MINISTÈRES
ÉCONOMIQUES
ET FINANCIERS

Liberté
Égalité
Fraternité

Secrétariat
général

SECRÉTARIAT GÉNÉRAL
SERVICE DE L'ENVIRONNEMENT PROFESSIONNEL
139 RUE DE BERCY
75572 PARIS CEDEX 12

POLITIQUES DE CERTIFICATION

DE L'AC3-FINANCES-SERVEURS

Document 01

OID : Authentification serveur : 1.2.250.1.131.1.13.2.3.1.1
OID : Authentification client : 1.2.250.1.131.1.13.2.3.1.2

Version - Date	Emetteur	Statut/Suivi des modifications
V1-Août 2023	SNUM-MCTI	Création

Entité	Rédaction	Vérification	Approbation
SNUM-MCTI	X	X	
SHFDS			X

Table des matières

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 ».

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 rénovation est portée par le Service du Numérique (SNUM), maîtrise d'ouvrage stratégique des IGC du Ministère de l'Economie et des Finances.

Cette IGC est opérée par la Service du Numérique du Secrétariat Général (SNUM), et comporte :

- Une AC racine (AC3 FINANCES RACINE),

- Quatre AC subordonnées :

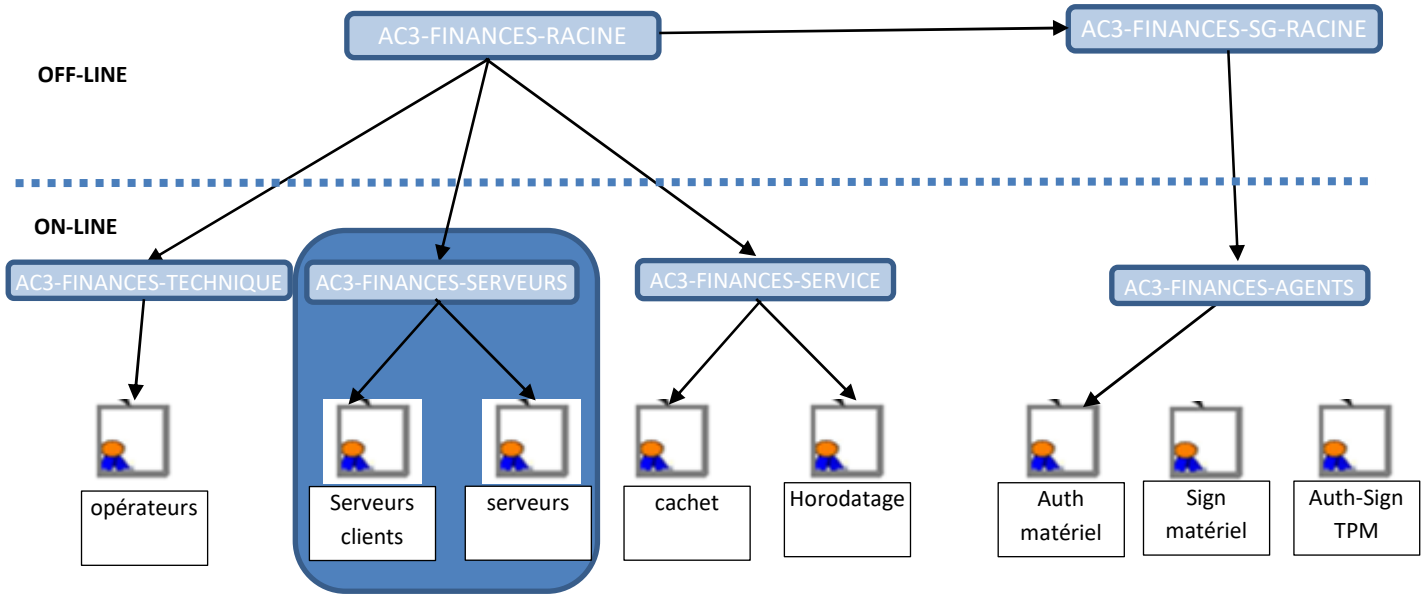
- L'AC3-FINANCES-SERVEURS pour les certificats d'authentification serveur ou serveur client,

- L'AC3-FINANCES-SERVICES pour les certificats cachet ou d'horodatage,

- L'AC3-FINANCES-TECHNIQUE pour les certificats aux opérateurs de ces IGC.
- L'AC3-FINANCES-SG-RACINE pour les certificats agents et prestataires

L'IGC FINANCES peut également signer les IGC de directions.

L'AC3-FINANCES-SERVEURS est filialisée à l'AC3-FINANCES-RACINE selon le schéma suivant :



L'objectif principal de cette IGC est de sécuriser les échanges et d'apporter la confiance afin que chaque usager des téléservices ou des téléprocédures puisse être assuré d'un niveau minimum élevé et constant de sécurité.

Les certificats sont délivrés uniquement pour des sites non exposés sur Internet.

L'AC3-FINANCES-SERVEURS délivre deux types de certificats dans le cadre de l'IGC Finances du Ministère de l'Economie et des Finances *:*

- *Certificats d'authentification **Serveurs** mono et multidomaine (certificat du serveur utilisé par les personnes physiques souhaitant l'authentifier, en mode TLS ou SSL) ;*
- *Certificats d'authentification C**lients** mono et multidomaine(certificat du serveur qu'il utilise pour s'authentifier vis à vis d'un autre serveur, en mode client).*

La délivrance de certificats de type 'wildcard' n'est pas autorisée.

Dans le présent document, le terme « serveur » représente un ou plusieurs serveurs physiques détenant un même FQDN *(fully qualified domain name*).

Le présent document, Politiques de Certification de l'Autorité de Certification Finances Serveurs, formalise les règles que l'AC3-FINANCES-SERVEURS respecte pour la gestion de ces deux types de certificats électroniques.

Ces Politiques de Certification sont conformes dans leur 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 1.0) et la politique de filialisation de l'IGC ministérielle version 1.2 en cours de validité.

Le niveau de sécurité cible couvert par cette IGC correspond au niveau 1 étoile du RGSv2 sans faire l'objet d'une qualification.

Convention d'écriture

Tout au long de ce document, le terme AC est utilisé pour désigner l'autorité de certification de

l'AC3-FINANCES-SERVEURS et le terme AC racine pour désigner l'AC3-FINANCES-RACINE.

La convention d'écriture suivante a été respectée :

- le texte en police normale reprend les principes énoncés dans les PC Type du RGS.

- le texte en police normale et avec un arrière-plan grisé est particulier aux présentes PC.

- les termes entre crochets sont définis en annexe 1.

1.2 Identification du document

Ce document décrit deux politiques de certification dénommées :

– Politique de Certification AC3-FINANCES-SERVEURS famille de certificats Authentification serveur
Le numéro OID de cette PC est : 1.2.250.1.131.1.13.2.3.1.1

– Politique de Certification AC3-FINANCES-SERVEURS famille de certificats Authentification client Le numéro OID de cette PC est : 1.2.250.1.131.1.13.2.3.1.2

Le présent document est conforme *aux RFC [5280] et [3647], au RGS V1* et s'appuie sur la *PC Type du RGS A3_RGS_PC Type Authentification Serveur V2.3*.

1.3 Définitions et acronymes

1.3.1 Acronymes

Les acronymes utilisés dans les présentes PC sont les suivants :

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

DN Distinguished Name

DPC Déclaration des Pratiques de Certification

ETSI European Telecommunications Standards Institute

FQDN Fully Qualified Domain Name

IGC Infrastructure de Gestion de Clés.

LAR Liste des certificats d'AC Révoqués

LCR Liste des Certificats Révoqués

MC Mandataire de Certification

MEF Ministère de l'Economie et des Finances

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

RC Responsable du Certificat

RSA Rivest Shamir et Adelman

SDAE Service du Développement de l'Administration Électronique

S/MIME Secure/Multipurpose Internet Mail Extensions

SG/SNUM Secrétariat Général / Service du Numérique

SHA Secure Hash Algorithm

SHFDS Service du Haut Fonctionnaire de Défense et de Sécurité

SP Service de Publication

SSI Sécurité des Systèmes d'Information

SSL Secure Sockets Layer

TLS Transport Layer Security

URL Uniform Resource Locator

1.3.2 Définitions

Les termes utilisés dans les présentes PC sont les suivants :

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

Applicatif de vérification d'authentification - Il s'agit de l'application mise en œuvre par l'utilisateur ou le serveur pour vérifier l'authentification d'un autre serveur et établir une session sécurisée avec ce serveur, notamment générer la clé symétrique de session et la chiffrer avec la clé publique du serveur contenue dans le certificat correspondant.

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins d'authentification, de chiffrement ou de signature du porteur du certificat ou des besoins d'authentification ou de cachet du serveur auquel le certificat est rattaché.

Autorités administratives - Ce terme générique, défini à l'article 1 de l'[ORDONNANCE], désigne les administrations de l'Etat, 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 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 des présentes PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la PC Type authentification Serveur V2.3, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

Autorité d'enregistrement - Cf. chapitre I.4.1.

Autorité d'horodatage - Autorité responsable de la gestion d'un service d'horodatage (cf. politique d'horodatage type du [RGS]).

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 la PC Type authentification Serveur V2.3, le terme "certificat électronique" désigne uniquement un certificat délivré à un serveur informatique sous la responsabilité d'un RC et portant sur une bi-clé d'authentification et d'échange de clés symétriques de session, 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.

Service du Numérique : Service numérique du Secrétariat Général du Ministère de l'Economie et des Finances Il définit et fait appliquer la politique de filialisation des IGC des directions et services du Ministère de l'Economie et des Finances. Il signe les certificats d'AC racine correspondants. Il est le propriétaire des clés de l'AC Racine du ministère (AC3-FINANCES-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'AC3-FINANCES-SERVEURS.

Dispositif de protection des clés privées - Il s'agit du dispositif matériel et/ou logiciel utilisé par le serveur pour stocker et mettre en œuvre sa clé privée.

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 I.4.1.

Fonction de génération des éléments secrets du porteur - Cf. chapitre I.4.1.

Fonction de gestion des révocations - Cf. chapitre I.4.1.

Fonction de publication - Cf. chapitre I.4.1.

Fonction de remise au porteur - Cf. chapitre I.4.1.

Fonction d'information sur l'état des certificats - Cf. chapitre I.4.1.

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.

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.

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

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

Mandataire de certification - Cf. chapitre I.4.1.

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 du ministère.

Personne autorisée - Cf. chapitre I.4.1.

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 RC et les utilisateurs de certificats.

Porteur - Cf. chapitre I.4.1.

Prestataire de services de certification électronique (PSCE) - L'[ORDONNANCE] introduit et définit les prestataires de service de confiance (PSCO). Un PSCE est un type de PSCO particulier. Un PSCE se définit comme 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 RC 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 - Le [DécretRGS] décrit la procédure de qualification des PSCO. Un PSCE étant un PSCO particulier, la qualification d'un PSCE est un 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.

Responsable du certificat d'authentification serveur - Cf. chapitre I.4.1.

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 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.

Serveur informatique - Il s'agit d'un service applicatif (disposant d'un certificat fourni par l'AC), rattachés à l'entité (identifiée dans le certificat). Ce service est hébergé sur un ou plusieurs serveurs physiques rattachés à un même nom de domaine (FQDN – fully qualified domain name).

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. Nota - Un agent d'une autorité administrative qui procède à des échanges électroniques avec une autre autorité administrative est, pour cette dernière, un usager.

Utilisateur de certificat - Cf. chapitre I.4.1.

Service du Haut Fonctionnaire de Défense et de Sécurité (SHFDS) : Il a en charge le contrôle de l'application des réglementations de sécurité. Il est responsable du dispositif de contrôle des IGC ministérielles et fait auditer périodiquement ces IGC.

