certificats met en œuvre des procédures de remontée d'incident et de traitement des incidents. Ceci est réalisé au travers de la sensibilisation et la formation des personnels et au travers de l'analyse des journaux d'événements.
Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui en informe immédiatement l'AC. Le cas de l'incident majeur est impérativement traité dès réception et la publication de l'information de révocation du certificat, s'il y a lieu, est faite dans la plus grande urgence, voire immédiatement, par tout moyen utile ou disponible.

L'AC prévient directement et sans délai le point de contact identifié sur le site https://ssi.gouv.fr.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses systèmes devient insuffisant pour son utilisation prévue restante, alors l'AC informe toutes les AC Subordonnées et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords. De plus tous les certificats concernés sont révoqués.

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

Chaque composante du service d'émission de certificats dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions du service d'émission de certificats découlant de la présente PC,

notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

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

Chaque composante du service d'émission de certificats dispose d'un plan de continuité.
Dans le cas de compromission d'une clé d'AC, le certificat correspondant est immédiatement révoqué comme précisé au chapitre 4.9.
De plus, l'AC respecte les engagements suivants :

- Arrêter immédiatement l'utilisation de la clé de la composante compromise,
- Informer sans délai toutes les AC Subordonnées et les tiers utilisateurs,
- Indiquer sans délai que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.
    - Prévenir l'ANSSI de la compromission dans les 24 heures,
    - Le cas échéant procéder à un dépôt de plainte auprès des autorités compétentes selon leurs modalités.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes du service d'émission de certificats disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC.

5.8 Fin de vie du service

Une ou plusieurs composantes du service d'émission de certificats peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.
L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.
Le transfert d'activité est défini comme la fin d'activité d'une composante du service d'émission de certificats ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.
La cessation d'activité est définie comme la fin d'activité d'une composante du service d'émission de certificats comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

5.8.1 Transfert d'activité ou cessation d'activité affectant une composante du service autre que l'AC

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, l'AC :

- Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (*notamment, archivage des certificats et des informations relatives aux certificats*),

- Assure la continuité de la révocation (*prise en compte d'une demande de révocation et publication des LAR*), conformément aux exigences de disponibilité pour ses fonctions définies dans la PC,
- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des AC Subordonnées ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire sous un délai d'un (1) mois,
- L'AC communique au point de contact identifié sur le site https://ssi.gouv.fr les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (*clés et informations relatives aux certificats*) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans la PC. L'AC communiquera à l'ANSSI, selon les différentes composantes du service d'émission de certificats concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (*juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.*) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les AC Subordonnées et les utilisateurs de certificats,
- L'AC tient informée l'ANSSI de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus.

5.8.2 Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle. La cessation partielle d'activité est progressive de telle sorte que seules les obligations visées ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

Dans l'hypothèse d'une cessation d'activité totale, l'AC ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, assurera la révocation des certificats et la publication des LAR conformément aux engagements pris dans la PC.

Les dispositions prises par l'AC en cas de cessation de service comprennent :

- La notification des entités affectées,
- Le transfert de ses obligations à d'autres parties,
- La gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés.

Lors de l'arrêt du service, l'AC :

- S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats,
- Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante,
- Révoque son certificat,
- Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité,
- Informe toutes les AC Subordonnées dont les certificats sont révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

6 MESURES DE SECURITE TECHNIQUES

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'AC

La génération des clés de signature de l'AC Racine est effectuée dans un environnement sécurisé (*Cf. chapitre 5*).
Les clés de signature de l'AC Racine sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré.

La génération des clés de signature de l'AC Racine est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (*Cf. Chapitre 5.2.1*), dans le cadre de « *cérémonies de clés* ». Ces cérémonies se déroulent suivant des scripts préalablement définis.

L'initialisation du service d'émission de certificats et/ou la génération des clés de signature d'AC s'accompagne de la génération de parts de secrets d'AC. 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.
Ces parts de secrets sont générées suivant un schéma à seuil de Shamir (*n parties parmi m sont nécessaires et suffisantes pour reconstituer le secret*), Ce secret permet de déclencher le chargement sécurisé, dans un nouveau module cryptographique, de la (ou des) clé(s) privée(s) d'AC sauvegardée(s) lors de la cérémonie de clés.

