SECRÉTARIAT GÉNÉRAL
SERVICE DE L'ENVIRONNEMENT PROFESSIONNEL
64 ALLEE DE BERCY
75012 PARIS

POLITIQUE DE CERTIFICATION

DE L'AC2 FINANCES
CRYPT RACINE

Document 01Bis

Politique de certification racine, OID : 1.2.250.1.131.1.7.1.3.1.1

HISTORIQUE DES REVISIONS		
VERSION	DATE	OBJET DE LA REVISION
V1.0	Février 2018	Création

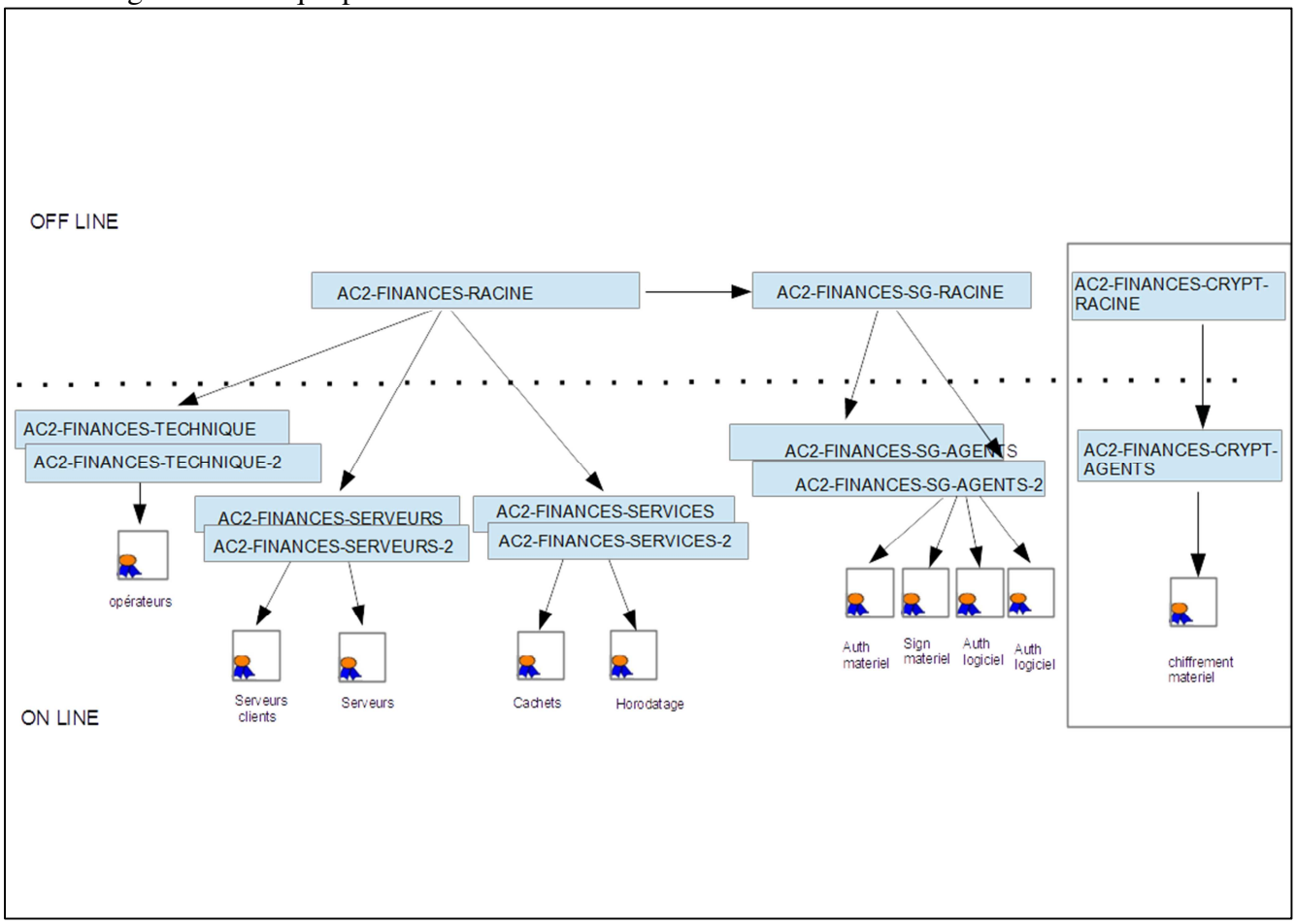
NOM	REDACTION	VERIFICATION	APPROBATION
SG-SEP1A	X		

SOMMAIRE

1 INTRODUCTION

1.1 Présentation générale

Dans le cadre général de la modernisation et de la rénovation des processus administratifs, le Ministère de l'Economie et des Finances s'est doté d'une infrastructure de Gestion de clés (IGC) internalisée appelée « IGC ministérielle », portée par la Délégation aux systèmes d'information, maîtrise d'ouvrage stratégique des IGC du Ministère de l'Economie et des Finances.
Cette infrastructure de gestion de clés, conforme au niveau de sécurité RGS * vise à délivrer des certificats électroniques pour les services qui ne sont pas exposés sur Internet.
Cette IGC est opérée par la Sous-Direction de l'Environnement Professionnel du Secrétariat Général (SEP).
Elle est organisée telle que présenté sur le schéma suivant :



Le périmètre du présent document est AC2 FINANCES-CRYPT-RACINE. Cette Autorité de Certification émet uniquement des certificats à destination d'AC subordonnées chargées d'émettre des certificats de chiffrement à destination d'utilisateurs finaux. A la date de publication de la présente version du document, une seule AC subordonnée, l'AC2 FINANCES-CRYPT-AGENTS, est prévue dans la hiérarchie d'AC. Cette AC émet des certificats de chiffrement à destination des agents.

L'objectif de ce document est de définir le niveau d'exigence que s'engage à respecter l'AC2 FINANCES CRYPT RACINE tout le long du cycle de vie des certificats qu'elle émet, qu'elle révoque et qu'elle publie. Cette Politique de Certification est conforme dans sa présentation à la RFC 3647.

Ce document s'appuie sur les préconisations, émises par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), le Référentiel Général de Sécurité (RGS 2.0) et la politique de filialisation de l'IGC ministérielle version 1.2 actuellement en cours de validité.
Le niveau de sécurité cible couvert par cette IGC reprend les exigences du niveau 1 étoile du RGSv2. Cependant, étant une AC Racine, la présente AC ne vise pas une certification.

1.2 Identification du document

La présente politique de certification est dénommée :

Politique de Certification AC2-FINANCES-CRYPT-RACINE.

Le numéro OID de cette PC est 1.2.250.1.131.1.7.1.3.1.1

1.3 Entités intervenant dans l'IGC

1.3.1 Autorité de certification racine

Pour assurer sa fonction d'AC et la gestion des certificats qu'elle émet, l'AC2-FINANCES-CRYPT-RACINE est constituée des différentes entités assurant chacune une fonction particulière :

Autorité d'enregistrement (AE) : Elle est chargée d'enregistrer la demande de certificat d'une autorité subordonnée au cas par cas et de vérifier l'authenticité des informations fournies par le demandeur, conformément à sa politique de certification et en rapport avec la politique de filialisation ministérielle.

- Elle vérifie l'identité des personnels responsables qui demandent la signature de l'AC subordonnée.
- Leurs responsabilité et rôles par rapport à l'AC dont le certificat doit être signé.
- Les conditions d'usage du certificat signé conformément à ce qui est décrit dans la PC de l'autorité subordonnée,
- Enfin les résultats de l'audit de cette AC.

Fonction de génération des certificats : Elle signe les demandes de certificat des AC subordonnées (CSR) avec sa clé privée de signature et restitue le certificat de l'AC subordonnée sur un support adéquat.

Fonction de publication des certificats : La fonction de publication a pour fonction de mettre à disposition des différentes parties l'ensemble des informations nécessaires :

- les politiques de certification des AC2-FINANCES-CRYPT-RACINE et subordonnée AC2-FINANCES-CRYPT-AGENTS (familles de certificats Chiffrement),
- les certificats de l'AC Racine et des AC de sa chaîne de confiance,
- la liste des certificats Révoqués signée par l'AC2-FINANCES-CRYPT-RACINE et l'AC2-FINANCES-CRYPT-AGENTS,
- les conditions générales.

Fonction de gestion des révocations : Cette fonction traite de la révocation des certificats des AC subordonnées. Le résultat du traitement est diffusé via la liste des autorité révoquées (ARL) de l'AC2-FINANCES-CRYPT-RACINE.

Fonction d'information sur l'état des certificats : Cette fonction fournit aux utilisateurs de certificats des informations sur le statut des certificats révoqués. Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) ou lors d'une révocation.

1.3.2 Autorité d'enregistrement

Dans le cadre de l'AC2-FINANCES-CRYPT-RACINE, la fonction d'enregistrement est assurée par les personnels suivants :

- un témoin de la procédure de signature (ou de la révocation) du certificat de l'AC demandeuse (maître de cérémonie de la Key Ceremony) en charge d'un compte-rendu de signature d'AC subordonnée,
- le responsable fonctionnel de l'IGC FINANCES CRYPT AGENTS,
- un responsable de la sécurité des systèmes d'informations de direction,
- un représentant du Haut Fonctionnaire de Défense,
- le responsable fonctionnel de l'AC subordonnée demandeuse.

1.3.3 Porteurs de certificats

Les porteurs de certificats sont les AC subordonnées. Les certificats sont émis selon cette PC, sous la responsabilité de la structure suivante :

La Sous-Direction de l'Environnement Professionnel du Secrétariat Général des Ministères économiques et financiers,
Sous-direction de l'Informatique,
139 Rue de Bercy,
750572 PARIS CEDX 12.

La responsabilité de cette entité est reconnue par la DSI du Secrétariat Général des ministères économiques et financiers.

1.3.4 Utilisateurs de certificats

L'utilisateur de certificat peut être :

- un service du ministère qui reconnaît les certificats de l'AC2-FINANCES-CRYPT-RACINE et vérifie la chaîne de certification des AC des Ministères,
- toute personne (agent de l'administration ou non) qui souhaite vérifier la chaîne de certification de l'autorité émettrice du certificat servant à chiffrer un message à l'attention d'un porteur.

