MINISTÈRE
DE L'ÉCONOMIE,
DES FINANCES
ET DE LA SOUVERAINETÉ
INDUSTRIELLE ET NUMÉRIQUE

Liberté
Égalité
Fraternité

Secrétariat général

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

Politique de Certification
Personnes physiques

*AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE (*1.2.250.1.131.1.11.6.3.1.1 *)*
*AC CONFIDENTIALITE MEF QUALIFIEE (*1.2.250.1.131.1.11.7.3.1.1 *)*

V 1.6
Diffusion : publique

TABLE DES MATIERES

1 INTRODUCTION

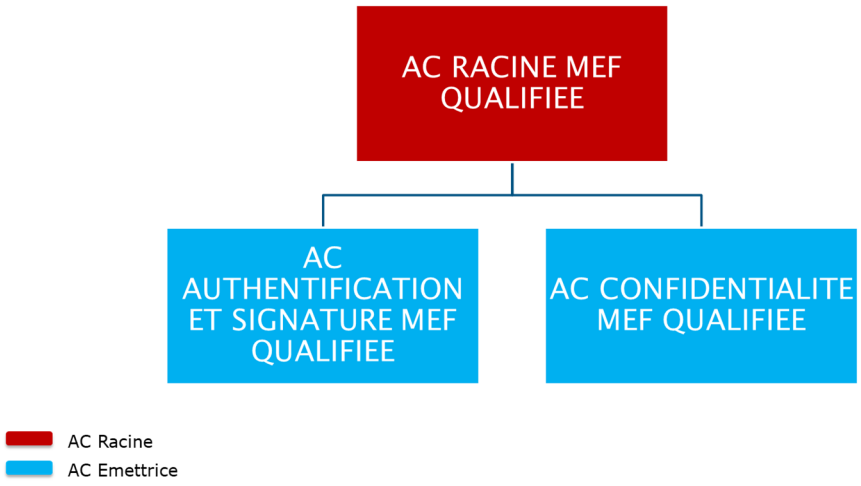
1.1 Présentation générale

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

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

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

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



Le présent document constitue la Politique de Certification (PC) des Autorités de Certification émettrices « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » et « *AC CONFIDENTIALITE MEF QUALIFIEE* » des MEF et contient les informations publiques de la Déclaration des Pratiques de Certification (DPC) associée.

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

Dans le cadre de la présente PC :

- L'AC « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » délivre des certificats double usage authentification et signature qualifiés au sens du RGS pour le niveau de sécurité 2 étoiles (**) et qualifiés au sens du règlement eIDAS.
- L'AC « *AC CONFIDENTIALITE MEF QUALIFIEE* » délivre des certificats de chiffrement qualifiés au sens du RGS pour le niveau de sécurité 1 étoile (*).

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

De manière à mettre en exergue les règles spécifiques à un type d'usage (*authentification/signature ou chiffrement*) ou à un type de porteur, celles-ci seront présentées dans un encadré, le titre du cadre précisant son périmètre d'application (*usage du certificat électronique, niveau de sécurité et type de porteur du certificat électronique*). La forme est la suivante :

Certificats d'authentification signature sur QSCD pour des personnes physiques

Certificats de chiffrement sur QSCD pour des personnes physiques

1.2 Identification du document

Ci-dessous les différents OID associés aux typologies de certificat portées par la présente PC :

Usage du certificat	**OID de la PC**	**Niveau de qualification**
Authentification et Signature	1.2.250.1.131.1.11.6.3.1.1	RGS ** / ETSI QCP-N-QSCD
Confidentialité	1 1.2.250.1.131.1.11.7.3.1.1	RGS *

La présente PC est associée à la Déclaration des Pratiques de Certification (DPC) contenant les informations des pratiques des AC, considérées comme confidentielles par les MEF, et identifiée par un OID.

1.3 Définitions et acronymes

1.3.1 Acronymes

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

AC	Autorité de certification
AE	Autorité d'enregistrement
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
ARL	Authority Revocation List, ou LAR
CS	Comité de Surveillance

CN	Common Name
CRL	Certificate Revocation List, ou LCR
CSR	Certificate Signing Request
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
HSM	Hardware Security Module
LAR	Liste des certificats d'AC révoqués, ou ARL
LCR	Liste des Certificats Révoqués
LDAP	Light Directory Access Protocol
MC	Mandataire de certification
OCSP	Online Certificate Status Protocol
OI	Organization Identifier
OID	Object Identifier
OU	Organizational Unit
PC	Politique de certification
PDS	PKI Disclosure Statement (*Déclaration des informations du service d'émission de certificats*)
PIN	Personal Identification Number
PSCE	Prestataire de services de certification électronique
PUK	PIN Unlock Key
QSCD	Qualified Signature Creation Device (Dispositif de création de signature qualifié)
RGPD	Règlement Général sur la Protection des Données
RSA	Rivest Shamir Adelman
SAN	Subject Alternative Name
SHA256	Secure Hash Algorithm 256
SP	Service de publication
SSI	Sécurité des systèmes d'information
UPN	User Principal Name
URL	Uniform Resource Locator

