MINISTÈRES ÉCONOMIQUES ET FINANCIERS

Liberté
Égalité
Fraternité

Secrétariat général

SECRÉTARIAT GÉNÉRAL
SERVICE DE L'ENVIRONNEMENT PROFESSIONNEL
139 RUE DE BERCY
75012 PARIS

POLITIQUE DE CERTIFICATION

DE L'AC3 FINANCES SG PRESTATAIRES

Document 01

Certificat d'authentification OID matériel : 1.2.250.1.131.1.13.20.3.1.1

Version - Date	Suivi des modifications
v1.0 – Juin 2023	Création

Entité	Rédaction	Vérification	Approbation
SG-SNUM-CTI	X		
SG-DSI-CTI			
SHFDS			

Table des matières

1 Introduction

1.1 Présentation générale

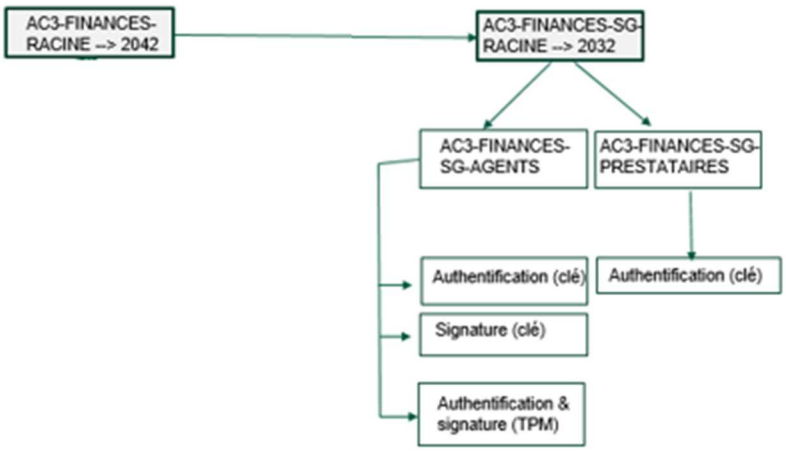
Dans le cadre général de la modernisation et de la rénovation des processus administratifs, le Ministère de l'Economie et des Finances s'est doté d'une infrastructure de Gestion de clés (IGC) internalisée appelée « IGC ministérielle ».

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

- une AC racine (AC3 FINANCES RACINE),
- une AC racine intermédiaire AC3 FINANCES SG RACINE
- Les AC subordonnées :
    - L'AC3-FINANCES-SG-AGENTS permet de délivrer des certificats d'authentification et des certificats de signature aux agents des ministères économiques et financiers.
    - L'AC3 FINANCES SG PRESTATAIRES permet de délivrer des certificats aux prestataires devant accéder à la plateforme ARTEMIS.

L'IGC FINANCES branche AC3 peut également signer les IGC de directions. Elle est organisée selon le schéma suivant :



Les certificats délivrés sont de type matériel, délivrés sur support cryptographique (token).

Le Service du Numérique opère également une IGC chiffrement indépendante des IGC FINANCES et FINANCES SG.

L'objectif de ce document est de définir le niveau d'exigence que s'engage à respecter l'AC3-FINANCES-SG-PRESTATAIRES tout le long du cycle de vie des certificats qu'elle émet, qu'elle révoque et qu'elle publie vis-à-vis de l'autorité de certification AC3 FINANCES SG RACINE. Cette Politique de Certification est conforme dans sa présentation à la RFC 3647.

Ce document s'appuie sur les préconisations, émises par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), le Référentiel Général de Sécurité (RGS 1.0) et la politique de filialisation de l'IGC ministérielle version 1.2 actuellement en cours de validité.

Le niveau de sécurité cible couvert par cette IGC 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 SG PRESTATAIRES et le terme AC racine pour désigner l'AC de l'IGC FINANCES SG 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 la politique de certification AC3 FINANCES SG PRESTATAIRES famille certificats matériels d'authentification sur token. Le numéro OID de cette PC est : 1.2.250.1.131.1.13.20.3.1.1

1.3 Définitions et acronymes

1.3.1 Acronymes

Les acronymes utilisés dans les présentes PC ou dans les PC type RGS 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

CMS Card Managment system

DN Distinguished Name

DPC Déclaration des Pratiques de Certification

ETSI European Telecommunications Standards Institute

IGC Infrastructure de Gestion de Clés.

IGC FINANCES SG PRESTATAIRES Infrastructure de gestion de clés dédiée aux certificats d'authentification et de signature pour les prestataires (ARTEMIS)

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

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

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.

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'AC 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 désigne les administrations de l'État, les collectivités territoriales, les établissements publics à caractère administratif, les organismes gérant des régimes de protection sociale et les autres organismes chargés de la gestion d'un service public administratif.

Autorité d'enregistrement (AE) : Chapitre 1.3.2.

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

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 du chapitre 1.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences des présentes PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

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 ces deux PC, le terme "certificat électronique" désigne uniquement un certificat délivré à une personne physique et portant sur une bi-clé d'authentification ou de signature, 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-SG-RACINE.

Dispositif d'authentification - Il s'agit du dispositif matériel et/ou logiciel utilisé par le porteur pour stocker et mettre en œuvre sa clé privée d'authentification.

Dispositif de création de signature - Il s'agit du dispositif matériel et/ou logiciel utilisé par le porteur pour stocker et mettre en œuvre sa clé privée de signature.

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

Fonction de génération des certificats - Cf. chapitre 1.4.1.

Fonction de génération des éléments secrets du porteur - Cf. chapitre 1.4.1.

Fonction de gestion des révocations - Cf. chapitre 1.4.1.

Fonction de publication - Cf. chapitre 1.4.1.

Fonction de remise au porteur - Cf. chapitre 1.4.1.

Fonction d'information sur l'état des certificats - Cf. chapitre 1.4.1.

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

Mandataire de certification - Cf. chapitre 1.4.1.1.

Personne autorisée - Cf. chapitre 1.4.1.1.

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 porteurs et les utilisateurs de certificats.

Porteur de certificats - Cf. chapitre 1.4.1.1.

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

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

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

Qualification d'un prestataire de services de certification électronique - Acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) à certaines exigences d'une PC Type pour un niveau de sécurité donné et correspondant au service visé par les certificats.

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

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

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

Utilisateur de certificat : Cf. chapitre 1.4.1.

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.

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

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

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

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

1.4 Entités intervenant dans l'IGC FINANCES SG

1.4.1 Autorité de certification

La notion d'Autorité de Certification (AC) telle qu'utilisée dans les présentes PC est définie au chapitre 1.6.2 ci-dessous.

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 (cf. ci-dessous).

Composition fonctionnelle de l'IGC

Afin de clarifier et faciliter l'identification des exigences, et en cohérence avec les documents de l'ETSI dans le domaine (cf. [ETSI_NQCP]), la décomposition fonctionnelle d'une IGC qui est retenue dans les présentes PC est la suivante :

Autorité d'enregistrement (AE) : Cette fonction vérifie les informations d'identification du futur porteur d'un certificat, 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 porteur 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 porteur provenant de la fonction de génération des éléments secrets du porteur.

Fonction de génération des éléments secrets du porteur : Dans le cas de l'AC, cette fonction n'est pas assurée par l'AC. Ces éléments secrets sont générés d'une manière décentralisée sur le support cryptographique du porteur, lors de sa demande de certificat dématérialisée.

Fonction de remise au porteur : Dans le cas de l'AC, cette fonction consiste à remettre au porteur le certificat par l'envoi d'un mèl . Le support cryptographique vérifie automatiquement la correspondance entre la clé privée du porteur et le certificat reçu lors de son intégration.

Auparavant, le support cryptographique a été remis au porteur de certificat. Il doit modifier le code PIN initial et le considérer comme confidentiel.

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

Fonction de gestion des révocations : Cette fonction traite les demandes de révocation (notamment identification et authentification du porteur) 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) ou lors d'une révocation.

1.4.1.1 Acteurs

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

- Porteur : La personne physique identifiée dans le certificat et qui est le détenteur de la clé privée correspondant à la clé publique qui est dans ce 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 porteurs de cette entité (il assure notamment le face-à-face pour l'identification des porteurs lorsque celui-ci est requis).

Dans le cas de l'IGC FINANCES SG-PRESTATAIRES, les mandataires de certification sont désignés par les Directions et structures utilisatrices ayant une relation contractuelle avec l'AC.

La désignation de nouveaux mandataires doit faire l'objet d'un courrier de la Direction ou de la structure utilisatrice à destination de l'autorité de certification de l'IGC FINANCES SG PRESTATAIRES.