1.4 Usage des certificats

1.4.1 Domaine d'utilisation applicables

1.4.1.1 Bi-clés et certificats d'AC

La bi-clé de l'AC2-FINANCES-CRYPT-RACINE est utilisée uniquement à des fins de :

- signature du certificat d'AC subordonnée,
- signature de la liste de révocation de l'autorité de certification subordonnée (ARL).

De ce fait, le certificat de l'AC2-FINANCES-CRYPT-RACINE est utilisé pour :

- vérifier l'intégrité et l'origine du certificat d'AC subordonnée ;
- vérifier l'intégrité et l'origine des ARL émises.

1.4.1.2 Bi-clés et certificat d'AC Subordonnée

L'AC2-FINANCES-CRYPT-RACINE n'émet de certificat qu'à des AC Subordonnées dont l'usage des certificats finaux émis est limité aux certificats de chiffrement.

1.4.2 Domaine d'utilisation interdits

Tous les usages qui ne sont pas indiqués au paragraphe 1.4.1 sont interdits.

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

Le bureau gouvernance de l'informatique centrale de la sous-direction informatique du SEP, maîtrise d'ouvrage du projet, est responsable de la rédaction de la politique de certification.

Le SHFDS du SG est responsable de l'approbation de cette politique de certification.

La délégation au système d'information du Secrétariat Général, maîtrise d'ouvrage stratégique est responsable de sa validation.

Elle est revue périodiquement pour s'assurer de sa conformité.

Le processus d'évolution et d'amendement de cette PC est précisé au chapitre 9.12 ci-dessous.

Les erreurs relevées à la lecture de ce document et les suggestions pourront être communiquées au point de contact ci-dessous.

1.5.2 Point de contact

L'entité à contacter concernant la présente PC est le Secrétariat Général des ministères économiques et financiers :

Le Secrétariat Général du Ministère de l'Economie et des Finances
139 Rue de Bercy,
75572 PARIS CEDEX 12.

La responsabilité de cette entité est reconnue par la DSI du SG des ministères en conformité avec la politique de filialisation.

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

La conformité entre DPC et PC est prononcée par la DSI du SG.

1.5.4 Procédure d'approbation de la conformité de la DPC

Le SHFDS, entité indépendante de l'AC fait auditer la conformité de la DPC avec la PC. Sur la base du rapport d'audit, la DSI du SG fait adapter, si besoin, le corpus documentaire de l'IGC FINANCES CRYPT.
Le chapitre 8 détaille les exigences en termes d'audits de conformité et autres évaluations relatives à cette PC.
L'AC est responsable de la gestion (mise à jour, révisions) de la DPC. Toute nouvelle demande de mise à jour de la DPC doit suivre le même processus d'approbation. Toute nouvelle version de la DPC doit être publiée sans délai, conformément aux exigences du paragraphe 2.2.

Le chapitre 8 détaille les exigences en termes d'audits de conformité et autres évaluations relatives à cette PC.

1.6 Définitions et acronymes

1.6.1 Acronymes

Les acronymes utilisés dans la présente PC ou dans les PC type RGS sont les suivants :

DSI	Délégation aux Systèmes d'Information du Secrétariat Général des ministères économique et financier
AC	Autorité de Certification
AE	Autorité d'Enregistrement
AH	Autorité d'Horodatage
ANSSI	Agence Nationale de la Sécurité des Systèmes d'information

CEN	Comité Européen de Normalisation
CISSI	Commission Interministérielle pour la SSI
DGME	Direction Générale de la Modernisation de l'État
SDAE	Service du Développement de l'Administration Électronique
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
IGC	Infrastructure de Gestion de Clés.
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
MEF	Ministères économique et financier
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocole
OID	Object Identifier
OSC	Opérateur de Service de Certification
OSS	Opérateur de Service de Séquestre
PC	Politique de Certification
PIN	Personal Identification Number
PP	Profil de Protection
PSCE	Prestataire de Services de Certification Électronique
RSA	Rivest Shamir et Adelman
S/MIME	Secure/Multipurpose Internet Mail Extensions
SG/SEP	Secrétariat Général / Service de l'Environnement Professionnel
SHA	Secure Hash Algorithm
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
URL	Uniform Resource Locator

1.6.2 Définitions

Les termes utilisés dans la présente PC sont les suivants :

Agent : Personne physique agissant pour le compte d'une autorité administrative.

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'AC pour des besoins de chiffrement ou déchiffrement pour ou par le porteur du certificat.

Autorités administratives - Ce terme générique désigne les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

Autorité d'enregistrement (AE) : Chapitre 1.3.2.

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 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.

Certificat électronique - Fichier électronique attestant qu'une bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié, directement ou indirectement (pseudonyme), dans le certificat. Il est délivré par une Autorité de Certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et la bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Dans le cadre de cette PC, le terme "certificat électronique" désigne uniquement un certificat délivré à une personne physique et portant sur une bi-clé de chiffrement, sauf mention explicite contraire (certificat d'AC, certificat d'une composante, …).

Composante - Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction de l'IGC. L'entité peut être le PSCE lui-même ou une entité externe liée au PSCE par voie contractuelle, réglementaire ou hiérarchique.

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

Délégation aux Systèmes d'Information : DSI du Secrétariat Général des ministères économiques et financiers.
Elle définit et fait appliquer la politique de filialisation des IGC des directions et services des ministères économiques et financiers.
Elle-signe les certificats d'AC racine correspondants.
Elle est le propriétaire des clés de l'AC Racine de chiffrement des ministères (AC2-FINANCES-CRYPT-RACINE) et, par là même, a la responsabilité de signature des certificats émis par l'opérateur de service de certification (OSC) pour les AC subordonnées dont l'AC2-FINANCES-CRYPT-AGENT.

Dispositif de protection des éléments secrets - Un dispositif de protection des éléments secrets désigne un dispositif de stockage des éléments secrets remis au porteur (exemples : clé privée, code PIN, etc). Il peut prendre la forme d'une carte à puce, d'une clé USB à capacités cryptographique.

Entité - Désigne une autorité administrative ou une entreprise au sens le plus large, c'est-à-dire également les personnes morales de droit privé de type associations.

Fonction de génération des certificats - Cf. chapitre 1.3.1.

Fonction de génération des éléments secrets du porteur - Cf. chapitre 1.3.1.

Fonction de gestion des révocations - Cf. chapitre 1.3.1.

Fonction de publication - Cf. chapitre 1.3.1.

Fonction de remise au porteur - Cf. chapitre 1.3.1.

Fonction d'information sur l'état des certificats - Cf. chapitre 1.3

Infrastructure de gestion de clés (IGC) - Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, etc.

Mandataire de certification - Cf. chapitre 1.3

Personne autorisée - Cf. chapitre 1.3

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

Porteur de certificats - Cf. chapitre 1.3

Prestataire de services de certification électronique (PSCE) - Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE comporte au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

Produit de sécurité - Un dispositif, de nature logicielle et/ou matérielle, dont l'utilisation est requise pour mettre en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information dématérialisée (lors d'un échange, d'un traitement et/ou du stockage de cette information). Ce terme générique couvre notamment les dispositifs de signature électronique, les dispositifs d'authentification et les dispositifs de protection de la confidentialité.

Promoteur d'application - Un responsable d'un service de la sphère publique accessible par voie électronique.

Qualification d'un prestataire de services de certification électronique - Acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de

certification électronique d'un PSCE (famille de certificats) à certaines exigences d'une PC Type pour un niveau de sécurité donné et correspondant au service visé par les certificats.

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

Système d'information – Tout ensemble de moyens destinés à élaborer, traiter, stocker ou transmettre des informations faisant l'objet d'échanges par voie électronique entre autorités administratives et usagers ainsi qu'entre autorités administratives.

Usager - Personne physique agissant pour son propre compte ou pour le compte d'une personne morale et procédant à des échanges électroniques avec des autorités administratives.

Utilisateur de certificat : Cf. chapitre 1.3

Identifiant d'objet (OID) : Identificateur alphanumérique unique enregistré conformément à la norme d'enregistrement ISO pour désigner un objet ou une classe d'objets spécifiques.

Liste de Certificats Révoqués (LCR) : liste de certificats de porteurs ayant fait l'objet d'une révocation.

Liste d'Autorités Révoquées (LAR) : liste de certificats d'AC ayant fait l'objet d'une révocation.

Opérateur de service de certification (OSC) : composante de l'IGC disposant d'une ou plusieurs plates-formes lui permettant d'assurer les fonctions dévolues à une ou plusieurs AC des ministères.

Référencement - Opération réalisée par l'Administration qui atteste que l'offre de certification électronique du PSCE est utilisable avec tous les systèmes d'information qui requièrent ce type d'offre et exigent le niveau de sécurité correspondant. Une offre référencée par rapport à un service donné et un niveau de sécurité donné d'une PC Type peut être utilisée dans toutes les applications d'échanges dématérialisés requérant ce service et ce niveau de sécurité ou un niveau inférieur. Pour les usagers, le référencement permet de connaître quelles offres de certificats électroniques ils peuvent utiliser pour quels échanges dématérialisés.

Révocation (d'un certificat) : opération demandée dont le résultat est la suppression de la caution de l'AC sur un certificat, avant la fin de sa période de validité. La demande peut être la conséquence de différents types d'événements tels que la perte d'une carte à puce, le changement d'informations contenues dans un certificat, etc. L'opération de révocation est considérée terminée quand le certificat mis en cause est publié dans la liste des certificats révoqués.

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

2.1 Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des porteurs et des utilisateurs de certificats, l'AC doit mettre en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats (liste de révocation cf. chapitre 1.3 ci-dessus).

La présente PC précise les méthodes de mise à disposition et les URL correspondantes (serveur Web de publication).