1.4 Entités intervenant dans l'IGC

1.4.1 Autorités de certification

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

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

La décomposition fonctionnelle de l'*AC* est la suivante :

- Autorité d'enregistrement (AE)

  Cette fonction vérifie les informations d'identification du futur responsable du certificat d'authentification serveur (RC) et du serveur informatique auquel le certificat doit être rattaché, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC.

  L'AE a également en charge, lorsque cela est nécessaire, la revérification des informations du RC et/ou du serveur informatique lors du renouvellement du certificat de celui-ci.

- Fonction de génération des certificats

  Cette fonction génère *(création du format, signature électronique avec la clé privée de l'AC)* les certificats à partir des informations transmises par l'autorité d'enregistrement et la clé publique du serveur provenant du RC.

- Fonction de génération des éléments secrets du serveur

  Cette fonction génère les éléments secrets du serveur.

De tels éléments secrets peuvent être, par exemple, directement la bi-clé du serveur, les codes (activation / déblocage) liés au dispositif de protection de la clé privée du serveur ou encore des codes ou clés temporaires permettant au RC de mener à distance le processus de génération / récupération du certificat du serveur.

Cette fonction n'est pas assurée par l'AC, les éléments secrets étant directement générés sur le serveur.

- Fonction de remise au RC

  Cette fonction remet au RC au minimum le certificat du serveur ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif de protection de la clé privée du serveur, clé privée du serveur, codes d'activation, …).

  Dans le cas de l'AC, cette fonction consiste à transmettre au RC le certificat en pièce jointe d'un courriel.

- Fonction de publication

  Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux RC et/ou aux utilisateurs de certificats, hors informations d'état des certificats.

  Dans le cas de l'AC, les certificats ne sont pas publiés.

- Fonction de gestion des révocations

  Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

- Fonction d'information sur l'état des certificats

  Cette fonction fournit aux utilisateurs de certificats des informations sur 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) *et lors de la révocation d'un certificat.*

Les fonctions ci-dessus sont les fonctions minimales que doit obligatoirement mettre en œuvre une IGC gérant des certificats d'authentification serveur, à l'exception de la fonction de génération des éléments secrets du serveur qui est optionnelle et qui dépend des prestations effectivement offertes par l'AC.

1.4.1.1 Acteurs

Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

- Responsable du certificat d'authentification serveur (RC) - La personne physique responsable du certificat d'authentification du serveur, notamment de l'utilisation de ce certificat et de la bi-clé correspondante, pour le compte de l'entité dont dépend le serveur informatique identifié dans le certificat ;
- Mandataire de certification (MC) - Le mandataire de certification est désigné par et placé sous la responsabilité de l'entité cliente. Il est en relation directe avec l'AE. Il assure pour elle un certain nombre de vérifications concernant l'identité et, éventuellement, les attributs des RC et des serveurs informatiques de cette entité (il assure notamment le face-à-face pour l'identification des RC lorsque celui-ci est requis).

  Dans le cas de l'IGC FINANCES, les mandataires de certification sont désignés par les Directions.

- Utilisateur de certificat - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une valeur d'authentification provenant du serveur auquel le certificat est rattaché, ou pour établir une clé de session.
- Personne autorisée - Il s'agit d'une personne autre que le RC et le mandataire de certification et qui est autorisée par la politique de certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du RC (demande de révocation, de renouvellement, …). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du RC ou d'un responsable des ressources humaines.

Les parties de l'AC concernées par la génération de certificat et la gestion des révocations doivent être indépendantes d'autres organisations en ce qui concerne leurs décisions concernant la mise en place, la fourniture, le maintien et la suspension des services ; en particulier, leurs cadres dirigeants, leur personnel d'encadrement et leur personnel ayant des rôles de confiance, doivent être libres de toute pression d'ordre commercial, financier ou autre, qui pourraient influer négativement sur la confiance dans les services fournis par l'AC. Les parties de l'AC concernées par la génération de certificat et de la gestion des révocations doivent avoir une structure documentée qui préserve l'impartialité des opérations.

L'organisation adoptée dépend notamment des prestations fournies par l'AC : génération ou non de la bi-clé du serveur, fourniture ou non du dispositif de protection de la clé privée du serveur et, si oui, fourniture avant ou après génération de la bi-clé du serveur, etc.

Dans la pratique, la mise en œuvre opérationnelle de ces fonctions peut être effectuée par une ou plusieurs composante(s) de l'IGC (opérateurs techniques et/ou autorités tel que OC, AE, SP, AH, …), qui peuvent être internes à l'AC et/ou opérées par des entités externes.

La Déclaration des Pratiques de Certification (DPC) de l'AC doit décrire l'organisation opérationnelle de son IGC et la répartition des rôles entre les différentes composantes en fonction de l'organisation fonctionnelle et de la définition des rôles décrites dans les présentes PC.

Les composantes de l'AC ne sont pas opérées par des entités externes. Quelle que soit l'organisation opérationnelle mise en œuvre, l'AC reste in fine responsable vis-à-vis de toute partie externe à l'IGC (utilisateurs, autorités publiques, etc.) des prestations fournies et doit garantir le respect des engagements pris dans sa PC et sa DPC, relatifs à son activité de certification.

1.4.1.2 Exigences

L'AC respecte les exigences décrites dans la PC Type Authentification Serveur V2.3 type RGS une étoile et s'engage à ce que les composantes de l'IGC, internes à l'AC, respectent aussi les exigences qui les concernent.

Dans le cadre de ses fonctions opérationnelles, les exigences qui incombent à l'AC en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- Être une entité légale au sens de la loi française.
- Être en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats d'authentification serveur de cette entité. L'AC peut aussi, le cas échéant, être en relation contractuelle / hiérarchique / réglementaire avec le ou les mandataires de certification choisis par l'entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux RC, aux utilisateurs de certificats, ceux qui mettent en œuvre ses certificats.

- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions obligatoires de la PC Type authentification Serveur V2.3, notamment en matière de génération des certificats, de remise au RC, de gestion des révocations et d'information sur l'état des certificats.
- Élaborer, mettre en œuvre, contrôler, et maintenir en condition de sécurité les composants et de de façon itérative les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, et correspondant au minimum aux exigences de la PC Type authentification Serveur V2.3, notamment en termes de fiabilité, de qualité et de sécurité. À ce titre, elle doit posséder un ou des systèmes de gestion de la qualité et de la sécurité de l'information adaptés aux services de certification qu'elle assure.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats et de LCR), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure.
- Diffuser ses certificats d'AC aux RC et utilisateurs de certificats.
- Suivre les demandes en capacité et réaliser des projections concernant les futurs besoins en capacité afin de garantir la disponibilité du service, notamment en matière de capacités de traitement et de stockage.

1.4.2 Autorité d'enregistrement

L'AE a pour rôle de vérifier l'identité du futur RC et les informations liées au serveur informatique.

Pour cela, l'AE assure les tâches suivantes :

- La prise en compte et la vérification des informations du futur RC et du serveur informatique, ainsi que de leur entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- Le cas échéant, la prise en compte et la vérification des informations du futur MC et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- L'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC suivant l'organisation de cette dernière et les prestations offertes ;
- L'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;
- La conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du RC ou, le cas échéant, du MC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

L'AE s'appuie sur des MC désignés et placés sous la responsabilité de l'entité cliente pour effectuer tout ou partie des opérations de vérification des informations. Dans ce cas, l'AE s'assure que les demandes sont complètes et exactes et effectuées par un MC dûment autorisé. Dans tous les cas, l'archivage des pièces du dossier d'enregistrement (sous forme électronique et/ou papier) est de la responsabilité de l'AE (cf. chapitre 5.5).

L'AE délègue également une partie de ses fonctions à des unités de proximités au sein des Directions à Réseaux. Ces unités sont désignées sous le nom d'autorités d'enregistrement déléguées (AED). La mise en place d'une AED nécessite la signature préalable d'une convention avec la Direction à Réseau.

1.4.3 Responsables de certificats d'authentification serveur

Dans le cadre des présentes PC, un RC est une personne physique qui est responsable de l'utilisation du certificat du serveur informatique identifié dans le certificat et de la clé privée correspondant à ce certificat, pour le compte de l'entité également identifiée dans ce certificat. Le RC a un lien contractuel / hiérarchique / réglementaire avec cette entité. Le RC respecte les conditions qui lui incombent définies dans la PC de l'AC, qui reprend les conditions définies dans la PC Type authentification Serveur V2.3.

Il est à noter que le certificat étant attaché au serveur informatique et non au RC, ce dernier peut être amené à changer en cours de validité du certificat : départ du RC de l'entité, changement d'affectation et de responsabilités au sein de l'entité, etc.

L'entité doit signaler à l'AC préalablement, sauf cas exceptionnel et dans ce cas sans délai, le départ d'un RC de ses fonctions et lui désigner un successeur. Une AC doit révoquer un certificat d'authentification serveur pour lequel il n'y a plus de RC explicitement identifié.

Pour rappel, les certificats sont délivrés uniquement pour des sites non exposés sur Internet.

1.4.4 Utilisateurs de certificats

Les présentes PC traitant de certificats d'authentification serveur (cf. chapitre 1.4), un utilisateur de certificats peut être notamment :

- Un agent (personne physique) accédant à un serveur informatique et qui utilise le certificat du serveur et un module de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat du serveur, afin d'établir une clé de session partagée entre son poste et le serveur. L'agent respecte la politique et les pratiques de sécurité édictées par le responsable de son entité.
- Un usager (personne physique) accédant à un serveur informatique d'une autorité administrative et qui utilise le certificat du serveur et un module de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat, afin d'établir une clé de session partagée entre son poste et le serveur.
- Un serveur informatique accédant à un autre serveur informatique et qui utilise un certificat et un applicatif de vérification d'authentification afin d'authentifier le serveur auquel il accède, qui est identifié dans le certificat, et afin d'établir une clé de session partagée entre les deux serveurs.

1.4.5 Autres participants

1.4.5.1 Mandataires de certification

Le recours à un mandataire de certification (MC) est obligatoire pour une entité. Une même entité peut s'appuyer sur un ou plusieurs MC. Le MC est formellement désigné par un représentant légal de l'entité concernée. Le MC est en relation directe avec l'AE de l'IGC.

Les engagements du MC à l'égard de l'AC sont précisés dans un contrat écrit avec l'entité responsable du MC. Ce contrat stipule notamment que le MC doit :

- Effectuer correctement et de façon indépendante les contrôles d'identité et des éventuels attributs des futurs RC et serveurs informatiques de l'entité pour laquelle il est MC,
- Respecter les parties de la PC et de la DPC de l'AC qui lui incombent.

L'entité doit signaler à l'AC, si possible préalablement mais au moins sans délai, le départ du MC de ses fonctions et, éventuellement, lui désigner un successeur.

Le MC ne doit en aucun cas avoir accès aux moyens qui lui permettraient d'activer et d'utiliser la clé privée associée à la clé publique contenue dans le certificat d'authentification serveur délivré au RC.

1.4.5.2 Autorité d'Enregistrement Déléguée

L'AED assure, par délégation de l'AE, pour le périmètre de sa direction de rattachement, une partie du rôle de l'AE dans le cadre de la vérification de l'identité du futur porteur de certificat. Pour cela, l'AED assure les tâches suivantes :

- La prise en compte et la vérification des informations du futur porteur et de son entité de rattachement ainsi que la constitution du dossier d'enregistrement correspondant.
- L'envoi à l'AE pour archivage des pièces du dossier d'enregistrement.
- L'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC suivant l'organisation de cette dernière et les prestations offertes.
- La conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du porteur ou, le cas échéant, du MC, y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment, elle respecte la législation relative à la protection des données personnelles).