- 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 porteur du certificat.

- **Personne autorisée :** Il s'agit d'une personne autre que le porteur et le mandataire de certification et qui est autorisée par la politique de certification de l'AC à mener certaines actions pour le compte du porteur (demande de révocation, de renouvellement, …).

Dans le cas de l'IGC FINANCES SG PRESTATAIRES, il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.

Les parties de l'AC concernées par la génération de certificats 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.

1.4.1.2 Exigences

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

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement, les exigences qui incombent à cette AC sont les suivantes :

- Être une entité légale au sens de la loi française,
- Être en relation par voie contractuelle avec l'entité pour laquelle elle a en charge la gestion des certificats des porteurs de cette entité. L'AC est également en relation contractuelle avec 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 porteurs, aux utilisateurs de certificats, à 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, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats.
- Élaborer, mettre en œuvre, contrôler, maintenir en condition de sécurité les composants et de façon itérative les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels.
- Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, notamment en termes de fiabilité, de qualité et de sécurité. A 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, de LCR et de réponses OCSP), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux porteurs 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 porteur de certificat. Pour cela, l'AE 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.

- La prise en compte et la vérification des informations du futur MC (cf. dernier paragraphe du 1.3.2) et de son entité de rattachement ainsi que la constitution du dossier d'enregistrement correspondant.

- L'établissement et la transmission de la demande de certificat à la fonction adéquate de l'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 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'AE peut s'appuyer sur un MC désigné et placé sous la responsabilité de l'entité cliente pour effectuer tout ou partie des opérations de vérification des informations (cf. chapitre 1.3.5.2 ci-dessous). 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 Porteurs de certificats

Dans le cadre des présentes PC, les porteurs des certificats émis suivant ces PC sont des Prestataires externes sous la responsabilité de la sous-direction de l'informatique du Secrétariat Général du Ministère de l'Economie et des Finances

Cette personne utilise sa clé privée et le certificat correspondant dans le cadre de ses activités en relation avec le SNUM et avec qui il a un lien contractuel.

Le porteur respecte les conditions qui lui incombent définies dans la PC de l'AC.

Cette personne doit utiliser sa clé privée et le certificat correspondant uniquement dans le cadre de ses activités professionnelles.

La relation entre le porteur de certificat et l'AC est formalisée par un engagement du porteur de certificat visant à certifier l'exactitude des renseignements et des documents fournis. Ce document comporte également une mention précisant les conditions d'usage des certificats émis par l'AC (Document DDC « Demande De Certificat »).

Le porteur s'engage à respecter les conditions d'usage des certificats définies dans ces PC et reprenant les conditions définies dans les PC type du RGS.

Les conditions d'usage sont conformes dans leur présentation au « PKI Disclosure Statement » de l'ETSI (*ETSI TS 101 456 V1.4.3)* .

1.4.4 Utilisateurs de certificats

1.4.4.1 Utilisateurs de certificats d'authentification

La PC (OID 1.2.250.1.131.1.13.20.3.1.1) traitant de certificats d'authentification (cf. chapitre 1.4), un utilisateur de certificats peut être notamment :

- Un service de l'administration accessible par voie électronique aux usagers (application, serveur Internet, base de données, etc.), sous la responsabilité d'une personne physique ou morale, qui utilise un dispositif de vérification d'authentification soit pour valider une demande d'accès faite par le porteur du certificat dans le cadre d'un contrôle d'accès, soit pour authentifier l'origine d'un message ou de données transmises par le porteur du certificat. L'application met en œuvre la politique et les pratiques de sécurité édictées par le responsable d'application.

Un usager destinataire d'un message ou de données provenant d'un agent et qui utilise un certificat et un dispositif de vérification d'authentification afin d'en authentifier l'origine.

Les utilisateurs de certificats doivent prendre toutes autres précautions prescrites dans les éventuels accords ou tout autre document notamment ceux listés au chapitre 9.6.4 de cette PC. En particulier, l'AC doit respecter ses responsabilités envers les utilisateurs qui ont « raisonnablement » confiance dans un certificat.

1.4.5 Autres participants

1.4.5.1 Composantes de l'IGC

La décomposition selon les fonctions de l'IGC est présentée au chapitre 1.4.1 ci-dessus. Les composantes de l'IGC mettant en œuvre ces fonctions sont présentées dans la DPC de l'AC.

1.4.5.2 Mandataire de certification

Le recours à un mandataire de certification (MC) est obligatoire.

Le MC est formellement désigné par un représentant légal du SNUM. Le MC est en relation directe avec l'AE de l'IGC.

Dans le cadre de l'IGC FINANCES SG PRESTATAIRES, 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 des futurs porteurs 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 délivré au porteur.

1.5 Usage des certificats

1.5.1 Domaine d'utilisation applicables

1.5.1.1 Bi-clés et certificats de porteurs

Certificats d'authentification :

La PC (OID1.2.250.1.131.1.13 .20.3.1.1), concernant les certificats d'authentification, traitent des bi-clés et des certificats à destination des catégories de porteurs identifiées au chapitre 1.3.3 ci-dessus, afin que ces porteurs puissent s'authentifier dans le cadre d'échanges dématérialisés avec les catégories d'utilisateurs de certificats identifiées au chapitre 1.3.4 ci-dessus. Il peut s'agir d'authentification dans le cadre d'un contrôle d'accès à un serveur ou une application, ou de l'authentification de l'origine de données dans le cadre de la messagerie électronique.

Ceci correspond notamment aux relations suivantes :

- Authentification d'un agent vis-à-vis d'un usager,
- Authentification d'un agent ou prestataire vis-à-vis d'un service de l'administration accessible par voie électronique aux agents ou prestataires.

L'utilisateur du certificat a ainsi un certain degré d'assurance que le porteur identifié dans le certificat est l'émetteur des données d'authentification, générées en tout ou partie à l'aide de la clé privée correspondante. Le niveau d'assurance dépend, notamment, des moyens mis en œuvre par l'AC tout au long du cycle de vie du certificat, ainsi que des mesures prises par le porteur afin de protéger sa clé privée.

Dans le cadre d'une application d'échanges dématérialisés avec l'Administration, le responsable de l'application décide quel niveau de sécurité est requis.

Niveau (*)

Les certificats d'authentification objets de cette PC sont utilisés par des applications pour lesquelles les risques de tentative d'usurpation d'identité pour pouvoir accéder aux applications et/ou aux biens de ces applications, ou pour pouvoir démontrer l'origine de données, existent mais sont **moyens** (intérêt pour les usurpateurs, attraits des biens, etc.).

De plus, certaines applications peuvent requérir des preuves d'accès et/ou de demande d'accès à des biens qui puissent être opposables au porteur du certificat par le responsable du contrôle d'accès sur le système informatique qui héberge les biens. La définition de la forme et du fond de la constitution et de la mise en contradiction de ces preuves est du ressort de l'application au travers des conditions d'utilisation de l'application. Ces preuves doivent reposer sur un cadre juridique propre au contrôle d'accès. Ces conditions d'utilisation doivent être reconnues par les porteurs de certificat et le responsable du contrôle d'accès et des biens.

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

Le SG du Ministère de l'Economie et des Finances dispose de bi-clés séparées, les certificats correspondants à ces bi-clés sont rattachés à une AC de niveau supérieur (AC3-FINANCES-RACINE).

Les présentes PC comportent des exigences, concernant les bi-clés et certificats de l'AC ainsi que les clés, bi-clés et certificats des composantes de l'IGC (sécurisation des échanges entre composantes, signature des journaux d'événements, 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 et LCR. Pour signer ces objets, cette AC dispose d'une bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur : l'AC Racine.

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

Les certificats des opérateurs de l'IGC sont délivrés par une autorité de certification, l'AC2 FINANCES TECHNIQUE (couverte par sa propre PC dont l'OID est 1.2.250.1.131.1.1.12.13.1.14 qui est signée par l'AC2 FINANCES RACINE.

1.5.2 Domaine d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.5 ci-dessous. L'AC respecte ces restrictions et impose leur respect par ses porteurs et ses utilisateurs de certificats.

A cette fin elle communique à tous les porteurs, MC et utilisateurs potentiels les termes et conditions relatives à l'utilisation du certificat.

De plus, l'usage des certificats attribués par l'AC est strictement limité aux activités professionnelles des agents. Tout autre usage n'est pas autorisé.

En conséquence, l'AC n'acceptera aucune plainte d'aucune sorte, liée à des litiges sans rapport avec les applications autorisées.

1.6 Gestion de la PC

1.6.1 Entité gérant la PC

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

Le SHFDS du SG est responsable de l'approbation de ces PC.