Suite à leur génération, les parts de secrets sont remis à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (*papier, support magnétique ou confiné dans une carte à puce ou une clé USB*), 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 cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins un est externe à l'AC et est impartial.
Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

6.1.1.2 Clés d'AC Subordonnée

La génération des clés d'AC Subordonnée est effectuée dans un environnement sécurisé (*Cf. chapitre 5*).
Les clés de signature d'AC Subordonnée sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré.

La génération des clés de signature d'AC Subordonnée est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (*Cf. Chapitre 5.2.1*), dans le cadre de « *cérémonies de clés* ». Ces cérémonies se déroulent suivant des scripts préalablement définis.

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet. La clé privée d'AC Subordonnée est générée sur un module cryptographique au cours de la cérémonie des clés.

6.1.3 Transmission de la clé publique à l'AC

Les clés publiques des AC Subordonnées sont transmises à l'AC Racine, aux fins de signature, dans des conditions qui garantissent leur intégrité et leur origine (*sous forme d'une requête PKCS10*).

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

La clé publique de l'AC Racine est diffusée sous la forme d'un certificat numérique qui est téléchargeable sur le site web de l'AC (*cf. chapitre 2.2*).
L'empreinte numérique du certificat de l'AC permettant de garantir l'authenticité de celui-ci est également diffusée sur le site web de l'AC.

6.1.5 Taille des clés

L'AC Racine dispose d'une clé RSA de 4096 bits.
Les AC Subordonnées disposent d'une clé RSA de 4096 bits.
Ces exigences sont revues à mesure de l'évolution de l'état de l'art technique et/ou de la législation.

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

L'équipement de génération des clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme RSA.
Les clés d'une AC Subordonnée sont générées en utilisant des paramètres respectant les normes de sécurité propres à l'algorithme RSA. Les paramètres et les algorithmes de signature sont documentés au chapitre 7.
Les clés d'une AC Subordonnée sont générées et protégées par un module cryptographique matériel répondant aux exigences du chapitre 11 pour le niveau de sécurité considéré.
Les clés de l'AC Racine sont générées et protégées par un module cryptographique matériel répondant aux exigences du chapitre 11 pour le niveau de sécurité considéré.

6.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée d'AC Racine et du certificat associé est strictement limitée à la signature de certificats et de LAR.
L'utilisation de la clé privée d'AC Subordonnée et du certificat associé est strictement limitée à la signature de certificats et de LCR/LAR.

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature, sont évalués selon les Critères Communs au niveau EAL 4+ et qualifié au minimum au niveau standard par l'ANSSI.

6.2.1.2 Dispositifs de création de signature des AC Subordonnées

Les modules cryptographiques des AC Subordonnées, pour la génération et la mise en œuvre de leurs clés de signature, respectent les exigences du chapitre 11.

6.2.2 Contrôles de la clé privée par plusieurs personnes

Le contrôle de la clé privée de l'AC est assuré par du personnel de confiance (*porteurs de secrets de l'AC*) et via un dispositif mettant en œuvre le partage des secrets (*n porteurs de secrets parmi m doivent s'authentifier*).

6.2.3 Séquestre de la clé privée

La clé privée de l'AC Racine ne sont pas séquestrées.
Les clés privées des AC Subordonnées ne sont pas séquestrées.

6.2.4 Copies de secours de la clé privée

La clé privée de l'AC Racine fait l'objet d'une copie de secours bénéficiant du même niveau de sécurité que la clé initiale.
Les opérations de copie sont conformes aux exigences du chapitre 11 permettant ainsi d'assurer les opérations cryptographiques à l'intérieur du module cryptographique.
Les clés privées des AC Subordonnées peuvent être sauvegardées par leur propre entité responsable. Le cas échéant, les clés sauvegardées doivent être enregistrées sous forme chiffrée et avec un mécanisme de contrôle d'intégrité.

6.2.5 Archivage de la clé privée

La clé privée de l'AC Racine n'est en aucun cas archivée.
Les clés privées des AC Subordonnées ne sont en aucun cas archivées.