Dans sa fonction de publication des informations, l'IGC FINANCES CRYPT s'appuie sur :

- Deux sites web externes dont les url sont :
  https://igc1.finances.gouv.fr/ et https://igc2.finances.gouv.fr/
- Un site web interne : l'Intranet des IGC du SG du Ministère de l'Economie et des Finances,

2.2 Informations devant être publiées

L'AC2-FINANCES-CRYPT-RACINE a pour obligation de publier au minimum les informations suivantes à destination des porteurs et utilisateurs de certificats :

- sa politique de certification, couvrant l'ensemble des rubriques du [RFC3647] ;
- la liste des autorités de certification révoquées (ARL) ;
- le certificat de l'AC2-FINANCES-CRYPT-RACINE, en cours de validité ;

L'AC2-FINANCES-CRYPT-RACINE n'émettant pas de certificats à destination des utilisateurs finaux, elle ne publie pas les éléments suivants :

- les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.) ;
- les conditions d'utilisation des certificats.

Ces informations, à l'exception des LAR (cf. chapitre 4.10), sont publiées dans les rubriques d'informations générales sur les sites suivants définis au chapitre 2.1.

Le moyen utilisé pour la publication garantit l'intégrité, la lisibilité, la compréhensibilité et la clarté des informations publiées.

2.3 Délais et fréquence de publication

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

- Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), l'information doit être publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC. En particulier, toute nouvelle version doit être communiquée au porteur ou MC lors d'une demande de renouvellement de clé et doit faire l'objet d'un nouvel accord. Les systèmes publiant ces informations doivent être disponibles les jours ouvrés.
- Pour les certificats d'AC RACINE, ils sont diffusés préalablement à toute diffusion de certificats de porteurs et/ou d'ARL correspondants et les systèmes les publiant ont une disponibilité de 24h/24 et 7j/7.
- Les délais et fréquences de publication des informations d'état des certificats ainsi que les exigences de disponibilité des systèmes les publiant sont décrites aux chapitres 9 et 10.

A noter qu'une perte d'intégrité d'une information mise à disposition (présence de l'information et intégrité de son contenu) est considérée comme une non disponibilité de cette information et que les exigences ci-dessus s'appliquent également à la disponibilité des informations publiées sur ces systèmes.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats doit être libre d'accès en lecture.

L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) doit être strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un **contrôle d'accès fort** (basé sur une authentification au moins à deux facteurs).
L'accès en modification aux systèmes de publication des autres informations doit être strictement limité aux fonctions internes habilitées de l'IGC, 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 doivent être conformes aux spécifications de la norme X.500.
Dans chaque certificat X509v3 l'AC émettrice (issuer) et le porteur (subject) sont identifiés par un "Distinguished Name" DN de type X.501 dont le format exact est précisé dans le document [RGS_A_4] décrivant le profil des certificats.

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner l'AC Racine ainsi que l'AC Subordonnée sont explicites. Ils sont construits à partir du nom de l'AC et du nom du service.

3.1.3 Anonymisation ou pseudonymisation des porteurs

Les certificats émis dans le cadre de l'AC2-FINANCES-CRYPT-RACINE portants sur les AC subordonnées ne peuvent en aucun cas être anonymes ou pseudonyme.

3.1.4 Règles d'interprétation des différentes formes de nom

Le DN est encodé en printableString ou en UTF8String.

3.1.5 Unicité des noms

Dans chaque certificat, le porteur (subject) est identifié par un "Distinguished Name" DN unique construit sur le nom de l'AC et le nom du service qui permet d'identifier de façon unique l'AC correspondante au sein du domaine de l'AC Racine.

3.1.6 Identification, authentification et rôles des marques déposées

La PC ne formule pas d'exigence spécifique sur le sujet.
L'AC2-FINANCES-CRYPT-RACINE est responsable de l'unicité des noms de ses AC subordonnées et de la résolution des litiges portant sur la revendication d'utilisation d'un nom.

3.2 Validation initiale de l'identité

L'identification doit être réalisée au cours d'un face à face entre l'AE et le responsable de l'AC subordonnée. Ce face à face est réalisé en présence d'un représentant du HFDS et du responsable sécurité du SG/SEP.

Dans le cas de l'AC2-FINANCES-CRYPT-AGENTS qui est une AC subordonnée de l'AC2-FINANCES-CRYPT-RACINE, le face à face est réalisé lors de la cérémonie de clés de création de l'AC2-FINANCES-CRYPT-AGENTS.

3.2.1 Méthode pour prouver la possession de la clé privée

L'AC subordonnée doit alors fournir à l'AC Racine une preuve de possession de la clé privée correspondant à la clé publique contenue dans sa demande de certificat. La preuve est fournie

techniquement par la transmission à l'AC2-FINANCES-CRYPT-RACINE d'une requête de certificat ou CSR au format PKC#S10.

Dans le cas de l'AC2-FINANCES-CRYPT-AGENTS, la bi-clé et le certificat sont générés lors de la cérémonie de clés de l'AC2-FINANCES-CRYPT-AGENTS.

3.2.2 Validation de l'identité d'un organisme

Cf. chapitre 3.2.3.

3.2.3 Validation de l'identité d'un individu

La validation de l'identité doit être réalisée au cours d'un face à face entre l'AE et le responsable de l'AC subordonnée. Ce face à face est réalisé en présence d'un représentant du SHFDS des ministères et du responsable sécurité du SG/SEP.

Le demandeur, responsable d'AC subordonnée, fournit au SEP/SG :

- Un justificatif d'identité et d'appartenance aux ministères économiques et financiers,
- Une lettre de mission attestant de sa responsabilité d'AC,
- Un engagement à respecter la Politique de Filialisation ([1]).

Le SG/SEP conserve une trace des justificatifs présentés lesquels sont versés au dossier de demande de certificat.

Dans le cas de l'AC2-FINANCE-CRYPT-AGENTS, le face à face est réalisé lors de la cérémonie de clés de l'AC2-FINANCES-CRYPT-AGENTS.

3.2.4 Information non vérifiées du porteur

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

3.2.5 Validation de l'autorité du demandeur

La validation de l'autorité du demandeur est réalisée par l'AE au moment de la validation de l'identité du responsable de l'AC subordonnée de l'entité ou du service des ministères dont émane la demande de certificat.
La lettre de mission signée par une autorité hiérarchique compétente, versée au dossier de demande de certificat comme indiqué au 3.2.3 est vérifiée et validée par l'AE de l'IGC FINANCES CRYPT.

3.2.6 Critères d'interopérabilité

L'AC gère, documente et le cas échéant publie les demandes d'accords et les accords de reconnaissance avec des AC extérieures au domaine de sécurité auquel l'AC appartient.

[1] En demandant un certificat, les AC subordonnées s'engagent à respecter la Politique de Filialisation des ministères économiques et financiers et en particulier à mettre en place qu'un seul niveau d'AC en dessous de l'AC filialisée et à ne délivrer de certificats que lorsque le porteur final est :
- Une personne physique : agent des ministères uniquement,
- Une entité matérielle : composant matériel ou logiciel sous la responsabilité des ministères.

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

La péremption d'un certificat ou sa révocation entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat ne peut pas être fourni au porteur sans renouvellement de la bi-clé correspondante (cf. chapitre 4.6).

Qu'il s'agisse d'une péremption normale ou après révocation, la procédure d'identification et de validation de la demande de certificat doit être identique à la procédure d'enregistrement initial.

3.4 Identification et Validation d'une demande de révocation

Les demandes de révocation de certificat d'AC subordonnées sont à transmettre en face à face à l'AE par le responsable de l'AC subordonnée. L'identité et l'autorité du demandeur sont vérifiées lors de ce face à face.
Le SG/SEP ou le SG/DSI peuvent déclencher la cellule de crise. Cette cellule de crise peut décider de la révocation du certificat d'une AC Subordonnée.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine de la demande

Une demande de certificat d'AC subordonnée émane du responsable de la future AC subordonnée avec le consentement préalable de sa direction.

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

Lorsqu'un futur porteur, responsable d'AC, demande un certificat, le SG/SEP réalise les étapes suivantes :

- Etablir l'identité et l'autorité du demandeur,
- S'assurer que la politique de certification de l'AC subordonnée respecte la politique de filialisation ministérielle et que le demandeur a pris connaissance des modalités applicables d'utilisation du certificat,
- Obtenir un rapport d'audit et de filialisation de l'AC.

Le SG/SEP conserve une trace des justificatifs présentés :

- les documents concernant la validation de l'identité du demandeur (paragraphe 3.2.3),
- la politique de certification de l'AC subordonnée,
- le rapport d'audit de l'AC subordonnée.

Ces justificatifs sont versés au dossier de demande de certificat.

4.2 Traitement d'une demande de certificat

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

Les identités "personne physique" sont vérifiées conformément aux exigences du chapitre 3.2.

4.2.2 4.2.2 Acceptation ou rejet de la demande

Le SG/SEP, après étude du dossier, accepte la demande (les modalités sont précisées au paragraphe 4.4).
Le SG/SEP informe le demandeur en cas de rejet de la demande en justifiant le rejet.

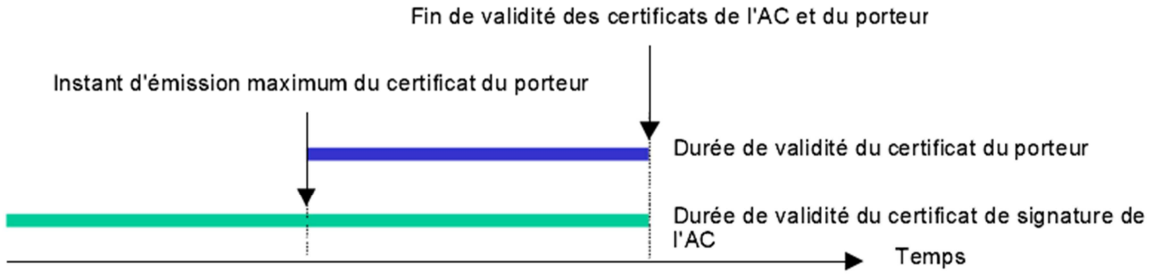
4.2.3 Durée d'établissement du certificat

La durée d'établissement devra être la plus brève possible ne peut excéder 24 heures ouvrables après la validation administrative de la demande.