La Délégation au Système d'Information du Secrétariat Général, maîtrise d'ouvrage stratégique est responsable de la validation de ces PC.

Elle est revue périodiquement pour s'assurer de sa conformité aux évolutions de ses PC authentification et signature.

Le processus d'évolution et d'amendement de ces 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 SNUMI du SG du ministère.

1.6.3 Entité déterminant la conformité d'une DPC avec ces PC

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

1.6.4 Procédure d'approbation de la conformité de la DPC

Le SHFDS, entité indépendante de l'AC fait auditer la conformité de la DPC avec les PC de l'AC. Sur la base du rapport d'audit, la DSI 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 la DPC.

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 ces PC.

2 RESPONSABILITÉ CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ETRE 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 porteurs 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 1.3.1 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 SG 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 dies IGC du SG du Ministère de l'Economie et des Finances,

Dans sa fonction d'information sur l'état du certificat de l'AC3-FINANCES-SG-PRESTATAIRES et des certificats de porteurs, l'IGC publie les listes de révocation aux adresses suivantes :

- http://igc1.finances.gouv.fr/ac3-finances-racine.crl
- http://igc2.finances.gouv.fr/ac3-finances-racine.crl
- http://igc1.finances.gouv.fr/ac3-finances-sg-racine.crl
- http://igc2.finances.gouv.fr/ac3-finances-sg-racine.crl
- http://igc1.finances.gouv.fr/ac3-finances-sg-prestataires.crl
- http://igc2.finances.gouv.fr/ac3-finances-sg-prestataires.crl

- Un site web interne : l'Intranet des IGC du SG SNUM du Ministère de l'Economie et des Finances ;

2.2 Informations devant être publiées

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

- Ses politiques de certification, couvrant l'ensemble des rubriques du [RFC3647] et conforme aux PC type RGS 'Authentification' ou 'Signature' ainsi que les éventuels documents complémentaires ;
- La liste des certificats révoqués (porteurs et AC) ;
- Les certificats de l'AC, en cours de validité,
- Les certificats en cours de validité des AC de la hiérarchie dont dépend la présente AC (AC3 FINANCES SG PRESTATAIRES), 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 porteurs de certificats, 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 porteurs ou des utilisateurs de certificats non spécialistes du domaine, il est **obligatoire** que l'AC publie également des conditions générales d'utilisation correspondant aux "PKI Disclosure Statement" (PDS) définis par [ETSI_NQCP] et [RFC3647]. Il est recommandé que ces conditions générales aient une structure conforme à celle décrite en annexe B de [ETSI_NQCP] et reprennent ainsi, à destination des porteurs et des utilisateurs de certificats, les informations pertinentes de la 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 garanties 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.

Ces informations, (cf. chapitre 4.10), sont publiées sur l'Intranet des IGC du SG du Ministère de l'Economie et des Finances.

Les PC, les certificats d'AC, les LAR et les LCR sont également publiés sur Internet aux adresses suivantes :

https://igc1.finances.gouv.fr/ et https://igc2.finances.gouv.fr/

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

2.3 Délais et fréquence de publication

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

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

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

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats 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 X509v3 l'AC émettrice (issuer) et le porteur (subject) sont identifiés par un "Distinguished Name" (DN) de type X.501 dont le format exact est précisé dans le document [RGS_A4] décrivant le profil des certificats.

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les porteurs de certificats doivent être explicites.

Les certificats émis dans le cadre de l'IGC FINANCES SG AGENTS ne comportent pas d'identité pseudonyme ou anonyme.

Le DN du porteur est construit à partir des nom et prénom de son état civil tel que portés sur les documents d'identité présentés lors de son enregistrement auprès de l'AE ou, le cas échéant, du MC.

3.1.3 Anonymisation ou pseudonymisation des porteurs

Les certificats émis dans le cadre de l'AC, ne comportent pas une identité pseudonyme ou anonyme.

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.

3.1.5 Unicité des noms

Afin d'assurer la continuité de l'identification unique du porteur au sein du domaine de l'AC dans ses certificats successifs (renouvellement) et pour éviter toute ambiguïté, le champ "subject" du DN de chaque certificat de porteur doit permettre d'identifier de façon unique le porteur correspondant au sein du domaine de l'AC.

Ce CN doit pour cela respecter les exigences correspondantes définies dans le document [RGS_A4], notamment pour le traitement des cas d'homonymie au sein du domaine de l'AC.

Durant toute la durée de vie de l'AC, un DN attribué à un porteur de certificats ne peut être attribué à un autre porteur.

Le DN comporte les éléments suivants :

- Le prénom du porteur (GN)
- Le nom du porteur (SN) tel qu'il figure dans l'annuaire ministériel
- Le CommonName du porteur (CN) Nom prénom-rang d'homonymie
- L'unité d'organisation (OU) = N° SIRET de la société du porteur
- L'organisation (O) = Société du porteur
- Le pays (C) = FR

A noter que l'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC, mais que ce numéro est propre au certificat et non pas au porteur et ne permet donc pas d'assurer une continuité de l'identification dans les certificats successifs d'un porteur donné.

L'AC s'engage également à ce que le champ « Objet » présente aussi un caractère d'unicité, obtenu par la présence d'un identifiant unique CommonName.

3.1.6 Identification, authentification et rôles 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 porteur se fait via un mandataire de certification de l'entité. Le MC doit être préalablement enregistré par l'AE.

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 et du rattachement du futur MC à l'entité.
- Enregistrement d'un porteur via un MC : validation par le MC de l'identité "personne physique" et de son rattachement à l'entité pour laquelle le MC intervient. Le MC transmet le dossier validé 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

Le porteur générant sa bi-clé au moment de la requête de demande de certificat, l'autorité de certification exige des agents la preuve de la possession de la clé privée associée à la clé publique à certifier.

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 aux besoins suivants :

- Utilisation du dossier du MC comme référence pour les données d'identification de l'entité de tous les porteurs présentés par le MC

Le dossier d'enregistrement d'un MC comprend :

- Un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le MC. Ce mandat doit être signé par le MC pour acceptation,
- 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 porteurs,
- 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 est 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.

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

L'authentification du porteur par le MC 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, porteur) certifiée conforme par le signataire concerné (date, de moins de 3 mois, et signature de la personne concernée sur la photocopie de ses papiers d'identité précédées de la mention "copie certifiée conforme à l'original").

3.2.3.4 Enregistrement d'un porteur via un MC

Le dossier d'enregistrement, déposé auprès d'un MC, doit au moins comprendre :

- Une demande de certificat, datée de moins de 3 mois, indiquant l'identité du porteur, cosigné par le porteur et le MC,
- Les conditions générales d'utilisation signées,
- Une copie d'un document officiel d'identité en cours de validité du porteur 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 par le futur porteur, la signature étant précédée de la mention manuscrite "copie certifiée conforme à l'original".

- L'adresse postale et / ou l'adresse mail permettant de contacter le porteur.

Le MC doit vérifier que l'identité du porteur 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 porteur doit être informé que les informations personnelles d'identité pourront être utilisées comme élément d'authentification lors de la demande de révocation, dans le cas où l'AC s'appuie sur un tel mécanisme.

L'authentification du porteur par le MC se fait par l'envoi du dossier papier par courrier accompagné d'une photocopie de son document d'identité certifiée conforme par le futur porteur (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").

Lors de la transmission des dossiers de porteurs par le MC, celui-ci doit s'authentifier auprès de l'AE au cours d'un face-à-face et/ou par le paraphe du MC apposé sur les différentes pages du dossier de demande, complété par sa signature sur les pages principales.

3.2.4 Informations non vérifiées du porteur

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

3.2.5 Validation de l'autorité du porteur

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

3.3.1 Identification et validation pour un renouvellement courant

Par sécurité et pour parer au cas de changement d'identité du porteur pendant la durée de validité de son certificat, une copie du document d'identité sera demandée pour tout renouvellement.

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 ou via un service en ligne (serveur web), le demandeur doit être formellement authentifié : vérification de l'identité du demandeur et de son autorité par rapport au certificat à révoquer.

Par exemple : série d'au moins une ou deux questions / réponses sur des informations propres au demandeur, utilisation éventuelle d'un identifiant / mot de passe envoyé préalablement au demandeur de façon sécurisée).

3.4.1 Dossier de Demande de Révocation planifiée, formulaire DDR

Une demande de révocation peut être transmise par courrier ou par télécopie. Elle doit alors être signée par le demandeur et le service de gestion des révocations doit s'assurer de l'identité du demandeur (vérification de la signature manuscrite par rapport à une signature préalablement enregistrée) et de son autorité par rapport au certificat à révoquer.