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

6.2.6.1 Clés privées d'AC

Pour les clés privées d'AC, tout transfert se fait sous forme chiffrée, conformément au chapitre 6.2.4.
Le transfert de la clé privée de l'AC Racine vers et depuis le module cryptographique est soumis à un dispositif mettant en œuvre le partage de secrets. Les moyens de transfert utilisés permettent d'assurer la confidentialité et l'intégrité de la clé privée.

6.2.6.2 Clés privées des AC Subordonnées

La clé privée d'une AC Subordonnée est générée dans un module cryptographique et tout transfert est réalisé sous forme chiffrée conformément aux exigences du chapitre conformément au chapitre 6.2.4.

6.2.7 Stockage de la clé privée dans un module cryptographique

La clé privée de l'AC Racine est stockée dans un module cryptographique répondant aux exigences du chapitre 11 pour le niveau de sécurité considéré.
Les clés privées d'AC Subordonnée sont stockées dans un module cryptographique répondant aux exigences du chapitre 11 pour le niveau de sécurité considéré.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'AC

La méthode d'activation de la clé privée de l'AC Racine dans un module cryptographique permet de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

L'activation de la clé privée d'AC Racine dans le module cryptographique est contrôlée via des données d'activation (*Cf. chapitre 6.4*) et fait intervenir au moins deux personnes dans des rôles de confiance (*par exemple, responsable sécurité et opérateur*).

6.2.8.2 Clés privées des AC Subordonnées

La méthode d'activation des clés privées d'AC Subordonnée dans un module cryptographique permet de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

L'activation des clés privées d'AC Subordonnée dans le module cryptographique est contrôlée via des données d'activation (*Cf. chapitre 6.4*) et fait intervenir au moins deux personnes dans des rôles de confiance (*par exemple, responsable sécurité et opérateur*).

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'AC

La désactivation de la clé privée de l'AC Racine dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.
Ces conditions de désactivation permettent de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

6.2.9.2 Clés privées des AC Subordonnées

La désactivation des clés privées d'AC Subordonnée dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.
Ces conditions de désactivation permettent de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

6.2.10 Méthode de destruction de la clé privée

6.2.10.1 Clés privées d'AC

La méthode de destruction de la clé privée de l'AC Racine est celle du module cryptographique de l'AC Racine et permet de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

En fin de vie de la clé privée de l'AC Racine, normale ou anticipée (*révocation*), cette clé est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.10.2 Clés privées des AC Subordonnées

La méthode de destruction des clés privées d'AC Subordonnée est celle du module cryptographique de l'AC Subordonnée et permet de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

En fin de vie d'une clé privée d'AC Subordonnée, normale ou anticipée (*révocation*), cette clé est systématiquement détruite, ainsi que toute copie et tout élément permettant de la reconstituer.

6.2.11 Niveau d'évaluation sécurité des modules cryptographiques

Les modules cryptographiques de l'AC Racine répondent aux exigences du chapitre 11.
Les modules cryptographiques des AC Subordonnées répondent aux exigences du chapitre 11.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

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

6.3.2 Durée de vie des bi-clés et des certificats

Les certificats et bi-clés des AC Subordonnées ont la même durée de vie.
Cette durée de vie est inférieure ou égale à 10 ans pour les certificats d'AC Subordonnée.

La fin de vie du certificat de l'AC Racine est postérieure à la fin de vie des certificats qu'elle émet.

Les certificats et bi-clés de l'AC Racine ont la même durée de vie.
Cette durée de vie est inférieure ou égale à 20 ans.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

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

La génération et l'installation des données d'activation d'un module cryptographique du service d'émission de certificats se fait lors de la phase d'initialisation et de personnalisation de ce module. Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (*Cf. chapitre 5.2.1*).

6.4.1.2 Génération et installation des données d'activation correspondant à la clé privée d'AC Subordonnée

La génération et l'installation des données d'activation d'un module cryptographique du service d'émission de certificats se fait lors de la phase d'initialisation et de personnalisation de ce module. Ces données d'activation ne sont connues que par les responsables nommément identifiés dans le cadre des rôles qui leurs sont attribués (*Cf. chapitre 5.2.1*).