1.3.2 Définitions

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

Entrée	Définition
Algorithme RSA	Inventé en 1978 par Ronald L. Rivest, Adi Shamir et Leonard M. Adleman. Il peut être utilisé pour chiffrer des informations et/ou pour les signer (signature numérique).

Entrée	Définition
Autorité de certification (AC)	Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre 1.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.
Autorité de certification émettrice	Autorité de certification dont le certificat est signé par l'autorité de certification racine. Une autorité de certification émettrice signe les certificats des porteurs.
Autorité de certification racine	Autorité de certification dont le certificat est auto-signé. L'autorité de certification racine signe les certificats des autorités de certification émettrices.
Autorité d'enregistrement (AE)	Cf. paragraphe 1.4.3.
Bi-clé	Ensemble constitué d'une clé publique et d'une clé privée, formant une paire indissociable utilisée par un algorithme cryptographique asymétrique.
Comité de Surveillance	Entité des MEF en charge de la validation des politiques de certification.
Certificat électronique	Document sous forme électronique attestant du lien entre une clé publique et l'identité de son propriétaire. Cette attestation prend la forme d'une signature électronique réalisée par un prestataire PSCE. Il est délivré par une Autorité de Certification. Le certificat est valide pendant une durée donnée précisée dans celui-ci. Les usages des certificats électroniques régis par le présent document sont le double usage signature électronique + authentification et la confidentialité.
Clé privée	Composant confidentiel d'une bi-clé, connu uniquement de son propriétaire et utilisé par lui seul pour déchiffrer une donnée dont il est destinataire ou pour signer des données dont il est l'auteur.
Clé publique	Composant non confidentiel d'une bi-clé, pouvant être communiqué à tous les membres d'une population. Une clé publique permet de chiffrer des données à destination du porteur de la bi-clé. Elle permet également de vérifier une signature apposée par le porteur.

Entrée	Définition
Composante	Plate-forme opérée par une entité et constituée d'au moins un poste informatique, une application et, le cas échéant, un moyen de cryptologie et jouant un rôle déterminé dans la mise en œuvre opérationnelle d'au moins une fonction du service d'émission de certificats.
Liste des certificats révoqués	Certificate Revocation List ou Liste de Certificats Révoqué (LCR) Liste des numéros de certificats ayant fait l'objet d'une révocation. La LCR est signée par l'autorité de certification pour assurer son intégrité et son authenticité.
Déclaration des pratiques de certification (DPC)	Ensemble des pratiques à mettre en œuvre pour satisfaire aux exigences de la PC.
Politique de certification (PC)	Ensemble de règles qui indique les conditions d'applicabilité d'un certificat pour une communauté donnée ou pour des applications ayant des besoins de sécurité communs.

1.4 Entités intervenant dans l'infrastructure de gestion de clés

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

1.4.1 Comité de surveillance du service d'émission de certificats

Le Comité de Surveillance du service d'émission de certificats est l'autorité responsable du service d'émission de certificats des MEF.
Le Comité de Surveillance est l'organe décisionnaire concernant la PC et la DPC du service et il est chargé de les faire appliquer.

1.4.2 Autorités de certification

Dans le cadre de la présente Politique de Certification, le Ministère de l'Economie, des Finances et de la Relance endosse le rôle d'Autorité de Certification (*AC*).
L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (*génération, diffusion, renouvellement, révocation,…*) et s'appuie pour cela sur une infrastructure technique.
Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats.