4.3 Délivrance du certificat

Pour l'AC2-FINANCES-CRYPT-RACINE, la délivrance du certificat se fait lors de la cérémonie de clé de celle-ci.
Pour une AC subordonnée « fille » à AC2-FINANCES-CRYPT-RACINE, la délivrance du certificat se fait lors d'un face à face entre l'AE de l'IGC FINANCES CRYPT et le responsable de l'AC subordonnée et lors de la cérémonie de clés de l'AC Subordonnée.

Note : L'AC Racine ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration de sa bi-clé. Pour cela la période de validité de l'AC doit être supérieure à celle des certificats qu'elle signe.



Au regard de la date de fin de validité de cette clé, son renouvellement doit être 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 bi-clé doit être utilisée pour signer des certificats.
Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que ces certificats signés avec la clé privée correspondante aient expirés.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

La vérification du contenu du certificat émis et l'acceptation du certificat sont réalisés lors de la cérémonie des clés, lors de la remise du certificat au responsable de l'AC subordonnée.
L'acceptation correspond à la réception du certificat et à son intégration dans le support de sécurité par le responsable de l'AC subordonnée.

4.4.2 Publication du certificat

Les certificats des AC subordonnées sont publiés conformément au chapitre 2.

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

Pas d'exigence spécifique.

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat

L'utilisation de la clé privée et du certificat associé est limitée aux conditions d'usage définies dans la présente PC (cf. chapitre 1.4) et dans la Politique de Filialisation. Dans le cas contraire, la responsabilité de l'AC subordonnée pourrait être envisagée.

L'usage autorisé de la bi-clé de l'AC subordonnée et du certificat associé doit par ailleurs être indiqué dans le certificat lui-même, via les extensions concernant les usages des clés. Le détail des usages autorisés est indiqué au chapitre 7 du présent document.

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

Cf. chapitre précédent et chapitre 1.4..
Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6 Renouvellement d'un certificat

Dans le contexte de L'AC2-FINANCES-CRYPT-RACINE, il n'y pas de renouvellement, mais une demande initiale de certificat.

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

Les modalités de délivrance d'un nouveau certificat suite à un changement de la bi-clé d'AC sont identiques à celles d'une demande initiale de certificat.

4.7.1 Causes possibles de changement de bi-clé

Les bi-clés d'AC subordonnées doivent être périodiquement renouvelées afin de minimiser les attaques cryptographiques.
Les certificats des AC subordonnées doivent expirer avant la fin de validité du certificat racine de l'AC2-FINANCES-CRYPT-RACINE.

Une bi-clé et un certificat pourront être renouvelés par anticipation, suite à la révocation du certificat d'une AC subordonnée.

4.7.2 Origine d'une demande d'un nouveau certificat

La demande d'un nouveau certificat émane du SG/SEP ou du responsable de l'AC subordonnée.

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

L'identification et la validation d'une demande de fourniture d'un nouveau certificat sont précisées au chapitre 3.3 ci-dessus.

Pour les actions de l'AC, cf. chapitre 4.3.

4.7.4 Notification au porteur de l'établissement d'un nouveau certificat

Cf. chapitre 4.3

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 du certificat

Nota - Conformément au [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre 4.7) et autres que uniquement la modification des dates de validité (cf. chapitre 4.6).

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

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

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

- Compromission, suspicion de compromission, vol, perte de la clé privée de l'AC,
- Non-respect de la politique de certification ou de la déclaration des pratiques de certification,
- Changement des informations contenues dans le certificat (les informations ou les attributs du certificat ne sont plus en cohérence avec l'utilisation prévue : changement de nom, etc.),
- Décision de la DSI du SG suite à un audit de conformité (non-conformité des procédures appliquées avec les exigences de la PC et/ou les pratiques annoncées dans la DPC),
- Cessation d'activité de l'AC.

Le certificat d'une AC subordonnée peut être révoqué sur demande de la DSI du SG ou du HFDS des ministères s'il a été démontré qu'elle n'a pas respecté les modalités applicables d'utilisation du certificat.

Note :

- En cas de compromission de clés d'une AC subordonnée, la révocation du certificat correspondant est obligatoire et invalide l'ensemble des certificats émis par l'AC subordonnée.
- En cas de compromission de la clé privée de l'AC2-FINANCES-CRYPT-RACINE, la révocation de l'ensemble des certificats émis par l'IGC FINANCES CRYPT est obligatoire.

4.9.2 Origine d'une demande de révocation

L'initiative de la révocation du certificat de l'AC subordonnée appartient :

- au responsable de l'AC subordonnée,
- au SEP du SG,
- à la DSI du SG,
- au SHFDS des ministères,
- par les autorités judiciaires via une décision de justice.

La révocation de l'ensemble des certificats émis par l'AC2-FINANCES-CRYPT-RACINE est décidée lors d'une réunion de la cellule de crise réunissant les responsables de la DSI du SG et du SEP du SG.

4.9.3 Procédure de traitement d'une demande de révocation

La demande de révocation d'AC subordonnée peut être traitée, suite à :

- un face à face entre l'AE de l'AC2-FINANCES-CRYPT-RACINE et le responsable de l'AC subordonnée,
- une télécopie et des échanges téléphoniques du responsable de l'AC subordonnée à l'AE. La télécopie doit contenir les informations suivantes :
    - Le numéro du certificat ;
    - Le nom d'usage de l'AC (ou « Common Name ») ;
    - L'identité du demandeur ;
    - La signature manuscrite du demandeur ;
    - Le motif de demande de révocation.

L'AE s'assure de l'identité du demandeur et de son autorité par rapport au certificat à révoquer. Elle vérifie également que tous les moyens de communication ad hoc (Journal Officiel, site institutionnel, etc.) ont été activés par l'AC subordonnée.

Les procédures à mettre en œuvre en cas de révocation de certificat d'AC sont précisés dans la DPC. Les opérations effectuées sont enregistrées dans les journaux d'événements.

Suite à ces opérations, le SEP du SG informe le demandeur du bon déroulement de l'opération et de la révocation effective du certificat par l'envoi d'un mèl d'information dans les boîtes aux lettres personnelles du responsable de l'AC subordonnée et à la DSI du SG.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC Racine informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des acteurs concernés que leurs certificats ne sont plus valides.

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

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

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

Par nature, une demande de révocation de certificat d'AC subordonnée est traitée en urgence par l'AC2-FINANCES-CRYPT-RACINE.

La fonction de gestion des révocations doit être disponible pendant les heures et jours ouvrés.

La révocation du certificat d'une AC subordonnée est effectuée dès la détection d'un événement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation émise par l'AC Racine.

Toute demande de révocation d'un certificat est traitée dans un délai inférieur à 24 heures pendant les jours ouvrés. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

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

L'utilisateur d'un certificat d'AC est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante à l'aide des LCR mises à sa disposition.
Il est recommandé d'utiliser des applications sécurisées dotées de fonctions d'accès aux LCR et de contrôles automatiques de l'état des certificats.

4.9.7 Fréquence d'établissement de la LCR

La LAR émise par l'AC2-FINANCES-CRYPT-RACINE est établie tous les mois et après toute révocation de certificat d'AC subordonnée.
Sa durée de validité est fixée à un mois.

4.9.8 Délai maximum de publication d'une LCR

Une LAR doit être publiée dans un délai maximum de 30 minutes suivant sa génération.

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

La LAR est accessible en ligne 24 heures sur 24 et 7 jours sur 7 via :

- deux sites web externes dont les url sont :
  - https://igc1.finances.gouv.fr/ac2-finances-crypt-racine.crl
  - https://igc2.finances.gouv.fr/ac2-finances-crypt-racine.crl
- un site web interne : le site Intranet des ministères économiques et financiers.

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

Cf. paragraphe 4.9.6.

4.9.11 Autres moyens disponibles d'information sur les révocations

Le SEP du SG peut utiliser tous les moyens qu'elle estime nécessaires pour informer les utilisateurs en cas de révocation de certificat d'AC subordonnée à condition qu'ils respectent les exigences d'intégrité des informations publiées.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats d'AC, outre les exigences du chapitre 4.9.3, la révocation suite à une compromission de la clé privée fait l'objet d'une information clairement diffusée au moins sur les sites Internet de l'AC https://igc1.finances.gouv.fr et https://igc2.finances.gouv.fr , sur le site intranet des ministères et relayée par d'autres moyens que le SG/SEP estime nécessaire.

4.9.13 Causes possibles d'une suspension

La suspension de certificat n'est pas autorisée par la présente PC.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

L'AC fournit aux utilisateurs de certificats, sur les sites https://igc1.finances.gouv.fr, https://igc2.finances.gouv.fr et sur le site Intranet des ministères économiques et financiers 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 et l'état du certificat de l'AC Racine.

Les sites précités mettent à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR. Ces LCR doivent être au format V2.

4.10.2 Disponibilité de la fonction

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4 heures (jours ouvrés) et une durée maximale totale d'indisponibilité par mois de 32 heures (jours ouvrés).

4.10.3 Dispositifs optionnels

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

4.11 Fin de la relation entre l'AC subordonnée et l'AC2-FINANCES-CRYPT-RACINE

En cas de fin de relation contractuelle entre l'AC2-FINANCES-CRYPT-RACINE et l'AC subordonnée avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

4.12 Séquestre de clé et recouvrement

Ce document traite des certificats d'AC et interdit donc le séquestre des clés privées de ces AC.

Seuls les certificats de chiffrement des porteurs finaux, émis par l'AC subordonnée, peuvent faire l'objet d'un séquestre.

5 MESURES DE SECURITE NON TECHNIQUES

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC doit respecter. Elles sont complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC.

5.1 Mesures de sécurité physique

Les mesures de sécurité physiques de l'IGC FINANCES CRYPT sont conformes aux exigences décrites dans la politique, les procédures et les mesures de sécurité des Ministères. Elles sont décrites dans la DPC et documents annexes de cette IGC (DPC).

5.1.1 Situation géographique des sites

L'IGC FINANCES CRYPT est située physiquement en France sur un site sous la responsabilité directe des ministères économiques et financiers.

La construction des sites respecte les règlements et normes en vigueur du domaine des centres informatiques.