Ce service est à utiliser lorsque la demande de révocation est non urgente et planifiée (changement de situation de l'agent à une date prévue).

La demande de révocation fait l'objet d'un document signé par le demandeur et transmis à l'AE, par courrier ou remis en mains propres à un opérateur d'AE

L'AE vérifie l'authenticité de la ou des demandes et le droit à révoquer le certificat.

3.4.2 Par intranet

- Pour les certificats sur token, sur le site d'enrôlement de l'IGC

3.4.3 Par Internet

Ce service est à utiliser à l'exception lorsque la révocation n'est pas planifiée (perte ou vol du certificat).

Le service en ligne est mis à disposition de l'agent 7 jours sur 7, 24 h/24, afin de révoquer son certificat dans les meilleurs délais. L'agent se connecte sur un des deux sites WEB de l'IGC FINANCES SG (https://igc1.finances.gouv.fr ou https://igc2.finances.gouv.fr) dans la partie destinée aux demandes de révocation. Il doit alors s'authentifier en complétant un formulaire électronique. Les informations à fournir comprennent notamment son code de révocation, tel qu'il l'a renseigné lors de sa demande dématérialisée de certificat. Les informations fournies, il peut alors révoquer son certificat.

3.4.4 Par Téléphone

Le prestataire peut demander la révocation de son certificat par téléphone à son mandataire de certification, s'il est dans l'impossibilité de le faire autrement. Celui-ci analyse la demande, vérifie l'authenticité du demandeur et le droit à révoquer.

Le mandataire de certification doit rappeler le prestataire et effectuer la vérification de son identité (une ou deux questions d'identification personnelle liée au demandeur, utilisation éventuelle d'un identifiant / mot de passe envoyé préalablement au demandeur de façon sécurisée).

Il transmet un formulaire de révocation à l'AE.

La fonction de gestion des révocations a une durée maximale d'indisponibilité de deux heures jour ouvré.

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine de la demande

La personne à l'origine d'une demande de certificat est le futur porteur.

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) :

- Le nom du porteur à utiliser dans le certificat (nom réel) ;
- Les données personnelles d'identification du porteur ;

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

Par ailleurs, l'AE, ou l'AED le cas échéant, doit s'assurer de disposer d'une information permettant de contacter le MC ou le futur porteur 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" sont vérifiées conformément aux exigences du chapitre 3.2.

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

- Valider l'identité du futur porteur ;
- Vérifier la cohérence des justificatifs présentés ;
- S'assurer que le futur porteur 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 (l'AED) transmet la demande de génération du certificat vers la fonction adéquate de l'IGC (cf. chapitre 1.4.1).

L'AE conserve ensuite une trace des justificatifs d'identité présentés :

- Le dossier étant au format papier, la photocopie de la pièce d'identité devra être signée par le futur porteur, la signature étant précédées de la mention "copie certifiée conforme à l'original".

4.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, l'AE, en informe le porteur, 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 en jours ouvrés et n'excède pas quelques minutes après la validation administrative de la demande.

4.3 Délivrance du certificat

4.3.1 Action 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 du certificat et de préparation des différents éléments destinés au porteur :

Au minimum, le certificat, et, selon les cas, son dispositif d'authentification ou de création de signature, les codes d'activation, etc. (cf. chapitre 1.3.1).

La bi-clé étant générée par le porteur, la clé publique est transmise à l'AC (cf. chapitre 6.1.3).

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

Dans le cas de l'AC FINANCES SG, pour les demandes de certificat sur token, l'AC génère automatiquement un courriel, à destination du porteur, contenant l'adresse de téléchargement du certificat.

L'AC n'ayant pas généré elle-même la bi-clé du porteur, elle s'assure que le certificat est bien associé, dans l'environnement du porteur, à la clé privée correspondante. Le certificat est alors téléchargé sur le bon token cryptographique.

Le module cryptographique demandeur contrôle avant d'installer le certificat rapatrié qu'il est bien associé à la bi-clé qu'il a générée.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

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

- le porteur informe l'AC d'inexactitudes dans les champs constitutifs de son certificat,
- le porteur notifie à l'AC, par écrit, son refus d'acceptation de celui-ci et n'en fait pas usage.

En cas de refus, le porteur notifie l'AC, par écrit, éventuellement à l'aide d'un formulaire, son refus d'acceptation de celui-ci (inexactitudes dans les champs constitutifs de son certificat, ...) et n'en fait pas usage. Le certificat est alors révoqué par un opérateur d'AE.

4.4.2 Publication du certificat

Les certificats d'authentification des agents ou prestataires ne sont pas publiés.

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

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

4.5 Usages de la bi-clé et du certificat

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

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée :

- Pour les certificats d'authentification, au service d'authentification (cf. chapitre 1.4.1.1).
- Pour les certificats de signature, au service de signature (cf. chapitre 1.4.1.1).

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

L'usage autorisé de la bi-clé du porteur et du certificat associé est par ailleurs indiqué dans le certificat lui-même, via les extensions concernant les usages des clés (cf. [RGS_A4]). Cet usage explicité dans les présentes PC figure également dans les conditions générales d'utilisation et/ou le contrat porteur. Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du porteur ou 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

Nota – Conformément au [RFC3647], la notion de "renouvellement de certificat" correspond à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique du porteur).

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, une nouvelle bi-clé est créée lors de chaque demande de certificat par le module cryptographique du porteur, il n'y a pas de renouvellement de certificat

Un porteur de certificat 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 porteur 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 de bi-clé

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

4.7.1 Causes possibles de changement de bi-clé

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

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

4.7.2 Origine d'une demande d'un nouveau certificat

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

L'entité, via son MC le cas échéant, peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un porteur qui lui est rattaché.

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 porteur de l'établissement d'un 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

Nota - Conformément au [RFC3647], la modification d'un certificat correspond à des modifications d'informations sans changement de la clé publique (cf. chapitre IV.7) et autres qu'uniquement la modification des dates de validité (cf. chapitre IV.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 porteur 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 de porteurs

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

- Les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple le changement d'entité du porteur d'un certificat, ceci avant l'expiration normale du certificat) ;
- Le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le porteur 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 du porteur ;
- La clé privée du porteur est suspectée de compromission, est compromise, est perdue ou est volée (éventuellement les données d'activation associées) ;
- Le porteur 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 porteur et/ou de son support) ;
- Le décès du porteur ou la cessation d'activité de l'entité du porteur.
- 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)

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 Certificat 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.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificats de porteurs

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

- Le porteur au nom duquel le certificat a été émis ;
- Le MC ;
- Un représentant légal de l'entité ;
- L'AC émettrice du certificat ou l'AE.

Nota : Le porteur doit être informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son certificat.

4.9.2.2 Certificat 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 de porteur

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

Les procédures d'identification et de validation d'une demande de révocation sont détaillées au chapitre 3.4.

Les points d'accès pour les demandes de révocations sont les suivants :

- Par Internet https://igc1.finances.gouv.fr ou https://igc2.finances.gouv.fr
- Sur le site d'enrôlement de l'IGC (intranet)
- Par formulaire DDR (demande de révocation) à remettre à l'AE.

Pour les demandes de révocation planifiées (changement de situation d'un agent à une date prévue), le formulaire de Demande De Révocation (DDR) doit contenir les informations suivantes :

- Le numéro du certificat ;
- L'identité du porteur de certificat ;
- L'identité du demandeur ;
- La signature manuscrite du demandeur ;
- Le motif de la demande de révocation.

Le processus de gestion de révocation via des demandes téléphoniques ou par Internet est détaillé au paragraphe 3.4.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats. L'information de révocation est diffusée via une LCR signée par l'AC3-FINANCES-SG-PRESTATAIRES.

Le porteur et le demandeur de la révocation (si le porteur du certificat n'est pas le demandeur) sont informés du bon déroulement de l'opération et de la révocation effective du certificat.

L'opération et l'identité de l'opérateur d'AE ayant effectué l'opération, ou du porteur dans le cas d'une révocation en ligne, sont enregistrées dans les journaux d'événements de l'IGC.

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

L'AC précisera 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 porteurs concernés que leurs certificats ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés à l'AE, et aux MC. Ces derniers devront informer les porteurs de certificats en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Le certificat de l'AC est signé par l'AC racine (AC3-FINANCES-SG-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 porteur pour formuler la demande de révocation

Dès que le porteur de certificat 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 de porteur

Par nature une demande de révocation doit être traitée en urgence, à l'exception des demandes de révocation planifiées correspondant au changement de situation du porteur à une date prévue. Dans ce cas, l'agent doit disposer de ses droits d'authentification ou de signature jusqu'à la date de changement de sa situation. Son certificat doit être révoqué dès que l'agent quitte ses fonctions.