L'AED peut s'appuyer sur un MC désigné et placé sous la responsabilité de son entité pour effectuer tout ou partie des opérations de vérification des informations. Dans ce cas, l'AED s'assure que les demandes sont complètes et exactes et effectuées par un MC dûment autorisé. Dans tous les cas, l'archivage des pièces du dossier d'enregistrement (sous forme électronique et/ou papier) est de la responsabilité de l'AE (cf. chapitre 5.5).

L'AED n'assure pas les opérations suivantes, ces tâches étant prises en charge par l'AE :

- La prise en compte et la vérification des informations du futur MC et de son entité de rattachement ainsi que la constitution du dossier d'enregistrement correspondant.
- L'archivage définitif des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage).

Une AED est mise en place par la signature d'une convention entre le Secrétariat Général et la Direction souhaitant mettre en place l'AED.

1.5 Usage des certificats

1.5.1 Domaines d'utilisation applicables

1.5.1.1 Bi-clés et certificats du serveur

Les présentes PC traitent des bi-clés et des certificats à destination de serveurs informatiques, afin que ces serveurs puissent être authentifiés dans le cadre de l'établissement de sessions sécurisées, de type SSL / TLS, avec les catégories d'utilisateurs de certificats identifiées au chapitre I.3.4 ci-dessus et établir une clé symétrique de session afin que les échanges au sein de ces sessions soient chiffrés.

L'établissement de la clé de session peut se faire par un mécanisme cryptographique asymétrique, de type RSA (génération de la clé symétrique par le client et chiffrement de cette clé symétrique par la clé publique du serveur).

Ceci correspond notamment aux relations suivantes :

- Établissement d'une session sécurisée entre un serveur d'une autorité administrative et un usager ;
- Établissement d'une session sécurisée entre un serveur et un agent,
- Établissement d'une session sécurisée entre deux serveurs.

Les certificats d'authentification serveur objets des présentes PC, respectant le niveau * RGS, sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité du serveur afin de tromper l'utilisateur et/ou d'accéder aux données protégées transmises par l'utilisateur sont moyens (intérêt pour les usurpateurs, attraits des données considérées comme sensibles, etc.).

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

Les présentes PC comportent également des exigences, lorsque nécessaire, concernant les bi-clés et certificats de l'AC (signature des certificats d'authentification serveur, des LCR / LAR) ainsi que des clés, bi-clés et certificats des composantes de l'IGC (sécurisation des échanges entre composantes, authentification des opérateurs, etc.).

Ces certificats sont délivrés par une AC interne à l'application IGC, initialisée lors de l'installation de cette application.

L'AC génère et signe différents types d'objets : certificats, LCR.

L'AC dispose d'une seule bi-clé et le certificat correspondant est rattaché à l'AC de niveau supérieur (hiérarchie d'AC).

Les bi-clés et certificats de l'AC pour la signature de certificats et de LCR ne doivent être utilisés qu'à cette fin. Ils ne doivent notamment être utilisés ni à des fins de confidentialité, ni à des fins d'authentification.

Conformément au [CWA14167-1], les différentes clés internes à l'IGC peuvent être décomposées suivant les catégories suivantes :

- La clé de signature d'AC, utilisée(s) pour signer les certificats générés par l'AC ainsi que les informations sur l'état des certificats (LCR) ;
- Les clés d'infrastructure, utilisées par les systèmes intervenant dans l'IGC à des fins d'authentification, de signature des journaux d'événements, de chiffrement des données échangées ou stockées au sein de l'IGC, etc. ;
- Les clés de contrôle, assignées au personnel de l'IGC afin de s'authentifier vis-à-vis des différents systèmes, de signer et/ou de chiffrer des messages ou des données échangés, etc.

Les deux derniers types de clés sont des clés asymétriques.

Ces différents types de clés, et éventuellement les certificats correspondants, sont couverts par leurs propres engagements, complets et à part entière. Ces engagements font partie directement de la propre PC de l'AC, couvrant les certificats d'authentification serveur ou bien font l'objet de PC séparées (par exemple, PC d'une AC Racine couvrant les certificats d'AC).

Les certificats des opérateurs de l'IGC sont délivrés par une autorité de certification, l'AC3-FINANCES TECHNIQUE (couverte par sa propre PC dont l'OID est 1.2.250.1.131.1.13.12.13.1.1 qui est signée par l'AC3 FINANCES RACINE.

La PC de l'AC répondant à la PC Type authentification Serveur V2.3 doit au minimum reprendre les exigences de cette dernière sur les certificats d'AC et de composantes. En cas de traitement de ces certificats dans des PC séparées, ces PC doivent être cohérentes avec les exigences de la PC de l'AC et de la PC Type authentification Serveur V2.3.

1.5.2 Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.5 ci-dessous, en fonction du niveau de sécurité.). Tout autre usage est interdit, notamment, le déchiffrement SSL de sessions sécurisées L'AC respecte ces restrictions et impose leur respect par les RC auxquels elle délivre des certificats d'authentification serveur et les utilisateurs de ces certificats serveur.

À cette fin, elle doit communiquer à tous les RC, MC et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

1.6 Gestion de la PC

1.6.1 Entité gérant la PC

Au sein de la Mission Coordination des Technologies de l'Information du Service du Numérique SNUM, maîtrise d'ouvrage du projet, une cellule est responsable de la rédaction de la politique de certification.

Le SHFDS du SG est responsable de l'approbation de cette PC. Une autre cellule, maîtrise d'ouvrage stratégique, au sein de la Mission Coordination des Technologies de l'Information du Service du Numérique SNUM du Secrétariat Général, est responsable de la validation de la politique de certification.

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

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.

1.6.2 Point de contact

L'entité à contacter concernant les présentes PC est le Secrétariat Général du Ministère de l'Economie et des Finances :

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 le SNUM du SG du ministère.

1.6.3 Entité déterminant la conformité de la DPC avec ces PC

La conformité entre la DPC associée à ces PC et les présentes PC est prononcée par le SNUM du SG.

1.6.4 Procédures d'approbation de la conformité de la DPC

Le SHFDS, entité indépendante de l'AC fait auditer la conformité de la DPC avec les PC de l'AC. Sur la base du rapport d'audit, le SNUM du SG fait adapter, si besoin, le corpus documentaire de l'AC.

Le chapitre 8 détaille les exigences en termes d'audits de conformité et autres évaluations relatives à ces 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 est 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 la DPC.

2 Responsabilités concernant la mise à disposition des informations devant être publiées

2.1 Entités chargées de la mise à disposition des informations

Pour la mise à disposition des informations devant être publiées à destination des RC et des utilisateurs de certificats, l'AC met en œuvre au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats (listes de révocation cf. chapitre I.4.1 ci-dessus).

Les présentes PC précisent les méthodes de mise à disposition et les URL correspondantes (serveur Web de publication).

Dans sa fonction de publication des informations, l'IGC FINANCES 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

Dans sa fonction d'information sur l'état des certificats de l'AC racine et de l'AC, l'IGC publie les listes de révocation aux adresses suivantes :

https://igc1.finances.gouv.fr/ac3-finances-racine.crl

https://igc2.finances.gouv.fr/ac3-finances-racine.crl

https://igc1.finances.gouv.fr/ac3-finances-serveurs.crl

https://igc2.finances.gouv.fr/ac3-finances-serveurs.crl

Ainsi que sur l'Intranet des IGC du SG du Ministère de l'Economie et des Finances ;

2.2 Informations devant être publiées

L'AC publie les informations suivantes à destination des RC et utilisateurs de certificats :

- Ses politiques de certification, couvrant l'ensemble des rubriques du [RFC3647] et conforme à la PC Type (RGS), à la [RFC5280], ainsi que les éventuels documents complémentaires (par exemple, profils des certificats s'ils sont définis dans un document séparé) ;
- La liste des certificats révoqués (serveurs et AC) ;
- Les certificats de l'AC, en cours de validité ;
- L'AC étant rattachée à une hiérarchie d'AC, les certificats en cours de validité des AC de cette hiérarchie, les différentes politiques de certification correspondantes et les éventuels documents complémentaires, ceci jusqu'à l'AC Racine.

L'AC publie, à destination de la MOA des IGC, des administrateurs d'IGC et des opérateurs d'AE sa déclaration des pratiques de certification ainsi que toute autre documentation pertinente pour rendre possible l'évaluation de la conformité avec sa politique de certification.

L'AC publie également, à destination des RC, les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.), ainsi que les conditions générales d'utilisation.

De plus, compte tenu de la complexité de lecture d'une PC pour des personnes non spécialistes du domaine, l'AC publie également des conditions générales d'utilisation correspondant aux "PKI Disclosure Statement" (PDS) définis par [ETSI_NQCP] et [RFC3647].

Ces conditions générales ont une structure conforme à celle décrite en annexe B de [ETSI_NQCP] et reprennent ainsi, à destination des RC et des utilisateurs de certificats, les informations pertinentes des PC de l'AC :

- Les conditions d'usages des certificats et leurs limites,
- L'identifiant : OID de la PC applicable.
- Les obligations et responsabilités des différentes parties, notamment les exigences relatives à la vérification du statut de révocation d'un certificat pour les utilisateurs,
- Les garanties et limites de garantie de l'AC,
- Les informations sur comment vérifier un certificat,
- La durée de conservation des dossiers d'enregistrement et des journaux d'événements,
- Les procédures pour la résolution des réclamations et des litiges,
- Le système légal applicable,
- Si l'AC a été déclarée conforme à la politique identifiée et dans ce cas au travers de quel schéma.

Ces conditions générales font notamment partie intégrante du dossier d'enregistrement (dossier de demande de certificat).

Ces informations sont publiées dans les rubriques d'informations générales sur les sites suivants :

- 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.

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

2.3 Délais et fréquences de publication

Les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.) sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC. En particulier, toute nouvelle version doit être communiquée au RC 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.

Les certificats d'AC doivent être diffusés préalablement à toute diffusion de certificats de serveurs et/ou de LCR correspondants et les systèmes les publiant ont une disponibilité de 24h/24 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 4.9 et 4.10.

Il est à 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 est libre d'accès en lecture.

L'accès en modification aux systèmes de publication des autres informations est 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 sont conformes aux spécifications de la norme [X.500].

Dans chaque certificat conforme à la norme [X.509], l'AC émettrice (issuer) et le serveur informatique (subject) sont identifiés par un "Distinguished Name" (DN) de type [X.501].

Des règles sur la construction du DN de ces champs sont précisées dans le document [RGS_A_14].

Les certificats peuvent comporter un second FQDN (alternative name).

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les serveurs dans les certificats doivent être explicites. L'identification de l'entité à laquelle le serveur est rattaché est obligatoire.

Le DN du serveur contient son FQDN (« Fully Qualified Domain Name » ou nom de domaine totalement qualifié. Exemple : www.monHote.monDomaine.fr) auquel le serveur est rattaché.

Nota – Le certificat d'authentification serveur est associé au FQDN et pas au serveur physique sur lequel la bi-clé est déployée. Autrement dit, une bi-clé d'authentification serveur peut être déployée sur plusieurs machines physiques rattachées à ce FQDN (cas notamment d'architecture de répartition de charge).

La délivrance de certificats de type 'wildcard' n'est pas autorisée.

3.1.3 Pseudonymisation des serveurs

S'agissant de certificats de machines, les notions d'anonymisation ou de pseudonymisation sont sans objet.

3.1.4 Règles d'interprétation des différentes formes de nom

Le DN est encodé en UTF8, excepté pour le champ Country qui est encodé en printableString.

Le DN comporte les éléments suivants :

- L'attribut CommonName qui doit être constitué du FQDN du serveur,
- L'unité d'organisation (OU) = code ISO 6523 du Ministère de l'Economie et des Finances : 0002 110 020 013
- L'organisation (O = MINISTERE DE L ECONOMIE ET DES FINANCES)

- L'attribut CountryName en majuscules qui indique le pays (C = FR).