6.4.2 Protection des données d'activation

6.4.2.1 Protection des données d'activation correspondant à la clé privée de l'AC

Les données d'activation qui sont générées par l'AC Racine pour les modules cryptographiques du service d'émission de certificats sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.4.2.2 Protection des données d'activation correspondant à la clé privée d'AC Subordonnée

Les données d'activation qui sont générées par une AC Subordonnée pour les modules cryptographiques du service d'émission de certificats sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Les systèmes informatiques du service d'émission de certificats offrent un niveau de sécurité qui couvre notamment les points suivants :

- Identification et authentification forte des utilisateurs pour l'accès au système (*authentification à deux facteurs, de nature physique et/ou logique*),
- Gestion des droits des utilisateurs (*permettant de mettre en œuvre la politique de contrôle d'accès définie par l'AC, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles*),
- Gestion de sessions d'utilisation (*déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur*),
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non autorisés et mises à jour des logiciels,
- Gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès,
- Protection du réseau contre toute intrusion d'une personne non autorisée,
- Protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- Fonctions d'audits (*non-répudiation et nature des actions effectuées*),
- Eventuellement, gestion des reprises sur erreur.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle fait l'objet de mesures particulières, définies suite à l'analyse de risques.
Des dispositifs de surveillance (*avec alarme automatique*) et des procédures d'audit des paramétrages du système (*en particulier des éléments de routage*) sont en place lorsque nécessaire.

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Le module cryptographique de l'AC Racine est qualifié par l'ANSSI au minimum au niveau standard.
Le module cryptographique des AC Subordonnées est qualifié par l'ANSSI au minimum au niveau standard.

6.6 Mesure de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurités liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes du service d'émission de certificats est documentée et respecte dans la mesure du possible des normes de modélisation et d'implémentation. La configuration du système, des composantes, ainsi que toute modification et mise à niveau, sont documentées et contrôlées.

6.6.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante du service d'émission de certificats est signalée à l'AC pour validation. Elle est documentée et apparaît dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

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

Sans objet.

6.7 Mesures de sécurité réseau

L'AC Racine est hors-ligne.
Les mesures suivantes sont applicables pour les composantes du service d'émission des certificats (*ex : fonction de publication, …*).
L'interconnexion entre les systèmes du service d'émission de certificats et les réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au bon fonctionnement du service d'émission de certificats.
Les composants du réseau local (*routeurs, par exemple*) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées.

6.8 Horodatage / Système de datation

Il n'y a pas d'horodatage utilisé par l'AC mais une datation des évènements qui permet à l'AC de séquencer les événements à partir de l'heure système du service d'émission de certificats.
Des procédures automatiques ou manuelles sont utilisées pour synchroniser les horloges des systèmes du service d'émission du certificat entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près.

7 PROFILS DES CERTIFICATS ET DES LCR / LAR

7.1 Profils de certificats

7.1.1 Profil du certificat de l'AC Racine

Le tableau suivant présente les champs de base du certificat de l'AC Racine :

Certificat d'AC	
Champs	**Valeur**
Version	2 (=version 3)
SerialNumber	Fourni par le service (*unique et généré de manière aléatoire*)
SignatureAlgorithm	sha256WithRSAEncryption
Issuer	CN = AC RACINE MEF QUALIFIEE OrgID = NTRFR-130013345 OU = 0002 130013345 O = MINISTERES ECONOMIQUES ET FINANCIERS C = FR
Validity	20 ans
NotBefore	Date de la génération de la bi-clé
NotAfter	Date de la génération de la bi-clé + 20 ans
SubjectPublicKeyInfo	La clé publique de l'AC avec une longueur de 4096 bits (RSA)
Subject	CN = AC RACINE MEF QUALIFIEE OrgID = NTRFR-130013345 OU = 0002 130013345 O = MINISTERES ECONOMIQUES ET FINANCIERS C = FR

Le tableau suivant présente les extensions du certificat d'AC Racine :