5.1.2 Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'AC, les accès aux locaux des différentes composantes de l'IGC sont contrôlés.

En outre, toute personne entrant dans ces zones physiquement sécurisées ne doit pas être laissée, pendant une période de temps significative, sans la surveillance d'une personne autorisée.

Pour les fonctions de génération des certificats, de génération des éléments secrets et de gestion des révocations :

L'accès doit être strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès doit être assurée. En dehors des heures ouvrables, la sécurité doit être 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 doit être limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines. Pour cela, les composantes concernées de l'IGC doivent définir un périmètre de sécurité physique où sont installées ces machines. La mise en œuvre de ce périmètre doit permettre de respecter la séparation des rôles de confiance telle que prévue dans la présente PC.

Nota - On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisés pour la mise en œuvre de ces fonctions.

5.1.3 Alimentation électrique et climatisation

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

Elles doivent également permettre de respecter les exigences des PC Type (RGS), en matière de disponibilité de ses fonctions, 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 doivent permettre de respecter les exigences des PC Type (RGS), en matière de disponibilité de ses fonctions, 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 doivent permettre de respecter les exigences des PC Type (RGS), en matière de disponibilité de ses fonctions, 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 de l'IGC doivent être identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).
L'AC doit maintenir un inventaire de ces informations. L'AC doit mettre en place des mesures pour éviter la compromission et le vol de ces informations.
Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations doivent être gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils doivent être manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.
Des procédures de gestion doivent protéger ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

5.1.7 Mise hors service des supports

En fin de vie, les supports devront être, 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 doivent être conformes à ce niveau de confidentialité (voir notamment le guide [972-1]).

5.1.8 Sauvegarde hors site

En complément de sauvegardes sur sites, il est recommandé que les composantes de l'IGC mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes doivent être organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conforme aux exigences de l'AC dans sa PC en

matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des certificats (cf. chapitres 4.9.5 et 4.10.2).
Les informations sauvegardées hors site doivent respecter les exigences de la présente PC en matière de protection en confidentialité et en intégrité de ces informations.

Les composantes de l'IGC en charge des fonctions de gestion des révocations et d'information sur l'état des certificats, au moins, doivent obligatoirement mettre 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 doivent être 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 de l'IGC doit distinguer au moins les cinq rôles fonctionnels de confiance suivants :

- **Responsable sécurité de l'IGC** : Le responsable sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est responsable des opérations de génération et de révocation des certificats.
- **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 de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
- **Ingénieur système** : il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
- **Opérateur** : Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
- **Contrôleur** : Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.

En plus de ces rôles de confiance au sein de chaque composante de l'IGC, et en fonction de l'organisation de l'IGC 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 part de secrets d'IGC : cf. chapitres 6.1 et 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.

Pour des raisons de sécurité, il est demandé de répartir les fonctions sensibles sur plusieurs personnes. La présente PC définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'AC (cf. chapitre 6).

La DPC de l'AC précisera quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter (positions dans l'organisation, liens hiérarchiques, etc.).

5.2.3 Identification et authentification pour chaque rôle

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

Ces contrôles doivent être décrits dans la DPC de l'AC et doivent être conformes à la politique de sécurité de la composante.

Chaque attribution d'un rôle à un membre du personnel de l'IGC doit être 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. Pour les rôles de confiance, il est néanmoins recommandé qu'une même personne ne détienne pas plusieurs rôles et, au minimum, les exigences ci-dessous de non cumul doivent être respectées.

Les attributions associées à chaque rôle doivent être décrites dans la DPC de l'AC et être conformes à la politique de sécurité de la composante concernée.

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

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

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC doivent être soumis à une clause de confidentialité vis-à-vis de leur employeur. Dans le cas des agents, ceux-ci sont soumis à leur devoir de réserve.
Chaque entité opérant une composante de l'IGC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.
Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.
L'AC doit informer toute personne intervenant dans des rôles de confiance de l'IGC :

- de ses responsabilités relatives aux services de l'IGC,
- des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.

En particulier, les personnes intervenant dans des rôles de confiance doivent y être formellement affectées par l'encadrement supérieur chargé de la sécurité.

5.3.2 Procédures de vérification des antécédents

Chaque entité opérant une composante de l'IGC doit mettre en œuvre tous les moyens légaux dont elle peut disposer pour s'assurer de l'honnêteté de ses personnels amenés à travailler au sein de la composante.

Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions. Les personnels, non agents de l'Etat, devront remettre à leur employeur une copie du bulletin n°3 de leur casier judiciaire.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications doivent être menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au moins tous les 3 ans).

5.3.3 Exigences en matière de formation initiale

Le personnel doit être préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

5.3.4 Exigences en matière de formation continue

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

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Aucune rotation des rôles n'est permise dans le cadre de la présente PC.

5.3.6 Sanctions en cas d'actions non autorisées

Lorsqu'un exploitant abuse de ses droits ou effectue une opération non conforme à ses attributions, le MEF décide des sanctions disciplinaires à appliquer (Règlement de la Fonction Publique).

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

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC doit également respecter les exigences du présent chapitre 5.3. Ceci doit être traduit en clauses adéquates dans les contrats avec ces prestataires.

5.3.8 Documentation fournie au personnel

Chaque personnel doit disposer de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, doit lui être remis la ou les politique(s) de sécurité l'impactant.

5.4 Procédures de constitution des données d'audit

La journalisation d'événements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.
Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Types d'événements à enregistrer

- Création de bi-clés de l'AC2-FINANCES-CRYPT-RACINE,
- Vérification des supports de parts de secrets,
- délivrance de certificats :
- génération de certificat d'une AC subordonnée (cérémonie de clés)
- révocation de certificat d'une AC subordonnée (cérémonie de clés)
- fin de vie de l'IGC FINANCES CRYPT.

Ces opération sont effectuées lors d'une cérémonie de clé de l'IGC FINANCES CRYPT et sont décrites dans les PV correspondants.

D'autres événements 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 (clés, données d'activation, renseignements personnels sur les porteurs,...),
- la réception d'une demande de certificat (initiale et renouvellement) ;
- la validation / rejet d'une demande de certificat ;
- publication et mise à jour des informations liées à l'AC (PC, certificats d'AC, conditions générales d'utilisation, etc.) ;
- réception d'une demande de révocation ;
- validation / rejet d'une demande de révocation ;

Chaque enregistrement d'un événement dans un journal contient les champs suivants :

- type de l'événement ;
- nom de l'exécutant ou référence du système déclenchant l'événement ;
- date et heure de l'événement (L'heure exacte des événements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat doit être enregistrée) ;
- résultat de l'événement (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 doit figurer explicitement dans l'un des champs du journal d'événements.

De plus, en fonction du type de l'événement, chaque enregistrement contient également les champs suivants :

- destinataire de l'opération ;
- nom 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, le numéro de série de ce certificat).

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

Les événements et données spécifiques à journaliser doivent être documentés par l'AC.

5.4.2 Fréquence de traitement des journaux d'événement

Cf. Paragraphe 5.4.8 ci-dessous.

5.4.3 Période de conservation des journaux d'événements

Les journaux d'événements 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 (recouvrement possible entre la période de conservation sur site et la période d'archivage).

La durée de conservation des archives est de 7 ans.

5.4.4 Protection des journaux d'événements

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

Les journaux d'événements doivent être protégés en disponibilité et en intégrité (contre la perte et la destruction partielle ou totale, volontaire ou non).

Le système de datation des événements doit respecter les exigences du chapitre 6.8.

La définition de la sensibilité des journaux d'événements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.5 Procédure de sauvegarde des journaux d'événements

Chaque entité opérant une composante de l'IGC doit mettre en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'événements pour la composante considérée, conformément aux exigences de la PC Type (RGS).

5.4.6 Système de collecte des journaux d'événements

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

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

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

5.4.8 Évaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC doit être en mesure de détecter la plupart des tentatives de violation de l'intégrité de la composante considérée.

Les journaux d'événements sont contrôlés une fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité au moins une fois toutes les 2 semaines et dès détection d'anomalie. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.

Par ailleurs, un rapprochement entre les différents journaux d'événements de fonctions qui interagissent entre elles (autorité d'enregistrement et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.) est effectué au moins une fois par mois, ceci afin de vérifier la concordance entre événements 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 doivent être également prises par l'AC. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

Il doit permettre également la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.

Les données à archiver sont les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC, notamment la PC de l'IGC FINANCES CRYPT ;
- les DPC, notamment la DPC de l'IGC FINANCES CRYPT ;
- les accords contractuels avec d'autres AC ;
- les certificats et LCR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement
- les journaux d'événements de l'IGC.

5.5.2 Période de conservation des archives

Dossiers de demande de certificat
Tout dossier de demande de certificat accepté doit être archivé pendant toute la durée de vie de l'IGC FINANCES CRYPT.
La durée de conservation des dossiers d'enregistrement doit être portée à la connaissance du responsable de l'AC subordonnée.
Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat doit pouvoir être présenté par l'AC lors de toute sollicitation par les autorités habilitées.
Ce dossier, complété par les mentions consignées par l'AE doit permettre de retrouver l'identité réelle des personnes physiques responsables de l'AC subordonnée.

Certificats et LAR émis par l'AC2-FINANCES-CRYPT-RACINE
Les certificats ainsi que les LAR produites, doivent être archivés pendant toute la durée de vie de l'IGC FINANCES CRYPT.

Journaux d'événements
Les journaux d'événements traités au chapitre 5.4 seront archivés pendant toute la durée de vie de l'IGC FINANCES CRYPT. Les moyens mis en œuvre par l'AC pour leur archivage devront offrir le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements devra être assurée tout au long de leur cycle de vie.

Autres journaux
Pour l'archivage des journaux autres que les journaux d'événements traités au chapitre 5.4, aucune exigence n'est stipulée. L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver ces journaux.

5.5.3 Protection des archives

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

- être protégées en intégrité ;
- être accessibles aux personnes autorisées ;
- pouvoir être relues et exploitées.

L'AC précisera dans sa DPC les moyens mis en œuvre pour archiver les pièces en toute sécurité.