Un nom DNS (Domain Name System) étant présent dans le commonName (FQDN du serveur), la [RFC1123] section 2.1 doit être appliquée en plus du [RFC1034] pour contrôler la validité du nom.

3.1.5 Unicité des noms

Afin d'assurer l'identification unique du FQDN d'un serveur au sein du domaine de l'AC, notamment dans le cas du renouvellement du certificat associé, et pour éviter toute ambiguïté, le DN du champ "subject" de chaque certificat d'authentification serveur doit permettre d'identifier de façon unique le FQDN du serveur au sein du domaine de l'AC.

L'unicité des noms (du FQDN) est assurée par les procédures organisationnelles décrites dans la DPC.

Durant toute la durée de vie de l'AC, le FQDN d'un serveur rattaché à une entité ne peut être attribué à une autre entité.

3.1.6 Identification, authentification et rôle des marques déposées

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

3.2 Validation initiale de l'identité

L'enregistrement d'un RC se fait via la première demande de certificat serveur (formulaire de demande de certificat cosigné par le demandeur et le mandataire de certification.

[SERVEUR-SERVEUR] (certificat d'authentification serveur de type SSL/TLS) : Le RC démontrera qu'il est bien autorisé à utiliser le nom de domaine inclus dans le FQDN du serveur au travers du formulaire 'délégation ou subdélégation de l'autorité responsable de noms de domaine' signé par le responsable du domaine concerné. Un RC peut être amené à changer en cours de validité du certificat d'authentification serveur correspondant. Dans ce cas, tout nouveau RC doit disposer d'un certificat d'authentification de personne délivré par l'IGC FINANCES SG.

L'enregistrement d'un RC, et du serveur informatique correspondant, se fait via un mandataire de certification de l'entité préalablement enregistré par l'AE ou l'AED de rattachement du RC.

La validation initiale de l'identité d'une entité ou d'une personne physique est ainsi réalisée dans les cas suivants :

- Enregistrement d'un MC : validation de l'identité "personne morale" de l'entité pour lequel le MC interviendra et de l'identité "personne physique" du futur MC.
- Enregistrement d'un RC via un MC pour un certificat d'authentification serveur à émettre ou d'un nouveau RC pour un certificat d'authentification serveur déjà émis : validation par le MC de l'identité "personne physique" du futur RC, de son habilitation à être RC pour le serveur informatique considéré et pour l'entité considérée, ainsi que du nom de domaine du serveur. Le MC transmet le dossier validé à son AED de rattachement ou à l'AE le cas échéant.

Pour des raisons de simplicité de présentation, ces différents cas sont regroupés dans le chapitre 3.2.3.

3.2.1 Méthode pour prouver la possession de la clé privée

La bi-clé du serveur n'étant pas générée par l'AC, le RC doit fournir à l'AC, via le MC, une preuve de possession de la clé privée correspondant à la clé publique contenue dans la demande de certificat d'authentification serveur.

Cette exigence se matérialise par des considérations techniques décrites dans la DPC.

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

3.2.3.1 Enregistrement d'un porteur (Particulier)

Sans objet.

3.2.3.2 Enregistrement d'un porteur sans MC

Sans objet.

3.2.3.3 Enregistrement d'un Mandataire de Certification

Une AE est amenée à constituer un dossier d'enregistrement pour un Mandataire de Certification pour répondre au besoin d'utilisation du dossier du MC comme référence pour les données d'identification de l'entité de tous les RC présentés par le MC.

Le dossier d'enregistrement d'un MC remis à l'AE ou envoyé par courrier comprend

- Un mandat, daté de moins de 3 mois, désignant le MC. Ce mandat doit être signé par un représentant légal de l'entité et co-signé, pour acceptation, par le MC,
- Un engagement signé, et daté de moins de 3 mois, du MC, auprès de l'AC, à effectuer correctement et de façon indépendante les contrôles des dossiers des demandeurs,
- Un engagement signé, et daté de moins de 3 mois, du MC à signaler à l'AE son départ de l'entité,
- Une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative,
- Un document officiel d'identité en cours de validité du MC comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour), qui est présenté à l'AE qui en conserve une copie.

Nota - Le MC doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors d'une demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

Il n'est pas attribué de certificat de mandataire de certification aux mandataires.

L'authentification du MC par l'AE peut se faire par l'envoi du dossier papier par courrier accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, MC) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ces papiers d'identité, précédées de la mention "copie certifiée conforme à l'original").

3.2.3.4 Enregistrement d'un RC via un MC pour un certificat d'authentification serveur à émettre

Le futur RC doit demander un certificat d'authentification délivré par l'IGC FINANCES SG.

Le dossier d'enregistrement, déposé auprès d'un MC ou envoyé par courrier comprend :

- Un formulaire de demande de certificat d'authentification serveur signé par un MC de l'entité du RC. Ce formulaire doit être daté de moins de 3 mois et doit comporter :
    - [SERVEUR-SERVEUR] (certificat pour des serveurs de type serveur SSL/TLS) : le FQDN du serveur concerné par cette demande,
    - [SERVEUR-CLIENT] (certificat pour un serveur qui lors de l'établissement d'une session sécurisée avec un autre serveur se trouve être en mode client) : le nom du serveur concerné par cette demande,

  Ce formulaire de demande de certificat cosigné par un MC de l'entité du RC et le RC fait état de la qualité de RC du demandeur de certificat ;

- Toute pièce justificative attestant de l'existence de l'entité demandant le certificat ;
- Une pièce, valide au moment de l'enregistrement, portant délégation ou subdélégation de l'autorité responsable de la structure administrative incluse dans le formulaire de demande de certificat ;
- L'adresse mail du RC ;
- Le RC est formellement authentifié auprès de l'AE à l'aide de son certificat d'authentification de personne délivré par l'IGC FINANCES SG ce qui l'exonère de fournir une photocopie de sa pièce d'identité, Celle-ci a déjà été fournie lors de sa demande de certificat d'authentification de personne.
- [SERVEUR-SERVEUR] (certificat pour des serveurs de type serveur SSL/TLS) une preuve de possession par l'entité du nom de domaine correspondant au FQDN du serveur,
- Les conditions générales d'utilisation signées par le RC.

Nota : Le RC doit être informé que les informations personnelles d'identité pourront être utilisées comme éléments d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme. En complément, ou à la place, de l'utilisation de ces informations personnelles, il pourra être convenu avec l'AC d'un jeu de questions/réponses ou équivalent.

La DPC précise les procédures mises en œuvre pour respecter ces exigences.

Lors de la transmission des dossiers de RC par le MC par courrier, celui-ci doit s'authentifier auprès de l'AE ou, le cas échéant, de son AED de rattachement, par sa signature sur les pages du dossier.

3.2.3.5 Enregistrement d'un nouveau RC via un MC pour un certificat d'authentification serveur déjà émis

Dans le cas de changement d'un RC pour un certificat d'authentification serveur en cours de validité, le nouveau RC doit être enregistré en tant que tel par l'AC et disposer d'un certificat d'authentification de personne délivré par l'IGC FINANCES SG ce qui l'exonère de fournir une photocopie de sa pièce d'identité.

Le MC remet ou envoie à l'AE un formulaire de prise en charge de serveur. Il comprend :

- les noms de l'ancien et du nouveau RC

- les noms des serveurs concernés

- les conditions générales d'utilisation

- les signatures du MC et du nouveau RC

Le RC sera formellement authentifié auprès de l'AE,ou, le cas échéant, de son AED de rattachement, à l'aide de son certificat d'authentification de personne délivré par l'IGC FINANCES SG lors de ses demandes de certificat serveur.

3.2.3.6 Enregistrement d'un Opérateur d'AED

L'enregistrement d'un Opérateur d'AED ne peut se faire qu'auprès de l'AE centrale. Le dossier d'enregistrement doit au moins comprendre :

- Un engagement écrit du futur opérateur
  - à respecter ses engagements
  - à signaler son départ ou sa réaffectation à l'AC et à sa hiérarchie
- Une copie d'un document officiel d'identité en cours de validité du futur opérateur comportant une photographie d'identité notamment carte d'identité, passeport ou carte de séjour. Le dossier étant au format papier, la photocopie de la pièce d'identité devra être signée à la fois par le futur opérateur, la signature étant précédées de la mention "copie certifiée conforme à l'original".
- Un formulaire de nomination du futur porteur signé par le responsable légal de la Direction ayant la responsabilité de l'AED.
- Un extrait n°3 de casier judiciaire pour les futurs opérateurs n'ayant pas le statut d'agent de la fonction publique.

L'AE doit vérifier que l'identité du futur opérateur correspond à celle qui a été contrôlée lors du recrutement de l'agent (présence de l'agent dans l'annuaire de l'entité, numéro de bureau…).

Nota - Le futur opérateur doit être informé que les informations personnelles d'identité pourront être utilisées comme élément d'authentification lors de la demande de révocation de son certificat opérateur, dans le cas où l'AC s'appuie sur un tel mécanisme.

L'authentification de l'opérateur par l'AE se fait par l'envoi du dossier papier par courrier accompagné d'une photocopie de son document d'identité certifiée conforme par lui-même (date de moins de 3 mois, et signature de la personne concernée sur la photocopie de ces papiers d'identité, précédées de la mention "copie certifiée conforme à l'original").

3.2.4 Informations non vérifiées du RC et/ou du serveur informatique

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

3.2.5 Validation de l'autorité du demandeur

La validation de l'autorité du porteur à réaliser une demande de certificat est effectuée lors de la signature du formulaire de demande de certificat par le MC, en même temps que la validation de l'identité de la personne physique.

3.2.6 Certification croisée d'AC

Sans objet.

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

Le renouvellement de la bi-clé d'un serveur entraîne automatiquement la génération et la fourniture d'un nouveau certificat. De plus, un nouveau certificat d'authentification serveur ne peut pas être fourni au RC sans renouvellement de la bi-clé correspondante (cf. chapitre 4.6).

3.3.1 Identification et validation pour un renouvellement courant

Lors du renouvellement, l'AE, saisie de la demande, identifie le RC et vérifie les informations du serveur informatique selon la même procédure que pour l'enregistrement initial.

3.3.2 Identification et validation pour un renouvellement après révocation

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

3.4 Identification et validation d'une demande de révocation

Si la demande de révocation est faite via un service téléphonique, elle doit faire l'objet d'un minimum d'authentification : vérification d'une ou deux informations de base du demandeur (adresse, n° de téléphone, etc.) et de son autorité par rapport au certificat à révoquer.

La demande de révocation n'est pas disponible sur Internet.

4 Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

La personne à l'origine d'une demande de certificat est le futur RC à la demande de son entité.

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

Les informations suivantes doivent au moins faire partie de la demande de certificat (cf. chapitre 3.2 ci-dessus) :

- [SERVEUR-SERVEUR] (certificat pour des serveurs de type serveur SSL/TLS) : le FQDN du serveur à utiliser dans le certificat ;
- [SERVEUR-CLIENT] (certificat pour des serveurs qui lors de l'établissement d'une session sécurisée avec un autre serveur se trouve être en mode client) : le nom du serveur à utiliser dans le certificat ;
- Les données personnelles d'identification du RC ;
- Les données d'identification de l'entité (sauf si l'enregistrement est effectué par l'intermédiaire d'un MC).

Le dossier de demande est établi soit directement par le futur RC à partir des éléments fournis par son entité, soit par son entité et signé par le futur RC.

Le dossier est remis ou envoyé au MC.

Par ailleurs, l'AE doit s'assurer de disposer d'une information permettant de contacter le MC ou le futur RC du 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" et "personne morale" sont vérifiées conformément aux exigences du chapitre 3.2.