Extensions	Criticité	Valeur
KeyUsage	***O***	• KeyCertSign • crlSigning
Certificate Policies	***N***	
PolicyIdentifier		2.5.29.32.0 (anyPolicy)
policyQualifierId		CPS
Qualifier		https://igc.finances.gouv.fr/pc-ac-racine-mef-qualifiee.pdf https://igc1.finances.gouv.fr/pc-ac-racine-mef-qualifiee.pdf https://igc2.finances.gouv.fr/pc-ac-racine-mef-qualifiee.pdf
CRL Distribution Point	***N***	http://crl.igc.finances.gouv.fr/ac-racine-mef-qualifiee.crl http://crl.igc1.finances.gouv.fr/ac-racine-mef-qualifiee.crl http://crl.igc2.finances.gouv.fr/ac-racine-mef-qualifiee.crl
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Identifiant de la clé publique de l'AC RACINE MEF QUALIFIEE
SubjectKeyIdentifier	***N***	
KeyIdentifier		Identifiant de la clé publique de l'AC RACINE MEF QUALIFIEE
BasicConstraints	***O***	
CA		Vrai
pathLenConstraint		1

7.1.2 Profil des certificats d'AC Subordonnée

Le tableau suivant présente les champs de base d'un certificat d'AC Subordonnée :

Certificat d'AC	
Champs	**Valeur**
Version	2 (=version 3)
SerialNumber	Fourni par le service (*unique et généré de manière aléatoire*)
SignatureAlgorithm	sha256WithRSAEncryption
Issuer	CN = AC RACINE MEF QUALIFIEE OrgID = NTRFR-130013345 OU = 0002 130013345 O = MINISTERES ECONOMIQUES ET FINANCIERS C = FR
Validity	10 ans
NotBefore	Date de la génération de la bi-clé
NotAfter	Date de la génération de la bi-clé + 10 ans
SubjectPublicKeyInfo	La clé publique de l'AC avec une longueur de 4096 bits (RSA)
Subject	CN = [NOM SIGNIFICATIF DE L'AC SUBORDONNEE] OrgID = NTRFR-130013345 OU = 0002 130013345 O = MINISTERES ECONOMIQUES ET FINANCIERS C = FR

Le tableau suivant présente les extensions d'un certificat d'AC Subordonnée :

Extensions	Criticité	Valeur
KeyUsage	***O***	• KeyCertSign • crlSigning
Certificate Policies	***N***	
PolicyIdentifier		2.5.29.32.0 (anyPolicy)
policyQualifierId		CPS
Qualifier		https://igc.finances.gouv.fr/pc-ac-racine-mef-qualifiee.pdf https://igc1.finances.gouv.fr/pc-ac-racine-mef-qualifiee.pdf https://igc2.finances.gouv.fr/pc-ac-racine-mef-qualifiee.pdf
CRL Distribution Point	***N***	http://crl.igc.finances.gouv.fr/ac-racine-mef-qualifiee.crl http://crl.igc1.finances.gouv.fr/ac-racine-mef-qualifiee.crl http://crl.igc2.finances.gouv.fr/ac-racine-mef-qualifiee.crl
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Identifiant de la clé publique de l'AC RACINE MEF QUALIFIEE
SubjectKeyIdentifier	***N***	
KeyIdentifier		Identifiant de la clé publique de l'AC Subordonnée
BasicConstraints	***O***	
CA		Vrai
pathLenConstraint		0

7.2 Profil des LAR

Les Autorités de Certification portées par la présente PC émettent chacune des LCR dont les caractéristiques sont présentées ci-dessous.

Le tableau suivant présente les champs de base d'une LCR :

LAR	
Champs	**Valeur**
Version	1 (=version 2)
SerialNumber	Fourni par le service
SignatureAlgorithm	sha256WithRSAEncryption
Issuer	DN de l'AC Racine
This Update	Date d'émission de la LCR
Next Update	Date limite d'émission de la prochaine LCR (*This update + 45 jours*)
Revoked certificates	Liste des numéros de série des certificats révoqués

Le tableau suivant présente les extensions d'une LAR :

Extensions	Criticité	Valeur
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Identifiant de la clé publique de l'AC Emettrice
CRL Number	***N***	Numéro de série de la LAR
ExpiredCertOnCRL	***N***	Indique que la LAR contient également les numéros de série des certificats arrivés à expiration après leur révocation

7.3 Protocole OCSP

Non-applicable

8 AUDITS DE CONFORMITE ET AUTRES EVALUATIONS

8.1 Fréquence et circonstances des évaluations

Avant la première mise en service d'une composante du service d'émission de certificats ou suite à toute modification significative au sein d'une composante, l'AC procède à un contrôle de conformité de cette composante.