5.5.4 Procédure de sauvegarde des archives

La présente PC ne formule pas d'exigence spécifique relative à la procédure de sauvegarde des archives. Le niveau de protection des sauvegardes doit être au moins équivalent au niveau de protection des archives (voir 5.5.3).

5.5.5 Exigences d'horodatage des données

Cf. chapitre 5.4.4 pour la datation des journaux d'événements.
Le chapitre 6.8 précise les exigences en matière de datation / horodatage.

5.5.6 Système de collecte des archives

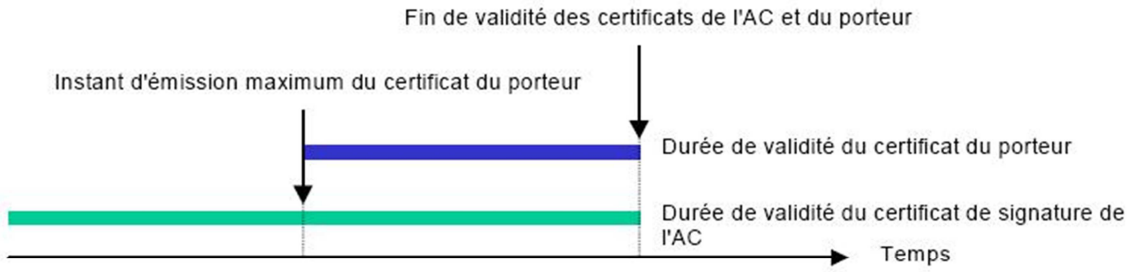
La présente PC ne formule pas d'exigence spécifique sur le sujet, si ce n'est que le système de collecte des archives, qu'il soit interne ou externe, doit respecter les exigences de protection des archives concernées.

5.5.7 Procédures de récupération et de vérification des archives

Les archives (papier et électroniques) doivent pouvoir être récupérées dans un délai inférieur à 2 jours ouvrés, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

5.6 Changement de clé de l'AC

L'AC2-FINANCES-CRYPT-RACINE ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration de son certificat. Pour cela la période de validité de ce certificat doit être supérieure à celle des certificats d'AC subordonnées qu'elle signe.



Au regard de la date de fin de validité de ce certificat, son renouvellement doit être 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 Racine est générée, seule la nouvelle clé privée doit être utilisée pour signer des certificats.
Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce au moins jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré (cf. nota à la fin du chapitre 1.4.1.1).

5.7 Reprise suite à compromission et sinistre

5.7.1 Procédures de remontée et de traitement des incidents et compromission

Chaque entité opérant une composante de l'IGC doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'événements. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.
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'AC2-FINANCES-CRYPT-RACINE, l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement le responsable de l'IGC FINANCES CRYPT. Le cas de l'incident majeur doit être impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé …).
Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC2-FINANCES-CRYPT-RACINE ou ses AC subordonnées devient insuffisant pour son utilisation prévue restante, alors l'AC2-FINANCES-CRYPT-RACINE doit :

- informer toutes les AC subordonnées et les tiers utilisateurs de certificats avec lesquels l'AC2-FINANCES-CRYPT-RACINE a passé des accords ou a d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;

- révoquer tout certificat concerné.

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

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

Ce plan doit être testé au minimum 1 fois tous les 2 ans.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante doit être traité dans le plan de continuité de la composante (cf. chapitre 5.7.2) en tant que sinistre.
Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué : cf. chapitre 4.9.

En outre, l'AC doit au minimum respecter les engagements suivants :

- informer les entités suivantes de la compromission : tous les entités avec lesquelles l'AC a passé des accords ou d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autres AC. En complément, cette information doit être mise à disposition des autres tiers utilisateurs ;
- indiquer que les certificats et les informations de statut de révocation délivrés en utilisant cette clé d'AC peuvent ne plus être valables.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC doivent disposer des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la présente PC (cf. chapitre 5.7.2).

5.8 Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.
L'AC doit prendre 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 de l'IGC 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 de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

Transfert d'activité ou cessation d'activité affectant une composante de l'IGC
Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AC doit entre autres obligations :

1) Mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats).
2) Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC. A défaut, les applications de l'Administration refuseront les certificats émis par des AC dont les LCR en cours de validité ne seraient plus accessibles, même si le certificat du porteur est encore valide.

L'AC s'engage également à réaliser les actions suivantes :
1) Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des porteurs ou des utilisateurs de certificats, l'AC doit les en aviser aussitôt que nécessaire et, au moins, sous le délai de un mois.
2) L'AC communiquera au responsables du SEP/SG et de la DSI/SG 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 sa PC.
3) 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 porteurs et les utilisateurs de certificats.
4) L'AC doit tenir informées la DSI du SG et le SEP du SG de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

Cessation d'activité affectant l'AC
La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement). La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) 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, devra assurer la révocation des certificats et la publication des ARL conformément aux engagements pris dans sa PC.

L'AC doit stipuler dans ses pratiques les dispositions prises en cas de cessation de service. Elles doivent inclure :

- 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 doit :

1) s'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
2) prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
3) révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
4) informer (par exemple par récépissé) tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre 3.2.3).

6 MESURES DE SECURITE TECHNIQUES

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC respecter. Elles doivent être complétées et déclinées en mesures de sécurité en fonction de l'environnement réel de l'IGC.

6.1 Génération et installation de bi clé

L'AC2-FINANCES-CRYPT-RACINE ne génère pas de bi-clé pour ces AC subordonnées.

6.1.1 Génération des bi clés

La génération des clés de signature de l'AC2-FINANCES-CRYPT-RACINE est effectuée dans un environnement sécurisé (cf. chapitre 5).
Les clés de signature d'AC Racine sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous.

La génération des clés de signature d'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 doivent se dérouler suivant des scripts préalablement définis.

L'initialisation de l'IGC et/ou la génération des clés de signature d'AC doit s'accompagner de la génération de parts de secrets d'IGC. 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.

Par exemple, ces parts de secrets peuvent être des parties de la (ou des) clé(s) privée(s) d'AC, décomposée(s) suivant un schéma à seuil de Shamir (n parties parmi m sont nécessaires et suffisantes pour reconstituer la clé privée), ou encore, il peut s'agir de données permettant 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 doivent être remises 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 doit être mise en œuvre par son porteur.

Les cérémonies de clés doivent se dérouler sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence d'un témoin qui atteste, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.
Toute manipulation de données secrètes en clair (clés privées d'AC, parts de secrets d'IGC) doit se faire dans un environnement protégé contre les rayonnements parasites compromettant :

- matériels protégés, cage de Faraday,

- locaux limitant les risques de fuites d'information par observation visuelle ou rayonnements électromagnétiques, etc.

La génération des bi-clés des AC subordonnées devront respecter les mêmes exigences.

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet.

6.1.3 Transmission de la clé publique à l'AC2-FINANCES-CRYPT-RACINE

En cas de transmission de la clé publique de l'AC subordonnée vers l'AC Racine (la bi-clé est générée par l'AC subordonnée), la clé devra être protégée en intégrité et son origine devra en être authentifiée.

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

Les clés publiques de vérification de signature de l'AC2-FINANCES-CRYPT-RACINE sont diffusées auprès des utilisateurs de certificats par un moyen qui en assure l'intégrité de bout en bout et qui en authentifie l'origine.

Le certificat AC2-FINANCES-CRYPT-RACINE est diffusé :

- sur le site Intranet des ministères économiques et financiers,
- les sites Internet des IGC FINANCES, aux adresses suivantes : https://igc1.finances.gouv.fr/ et https://igc2.finances.gouv.fr/

6.1.5 Tailles des clés

Les clés d'AC et de porteurs doivent respecter les exigences de caractéristiques (tailles, algorithmes, etc.) décrites au chapitre 7.

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

L'équipement de génération de bi-clés doit utiliser des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé (cf. [RGS_A_4]).

Les clés des certificats des AC subordonnées ont une longueur 4096 bits minimale et sont générées avec l'algorithme RSA.

6.1.7 Objectifs d'usage de la bi-clé

L'utilisation d'une clé privée de l'AC2-FINANCES-CRYPT-RACINE et du certificat associé est strictement limitée à la signature de certificats, de LAR (cf. chapitre 1.4.1.2 et document [RGS_A_4]).

L'utilisation de la clé privée de l'AC subordonnée et du certificat associé est strictement limitée à la signature de certificats et de LCR (cf. chapitre 1.4.1.2 et document [RGS_A_4]). Les certificats émis sont limités à l'usage certificats de confidentialité (chiffrement).

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' AC2-FINANCES-CRYPT-RACINE

Les modules cryptographiques, utilisés par l'AC2-FINANCES-CRYPT-RACINE, pour la génération et la mise en œuvre de ses clés de signature doivent être des modules cryptographiques répondant au minimum aux exigences du chapitre 11 ci-dessous.

6.2.1.2 Dispositifs de protection de clés privées des AC subordonnées

Les dispositifs de création de signature des AC subordonnées, pour la mise en œuvre de leurs clés privées de signature, doivent respecter les exigences du chapitre 11 ci-dessous.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'AC2-FINANCES-CRYPT-RACINE pour l'exportation / l'importation hors / dans un module cryptographique. La génération de la bi-clé est traitée au chapitre 6.1.1, l'activation de la clé privée au chapitre 6.2.8 et sa destruction au chapitre 6.2.10.

Le contrôle des clés privées de signature de l'AC2-FINANCES-CRYPT-RACINE doit être assuré par du personnel de confiance (porteurs de secrets d'IGC) et via un outil mettant en œuvre le partage des secrets (systèmes où n exploitants parmi m doivent s'authentifier, avec n au moins égal à 3).

6.2.3 Séquestre de la clé privée

Ni les clés privées de l'AC2-FINANCES-CRYPT-RACINE, ni les clés privées des AC subordonnées ne sont séquestrées.

6.2.4 Copie de secours de la clé privée

Les clés privées des AC subordonnées ne doivent faire l'objet d'aucune copie de secours par l'IGC FINANCES CRYPT.