La fonction de gestion des révocations doit être disponible en heures ouvrées.

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

Toute demande de révocation d'un certificat porteur 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 et de LCR / LAR) 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 agent est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante à l'aide des LCR mises à sa disposition.

Il est recommandé d'utiliser des applications sécurisées dotées de fonctions d'accès aux LCR et de contrôles automatiques de l'état des certificats.

4.9.7 Fréquence d'établissement de la LCR

La fréquence de publication des LCR est de 24 heures

La LCR est également publiée après chaque révocation d'un certificat de porteur.

Sa durée de validité est de 6 jours.

L'AC ne met pas en œuvre de mécanisme de deltaLCR

Les LAR émises par l'AC Racine de rattachement de la présente AC a une durée maximale d'un mois. La fréquence de publication de nouvelles LAR est cohérente avec cette durée et est précisée dans la politique de certification de l'AC Racine.

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. Dans les faits, elle est publiée immédiatement après 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. paragraphe 4.9.6

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 agent à condition qu'ils respectent les exigences d'intégrité, de disponibilité et de délai de publication décrites dans la PC type.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats de porteur, 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 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 fait l'objet d'une information clairement diffusée sur le site Internet de l'AC et éventuellement relayée par d'autres moyens (autres sites Internet Institutionnels, journaux, etc.).

4.9.13 Causes possibles d'une suspension

La suspension de certificat n'est pas autorisée par 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 fournit aux utilisateurs de certificats, sur les sites https://igc1.finances.gouv.fr, https://igc2.finances.gouv.fr et sur le site Intranet des IGC du SG du Ministère de l'Economie et des Finances 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 au format V2. 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 à 24h/24 7j/j.

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

4.10.3 Dispositifs optionnels

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

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

En cas de fin de relation contractuelle entre l'AC et le porteur avant la fin de validité du certificat, pour une raison ou pour une autre, ce dernier doit être révoqué.

4.12 Séquestre de clé et recouvrement

Ce document traite des aspects d'authentification et de signature électronique et interdit donc le séquestre des clés privées des porteurs.

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 SECURITE NON TECHNIQUES

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

5.1 Mesures de sécurité physique

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

5.1.1 Situation géographique des sites

L'IGC FINANCES doit être 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 du domaine des centres informatiques.

5.1.2 Accès physique

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

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

5.1.3 Alimentation électrique et climatisation

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

Elles doivent également permettre de respecter les exigences des PC Type (RGS), ainsi que les engagements pris par l'AC dans les présentes 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 des PC Type (RGS), ainsi que les engagements pris par l'AC dans les présentes 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 des PC Type (RGS), ainsi que les engagements pris par l'AC dans les présentes 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 doivent être identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).

L'AC doit maintenir un inventaire de ces informations. L'AC doit mettre en place des mesures pour éviter la compromission et le vol de ces informations.

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations doivent être gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils doivent être manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.

Des procédures de gestion doivent protéger ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle l'AC s'engage à conserver les informations qu'ils contiennent.

5.1.7 Mise hors service des supports

En fin de vie, les supports devront être, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

Les procédures et moyens de destruction et de réinitialisation doivent être conformes à ce niveau de confidentialité (voir notamment le guide [972-1]).

5.1.8 Sauvegarde hors site

En complément de sauvegardes sur sites, il est recommandé que les composantes de l'IGC mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes doivent être organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conformes aux exigences de la PC type RGS 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 doivent respecter les exigences des PC Type (RGS) 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 de confiance suivants :

- **Responsable sécurité de l'IGC** : Le responsable sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est responsable des opérations de génération et de révocation des certificats.
- **Responsable d'application** : Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.

- **Ingénieur système** : il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.
- **Opérateur** : Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
- **Contrôleur** : Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.

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

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

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

Ces rôles doivent être 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 doivent être 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 doivent être 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, il est demandé de répartir les fonctions sensibles 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'AC (cf. chapitre 6).

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

5.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante de l'IGC doit faire vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

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

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

Chaque attribution d'un rôle à un membre du personnel de l'IGC doit être notifiée par écrit. Ce rôle doit être 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 doivent être soumis à une clause de confidentialité vis-à-vis de leur employeur. Dans le cas des agents, ceux-ci sont soumis à leur devoir de réserve.

Chaque entité opérant une composante de l'IGC doit s'assurer que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles.

Le personnel d'encadrement doit posséder l'expertise appropriée à son rôle et être familier des procédures de sécurité en vigueur au sein de l'IGC.

L'AC doit informer toute personne intervenant dans des rôles de confiance de l'IGC :

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

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

5.3.2 Procédures de vérification des antécédents

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

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

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

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

5.3.3 Exigences en matière de formation initiale

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

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

5.3.4 Exigences en matière de formation continue

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

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Aucune rotation des rôles n'est permise dans le cadre 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 MEF décide des sanctions disciplinaires à appliquer (Règlement de la Fonction Publique).

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

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

5.3.8 Documentation fournie au personnel

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

5.4 Procédures de constitution des données d'audit

La journalisation d'événements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

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

5.4.1 Types d'événements à enregistrer

Chaque entité opérant une composante de l'IGC journalise les évènements suivants, automatiquement dès le démarrage d'un système et sous forme électronique, concernant les systèmes liés aux fonctions qu'elle met en œuvre dans le cadre de l'IGC :

- 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 ;
- Evénements 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 recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- Les accès physiques ;
- Les actions de maintenance et de changements de la configuration des systèmes ;

- Les changements apportés au personnel ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,...).

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 ;
- Evénements 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 porteur (bi-clé, codes d'activation,…) ;
- Génération des certificats des porteurs ;
- Transmission des certificats aux porteurs et, selon les cas, acceptations / rejets explicites par les porteurs ;
- Le cas échéant, remise de son dispositif de création d'authentification ou de signature au porteur ;
- 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 et, éventuellement, deltaLCR ;
- Le cas échéant, requêtes / réponses OCSP.

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

- Type de l'événement ;
- Nom de l'exécutant ou référence du système déclenchant l'événement ;
- Date et heure de l'événement (L'heure exacte des événements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat doit être enregistrée) ;
- Résultat de l'événement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'événements.

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

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

Les opérations de journalisation sont effectuées au cours du processus.

En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'événement.

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

5.4.2 Fréquence de traitement des journaux d'événements

Cf. Paragraphe 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 1 mois.

Les journaux d'événements sont conservés sur site pendant au moins 1 mois.

Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous 1 mois (recouvrement possible entre la période de conservation sur site et la période d'archivage). La durée de conservation des archives est de 7 ans.

5.4.4 Protection des journaux d'événements

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

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

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

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

5.4.5 Procédure de sauvegarde des journaux d'événements

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

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

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

Les journaux sont analysés dans leur totalité au moins une fois toutes les 2 semaines et dès détection d'anomalie. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé 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.) est effectué au moins une fois par mois, ceci afin de vérifier la concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie.

5.5 Archivage des données

5.5.1 Types de données à archiver

Des dispositions en matière d'archivage doivent être également prises par l'AC. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

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

Les données à archiver sont les suivantes :

- Les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- Les PC ;
- 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 mandataires de certification,
- Les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement
- Les journaux d'événements de l'IGC.

5.5.2 Période de conservation des archives

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté doit être archivé aussi longtemps que nécessaire, et pendant au moins sept (7) ans 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 porteurs 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 porteur 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 des personnes physiques désignées dans le certificat émis par l'AC.

Certificats et LCR émis par l'AC

Les certificats de clés de porteurs et d'AC ainsi que les LCR / LAR produites, sont archivés pendant cinq ans après l'expiration de ces certificats.

Journaux d'événements

Les journaux d'événements traités au chapitre 5.4 seront archivés pendant sept 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 :

- Etre protégées en intégrité ;
- Etre 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 (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

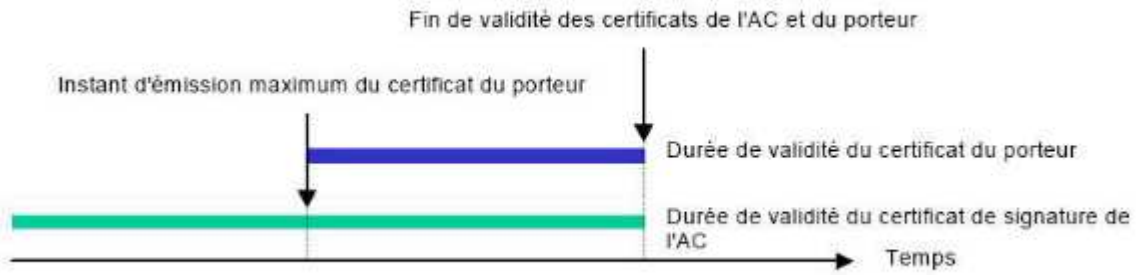
Les présentes PC ne formulent pas d'exigence spécifique sur le sujet, si ce n'est que le système de collecte des archives, qu'il soit interne ou externe, doit respecter les exigences de protection des archives concernées.