L'AE, ou le MC effectue les opérations suivantes :

- [SERVEUR-SERVEUR] (certificat pour des serveurs de type serveur SSL/TLS) valider le FQDN du serveur informatique auquel le certificat doit être rattaché. Il peut utiliser le service d'interrogation whois de l'AFNIC par exemple pour vérifier les FQDN se terminant par « .fr ». Par ailleurs l'AE, ou le MC, vérifiera que le FQDN du serveur est correctement formaté et ne contient pas le caractère NUL ;
- [SERVEUR-CLIENT] (certificat pour un serveur qui lors de l'établissement d'une session sécurisée avec un autre serveur se trouve être en mode client) l'AE, ou le MC, vérifiera que le nom du serveur est correctement formaté ;
- Valider l'identité du futur RC ;
- Vérifier la cohérence des justificatifs présentés ;
- S'assurer que le futur RC a pris connaissance des modalités applicables pour l'utilisation du certificat (voir les conditions générales d'utilisation).

Le MC retransmet le dossier à l'AE après avoir effectué les opérations ci-dessus. L'AE doit alors s'assurer que la demande correspond bien au mandat du MC.

Une fois ces opérations effectuées, l'AE émet la demande de génération du certificat vers la fonction adéquate de l'IGC (cf. chapitre I.4.1).

L'AE conserve ensuite une trace des justificatifs présentés.

La DPC précise les procédures mises en œuvre pour respecter ces exigences.

4.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE en informe le RC, ou le MC le cas échéant, en justifiant le rejet.

4.2.3 Durée d'établissement du certificat

La durée d'établissement est normalement immédiate après la validation administrative de la demande en jours ouvrés.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération et de préparation des différents éléments destinés au RC : au minimum, le certificat.

La bi-clé étant générée au niveau du serveur, la clé publique est transmise à l'AC.

Les conditions de génération des clés et des certificats et les mesures de sécurité à respecter sont précisées aux chapitres 5 et 6 ci-dessous, notamment la séparation des rôles de confiance (cf. chapitre 5.2).

4.3.2 Notification par l'AC de la délivrance du certificat au RC

Dans le cas de l'IGC FINANCES-SERVEURS, l'AC génère automatiquement un courriel, à destination du RC, contenant le certificat en pièce jointe.

L'AC n'ayant pas généré elle-même la bi-clé du serveur, le RC contrôle, avant d'installer le certificat rapatrié, que celui-ci est bien associé à la bi-clé qu'il a générée.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

L'acceptation est tacite à compter de la date d'envoi du certificat au RC. Le processus d'acceptation du certificat et les obligations correspondantes du RC sont clairement mentionnés dans les présentes PC ainsi que dans les conditions générales d'utilisation pour le certificat d'authentification serveur considéré.

Le certificat délivré est considéré comme accepté par le demandeur à l'exception des cas suivants, dans les 5 jours ouvrés après l'envoi du certificat :

- le demandeur informe l'AC d'inexactitudes dans les champs constitutifs du certificat,

- le demandeur notifie à l'AC, par écrit, son refus d'acceptation de celui-ci et n'en fait pas usage.

Le certificat est alors révoqué.

4.4.2 Publication du certificat

Les certificats ne sont pas publiés mais sont conservés.

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

L'AC informe l'AE de la délivrance du certificat, qui se charge d'en informer le MC le cas échéant.

4.5 Usages du bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le RC

L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service d'authentification et d'établissement d'une session sécurisée : authentification du serveur, échange de la clé symétrique de session (cf. chapitre 1.4.1). Tout autre usage est interdit, notamment, le déchiffrement SSL de sessions sécurisées. Les RC doivent s'assurer du respect strict des usages autorisés des bi-clés et des certificats au niveau des serveurs. Dans le cas contraire, leur responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé du serveur et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des clés (cf. chapitre 7 profils des certificats), ainsi que dans les conditions générales d'utilisation.

Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du RC et du MC par l'AC avant d'entrer en relation contractuelle.

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

Les présentes PC imposent que les certificats et les bi-clés correspondantes aient la même durée de vie. Il ne peut donc pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé.

Dans le cas de l'AC, la bi-clé est renouvelée lors de chaque demande de certificat.

Un RC a la possibilité de redemander un certificat 1 mois avant l'expiration de son certificat. Cette opération nécessite la fourniture d'un dossier complet.

4.6.1 Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification au RC de l'établissement du nouveau certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6 Publication du nouveau certificat

Sans objet.

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

Sans objet.

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

Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat d'authentification serveur liée à la génération d'une nouvelle bi-clé.

4.7.1 Causes possibles de changement d'un bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi, les bi-clés des serveurs, et les certificats correspondants, seront renouvelées au minimum à une fréquence 3 ans.

Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat du serveur (cf. chapitre 4.9, notamment le chapitre 4.9.1.1 pour les différentes causes possibles de révocation).

Nota - Dans la suite du présent chapitre, le terme utilisé est "fourniture d'un nouveau certificat".

4.7.2 Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat d'authentification serveur est à l'initiative du RC.

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 4.3.1.

4.7.4 Notification au RC de l'établissement du nouveau certificat

Cf. chapitre 4.3.2.

4.7.5 Démarche d'acceptation du nouveau certificat

Cf. chapitre 4.4.1.

4.7.6 Publication du nouveau certificat

Cf. chapitre 4.4.2.

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

Cf. chapitre 4.4.3.

4.8 Modification du certificat

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 qu'uniquement la modification des dates de validité (cf. chapitre 4.6).

La modification de certificat n'est pas autorisée dans les présentes PC.

4.8.1 Causes possibles de modification d'un certificat

Sans objet.

4.8.2 Origine d'une demande de modification d'un certificat

Sans objet.

4.8.3 Procédure de traitement d'une demande de modification d'un certificat

Sans objet.

4.8.4 Notification au RC de l'établissement du certificat modifié

Sans objet.

4.8.5 Démarche d'acceptation du certificat modifié

Sans objet.

4.8.6 Publication du certificat modifié

Sans objet.

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

Sans objet.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificats d'authentification serveur

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

- Les informations du serveur figurant dans son certificat ne sont plus en conformité avec l'identité de ce serveur ou l'utilisation prévue dans le certificat (par exemple, modification du FQDN ou du nom du serveur), ceci avant l'expiration normale du certificat ;
- Le RC n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le RC et/ou, le cas échéant, le MC / l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- La clé privée du serveur est suspectée de compromission, est compromise, est perdue ou est volée, (éventuellement les données d'activation associées) ;
- Le RC ou une entité autorisée (représentant légal de l'entité ou MC par exemple) demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du serveur et/ou de son support) ;
- L'arrêt définitif du serveur ou la cessation d'activité de l'entité du RC de rattachement du serveur.
- Décision du SG suite à un audit de conformité (non-conformité des procédures appliquées avec les exigences de la présente PC et/ou des pratiques annoncées dans la DPC.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné doit être révoqué.

4.9.1.2 Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC (y compris un certificat d'AC pour la génération de certificats, de LCR) :

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante ;
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.
- Décision 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)

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats serveurs

Les personnes / entités qui peuvent demander la révocation d'un certificat d'authentification serveur sont les suivantes :

- Le RC pour le serveur considéré ;
- Le MC
- Un représentant légal de l'entité ;

- L'AC émettrice du certificat ou l'une de ses composantes (AE).

Nota : Le RC doit être informé des personnes / entités susceptibles d'effectuer une demande de révocation pour le certificat dont il a la responsabilité.

4.9.2.2 Certificats d'une composante de l'IGC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice.

La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Révocation d'un certificat d'authentification serveur

Les exigences d'identification et de validation d'une demande de révocation, effectuée par la fonction de gestion des révocations, sont décrites au chapitre 3.4.

Il n'est pas autorisé de demande de révocation sur Internet.

Les informations suivantes doivent au moins figurer dans le formulaire de demande de révocation de certificat (format papier ou informations requises pour la demande par téléphone en cas d'urgence) :

- [SERVEUR-SERVEUR] (certificat pour des serveurs de type serveur SSL/TLS) le FQDN du serveur utilisé dans le certificat ;
- [SERVEUR-CLIENT] (certificat pour des serveurs qui lors de l'établissement d'une session sécurisée avec un autre serveur se trouve être en mode client) le nom du serveur utilisé dans le certificat
- Le nom du demandeur de la révocation ;
- Toute information permettant de retrouver rapidement et sans erreur le certificat à révoquer (n° de série, ...) ;
- La cause de révocation.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation doit être diffusée au minimum via une LCR signée par l'AC.

D'autres moyens de diffusion complémentaires peuvent également être utilisés par l'AC (cf. chapitre 4.9.9).

Le demandeur de la révocation doit être informé du bon déroulement de l'opération et de la révocation effective du certificat. De plus, si le RC n'est pas le demandeur, il doit également être informé de la révocation effective de ce certificat.

L'entité, directement ou via son MC le cas échéant (au choix de l'entité), doit être informée de la révocation de tout certificat d'authentification serveur qui lui sont rattachés.

L'opération est enregistrée dans les journaux d'événements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat

Les causes détaillées de révocation ne sont pas publiées.

4.9.3.2 Révocation d'un certificat d'une composante de l'IGC

L'AC précise dans sa DPC les procédures à mettre en œuvre en cas de révocation d'un certificat d'une composante de l'IGC.

En cas de révocation d'un des certificats de la chaîne de certification, l'AC doit informer dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des RC concernés que leurs certificats d'authentification serveur correspondants ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE et aux MC. Ces derniers devront informer les RC en leur indiquant explicitement que leurs certificats d'authentification serveur ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Afin de faciliter la révocation du certificat de l'AC, il est recommandé que le certificat associé à la clé de l'AC signant les certificats d'authentification serveur soit signé par une autre AC et ne soit pas uniquement autosigné (cf. chapitre I.4.1.2).

Le certificat de l'AC est signé par l'AC racine (AC3-FINANCES-RACINE) afin de faciliter sa révocation

Le point de contact identifié sur le site : https://ssi.gouv.fr doit être immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification. L'ANSSI se réserve le droit de diffuser par tout moyen l'information auprès des promoteurs d'applications au sein des autorités administratives et auprès des usagers.

4.9.4 Délai accordé au RC pour formuler la demande de révocation

Dès que le RC (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

4.9.5.1 Révocation d'un certificat d'authentification serveur

Par nature, une demande de révocation doit être traitée en urgence, à l'exception des demandes de révocation planifiées correspondant à un arrêt de service planifié.

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

Cette fonction doit avoir une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 2h en jours ouvrés et une durée maximale totale d'indisponibilité par mois de 16 h en jours ouvrés.

Toute demande de révocation d'un certificat d'authentification serveur doit être traitée dans un délai inférieur à 72 heures, 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.

4.9.5.2 Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC doit être 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 de l'AC qui a émis le certificat, et que cette liste est accessible au téléchargement.

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR) doit être effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

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

L'utilisateur d'un certificat d'authentification serveur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante.

Les applications utilisées doivent être sécurisées, dotées de fonctions d'accès aux LCR et de contrôles automatiques de l'état des certificats.

4.9.7 Fréquence d'établissement des LCR

La fréquence de publication des LCR est de 24 heures.

La LCR est publiée après chaque révocation d'un certificat serveur.

Sa durée de validité est de 7 jours.

Le mécanisme des deltaLCR n'est pas mis en œuvre.

4.9.8 Délai maximum de publication d'une LCR

Une LCR doit être publiée dans un délai maximum de 30 mn suivant sa génération.

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

L'AC ne propose pas d'autres formes de publication complémentaire (OCSP par exemple).