Les clés privées d'AC peuvent faire l'objet de copies de secours, soit dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous, soit hors d'un module cryptographique mais dans ce cas sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les règles à respecter sont définies dans le document [RGS_B_1].
Les opérations de chiffrement et de déchiffrement doivent être effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique.
Le contrôle des opérations de chiffrement / déchiffrement doit être conforme aux exigences du chapitre 6.2.2.

6.2.5 Archivage de la clé Privée

La clé privée de l' AC2-FINANCES-CRYPT-RACINE ne doit en aucun cas être archivée.
Les clés privées des AC subordonnées ne doivent en aucun cas être archivées ni par l' AC2-FINANCES-CRYPT-RACINE ni par aucune des composantes de l'IGC FINANCES CRYPT.

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

Les clés privées des AC subordonnées sont générées et stockées au sein de leur module cryptographique.

Pour les clés privées d'AC, tout transfert doit se faire sous forme chiffrée, conformément aux exigences du chapitre 6.2.4.

6.2.7 Stockage de la clé dans un module cryptographique

Les clés privées de l'AC2-FINANCES-CRYPT-RACINE sont stockées dans un module cryptographique répondant au minimum aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées de l' AC2-FINANCES-CRYPT-RACINE

La méthode d'activation des clés privées de l'AC2-FINANCES-CRYPT-RACINE dans un module cryptographique doit permettre de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

L'activation des clés privées de l'AC2-FINANCES-CRYPT-RACINE dans un module cryptographique doit être contrôlée via des données d'activation (cf. chapitre 6.4) et doit faire 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 de la clé privée de l'AC subordonnée dépend du dispositif utilisé. L'activation de la clé privée de l'AC doit au minimum être contrôlée via des données d'activation (cf. chapitre 6.4) et doit permettre de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

6.2.9 Méthode désactivation de la clé privée

6.2.9.1 Clés privées de l' AC2-FINANCES-CRYPT-RACINE

La désactivation des clés privées de l'AC2-FINANCES-CRYPT-RACINE dans un module cryptographique doit être automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.
Une clé privée d'AC Racine peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation doivent permettre de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

6.2.9.2 Clés privées des AC subordonnées

Les conditions de désactivation de la clé privée d'une AC subordonnée doivent permettre de répondre aux exigences définies dans le chapitre 11.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées de l'AC2-FINANCES-CRYPT-RACINE

La méthode de destruction des clés privées d'AC Racine doit permettre 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'AC2-FINANCES-CRYPT-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

Lorsqu'un certificat d'AC subordonnée est expiré ou révoqué, la clé privée correspondante doit être détruite.

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

Les modules cryptographiques de l'AC2-FINANCES-CRYPT-RACINE doivent être qualifiés au niveau correspondant à l'usage visé, tel que précisé au chapitre 11 ci-dessous.
Les dispositifs de création de signature des AC subordonnées doivent être également qualifiés au niveau tel que précisé au chapitre 11 ci-dessous.

6.3 Autres aspects de la gestion des bi clés

6.3.1 Archivage des clés publiques

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

6.3.2 Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des AC subordonnées couverts par la présente PC doivent avoir la même durée de vie, au moins égale à 3 mois, et au maximum de 10 ans.
La durée de validité des certificats des AC subordonnées est de 10 ans.

La fin de validité d'un certificat d'AC Racine doit être postérieure à la fin de vie des certificats d'AC subordonnées qu'elle émet. La durée de validité du certificat de l'AC2-FINANCES-CRYPT-RACINE est de 10 ans.
Cette durée de vie est cohérente avec les caractéristiques de l'algorithme et de la longueur de clés utilisés définies au chapitre 7.

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'AC2-FINANCES-CRYPT-RACINE

La génération et l'installation des données d'activation d'un module cryptographique de l'AC2-FINANCES-SCRYPT-RACINE doivent se faire lors de la phase d'initialisation et de personnalisation de ce module. Si les données d'activation ne sont pas choisies et saisies par

les responsables de ces données eux-mêmes, elles doivent leur être transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne doivent être 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 des AC subordonnées

La génération et l'installation des données d'activation d'un module cryptographique de l'AC subordonnée doivent se faire lors de la phase d'initialisation et de personnalisation de ce module. Si les données d'activation ne sont pas choisies et saisies par les responsables de ces données eux-mêmes, elles doivent leur être transmises de manière à en garantir la confidentialité et l'intégrité. Ces données d'activation ne doivent être 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'AC2-FINANCES-CRYPT-RACINE

Les données d'activation qui sont générées par l'AC2-FINANCES-CRYPT-RACINE pour les modules cryptographiques de l'IGC FINANCES CRYPT doivent être 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 aux clés privées des AC subordonnées

Les données d'activation qui sont générées par l'AC subordonnée pour les modules cryptographiques de l'IGC subordonnée doivent être 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

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

6.5 Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque que l'AC peut mener (cf. chapitre 1.3.1)
Une analyse des objectifs de sécurité peut être effectuée en amont de tout projet d'IGC par l'AC, de façon à garantir la prise en compte de la sécurité dans les systèmes informatiques.

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC doit être défini dans la DPC de l'AC. Il doit au moins répondre aux objectifs de sécurité suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs),

- 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),
- éventuellement, gestion des reprises sur erreur.

Les clés privées ou secrètes d'infrastructure et de contrôle (cf. chapitre 1.4.1.2) doivent faire l'objet de mesures particulières afin d'en garantir la confidentialité et l'intégrité.

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

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Les systèmes informatiques de l'IGC mettant en œuvre le module cryptographique font l'objet d'une qualification tel qu'indiqué au chapitre 11.

6.6 Mesures de sécurité liées au développement des systèmes

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques doivent satisfaire aux objectifs de sécurité.

6.6.1 Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC doit être documentée et doit respecter dans la mesure du possible des normes de modélisation et d'implémentation.
La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau doivent être documentées et contrôlées.

L'AC doit :

- garantir que les objectifs de sécurité sont définis lors des phases de spécification et de conception,
- utiliser des systèmes et des produits fiables qui sont protégés contre toute modification.

6.6.2 Mesures liés à la gestion de sécurité

Toute évolution significative d'un système d'une composante de l'IGC doit être signalée à l'AC pour validation. Elle doit être documentée et doit apparaître 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.

Toute évolution significative d'un système d'une composante de l'IGC doit faire l'objet d'une validation préalable de l'AC.
Ces évolutions logicielles ou matérielles sont contrôlées et validées sur une plateforme de test et d'intégration avant d'être portées sur la plateforme de production.

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

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

6.7 Mesures de sécurité réseau

Afin d'offrir un niveau de sécurité optimal, l'AC Racine est opérée hors-ligne. De ce fait, elle fait l'objet d'une isolation des autres réseaux.

Les mesures de sécurité réseau décrites ci-dessous sont cependant applicables aux fonctions de publication.

L'interconnexion vers des réseaux publics doit être protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.
L'AC doit garantir que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de leur conformité avec les exigences spécifiées par l'AC.
De plus, les échanges entre composantes au sein de l'IGC peuvent nécessiter la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

6.8 Horodatage / Système de datation

Plusieurs exigences de la présente PC nécessitent la datation par les différentes composantes de l'IGC d'événements liés aux activités de l'IGC (cf. chapitre 5.4).

Pour dater ces événements, les différentes composantes de l'IGC ont recours à l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près.

Pour les opérations faites hors ligne (ex : administration d'une AC Racine), cette précision de

synchronisation par rapport au temps UTC n'est pas requise. Le système doit toutefois pouvoir ordonner les événements avec une précision suffisante. De ce fait, l'horloge est vérifiée avant toute opération, pour s'assurer qu'elle n'a pas dérivé. Pour la synchronisation par rapport au temps UTC, il est recommandé de se référer à un système comprenant au moins deux sources indépendantes de temps.

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 Profil du certificat de l'AC2-FINANCES-CRYPT-RACINE

Ces certificats au format X509 v3 sont conformes à la RFC5280, RFC3739 et ETSI_QC

7.1.1 Champs de base

Champ	**valeur**
Version	La valeur de ce champ doit être "2", indiquant qu'il s'agit d'un certificat version 3.
Serial number	Numéro de série unique du certificat
Signature	Identifiant de l'algorithme de signature de l'AC émettrice Sha256RSA
Issuer	CN = AC2-FINANCES-CRYPT-RACINE OU = 0002 130013345 O = MINISTERE DE L ECONOMIE ET DES FINANCES C = FR
Validity period (Valide à partir du)	Date de validité du certificat
Validity period (Valide jusqu'au)	Date d'expiration du certificat – durée de validité 10 ans
Subject	voir issuer (certificat auto-signé)
Subject Public Key Info	Valeur de la clé publique RSA (4096)
Unique Identifiers (issuer et subject)	Non utilisé
Extensions	Cf. chapitre suivant.

7.1.2 Extensions du certificat

Champ	**Critique**	**Description et valeur**
Authority Key Identifier	N	Cette extension contient l'identifiant de la clé publique de l'AC émettrice
Subject Key Identifier	N	voir « *Authority Key Identifier » (certificat auto-signé)*
Key Usage	O	Cette extension doit être marquée "critique". Certsign et CRL Sign
Certificate Policies	N	PC OID = 2.5.29.32.0 (AnyPolicy) https://igc1.finances.gouv.fr/ac2-finances-crypt-racine.pdf https://igc2.finances.gouv.fr/ac2-finances-crypt-racine.pdf
CRL Distribution Points	N	http://igc1.finances.gouv.fr/ac2-finances-crypt-racine.crl http://igc2.finances.gouv.fr/ac2-finances-crypt-racine.crl
Basic Constraints	O	Type d'objet = CA

		Maximum Path Length = non spécifié

7.1.3 OID des algorithmes

Cf. Chapitre 7.1.1

7.1.4 Forme des noms

Cf. Chapitre 7.1.1

7.1.5 Contraintes sur les noms

Le Distinguish Name (DN) doit respecter le format Printable String ou le format UTF8 String.