5.5.7 Procédures de récupération et de vérification des archives

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

5.6 Changement de clé de l'AC

L'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 au moins jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré (cf. nota à la fin du chapitre 1.4.1.1).

5.7 Reprise suite à compromission et sinistre

5.7.1 Procédures de remontée et de traitement des incidents et compromission

Chaque entité opérant une composante de l'IGC doit mettre en œuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'événements. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'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 porteurs devient insuffisant pour son utilisation prévue restante, alors l'AC doit :

- informer tous les porteurs et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou avec lesquels elle a d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;

- révoquer tout certificat concerné.

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

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

Ce plan 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 doit être traité dans le plan de continuité de la composante (cf. chapitre 5.7.2) en tant que sinistre.

Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué : cf. chapitre 4.9.

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

- Informer les entités suivantes de la compromission : tous les porteurs, 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 doivent disposer des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences des présentes PC (cf. chapitre 5.7.2).

5.8 Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses.

L'AC doit prendre les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

Le transfert d'activité est défini comme la fin d'activité d'une composante de l'IGC ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par l'AC en collaboration avec la nouvelle entité.

La cessation d'activité est définie comme la fin d'activité d'une composante de l'IGC comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

Transfert d'activité ou cessation d'activité affectant une composante de l'IGC

Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AC doit entre autres obligations :

1) Mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats).

2) Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans les présentes PC. A défaut, les applications de l'Administration refuseront les certificats émis par des AC dont les LCR en cours de validité ne seraient plus accessibles, même si le certificat du porteur est encore valide.

L'AC s'engage également à réaliser les actions suivantes :

1) Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des porteurs ou des utilisateurs de certificats, l'AC doit les en aviser aussitôt que nécessaire et, au moins, sous délai d'un mois.

2) L'AC doit communiquer au point de contact identifié sur le site : https://ssi.gouv.fr les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans 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 informé 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 doit stipuler dans ses pratiques les dispositions prises en cas de cessation de service. Elles doivent inclure :

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

Lors de l'arrêt du service, l'AC 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) révoquer tous les certificats qu'elle a signés et qui seraient encore en cours de validité.

4) demander la révocation de son certificat à l'AC racine.

5) informer (par exemple par récépissé) tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant (cf. chapitre 3.2.3).

6 MESURES DE SECURITE TECHNIQUES

Les exigences définies dans la suite du présent chapitre sont les exigences minimales que l'AC 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. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets doit être mise en œuvre par son porteur.

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 des rôles de confiance et en présence d'un témoin qui atteste, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

6.1.1.2 Clés des porteurs générées par l'AC

Sans objet dans la mesure où l'AC ne génère pas les bi-clés des porteurs.

6.1.1.3 Clés des porteurs générées par le porteur

L'offre de certificats proposée aux agents du Ministère de l'Economie et des Finances intègre la fourniture de dispositifs cryptographiques, dans le cas de certificats sur support matériel (token), conformes aux exigences du chapitre XII ci-dessous pour le niveau de sécurité considéré.

Dans ce cas, les porteurs s'engagent, en signant les conditions générales d'utilisation des certificats, à ne pas utiliser d'autres dispositifs cryptographiques pour supporter les clés et certificats de l'AC3-FINANCES-SG-PRESTATAIRES.

Les Directions qui utilisent les services de l'IGC FINANCES SG doivent s'engager à respecter cette exigence.

Dans le cas de certificats logiciels les exigences de sécurité sont également satisfaites par l'utilisation de mécanisme décrit dans la DPC,

6.1.2 Transmission de la clé privée à son propriétaire

Sans objet dans la mesure où la bi-clé du porteur est générée

- Soit par son dispositif cryptographique relié à son poste de travail et non par l'AC ;
- Soit de façon logicielle sur son poste de travail.

6.1.3 Transmission de la clé publique de l'agent à l'AC

En cas de transmission de la clé publique du porteur vers une composante de l'AC (cas où la bi-clé est générée par le porteur), la clé doit être protégée en intégrité et son origine doit être authentifiée.

Cette exigence se matérialise par des considérations techniques décrites dans la DPC (le numéro de demande dématérialisée est reporté dans la demande administrative, l'opérateur vérifie la concordance des deux numéros de demande).

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.

Le certificat de l'AC3-FINANCES-SG-PRESTATAIRES et sa chaîne de certificats d'AC racines : AC3-FINANCES-SG-RACINE, AC racine de l'IGC FINANCES 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 SG aux adresses suivantes : https://igc1.finances.gouv.fr/ et https://igc2.finances.gouv.fr/

6.1.5 Tailles des clés

Les clés d'AC et de porteurs sont décrites au chapitre 7 de cette PC.

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

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

6.1.7 Objectifs d'usage de la bi-clé

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR (cf. chapitre 1.4.1.2 et document [RGS_A4]).

Dans le cas du certificat d'authentification, l'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service d'authentification (cf. chapitres 1.4.1.1, 4.5 et le document [RGS_A4]).

Dans le cas du certificat de signature, l'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service de signature (cf. chapitres 1.4.1.1, 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

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

6.2.1.2 Dispositifs d'authentification et de signature des porteurs

Les dispositifs d'authentification et de création de signature des porteurs, dans le cas des certificats sur token cryptographiques, sont qualifiés au niveau de sécurité élémentaire par l'ANSSI et respectent les exigences du chapitre 12 ci-dessous pour le niveau de sécurité considéré.

L'AC fournit ce dispositif sans personnalisation au porteur, elle s'assure que :

- Les dispositifs sont stockés et distribués de façon sécurisée.
- Les désactivations et réactivations des dispositifs sont contrôlées de façon sécurisée.

Dans le cas d'un certificat sur token ou clé cryptographique, les porteurs s'engagent, en signant les conditions générales d'utilisation des certificats, à ne pas utiliser d'autres dispositifs cryptographiques pour supporter les clés et certificats de l'AC3-FINANCES-SG-PRESTATAIRES que celui fourni par l'AE.

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 est 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 porteurs ne doivent en aucun cas être séquestrées

6.2.4 Copie de secours de la clé privée

Les clés privées des porteurs ne doivent faire l'objet d'aucune copie de secours par l'AC.

Les clés privées d'AC font l'objet de copies de secours, hors du module cryptographique mais sous forme chiffrée et avec un mécanisme de contrôle d'intégrité. Le chiffrement correspondant doit offrir un niveau de sécurité

équivalent ou supérieur au stockage au sein du module cryptographique et, notamment, s'appuyer sur un algorithme, une longueur de clé et un mode opératoire capables de résister aux attaques par cryptanalyse pendant au moins la durée de vie de la clé ainsi protégée. Les règles à respecter sont définies dans le document [RGS_B1].

Les opérations de chiffrement et de déchiffrement doivent être effectuées à l'intérieur du module cryptographique de telle manière que les clés privées d'AC ne soient à aucun moment en clair en dehors du module cryptographique.

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

6.2.5 Archivage de la clé privée

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

Les clés privées des porteurs 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

Les clés privées des porteurs sont générées et stockées au sein de leur module cryptographique ou dans le magasin de certificat du navigateur du poste de travail du porteur. Elles ne font l'objet d'aucun transfert.

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

6.2.7 Stockage de la clé dans un module cryptographique

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

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées 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 dans un rôle de confiance (par exemple, responsable sécurité et opérateur) et trois porteurs de secret sur cinq.

6.2.8.2 Clés privées des porteurs

Dans le cas d'un certificat sur support matériel token l'activation de la clé privée du porteur est contrôlée par un code PIN d'activation (cf. chapitre 6.4) et répond aux exigences définies dans le chapitre 12 pour le niveau de sécurité considéré.

Dans le cas d'un certificat sur support matériel, token il est de la responsabilité du porteur de certificat de protéger par mot de passe la clé privée de sa bi-clé et pour le token d'assurer la conservation de son support physique.

Ces données d'activation doivent être considérées, par l'agent, comme secrètes.