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

Cf. chapitre 4.9.6 ci-dessus

4.9.11 Autres moyens disponibles d'information sur les révocations

Le SG/SNUM peut utiliser tous les moyens qu'il estime nécessaires pour informer les utilisateurs en cas de révocation de certificat serveur à condition qu'ils respectent les exigences d'intégrité, de disponibilité et de délai de publication décrites dans la PC type Serveur V2.3.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats serveurs, les entités autorisées à effectuer une demande de révocation sont tenues de le faire dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée.

Pour les certificats d'AC, outre les exigences du chapitre 4.9.3.2 ci-dessus, la révocation suite à une compromission de la clé privée doit faire l'objet d'une information clairement diffusée au moins sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

4.9.13 Suspension des certificats

La suspension de certificats n'est pas autorisée dans les présentes PC.

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

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

La fonction d'information sur l'état des certificats doit au moins mettre à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR / LAR.

Ces LCR / LAR doivent être des LCR au format V2, publiées conformément au RGS (cf. annexe A4 du RGS Version 3.0 § 3, faisant référence au document de l'ETSI : ETSI TS 102 280 v1.1.1 et conforme à la [RFC 5280].

Les LCR ne sont pas publiées dans un annuaire LDAP.

4.10.2 Disponibilité de la fonction

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

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

4.10.3 Dispositifs optionnels

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

4.11 Fin de la relation entre le RC et l'AC

En cas de fin de relation contractuelle / hiérarchique / réglementaire entre l'AC et l'entité de rattachement du serveur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

De plus, l'AC doit révoquer un certificat d'authentification serveur pour lequel il n'y a plus de RC explicitement identifié.

4.12 Séquestre de clé et recouvrement

Le séquestre des clés privées des serveurs est interdit par la PC Type authentification Serveur V2.3.

Les clés privées d'AC ne doivent pas non plus être séquestrées.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

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

Sans objet.

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physique

Les mesures de sécurité physiques de l'IGC FINANCES SERVEURS sont conformes aux exigences décrites dans les politiques, les procédures et les mesures de sécurité du ministère et aux normes en vigueur. Elles sont décrites dans la DPC et documents annexes de cette IGC.

5.1.1 Situation géographique et construction des sites

L'IGC FINANCES est située physiquement en France, sur un site sous la responsabilité directe du Ministère de l'Economie et des Finances.

La construction des sites doit respecter les règlements et normes en vigueur ainsi qu'éventuellement des exigences spécifiques face à des risques de type tremblement de terre ou explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques, ...).

5.1.2 Accès 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 doivent être 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.

5.1.3 Alimentation électrique et climatisation

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

Elles permettent également de respecter les exigences de la PC Type (RGS), ainsi que les engagements pris par l'AC dans sa PC, 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 de la PC Type (RGS), ainsi que les engagements pris par l'AC dans sa PC, 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 de la PC Type (RGS), ainsi que les engagements pris par l'AC dans sa PC, 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 sont identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité). L'AC maintient un inventaire de ces informations. L'AC met 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 sont gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils sont manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.

Des procédures de gestion protègent 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 sont conformes à ce niveau de confidentialité (voir notamment le guide [972-1]).

5.1.8 Sauvegardes hors site

En complément de sauvegardes sur sites, il est mis en œuvre des sauvegardes hors sites des applications et des informations. Ces sauvegardes sont organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conforme aux exigences de la PC Type authentification Serveur V2.3 et aux engagements de l'AC dans les présentes PC en matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des certificats (cf. chapitres 4.9.5.1 et 4.10.2).

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

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 :

- **Responsable de sécurité** - Le responsable de 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 est amenée à distinguer également en tant que rôle de confiance, les rôles de porteur de parts 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. Les formulaires 'prise en charge de secret' et 'transfert de secret', signés par les porteurs de secret, mentionnent ces engagements.

De manière générale, des procédures sont établies et appliquées pour tous les rôles administratifs et les rôles de confiance ayant trait à la fourniture de services de certification.

Ces rôles sont décrits et définis dans la description des postes propre à chaque entité opérant une des composantes de l'IGC sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles doivent déterminer la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilisation des employés.

Lorsqu'approprié, ces descriptions doivent différencier entre les fonctions générales et les fonctions spécifiques à l'AC. L'AC doit implémenter techniquement ce principe de moindre privilège via les mécanismes de contrôle d'accès qu'elle met en œuvre.

De plus, les opérations de sécurité de l'AC sont séparées des opérations normales.

Les responsabilités des opérations de sécurité incluent :

- Les procédures et responsabilités opérationnelles ;
- La planification et la validation des systèmes sécurisés ;
- La protection contre les logiciels malicieux ;
- L'entretien ;
- La gestion de réseaux ;
- La surveillance active des journaux d'audit, l'analyse des événements et les suites ;
- La manipulation et la sécurité des supports ;
- L'échange de données et de logiciels.

Ces responsabilités sont gérées par les opérations de sécurité de l'AC, mais peuvent être effectivement réalisées par du personnel opérationnel non spécialiste (en étant supervisé), tel que défini dans la politique de sécurité appropriée et les documents relatifs aux rôles et responsabilités.

Des mesures sont mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux services de l'AC soient sortis du site sans autorisation.

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, les fonctions sensibles sont réparties sur plusieurs personnes. Les présentes PC définissent un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC (cf. chapitre 6).

La DPC de l'AC précise 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 fait vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

- Que 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 est notifiée par écrit. Ce rôle est clairement mentionné et décrit dans sa fiche de poste.

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

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 sont 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 s'assure 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 sont 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 sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum 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.

Il est important que le MC soit formé aux procédures d'attribution et de gestion des certificats. L'IGC doit s'assurer de ses compétences professionnelles en ce domaine et, si besoin, apporter toute l'aide nécessaire à l'accomplissement de ses tâches.

5.3.4 Exigences et fréquence 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 des présentes 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 Ministère de l'Economie et des Finances 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 respecte également 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 dispose au minimum 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, il lui est 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 de façon manuelle ou automatique.

Les fichiers résultants, sous forme papier ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Type d'événements à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en œuvre dans le cadre de l'IGC, chaque entité opérant une composante de l'IGC doit au minimum journaliser les événements tels que décrits ci-dessous, sous forme électronique :

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

D'autres événements sont aussi être 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 RC, ...).

La journalisation doit être automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

En plus de ces exigences de journalisation communes à toutes les composantes et toutes les fonctions de l'IGC, des événements spécifiques aux différentes fonctions de l'IGC sont également journalisés, notamment :

- Réception d'une demande de certificat (initiale et renouvellement) ;
- Validation / rejet d'une demande de certificat ;
- Événements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction, ...) ;
- Le cas échéant, génération des éléments secrets du serveur (bi-clé, codes d'activation, …) ;
- Génération des certificats d'authentification serveur ;
- Transmission des certificats aux RC et, selon les cas, acceptations / rejets explicites par les RC ;
- 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 ;
- Génération puis publication des LCR ;

Chaque enregistrement d'un événement dans un journal doit contenir au minimum 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 devra également contenir 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 doit se faire, sauf exception, le même jour ouvré que l'événement.

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

5.4.2 Fréquence de traitement des journaux d'événements

Cf. chapitre 5.4.8 ci-dessous.

5.4.3 Période de conservation des journaux d'événements

Les journaux d'événements doivent être conservés sur site pendant au moins le délai d'un mois.

Ils doivent être archivés le plus rapidement possible après leur génération et au plus tard sous le délai de 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 est 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 permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.

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

Le système de datation des événements respecte 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 met 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

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

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

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

5.4.8 Evaluation des vulnérabilités

Chaque entité opérant une composante de l'IGC est 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 doit faire 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.) doit être effectué 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 sont également prises par l'AC. Cet archivage permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

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

Les données à archiver sont au moins les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- Les PC ;
- Les DPC ;
- Les accords contractuels avec d'autres AC ;
- Les certificats et LCR tels qu'émis ou publiés ;
- Les récépissés ou notifications (à titre informatif) ;
- Les engagements signés des MC ;
- Les justificatifs d'identité des RC et, le cas échéant, de leur entité de rattachement ;
- Les justificatifs de possession des serveurs ainsi que leurs noms ;
- [SERVEUR-SERVEUR] (certificat pour des serveurs de type serveur SSL/TLS) les justificatifs de possession des noms de domaine des FQDN des serveurs ;
- Les journaux d'événements des différentes entités de l'IGC.

5.5.2 Période de conservation des archives

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable.

Les facteurs à prendre en compte dans la détermination de la "loi applicable" sont la loi du pays dans lequel l'AC est établie. Lorsque les RC sont enregistrés par une autorité d'enregistrement dans un autre pays que celui ou l'AC est établie, alors il convient que cette AE applique également la réglementation de son propre pays. Lorsque des MC sont également dans un autre pays, alors il convient de prendre également en compte les exigences contractuelles et légales applicables à ces MC.

Les dossiers de demande de certificat (DDC) et de révocation de certificat (DDR) sont conservés pendant 8 ans à partir du traitement de la demande.

La durée de conservation des dossiers d'enregistrement est portée à la connaissance du RC ou du MC. 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 ou le MC, doit permettre de retrouver l'identité réelle du RC responsable, à un instant "t" du serveur désigné dans le certificat émis par l'AC.

Certificats et LCR émis par l'AC

Les certificats d'authentification serveur et d'AC, ainsi que les LCR / LAR produites, sont archivés pendant cinq ans après leur expiration.

Journaux d'événements

Les journaux d'événements traités au chapitre 5.4 seront archivés pendant cinq ans après leur génération. 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 procédure de sauvegarde électronique des archives dispose d'un niveau de protection équivalent voir supérieur au niveau de protection des archives défini en 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

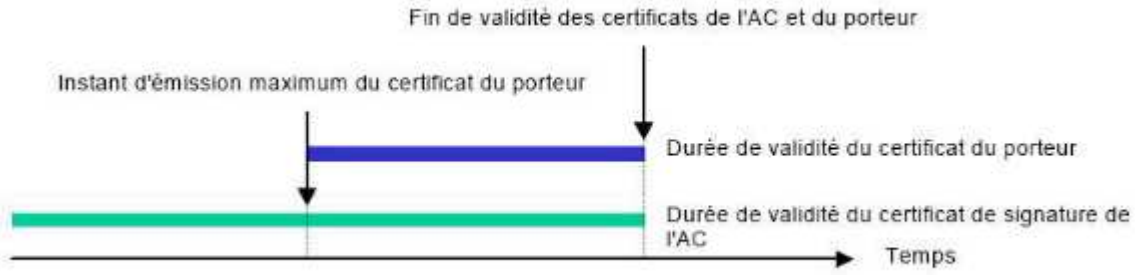
La PC Type (RGS) ne formule pas d'exigence spécifique sur le sujet.

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 d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité de ce certificat de l'AC doit être supérieure à celle des certificats 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 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 jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7 Reprise suite à compromission et sinistre

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

Chaque entité opérant une composante de l'IGC met 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'AC, l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC. 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 …). L'AC doit également prévenir directement et sans délai le point de contact identifié sur le site : https://ssi.gouv.fr.

Si l'un des algorithmes, ou des paramètres associés, utilisés par l'AC ou ses serveurs devient insuffisant pour son utilisation prévue restante, alors l'AC doit :

- Informer tous les RC et les tiers utilisateurs de certificats avec lesquels l'AC 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 dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant de la PC Type authentification Serveur V2.3, 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 est testé au minimum 1 fois tous les 3 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 est 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 RC, MC et les autres entités avec lesquelles l'AC a passé des accords ou a 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 disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la PC Type authentification Serveur et de la PC de l'AC (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 (d'une composante autre que l'AC) 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 PC Type (RGS). À 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 RC ou des utilisateurs de certificats, l'AC doit les en aviser aussitôt que nécessaire et, au moins, sous le délai d'un mois.
2. L'AC doit communiquer au contact identifié, sur le site https://ssi.gouv.fr , les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC devra communiquer à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet événement. 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.
3. L'AC doit tenir informées l'ANSSI 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 LCR conformément aux engagements pris dans sa PC.