L'AC procède également régulièrement à un contrôle de conformité de l'ensemble du service d'émission de certificats, suivant la fréquence de 1 fois tous les 2 ans.

Des contrôles internes sont effectués pour s'assurer du bon fonctionnement du service d'émission de certificats entre 2 audits de conformité.

8.2 Identité et qualification des évaluateurs

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

8.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit ne peut pas appartenir à l'entité opérant la composante du service d'émission de certificats contrôlée, quelle que soit cette composante, et être dûment autorisée à pratiquer les contrôles visés.

8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante du service d'émission de certificats (*contrôles ponctuels*) ou sur l'ensemble de l'architecture du service d'émission de certificats (*contrôles périodiques*) et visent à vérifier le respect des engagements et pratiques définis dans la présente PC/DPC.

8.5 Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, 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'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (*temporaire ou définitive*) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.

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

8.6 Communication des résultats

Les résultats des audits de conformité sont tenus à la disposition de l'organisme de qualification en charge de la qualification de l'AC.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Sans objet.

9.1.2 Tarifs pour accéder aux certificats

Sans objet.

9.1.3 Tarifs pour accéder aux informations d'état et de révocation de certificats

Les informations d'état et de révocation de certificats sont mises à disposition gratuitement.

9.1.4 Tarifs pour d'autres services

Sans objet.

9.1.5 Politique de remboursement

Sans objet.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

L'Etat est son propre assureur.

9.2.2 Autres ressources

Sans objet.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles suivantes ne sont accessibles qu'aux personnes habilitées :

- La partie non-publique de la DPC de l'AC,
- Les clés privées de l'AC, des composantes et des certificats émis,
- Les données d'activation associées aux clés privées de l'AC et des certificats émis,

- Tous les secrets du service,
- Les journaux d'évènements des composantes du service,
- Le dossier d'enregistrement d'une AC Subordonnée,
- Les causes de révocation, sauf accord explicite de publication.

9.3.2 Informations hors du périmètre des informations confidentielles

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

9.3.3 Responsabilité en termes de protection des informations confidentielles

L'AC applique des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles au chapitre 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage. Lors d'échange de ces données, l'intégrité est garantie par un moyen adapté au type d'information (chiffrement, signature, enveloppe sécurisée…).

9.4 Protection des données à caractère personnel

9.4.1 Politique de protection des données à caractère personnel

La collecte et l'usage de données personnelles par l'AC et l'ensemble de ses composantes sont réalisés dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, en particulier du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable à compter du 25 mai 2018 (*règlement général sur la protection des données – RGPD*) et de la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

9.4.2 Données à caractère personnel

Les données suivantes sont considérées à caractère personnel :

- Toutes les données nominatives des représentants légaux et représentants habilités enregistrés par le service d'émission de certificats (*prénom, nom, adresse email, …*),

9.4.3 Données à caractère non personnel

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

9.4.4 Responsabilité en termes de protection des données à caractère personnel

Cf. législation et réglementation en vigueur sur le territoire français.

9.4.5 Notification et consentement d'utilisation des données à caractère personnel

Cf. législation et réglementation en vigueur sur le territoire français.
Aucune des données personnelles ne peut être collectée et traitée par l'AC, pour une utilisation autre que celle définie dans le cadre de la PC, sans consentement exprès et préalable de la personne concernée.

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

Cf. législation et réglementation en vigueur sur le territoire français.

9.4.7 Autres circonstances de divulgation de données personnelles

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

9.5 Droits de propriété intellectuelle et industrielle

La présente PC s'inscrit dans le cadre du respect des droits de propriété intellectuelle et industrielle. Cf. législation et réglementation en vigueur sur le territoire français.