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 porteurs

Lorsqu'un certificat de porteur est expiré ou révoqué, la clé privée correspondante est détruite par l'utilisateur ou son MC, ou son correspondant informatique à l'aide de l'utilitaire fourni avec l'équipement cryptographique, selon le support.

Lorsque tous les certificats du porteur sont expirés ou révoqués le token de l'agent est réinitialisé par l'utilisateur ou son MC ou correspondant informatique pour retour au stock de l'IGC.

Dans le cas d'un équipement cryptographique bloqué ou dont le code PIN est inconnu, la carte SIM contenue dans le token est détruite.

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 doit permettre 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 porteurs

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

Lorsqu'un certificat de porteur est expiré ou révoqué, la clé privée correspondante est détruite.

Dans le cas de certificat matériel, la clé cryptographique de l'agent est réinitialisée pour retour au stock de l'IGC.

Dans le cas d'un support logiciel, le fichier contenant la clé privée et toutes les copies de ce fichier sont effacées par le porteur.

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

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

Dans le cas de certificats sur token cryptographique, les dispositifs d'authentification et de création de signature des porteurs sont qualifiés au niveau de sécurité renforcé par l'ANSSI.

Dans le cas de certificats logiciels les clés privées sont stockées dans un magasin de certificats sous Windows protégées par mot de passe répondant aux exigences de la PSSI.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

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

6.3.2 Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des porteurs couverts par les présentes PC doivent avoir une durée de vie maximale de 3 ans.

Dans le cas de l'AC, la durée de validité des certificats de porteur est de 3 ans.

La fin de validité d'un certificat d'AC doit être postérieure à la fin de vie des certificats porteurs qu'elle émet.

La durée de validité du certificat de l'AC est de 6 ans.

Cette durée de vie est cohérente avec les caractéristiques de l'algorithme et de la longueur de clés utilisés définies au chapitre 7.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

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

6.4.1.2 Génération et installation des données d'activation correspondant à la clé privée du porteur

Dans le cas de l'AC, ces données d'activations sont définies par le porteur après intégration de son certificat dans son équipement cryptographique.

Ces données d'activation doivent être considérées comme confidentielles par le porteur.

Dans le cas d'un certificat logiciel, un mot de passe doit être défini par le porteur. Ce mot de passe doit respecter les exigences définies par l'entité du porteur (règles imposées automatiquement par le domaine Windows de l'entité lorsqu'elles sont définies et mentionnées dans le guide utilisateur de demande de certificat publié sur l'intranet ministériel).

Si les données d'activation sont sous forme de mots de passe dont les règles de constitution ne sont pas imposées par domaine Windows, le porteur est informé de la politique de constitution des mots de passe dans le guide utilisateur de demande de certificat publié sur l'intranet ministériel,

6.4.2 Protection des données d'activation

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

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

6.4.2.2 Protection des données d'activation correspondant aux clés privées de porteurs

Le porteur doit considérer ces données comme confidentielles. De plus, dans le cas d'un certificat sur support matériel, il doit conserver soigneusement et de manière séparée son équipement cryptographique et son code d'activation.

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

Les mesures de sécurité relatives aux systèmes informatiques doivent satisfaire aux objectifs de sécurité qui découlent de l'analyse de risque que l'AC peut mener. (cf. chapitre 1.3.1)

Une analyse des objectifs de sécurité peut être effectuée en amont de tout projet d'IGC par l'AC, de façon à garantir la prise en compte de la sécurité dans les systèmes informatiques.

L'AC met en place les mesures nécessaires pour assurer la protection des échanges d'informations entre les différentes composantes de l'IGC et vérifie périodiquement les mesures de sécurité prises dans ce cadre. L'AC documente les mesures mises en œuvre et conserve une traçabilité des vérifications périodiques réalisées.

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 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 1.4.1.2) fait l'objet de mesures particulières, qui découlent de l'analyse de risque (cf. rappel au début du présent chapitre 6).

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 pour le niveau une étoile.

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.

6.6.1 Mesures de sécurité liées au développement des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'IGC doit être documentée et doit respecter dans la mesure du possible des normes de modélisation et d'implémentation.

La configuration du système des composantes de l'IGC ainsi que toute modification et mise à niveau doivent être documentées et contrôlées.

L'AC doit :

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

6.6.2 Mesures liées à la gestion de sécurité

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

Toute évolution significative d'un système d'une composante de l'IGC doit faire l'objet d'une validation préalable de l'AC.

Ces évolutions logicielles ou matérielles sont contrôlées et validées sur une 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 doit être protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

L'AC doit garantir que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de leur conformité avec les exigences spécifiées par l'AC.

De plus, les échanges entre composantes au sein de l'IGC font l'objet de la mise en place de mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.).

6.8 Horodatage / Système de datation

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

Pour dater ces événements, les différentes composantes de l'IGC peuvent recourir :

- soit à une autorité d'horodatage, interne ou externe à l'IGC, conforme à la politique d'horodatage [RGS_A5] ;

- soit en utilisant l'heure système de l'IGC en assurant une synchronisation des horloges des systèmes de l'IGC entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près.

Pour les opérations faites hors ligne (ex : administration d'une AC Racine), cette précision de synchronisation par rapport au temps UTC n'est pas requise. Le système devra toutefois pouvoir ordonner les événements avec une précision suffisante. Pour la synchronisation par rapport au temps UTC, il est recommandé de se référer à un système comprenant au moins deux sources indépendantes de temps.

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

7.1 Profil 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 présente les champs de base

Champ	**Valeur**	**Explications**
Version	2 pour version V3	Version du certificat X509
SerialNumber (Numéro de série)		Numéro de série unique du certificat. Celui -ci est généré de façon aléatoire.
Signature algorithm identifier (Algorithme de signature)	Sha256 RSA 2048 bits	
Issuer (Emetteur) au format UTF8	CN=AC3-FINANCES-SG-prestataires OU = 0002 130013345 O=MINISTERE DE L ECONOMIE ET DES FINANCES C=FR	Nom de l'AC émettrice. DN de l'AC.
Validity period	Not before	Date de génération du certificat
	Not after de génération + 3 ans	Date d'expiration du certificat – durée de validité 3 ans
Subject (Objet) au format UTF8 à l'exception de l'attribut Country qui est au format printable string	GN = Prénom du porteur SN = Nom du porteur CN=Nom prénom SERIALNUMBER = identifiant* (unique) de l'agent dans la base des porteurs ARTEMIS OU= SIRET entreprise du prestataire O=entreprise du prestataire C=FR	Nom distinctif de l'entité identifiée

SubjectPublicKeyInfo(Clé publique)	Valeur de la clé publique RSA (2048)	Valeur de la clé publique RSA

*pour exemple l'identifiant Anaïs est composé des premières lettres du prénom suivi du nom-identifiant de la direction

7.1.2 Extensions du certificat pour les certificats d'authentification

Champ	**Valeur**	**Critique**	**Explications**
authorityKeyIdentifier	Doit avoir pour valeur le keyIdentifier de l'AC	Non critique	Identifiant de la clé publique de l'AC émettrice
KeyUsage	digitalSignature	Critique	Cette extension définit l'utilisation prévue du certificat.
certificatePolicies	PC OID= 1.2.250.1.131.1.13.20.3.1.1 https://igc1.finances.gouv.fr/ac3-finances-sg-prestataires.pdf https://igc2.finances.gouv.fr/ac3-finances-sg-prestataires.pdf	Non critique	Identifiants de la politique de certification
CRLDistributionPoints	https://igc1.finances.gouv.fr/ac3-finances-sg-prestataires.crl https://igc2.finances.gouv.fr/ac3-finances-sg-prestataires.crl	Non critique	Adresse de publication de la liste de révocation
SubjectKeyIdentifier	keyIdentifier	Non critique	Identifie la clé publique contenue dans le certificat.
subjectAltName	Nom RFC822 (Adresse courriel du porteur)	Non critique	Nom supplémentaire pour le porteur de certificat
extendedKeyUsage	ClientAuth	Non critique	Utilisé pour les clients RADIUS.

7.1.3

7.1.3 OID des algorithmes

Cf. Chapitre 7.1.2 et 7.1.3

7.1.4 Forme des noms

Cf. Chapitre 7.1.1

7.1.5 Contraintes sur les noms

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

7.1.6 OID des PC

Cf. Chapitre 7.1.2 et 7.1.3

7.1.7 Utilisation de l'extension « Contraintes Politiques »

Cf. Chapitre 7.1.2 et 7.1.3

7.1.8 Sémantique et syntaxe des qualifiants de politique

Cf. Chapitre 7.1.2 et 7.1.3

7.1.9 Sémantique de traitement des extensions critiques de PC

Cf. Chapitre 7.1.2 et 7.1.3

7.2 Profil 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-SG-PRESTATAIRES

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 6 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

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 d'une manière détaillée.