L'AC stipule 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 s'engage à :

1. S'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
2. La détruire ou la rendre inopérante ;
3. Demander la révocation de son certificat à l'AC racine ;
4. Révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
5. Informer (par exemple par récépissé) tous les MC et/ou RC des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre 3.2.3).

6 Mesures de sécurité techniques

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

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé (cf. chapitre 5).

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré.

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. chapitre 5.2.1), dans le cadre de "cérémonies de clés". Ces cérémonies se déroulent suivant des scripts préalablement définis.

L'initialisation de l'IGC et/ou la génération des clés de signature d'AC s'accompagne 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.

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

L'AC autorise un porteur de secret à transmettre temporairement ou définitivement son secret. Les transferts sont tracés par l'AC.

Les cérémonies de clés se déroulent sous le contrôle d'au moins une personne ayant au moins un rôle 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.

6.1.1.2 Clés serveurs générées par l'AC

Les clés des serveurs sont générées directement au niveau du serveur.

6.1.1.3 Clés serveurs générées au niveau du serveur

La bi-clé étant générée au niveau du serveur, cette génération doit être effectuée dans un dispositif répondant aux exigences du chapitre 12 ci-dessous pour le niveau de sécurité considéré.

6.1.2 Transmission de la clé privée au serveur

Sans objet. La clé privée du serveur est générée directement sur le serveur, sans droit d'en sortir.

6.1.3 Transmission de la clé publique à l'AC

En cas de transmission de la clé publique du serveur vers une composante de l'AC (cas où la bi-clé est générée au niveau du serveur), la clé devra être protégée en intégrité et son origine devra en être authentifiée.

Cette exigence se matérialise par des considérations techniques décrites dans la DPC (au-delà des mécanismes cryptographiques).

La clé publique est transmise à l'AC par des moyens cryptographiques et un contrôle d'authenticité est réalisé en vérifiant que le numéro de demande dématérialisé est identique au numéro reporté sur la demande administrative.

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

Les clés publiques de vérification de signature de l'AC 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.

Chaque clé publique d'AC est diffusée dans un certificat qui est rattaché à une hiérarchie d'AC jusqu'à une AC racine (cf. chapitre I.4.1.2 ci-dessus).

Le certificat de l'AC et son certificat d'AC racine sont diffusés :

- *Sur le site Intranet des IGC du SG du Ministère de l'Economie et des Finances,*
- *Sur le site Internet de l'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 serveurs respectent les exigences de caractéristiques (tailles, algorithmes, etc.) du chapitre 7 de ces PC.

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

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

6.1.7 Objectifs d'usage de la clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR (cf. chapitre I.4.1.2 et document [RGS_A4]).

L'utilisation de la clé privée du serveur et du certificat associé est strictement limitée au service d'authentification et d'établissement d'une session sécurisée (cf. chapitres I.4.1.1, 4.5 et le document [RGS_A4]).

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature, ainsi que le cas échéant pour la génération des clés des serveurs, doivent être des modules cryptographiques répondant au minimum aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré.

6.2.1.2 Dispositifs de protection de clés privées des serveurs

Les dispositifs de protection de clés privées des serveurs, pour la mise en œuvre de leurs clés privées, respectent les exigences du chapitre 12 ci-dessous pour le niveau de sécurité considéré.

L'AC ne fournit pas elle-même ce dispositif au RC. Elle doit s'assure auprès du RC de la conformité du dispositif mis en œuvre par le serveur, au minimum au travers d'un engagement contractuel clair et explicite du RC vis-à-vis de l'AC.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'AC pour l'exportation / l'importation hors / dans un module cryptographique.

La génération de la bi-clé est traitée au chapitre 6.1.1.1, 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'AC doit être assuré par du personnel de confiance (porteurs de secrets d'IGC).

6.2.3 Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des serveurs ne doivent être séquestrées.

6.2.4 Copie de secours de la clé privée

Les clés privées des serveurs ne font l'objet d'aucune copie de secours par l'AC.

Les clés privées d'AC font l'objet de copies de secours, hors d'un module cryptographique sous forme chiffrée et avec un mécanisme de contrôle d'intégrité.

Le chiffrement correspondant offre un niveau de sécurité équivalent ou supérieur au stockage au sein du module cryptographique et s'appuie 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 opérations de chiffrement et de déchiffrement sont effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne sont à aucun moment en clair en dehors du module cryptographique.

Le contrôle des opérations de chiffrement / déchiffrement est conforme aux exigences du chapitre 6.2.2.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC ne sont pas archivées.

Les clés privées des certificats serveurs ne sont pas archivées ni par l'AC ni par aucune des composantes de l'IGC.

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

Les clés privées de l'AC sont stockées dans un module cryptographique répondant au minimum aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité * RGS.

Cependant, dans le cas des copies de secours, le stockage peut être effectué en dehors d'un module cryptographique moyennant le respect des exigences du chapitre 6.2.4. Quel que soit le moyen utilisé, l'AC doit garantir que les clés privées d'AC ne sont pas compromises pendant leur stockage ou leur transport.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'AC

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

L'activation des clés privées d'AC dans un module cryptographique est contrôlée via des données d'activation (cf. chapitre 6.4) et fait intervenir au moins une personne ayant au moins un rôle de confiance et trois porteurs de secret sur cinq.

6.2.8.2 Clés privées des serveurs

L'activation de la clé privée du serveur est protégée par mot de passe, défini par le RC et respectant les exigences de la PSSI de sa direction.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'AC

La désactivation de la clé privée d'AC du module cryptographique de l'IGC est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module.

Ces conditions de désactivation permettent de répondre aux exigences définies dans le chapitre 11.

Ce module a été évalué par l'ANSSI au niveau de sécurité renforcé et ce fonctionnement a été constaté.

6.2.9.2 Clés privées des serveurs

Lorsqu'un certificat de serveur est expiré ou révoqué, la clé privée correspondante est détruite par le RC. La DPC détaille la procédure à mettre en œuvre pour détruire la clé privée.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées d'AC

La méthode de destruction des clés privées d'AC permet de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

En fin de vie d'une clé privée d'AC, 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 serveurs

En fin de vie de la clé privée d'un serveur, la méthode de destruction de cette clé privée permet de répondre aux exigences définies dans le chapitre 12 pour le niveau de sécurité considéré.

6.2.11 Niveau de qualification du module cryptographique et des dispositifs d'authentification et de signature

Les modules cryptographiques de l'AC sont qualifiés au niveau de sécurité renforcé par l'ANSSI.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques de l'AC et des serveurs 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 serveurs couverts par la PC Type authentification Serveur V2.3 doivent avoir une durée de vie au maximum de 3 ans. Les bi-clés et les certificats des serveurs couverts par ces PC ont une durée de validité de 3 ans.

La fin de validité d'un certificat d'AC doit être postérieure à la fin de vie des certificats d'authentification serveur qu'elle émet. L'AC doit préciser dans sa PC la durée de vie des clés de signature d'AC et des certificats correspondants. Cette durée de vie doit être cohérente avec les caractéristiques de l'algorithme et la longueur de clé utilisés (cf. [RGS_A_4]) et doit être au maximum égal à 10 ans.

La durée de validité du certificat de l'AC est de 10 ans.

Cette durée de vie est cohérente avec les caractéristiques de l'algorithme et la longueur de clé utilisés (cf. [RGS_A4]).

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

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

La génération et l'installation des données d'activation du module cryptographique de l'AC se fait lors de la phase d'initialisation et de personnalisation de ce module (cérémonie de clés de création du domaine de confiance).

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 du serveur

Les données d'activation sont sous forme de mots de passe respectant les exigences fixées par la PSSI de la direction du demandeur

6.4.2 Protection des données d'activation

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

Les données d'activation qui sont générées par l'AC pour les modules cryptographiques de l'IGC sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire.

Cette exigence est satisfaite au moyen de systèmes cryptographiques décrits dans la DPC.

Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

Protection des données d'activation correspondant aux clés privées des serveurs

L'AC ne générant pas les clés privées des serveurs, les données d'activation de ces clés privées sont définies par le RC en respectant la politique de mot de passe de sa direction.

6.4.3 Autres aspects liés aux données d'activation

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

6.5 Mesures de sécurité des systèmes informatiques

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 est défini dans la DPC de l'AC. Il répond aux objectifs de sécurité suivants :

- Identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs de type mot de passe ou certificat),
- 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 (accès aux fichiers contrôlé par rôle et nom d'utilisateur), les systèmes d'exploitation sont configurés par l'ingénieur système et l'administrateur sécurité,
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels, antivirus,
- 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, les systèmes d'exploitation sont configurés par l'ingénieur système et l'administrateur sécurité,
- 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), Les journaux d'événements de l'IGC sont protégés en intégrité par signature numérique.
- Gestion des reprises sur erreur.

Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires.

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle (cf. chapitre I.4.1.2) fait l'objet de mesures particulières.

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

6.5.2 Niveau de qualification des systèmes informatiques

Pas d'exigence spécifique.

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque que l'AC peut mener (cf. rappel au début du présent chapitre 6).

6.6.1 Mesures de sécurité liées au développement des systèmes

L'implémentation du système permettant de mettre en œuvre les composantes de l'IGC est documentée et respecte 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 sont documentées et contrôlées.

L'AC s'engage à :

- 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 liées à la gestion de la 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.

Ces évolutions logicielles ou matérielles sont contrôlées et validées sur une plate-forme de test et d'intégration avant d'être portées sur la plate-forme de production.

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

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

6.7 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

L'AC garantit 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 vérifier leur conformité avec les exigences spécifiées par l'AC.

De plus, les échanges entre composantes au sein de l'IGC font l'objet de 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 PC Type (RGS) 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 utilisent l'heure système des serveurs NTP pour dater les événements.

7 Profils des certificats et des LCR

Les chapitres suivants donnent la description du profil des certificats de [SERVEUR-SERVEUR] et [SERVEUR-CLIENT].

7.1 Profil des certificats émis par l'AC

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

7.1.1 Champs de base

Le tableau ci-dessous détaille le contenu du certificat [SERVEUR-SERVEUR] et [SERVEUR-CLIENT] :

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 Sha256 RSA 2048 bits
Issuer *Au format UTF8 à l'exception de l'attribut Country qui est au format printable string*	CN = AC3-FINANCES-SERVEURS OU = 0002 130013345 O = MINISTERE DE L ECONOMIE ET DES FINANCES C = FR
Validity period	Date de génération du certificat Date d'expiration du certificat – durée de validité 3 ans
Subject *Au format UTF8 à l'exception de l'attribut Country qui est au format printable string*	CN = FQDN du serveur OU = 0002 110020013 O = MINISTERE DE L ECONOMIE ET DES FINANCES C = FR
Subject Public Key Info	Valeur de la clé publique RSA (2048)
Unique Identifiers (issuer et subject)	Non utilisé
Extensions	Cf. chapitre suivant.