7.1.6 OID des PC

Cf. Chapitre 7.1.2

7.1.7 Utilisation de l'extension « Contraintes Politiques »

Cf. Chapitre 7.1.2

7.1.8 Sémantique et syntaxe des qualifiants de politique

Cf. Chapitre 7.1.2

7.1.9 Sémantique de traitement des extensions critiques de PC

Cf. Chapitre 7.1.2

7.2 Profil des LCR

7.2.1 Champs de base

Les LCR de l'AC contiennent les champs suivants :

Champ	**valeur**
Version	Contient la valeur 1 pour indiquer que la LCR est en version 2 ;
Signature	contient l'identifiant (OID) de l'algorithme utilisé par l'AC pour signer la LCR (SHA 256) et (RSA 4096) ;
Issuer	CN = AC2-FINANCES-CRYPT-RACINE OU = 0002 130013345 O = MINISTERE DE L ECONOMIE ET DES FINANCES C = FR
ThisUpdate	Contient la date de publication de la LCR
NextUpdate	Contient la date de publication de la prochaine mise à jour de la LCR (ThisUpdate + 1 mois)
RevokedCertificate	Contient la liste des certificats révoqués avec, pour chacun, les champs suivants : • **userCertificat** (numéro de série du certificat révoqué), • **revocationDate** (date de révocation du certificat). • **CrlExtensions :** Cf. ci-après

7.2.2 Extensions de LCR

Le tableau suivant présente les extensions utilisées

Nom de l'extension	Criticité	Valeur
authorityKeyIdentifier	non critique	Cette extension identifie la bi-clé de l'AC utilisée pour signer la CRL
CRLNumber	non critique	Cette extension contient le numéro de série de la LCR. Cette extension doit obligatoirement être renseignée. Ce numéro doit être incrémenté de 1 à chaque nouvelle CRL.

7.2.3 Extensions d'entrée de LCR

ReasonCode : Cette extension, non critique, contient le motif de la révocation. Cette extension n'est pas renseignée d'une manière détaillée.

7.3 Profil OCSP

7.3.1 Numéro de version

Sans Objet.

7.3.2 Extension OCSP

Sans Objet.

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits et les évaluations concernent, d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification et, d'autre part, ceux que doit réaliser, ou faire réaliser, l'AC afin de s'assurer que l'ensemble de son IGC, ainsi que le cas échéant le ou les MC, est bien conforme à ses engagements affichés dans sa PC et aux pratiques identifiées dans sa DPC.

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

8.1 Fréquences et/ ou circonstances des évaluations

Avant la première mise en service d'une composante de son IGC 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 de son IGC, à la fréquence suivante : 1 fois tous les 2 ans.

8.2 Identités / Qualifications des évaluateurs

Le contrôle d'une composante doit être 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.

Le contrôle d'une composante peut également être assigné par la DSI des ministères économiques et financiers à une équipe d'auditeurs compétents en sécurité des systèmes d'information pour vérifier sa conformité aux exigences de la politique de filialisation ministérielle.

8.3 Relations entre évaluateurs et entités évaluées

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

8.4 Sujets couverts par les évaluations

Les contrôles de conformité porte sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et vise à vérifier le respect des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5 Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend 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 respecte 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 PC et la 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 METRIERS LEGALES

9.1 Tarifs

Sans Objet.

9.2 Responsabilité financière

Sans Objet.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- la partie non-publique de la DPC de l'AC,
- les clés privées de l'AC, des composantes et des porteurs de certificats,
- les données d'activation associées aux clés privées d'AC et des porteurs,
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- le dossier d'enregistrement du porteur,
- les causes de révocations, sauf accord explicite du porteur.

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 est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles au 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, l'AC doit en garantir l'intégrité.

L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des porteurs à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations au porteur et éventuellement au MC.

9.4 Protection des données professionnelles

9.4.1 Politique de protection des données personnelles

Il est entendu que toute collecte et tout usage de données à caractère personnel 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 de la loi [CNIL] et la Réglementation Européenne [RGPD].

9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont les suivantes :

- Les causes de révocation des certificats des porteurs (qui sont considérées comme confidentielles sauf accord explicite du responsable de l'AC subordonnée) ;
- Les dossiers d'enregistrement.

9.4.3 Informations à caractère non personnel

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

9.4.4 Responsabilités en termes de protection des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci-dessous).

9.4.5 Notification et consentement d'utilisation des données personnelles

Les informations que tout porteur remet à l'AC doivent être intégralement protégées contre la divulgation sans le consentement de celui-ci, une décision judiciaire ou autre autorisation légale.

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci-dessous).

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

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci-dessous).

9.4.7 Autres circonstances de divulgation d'informations personnelles

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

9.5 Droits sur la propriété intellectuelle et industrielle

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.

9.6 Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC 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 PC de l'AC et les documents qui en découlent,
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l’équipe d'audit mandatée par l'AC (cf. chapitre 8) et l'organisme de qualification,
- respecter les accords ou contrats qui les lient entre elles ou aux porteurs,
- 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 a pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu’elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, conformément aux exigences du chapitre 4.4 ci-dessus.
- Garantir et maintenir la cohérence de sa DPC avec sa PC.
- Prendre toutes les mesures raisonnables pour s’assurer que ses porteurs 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 de l’IGC. La relation entre un porteur et l’AC est formalisée par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l’AC.

L’AC est responsable de la conformité de ses politiques de certification avec les exigences émises dans les PC Type du RGS
L’AC assume toute conséquence dommageable résultant du non-respect de sa PC par elle-même ou l’une de ses composantes. Elle doit prendre les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique.

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

Par ailleurs, l’AC reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l’intégrité des certificats délivrés par elle-même 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. les obligations pertinentes du chapitre 9.6.1.

9.6.3 Porteurs de certificats

Le porteur de certificat (l'AC subordonnée) a le devoir de :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- Protéger sa clé privée, dont il a la responsabilité, par des moyens appropriés à son environnement ;
- Protéger les données d'activation de cette clé privée et, le cas échéant, les mettre en œuvre ;
- Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
- Informer l'AC Racine de toute modification concernant les informations contenues dans son certificat ;
- Faire, sans délai, une demande de révocation de son certificat, dont il est responsable, 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).

La relation entre le porteur et l'AC ou ses composantes est formalisée par un engagement du porteur visant à certifier l'exactitude des renseignements et des documents fournis.

9.6.4 Utilisateurs de certificats

Les utilisateurs de la Sphère publique utilisant les certificats doivent :

- vérifier et respecter l'usage pour lequel un certificat a été émis ;
- contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application ;
- pour chaque certificat de la chaîne de certification, du certificat du porteur 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.

L'AC ne doit pas émettre dans sa propre PC d'obligations supplémentaires, par rapport aux obligations de la PC Type (RGS), à l'encontre des utilisateurs de la Sphère publique.

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 responsabilité

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

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 PC de l'AC doit rester en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PC.

9.10.2 Fin anticipée de la validité

La publication d'une nouvelle version des PC Type (RGS) ou de la politique de filialisation des ministères économiques et financiers peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC correspondante.
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 restants applicables

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

9.11 Notifications individuelles et communications entre participants

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

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

9.12 Amendements de la PC

9.12.1 Procédures d'amendements

L'AC doit contrôler que tout projet de modification de cette PC reste conforme aux exigences de la politique de filialisation des ministères et des éventuels documents complémentaires du [RGS]. En cas de changement important, il est recommandé à l'AC de faire appel à une expertise technique pour en contrôler l'impact.

9.12.2 Mécanisme et période d'information sur les amendements

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

9.12.3 Circonstances selon lesquelles l'OID doit être changé

L'OID de la PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de cette PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.
En particulier, l'OID de la PC de l'AC doit évoluer dès lors qu'un changement majeur (et qui sera signalé comme tel, notamment par une évolution de l'OID de la présente PC) intervient dans les exigences de la politique de filialisation applicable à la famille de certificats considérée.

9.13 Dispositions concernant la résolution des conflits

L'AC doit mettre en place des politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles elle fournit des services électroniques de confiance ou d'autres points qui y sont liés.

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

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'activité

Cf. Paragraphe 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

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

9.17 Autres dispositions

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

10 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 Réglementation

Renvoi	Document
[CNIL]	*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.*
[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.*
[RGPD]	*Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*
[DécretRGS]	*Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005*

10.2 Documents techniques

Renvoi	Document
[RGS]	*Référentiel Général de Sécurité – Version 2.0*
[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 (2004-02) Cryptographic Module for CSP Signing Operations with Backup – Protection Profile (CMCSOB-PP). Ce PP a été certifié EAL4+.*
[CWA14167-3]	*CWA 14167-3 (2004-02) Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)*
[CWA14167-4]	*CWA 14167-4 (2004-02) Cryptographic Module for CSP Signing. Operations with Backup – Protection Profile (CMCSO-PP). Ce PP a été certifié EAL4+.*
[ExigencesSitesPerso]	*Exigences de sécurité des sites de personnalisation, V1.0 (août 2007) https://www.references.modernisation.gouv.fr/sites/default/files/Exigences_sites_de_perso_V1_0.pdf*
[ETSI_NQCP]	*ETSI EN 319411-1 v1.1.1 de Février 2016. Policy and Security Requirements for Trusted Service Issuing Certificates ; Part 1 : General Requirements.*
[PROG_ACCRED]	*COFRAC -Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 -publié cf*

	www.cofrac.fr
[RFC3647]	*IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003*
[RFC5280]	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
[RGS_B_1]	*Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 1.20*
[X.509]	*Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version mars 2000 (complétée par les correctifs techniques n° 1 d'octobre 2001, n° 2 d' avril 2002 et n° 3 d'avril 2004)*
[972-1]	*DCSSI - Guide Technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter – N° 972-1/SGDN/DCSSI du 17/07/2003*

11 ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC2-FINANCES-CRYPT-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), ainsi que, le cas échéant, générer les bi-clés des porteurs, doit répondre aux exigences de sécurité suivantes :

- assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- être capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné;
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- permettre de 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 privée 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.

Il est recommandé que le module cryptographique de l'AC détecte les tentatives d'altérations physiques et entre dans un état sûr quand une tentative d'altération est détectée.

11.2 Exigences sur la qualification

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

La qualification du module cryptographique a été réalisée conformément à [ORDONNANCE], au niveau renforcé défini par le [RGS] et en respectant les exigences du [CWA 14167-1]