7.3 Profil OCSP

7.3.1 Numéro de version

Sans Objet.

7.3.2 Extension OCSP

Sans Objet.

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

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

La démarche et les exigences liées aux audits de qualification sont définies dans [PROG_ACCRED] et ne sont donc 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 procède à un contrôle de conformité de cette composante.

L'AC procède également régulièrement à un contrôle de conformité de l'ensemble de son IGC, au moins une fois tous les 3 ans.

8.2 Identités / Qualifications des évaluateurs

Le SNUM du SG assigne les audits de composantes de l'IGC qu'elle souhaite contrôler y compris les AED, 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.

8.3 Relations entre évaluateurs et entités évaluées

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. Les AED entrent dans le périmètre de ces audits.

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

8.4 Sujets couverts par les évaluations

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

L'AC met en place les mesures nécessaires pour assurer la protection des échanges d'informations entre les différentes composantes de l'IGC et vérifie périodiquement les mesures de sécurité prises dans ce cadre. L'AC documente les mesures mises en œuvre et conserve une traçabilité des vérifications périodiques réalisées.

- **8.5 Actions prises suite aux conclusions des évaluations**

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

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

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (temporaire ou définitive) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et respecte ses politiques de sécurité internes.
- En cas de résultat "A confirmer", l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être 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.

8.5 Communication des résultats

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

9 AUTRES PROBLEMATIQUES MÉTIERS et LÉGALES

9.1 Tarifs

Les tarifs des opérations de gestion du cycle de vie des certificats sont établis dans le cadre d'une convention entre le Secrétariat Générale et la Direction souscrivant au service.

9.2 Responsabilité financière

Sans Objet.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

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

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 Responsabilité en terme de protection des informations confidentielles

L'AC et l'AE sont tenues d'appliquer des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles au chapitre 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, chacune des entités susnommées doit en garantir l'intégrité.

L'AC et l'AE sont notamment tenues de respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elles peuvent devoir mettre à disposition les dossiers d'enregistrement des porteurs à des tiers dans le cadre de procédures légales. Elles doivent également donner l'accès à ces informations au porteur 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 règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données [RGPD]et de la loi [CNIL] loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés.

9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont les suivantes :

- Les causes détaillées de révocation des certificats des porteurs (qui sont considérées comme confidentielles sauf accord explicite de l'agent) ;
- Les dossiers d'enregistrement des porteurs et des MC.

9.4.3 Informations à caractère non personnel

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

9.4.4 Responsabilités en termes de protection des données personnelles

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

9.4.5 Notification et consentement d'utilisation des données personnelles

Les informations que tout porteur remet à l'AC 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.

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

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

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

9.4.7 Autres circonstances de divulgation d'informations personnelles

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 les PC de l'AC et les documents qui en découlent,
- Respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante),
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre 8) et l'organisme de qualification,
- Respecter les accords ou contrats qui les lient entre elles ou aux porteurs,
- Documenter leurs procédures internes de fonctionnement,
- Mettre en œuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.6.1 Autorités de Certification

L'AC a pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, conformément aux exigences du chapitre 4.4 ci-dessus.
- Garantir et maintenir la cohérence de sa DPC avec ses PC.
- Prendre toutes les mesures raisonnables pour s'assurer que ses porteurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC. La relation entre un porteur et l'AC est formalisée par un lien contractuel / hiérarchique / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

L'AC est responsable de la conformité de ses Politiques de Certification avec les exigences émises dans les PC Type RGS * Authentification et Signature et dans la politique de filialisation ministérielle.

L'AC assume toute conséquence dommageable résultant du non-respect de ses PC par elle-même ou l'une de ses composantes. Elle doit prendre les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec 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 porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

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

En cas de non-respect ponctuel des obligations décrites dans la présente PC, l'administration se réserve le droit de refuser temporairement ou définitivement des 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 Porteurs de certificats

Le porteur de certificat a le devoir de :

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

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

Les exigences à respecter par le porteur de certificat sont consignées dans les conditions générales signées par le porteur lors de la demande de certificat.

9.6.4 Mandataires de certification

Le mandataire s'engage à :

- Communiquer des informations exactes et à jour lors de sa demande d'engagement ;
- Signaler, sans délai, son départ de l'entité
- Effectuer correctement et de façon indépendante les contrôles d'identité des futurs porteurs de l'entité pour laquelle il est MC,
- Respecter les parties des PC et de la DPC de l'AC qui lui incombent.
- Contrôler le bon déroulement des opérations de demande, renouvellement et révocation de certificat. Aider le porteur à effectuer ces opérations.

9.6.5 Utilisateurs de certificats

Les utilisateurs de la Sphère publique utilisant les certificats doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis.
- Contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application.
- Pour chaque certificat de la chaîne de certification, du certificat du porteur jusqu'à l'AC Racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation).
- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans les présentes PC.

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

9.6.6 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 des 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 la validité

La publication d'une nouvelle version des PC Type (RGS) ou de la politique de filialisation du Ministère de l'Economie et des Finances peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer ses PC.

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

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

9.10.3 Effets de la fin de validité et clauses restants applicables

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

9.11 Notifications individuelles et communications entre participants

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

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

9.12 Amendements aux PC

9.12.1 Procédures d'amendements

L'AC contrôle que tout projet de modification de ces PC reste conforme aux exigences de des PC Type RGS, des éventuels documents complémentaires du RGS et de la politique de filialisation du Ministère de l'Economie et des Finances. En cas de changement important, l'AC fait appel à une expertise technique pour en contrôler l'impact.

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 chaque PC de l'AC étant inscrit dans les certificats qu'elle émet, toute évolution de ces PC ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences.

En particulier, les OID des PC de l'AC doivent évoluer dès lors qu'un changement majeur intervient dans les exigences des PC Type (RGS) et de la politique de filialisation applicable à la famille de certificats considérée.

9.13 Dispositions concernant la résolution des conflits

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

9.14 Juridictions compétentes

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.

9.15 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'activité

Cf. Paragraphe 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 CITES EN REFERENCE

10.1 Réglementation

Renvoi	Document
[CNIL]	*Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2004-801 du 6 août 2004.*
[DécretRGS]	*Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005*
[RGPD]	*Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016. Règlement relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)*
[LSQ]	*Loi n°2001-1062 du 15 Novembre 2001 relative à la sécurité quotidienne.*

10.2 Documents techniques

Renvoi	Document
[RGS]	*Référentiel Général de Sécurité – Version 2.0*
[RGS_A4]	*RGS - Politiques de Certification Types - Profils de certificats, de LCR et OCSP et algorithmes cryptographiques – Version 3.0*
[ETSI_NQCP]	*ETSI EN 319411-1 v1.1.1 de Février 2016. Policy and Security Requirements for Trusted Service Issuing Certificates ; Part 1 : General Requirements*
[PROG_ACCRED]	*COFRAC -Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 -publié cf www.cofrac.fr*
[RFC3647]	*IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003*
[RFC5280]	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*
[RGS_B1]	*Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI, Version 2.0*
[X.509]	*Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version mars 2000 (complétée par les correctifs techniques n° 1 d'octobre 2001, n° 2 d' avril 2002 et n° 3 d'avril 2004)*
[972-1]	*DCSSI - Guide Technique pour la confidentialité des informations enregistrées sur les disques durs à recycler ou exporter – N° 972-1/SGDN/DCSSI du 17/07/2003*

11 ANNEXE 2 : EXIGENCES DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'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 et, éventuellement, des réponses OCSP), 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 ;
- Etre 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 ;
- Etre capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Si une fonction de sauvegarde et de restauration des clés privée de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration.

11.2 Exigences sur la qualification

Le token 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 SECURITE DU MODULE CRYPTOGRAPHIQUE DU PORTEUR

12.1 Exigences sur les objectifs de sécurité

12.1.1 Pour les certificats d'authentification

Le dispositif d'authentification, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, répond aux exigences de sécurité suivantes :

- Si la bi-clé d'authentification du porteur est générée par le dispositif, 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 régénération 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 la fonction d'authentification pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ;
- 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

12.2.1 Pour les certificats d'authentification

Pour les certificats sur token cryptographique, le dispositif de création d'authentification utilisé par le porteur est qualifié au niveau renforcé par l'ANSSI selon le processus décrit dans le [RGS], et est conforme aux exigences du chapitre 12.1.1.