7.1.2 Extensions du certificat

Le tableau ci-dessous décrit les extensions pour le certificat [SERVEUR-SERVEUR] :

Champ	Critique	Valeur
Authority Key Identifier	N	Identifiant de la clé publique de l'AC émettrice
Subject Key Identifier	N	Identifiant de la clé publique du sujet
Key Usage	O	keyEncipherment, digitalSignature Errata de l'ANSSI (23 avril 2012) autorisant en RGS V1 l'usage de keyEncipherment et de digitalSignature
Certificate Policies	N	PC OID = 1.2.250.1.131.1.13.2.3.1.1 https://igc1.finances.gouv.fr/ac3-finances-serveurs.pdf https://igc2.finances.gouv.fr/ac3-finances-serveurs.pdf
Subject Alternative Name	N	FQDN du serveur Le champ Subject Alternative Name doit être présent. Il doit contenir au moins une entrée de type DNS Name correspondant à l'un des FQDN du service applicatif hébergé par la machine »
CRL Distribution Points	N	https://igc1.finances.gouv.fr/ac3-finances-serveurs.crl https://igc2.finances.gouv.fr/ac3-finances-serveurs.crl
Extended Key Usage	N	id-kp-serverAuth id-kp-smartcardlogon

Le tableau ci-dessous décrit les extensions pour le certificat [SERVEUR-CLIENT] :

Extensions pour les certificats d'authentification serveur de type client :

Champ	Critique	Valeur
Authority Key Identifier	N	identifiant de la clé publique de l'AC émettrice
Subject Key Identifier	N	identifiant de la clé publique du sujet
Key Usage	O	digitalSignature
Certificate Policies	N	PC OID = 1.2.250.1.131.1.13.2.3.1.2
CRL Distribution Points	N	https://igc1.finances.gouv.fr/ac3-finances-serveurs.crl https://igc2.finances.gouv.fr/ac3-finances-serveurs.crl
Extended Key Usage	N	id-kp-clientAuth

7.1.3 OID des algorithmes

Cf. Chapitre 7.1.2

7.1.4 Forme des noms

Cf. Chapitre 7.1.1

7.1.5 Contraintes sur les noms

Le Distinguish Name (DN) respecte le format Printable String ou le format UTF8 String. (voir profil §7.1.1)

7.1.6 OID des PC

Cf. Chapitre 7.1.2

7.1.7 Utilisation de l'extension "contraintes de politique"

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 la PC

Conformément à la norme X.509v3, le caractère critique doit être traité de la façon suivante selon que l'extension est critique ou non :

- Si l'extension est non - critique, alors :
  - Si l'application ne sait pas la traiter, l'extension est abandonnée mais le certificat est accepté,
  - Si l'application sait la traiter, alors :
    - Si l'extension est conforme avec l'usage que l'application veut en faire, l'extension est traitée,
    - Si l'extension n'est pas conforme avec l'usage que l'application veut en faire, l'extension est abandonnée, mais le certificat est accepté.
- Si l'extension est critique, alors :
  - Si l'application ne sait pas la traiter, le certificat est rejeté,
  - Si l'application sait la traiter, alors :
    - Si l'extension est conforme avec l'usage que l'application veut en faire, l'extension est traitée,
    - Si l'extension n'est pas conforme avec l'usage que l'application veut en faire, le certificat est rejeté.

7.2 Profils des LCR

7.2.1 Champs de base

Les LCR de l'AC contiennent les champs suivants :

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 2048) ;

Issuer : Contient le Distinguished Name (X.500) de l'AC :

CN=AC3-FINANCES-SERVEURS

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 (validité de

7 jours) ;

RevokedCertificate : Contient la liste des certificats révoqués avec, pour chacun, les champs suivants :

- **userCertificate** (numéro de série du certificat révoqué),
- **revocationDate** (date de révocation du certificat).

CrlExtensions : Cf. ci-après

7.2.2 Extensions de LCR et d'entrées de LCR

Les extensions suivantes sont utilisées :

authorityKeyIdentifier : Cette extension, non critique, identifie la bi-clé de l'AC utilisée pour signer la CRL,

CRLNumber : Cette extension, non critique, 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.

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

7.3 Profil OCSP

L'AC ne met pas en œuvre de service OCSP.

7.3.1 Numéro de version

Sans objet.

7.3.2 Extensions OCSP

Sans objet.

8 Audit de conformité et autres évaluations

Les audits et les évaluations concernent, d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification au sens de l'[ORDONNANCE] (schéma de qualification des prestataires de services de confiance conformément au [DécretRGS]) 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 démarche et les exigences liées aux audits de qualification de PSCO de type PSCE sont définies dans [PROG_ACCRED] et ne sont pas reprises ici. La suite du présent chapitre ne concerne donc 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 doit procéder à un contrôle de conformité de cette composante.

L'AC procède régulièrement à un contrôle de conformité de l'ensemble de son IGC 1 fois tous les 3 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 SNUM du SG assigne les audits de composantes de l'IGC qu'elle souhaite contrôler, à une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité de la composante contrôlée, ceci afin de contrôler sa conformité aux exigences du RGS ainsi qu'à celles de la politique de filialisation ministérielle.

Les audits de conformité et autres évaluations sont confiés par le SNUM au SHFDS du Ministère de l'Economie et des Finances pour vérifier la conformité d'une composante ou de l'ensemble des IGC à la réglementation en vigueur ainsi qu'aux exigences de la politique de filialisation ministérielle.

8.3 Relations entre évaluateurs et entités évaluées

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

8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définies dans les 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

À l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC, un avis parmi les suivants : "réussite", "échec", "à confirmer".

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

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le

dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.

- En cas de résultat "à confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. 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 des PC et de la DPC.

8.6 Communication des résultats

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

9 Autres problématiques métiers et légales

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 serveurs,
- Les données d'activation associées aux clés privées d'AC et des serveurs,
- Tous les secrets de l'IGC,
- Les journaux d'événements des composantes de l'IGC,
- Les dossiers d'enregistrement des serveurs et des RC,
- Les causes de révocations, sauf accord explicite du RC.

9.3.2 Informations hors du périmètre des informations confidentielles

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

9.3.3 Responsabilités en termes de protection des informations confidentielles

L'AC est tenue d'appliquer des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre 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 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 certificats d'authentification serveur à des tiers dans le cadre de procédures légales. Elle doit également donner l'accès à ces informations au RC et au MC.

9.4 Protection des données personnelles

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].

9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au moins les suivantes :

- Les causes de révocation des certificats des serveurs (qui sont considérées comme confidentielles sauf accord explicite du RC) ;
- Les dossiers d'enregistrement des RC.

9.4.3 Informations à caractère non personnel

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

9.4.4 Responsabilité 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

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les porteurs à l'AC ne doivent ni être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

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

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

9.5 Droits sur la propriété intellectuelle et industrielle

Les présentes PC ne formulent 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 RC,
- 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 serveur donné et que le RC correspondant a accepté le certificat, conformément aux exigences du chapitre 4.4 ci-dessus.
- Garantir et maintenir la cohérence de sa DPC avec ses PC.
- Prendre toutes les mesures raisonnables pour s'assurer que ses RC 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 RC 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 sa Politique de Certification, avec les exigences émises dans les PC Type authentification Serveur et authentification client V2.3 pour le niveau de sécurité * RGS. L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, conforme aux exigences des PC Type authentification Serveur et authentification client V2.3, 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 les présentes politiques.

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 RC 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.

En cas de non-respect ponctuel des obligations décrites dans les présentes PC, l'Administration se réserve le droit de refuser temporairement ou définitivement les certificats de l'AC conformément à la réglementation en vigueur.

9.6.2 Service d'enregistrement

Cf. les obligations pertinentes du chapitre 9.6.1.

9.6.3 RC

Le RC a le devoir de :

- Communiquer des informations exactes et à jour lors de la demande ou du renouvellement du certificat ;
- Protéger la clé privée du serveur 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 ;
- Protéger l'accès à la base de certificats du serveur ;
- Respecter les conditions d'utilisation de la clé privée du serveur et du certificat correspondant ;
- Informer l'AC de toute modification concernant les informations contenues dans le certificat
- Faire, sans délai, une demande de révocation du certificat dont il est responsable auprès de l'AE, du MC de son entreprise ou de l'AC en cas de compromission ou de suspicion de compromission de la clé privée correspondante (ou de ses données d'activation).

- En cas de cessation définitive de fonction, le RC s'engage à :
- - à informer l'autorité d'enregistrement par tous moyens écrits ;
- - à informer sa hiérarchie de la nécessité de désigner sans délai son successeur ;
    - - à fournir à son successeur tous les moyens et documents à jour indispensables à la poursuite des travaux et à la prise en charge de cette responsabilité.

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

Ces informations s'appliquent également aux MC.

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 serveur 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 les présentes PC

L'AC ne doit pas émettre dans ses propres 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

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

9.7 Limite de garantie

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

9.8 Limite de responsabilité

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

9.9 Indemnités

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

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

9.10.2 Fin anticipée de validité

La publication d'une nouvelle version de la PC Type (RGS) peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer ses PC correspondantes.

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

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

9.10.3 Effets de la fin de validité et clauses restant applicables

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

9.11 Notifications individuelles et communications entre les 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 aux PC

9.12.1 Procédures d'amendements

L'AC contrôle que tout projet de modification de ces PC reste conforme aux exigences des PC Type RGS, des éventuels documents complémentaires du RGS.

En cas de changement important, l'AC fait appel à une expertise technique pour en contrôler l'impact.

Toute modification d'architecture, création d'AC fille subordonnées doit faire l'objet d'une demande d'autorisation au SNUM et au SHFDS, de l'obtention d'un OID de la part du SNUM. De même toute création de nouvelles offres de certificats est soumise à l'accord du SNUM et du SHFDS.

9.12.2 Mécanisme et période d'information sur les amendements

Les présentes PC ne formulent 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 RC, 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.

9.13 Dispositions concernant la résolution de conflits

L'AC propose des procédures de résolution à l'amiable aux entités concernées pour le traitement des réclamations et le règlement des litiges. 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 PC Type (RGS) 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 aux présentes PC sont, notamment, ceux indiqués au chapitre 10 ci-dessous

9.16 Dispositions diverses

9.16.1 Accord global

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

9.16.2 Transfert d'activités

Cf. chapitre 5.8.

9.16.3 Conséquences d'une clause non valide

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

9.16.4 Application et renonciation

Les présentes PC ne formulent 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 événement irrésistible, insurmontable et imprévisible.

9.17 Autres dispositions

Les présentes PC ne formulent pas d'exigence spécifique sur le sujet.

10 Annexe 1 : documents cités en référence

- **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
[DécretRGS]	Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005

- **10.1 Documents techniques**

Renvoi	Document
[RGS]	*Référentiel Général de Sécurité – Version 1.0*
[RGS_A_14]	*RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 2.3*
[RGS_B_1]	*Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 1.20*
[CWA14167-1]	*CWA 14167-1 (2003-06) Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1*
[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 – disponible : www.cofrac.fr*
[RFC3647]	*IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003*
[X.509]	*Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version 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 17/05/2004*

11 Annexe 2 : exigences de sécurité du module cryptographique de l'AC

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, répond 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 privées de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

11.2 Exigences sur la qualification

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

12 Annexe 3 : Exigences de sécurité du dispositif de protection de clés privées

12.1 Exigences sur les objectifs de sécurité

Le dispositif de protection de clés privées, utilisé par le serveur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, répond aux exigences de sécurité suivantes :

- Garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- Détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de re-génération de la clé privée ;
- Garantir la confidentialité et l'intégrité de la clé privée ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Générer une authentification qui ne peut être falsifiée sans la connaissance de la clé privée ;
- Assurer pour le serveur légitime uniquement, d'une part, la fonction d'authentification et, d'autre part, la fonction de déchiffrement de clés symétriques de session, et protéger la clé privée contre toute utilisation par des tiers ;
- Permettre de garantir l'authenticité et l'intégrité de la clé symétrique de session, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données ;
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

12.2 Exigences sur la qualification

Les exigences du RGS ne sont applicables que lorsque le PSCE fournit au RC le dispositif de protection des clés privées.

Sans objet, l'AC ne fournissant pas le dispositif de génération et de protection des clés privées du serveur.