9.6 Interprétations contractuelles et garanties

Les obligations communes aux composantes du service d'émission de certificats sont les suivantes :

- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- N'utiliser leurs clés cryptographiques (*publiques, privées et/ou secrètes*) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la présente PC/DPC et les documents qui en découlent,
- Respecter et appliquer la partie de la PC/DPC leur incombant,
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC,
- Respecter les accords ou contrats qui les lient entre elles ou aux AC Subordonnées,
- Documenter leurs procédures internes de fonctionnement,
- 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 Autorités de certification

L'AC Racine a pour obligation de :

- Démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour une AC Subordonnée et que le représentant légal de l'entité responsable de l'AC Subordonnée ou un représentant habilité a accepté le certificat, conformément aux exigences du chapitre 4.4,
- Garantir et maintenir la cohérence de sa DPC avec sa PC,
- Prendre toutes les mesures pour s'assurer que le représentant légal ou le représentant habilité le cas échéant sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins du service d'émission de certificats. La relation entre une AC Subordonnée et l'AC Racine est formalisée par un lien contractuel ou hiérarchique ou réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC Racine assume toute conséquence directe dommageable qui résulterait du non-respect de sa propre PC, par elle-même ou l'une de ses composantes. Elle prévoit les

dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et possède la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique.

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

L'AC Racine reconnaît avoir à sa charge une obligation de garantir la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes. Elle est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services. Toute modification ayant un impact sur le niveau de sécurité fourni doit être approuvée par les instances de haut niveau de l'AC.

9.6.2 Service d'enregistrement

Cf. obligations précisées au chapitre 9.6.1.

9.6.3 AC Subordonnée

Les obligations des AC Subordonnées sont les suivantes :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat,
- Protéger sa clé privée par des moyens appropriés à son environnement,
- Protéger ses données d'activation et, le cas échéant, les mettre en œuvre,
- Protéger l'accès à sa base de certificats,
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant,
- Informer l'AC de toute modification concernant les informations contenues dans son certificat,
- Faire, sans délai, une demande de révocation de son certificat auprès de l'AE ou de l'AC en cas de compromission ou de suspicion de compromission de sa clé privée (*ou de ses données d'activation*).

9.6.4 Utilisateurs de certificats

Les obligations de l'Utilisateur et de l'application utilisatrice sont les suivantes :

- Vérifier et respecter l'usage pour lequel un certificat a été émis,
- Pour chaque certificat de la chaîne de certification, du certificat de l'AC Subordonnée jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (*dates de validité, statut de révocation*),
- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC,

9.6.5 Autres participants

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

9.7 Limite de garantie

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

9.8 Limite de responsabilités

Sans objet.

9.9 Indemnités

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

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

La présente PC est applicable jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Fin anticipée de validité

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

De plus, la mise en conformité n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

9.10.3 Effets de la fin de validité et clauses restant applicables

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

9.11 Notifications individuelles et communication entre les participants

En cas de changement de toute nature intervenant dans la composition du service d'émission de certificats, 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 de qualification.

9.12 Amendements de la PC

9.12.1 Procédures d'amendement

L'AC devra contrôler que tout projet de modification de sa PC reste conforme aux exigences de la présente PC, du RGS et des éventuels documents complémentaires du RGS. En cas de changement important, l'AC fera appel à une expertise technique pour en contrôler l'impact.

9.12.2 Mécanisme et période d'information sur les amendements

Sans objet.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

Toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis peut se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.
L'OID de la PC de l'AC Racine évoluera dès lors qu'un changement majeur (*et qui sera signalé comme tel*) interviendra dans les exigences de la présente PC.

9.13 Dispositions concernant la résolution de conflits

L'AC propose des procédures de résolution à l'amiable aux entités concernées pour le traitement des réclamations et le règlement des litiges.

9.14 Juridictions compétentes

La présente PC ne formule pas d'exigence spécifique sur le sujet. Application de la législation et de la réglementation en vigueur sur le territoire français.

9.15 Conformité aux législations et réglementations

La politique et les pratiques de l'AC sont non-discriminatoires.
Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre 10 ci-dessous.

9.16 Dispositions diverses

9.16.1 Accord global

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

9.16.2 Transfert d'activités

Cf. chapitre 5.8

9.16.3 Conséquences d'une clause non valide

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

9.16.4 Application et renonciation

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

9.16.5 Force majeure

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

9.17 Autres dispositions

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

10 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 Règlementation

[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles puis par ordonnance n°2018-1125 du 12 décembre 2018
[DIRSIG]	Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.
[LCEN]	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
[ORDONNANCE]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives modifiée par ordonnance n°2017-1426 du 4 octobre 2017.
[PSCO_QUALIF]	Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur.
[PSCE_RGS_EIDAS]	Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet - Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS, version en vigueur.
[DEC_EXEC_1506]	Décision d'exécution (UE) 2015/1506 de la Commission du 8 septembre 2015 établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public visés à l'article 27, paragraphe 5, et à l'article 37, paragraphe 5, du règlement [eIDAS].
[eIDAS]	Règlement n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n°1999/93/CE.
[DécretRGS]	Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005
[SIG]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.

10.2 Documents techniques

[RGS]	Référentiel Général de Sécurité – Version 2.0
[PROFILS]	Profils de certificats / LCR / OCSP et Algorithmes Cryptographiques DT-FL-1310-002-PC-PROFILS
[RGS_A1]	RGS – Règles relatives à la mise en oeuvre des fonctions de sécurité basées sur l'emploi de certificats électroniques – Version 3.0.
[RGS_A4]	RGS – Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 3.0.
[CWA14167-1]	CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1
[CWA14167-2]	CWA 14167-2 (2003-10) Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP). Ce PP a été certifié EAL4+
[CWA14167-3]	CWA 14167-3 (2003-10) Cryptographic Module for CSP
[ETSI EN 319401]	General Policy Requirements for Trust Service Providers
[ETSI EN 319411-1]	Policy & Security Requirements for TSPs Issuing Certificates - Part 1: General requirements
[ETSI EN 319411-2]	Policy & Security Requirements for TSPs Issuing Certificates - Part 2: Requirements for trust service providers issuing EU qualified certificates
[ETSI EN 319412-1]	Certificate Profiles - Part 1: Overview and common data structures
[ETSI EN 319412-2]	Certificate Profiles - Part 2: Certificate profile for certificates issued to natural persons
[ETSI EN 319412-5]	Certificate Profiles - Part 5: QCStatements
[RFC_5280]	Internet Engineering Task Force (IETF) - Request for Comments : 5280 X.509 Internet Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile.
[RFC_6960]	Internet Engineering Task Force (IETF) - Request for Comments : 6960 X.509 Internet Public Key Infrastructure. Online Certificate Status Protocol – OCSP.
[RFC_3647]	IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003
[X.509]	Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version d'août 2005 (complétée par les correctifs techniques Corrigendum 1 de janvier 2007et Corrigendum 2 de novembre 2008)
[TS_119_312]	ETSI TS 119 312 V1.1.1 (2014-11) : Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

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

11.1 Exigences sur les objectifs de sécurité

Le module cryptographique, utilisé par l'AC pour générer et mettre en œuvre ses clés de signature (pour la génération des certificats électroniques, des LCR / LAR ou des réponses OCSP), ainsi que, le cas échéant, générer les bi-clés des porteurs, doit répondre aux exigences de sécurité suivantes :

- Si les bi-clés des porteurs sont générées par ce module, garantir que ces générations sont réalisées exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique des bi-clés générées ;
- Si les bi-clés des porteurs sont générées par ce module, assurer la confidentialité des clés privées et l'intégrité des clés privées et publiques des porteurs lorsqu'elles sont sous la responsabilité de l'AC et pendant leur transfert vers le dispositif de protection des éléments secrets du porteur et assurer leur destruction sûre après ce transfert ;
- Assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- Être capable d'identifier et d'authentifier ses utilisateurs ;
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- Être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Si une fonction de sauvegarde et de restauration des clés privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.
- Détecter les tentatives d'altérations physiques et entrer dans un état sûr quand une tentative d'altération est détectée.

11.2 Exigences sur la qualification

Le module cryptographique utilisé par l'AC doit être qualifié au minimum au niveau standard par l'ANSSI.

12 ANNEXE 3 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC SUBORDONEE

12.1 Exigences sur les objectifs de sécurité

Cf. §11.1

12.2 Exigences sur la qualification

Cf. §11.2

13 HISTORIQUE DES PRINCIPALES MODIFICATIONS

V1.0 Document initial validé en comité de surveillance le 14/02/2022

V1.1 22/04/2022 Prise en compte des remarques de l'auditeur lors de l'audit de qualification RGS

- Précisions sur l'identification, authentification et rôle des marques déposées (§ 3.1.6)
- Modification du paragraphe 4.8