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

- **Autorité d'enregistrement (AE)** (*aussi appelée « service d'enregistrement »*) - Cette fonction vérifie les informations d'identification du futur porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate du service, en fonction des services rendus et de l'organisation du service. L'AE a également en charge, lorsque cela est nécessaire, la re vérification 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'AE et de la clé publique du porteur provenant soit du porteur, soit de la fonction de génération des éléments secrets du porteur, si c'est cette dernière qui génère la bi-clé du porteur.
- **Fonction de génération des éléments secrets du porteur** - Cette fonction génère les éléments secrets à destination du porteur, si l'AC a en charge une telle génération, et les prépare en vue de leur remise au porteur (*par exemple, personnalisation du dispositif destiné au porteur, courrier sécurisé avec le code d'activation, etc.*). Ces éléments secrets sont directement la bi-clé du porteur, les codes (*activation, déblocage*) liés au dispositif de stockage de la clé privée du porteur.
- **Fonction de remise au porteur** - Cette fonction remet au porteur au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (*dispositif du porteur, clé privée du porteur, codes d'activation,…*).
- **Fonction de publication** - Cette fonction met à disposition des différentes parties concernées, les politiques et 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. Elle peut également mettre à disposition, en fonction de la politique de l'AC, les certificats valides de ses porteurs.
- **Fonction de gestion des révocations** - Cette fonction traite les demandes de révocation (*notamment identification et authentification du demandeur*) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.
- **Fonction d'information sur l'état des certificats** - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (*révoqués, suspendus, etc.)*. Cette fonction peut être mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (LCR, LAR) et éventuellement également selon un mode requête-réponse temps réel (OCSP).
- **Fonction de gestion des recouvrements** - Cette fonction traite les demandes de recouvrement de clés privées des porteurs (notamment identification et authentification du demandeur) et détermine les actions à mener. Dans le cas d'une décision positive, le recouvrement est réalisé par la fonction de séquestre et recouvrement.
- **Fonction de séquestre et recouvrement** - Cette fonction fournit la capacité de séquestrer de manière sécurisée les clés privées de confidentialité des porteurs, puis de les recouvrer en cas de besoin, sur la base de demandes authentifiées et traitées par la fonction de gestion des recouvrements (*cf. chapitre 4.12*).

Ces fonctions sont assurées par l'OT excepté la fonction de publication, la fonction d'information sur l'état des certificats ainsi que l'archivage.

Un certain nombre d'entités et personnes physiques externes au service d'émission de certificats des MEF interagissent avec ce dernier. 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.

- **Utilisateur de certificat** - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique 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 ou par contrat avec l'AC à mener certaines actions pour le compte du porteur (*demande de révocation).* Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du porteur ou d'un responsable des ressources humaines.

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

- Être une entité légale au sens de la loi française.
- Être en relation par voie contractuelle ou hiérarchique ou réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats des porteurs de cette 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, ceux qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes du service et sont adéquates et conformes aux normes en vigueur.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions obligatoires de la présente PC, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats.
- Élaborer, mettre en œuvre, contrôler et maintenir les mesures de sécurité et les procédures opérationnelles, concernant ses installations, ses systèmes et ses biens informationnels.
- Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble du service 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 ce qui est nécessaire pour respecter les engagements définis dans sa PC, notamment en termes de fiabilité, de qualité et de sécurité.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (*signature de certificats, de 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.

1.4.3 Autorité d'enregistrement

Dans le cadre de la présente Politique de Certification (*PC*), le rôle d'Autorité d'Enregistrement (*AE*) a pour objectif d'être endossé par chaque direction du Ministère sur laquelle les cartes Rossignol sont déployées.
Aussi, dans le cadre de la présente PC, les directions du Ministère endossant le rôle d'AE sont les suivantes :

Liste des directions des MEF endossant le rôle AE
La Direction Générale des Douanes et Droits Indirects (DGDDI),
L'Administration Centrale.

Le rôle d'AE est endossé par les directions citées ci-dessus sur tout le territoire.

L'AE applique des procédures d'identification des personnes physiques ou morales, conformément aux règles définies par l'Autorité de Certification. Son but est d'établir que le demandeur a bien l'identité et les qualités qui seront indiquées dans le certificat.

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 et la constitution du dossier d'enregistrement correspondant,
- L'établissement et la transmission de la demande de certificat à la fonction adéquate du service d'émission de certificats suivant l'organisation de ce dernier 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 y compris lors des échanges de ces données avec les autres fonctions du service (*notamment, elle respecte la législation relative à la protection des données personnelles*).

L'AE assure également la fonction de remise au porteur.

1.4.4 Porteurs de certificats

Dans le cadre de la présente PC, un porteur de certificats ne peut être qu'une personne physique. Le porteur est un agent des MEF ou une personne externe liée contractuellement aux MEF, qui utilise sa clé privée et le certificat électronique associé pour ses activités en lien avec l'entité, identifiée dans le certificat électronique, avec laquelle il a une relation contractuelle, hiérarchique ou réglementaire.

Le porteur respecte les conditions qui lui incombent et qui sont définies dans la présente PC et dans les Conditions Générales d'Utilisation.

1.4.5 Utilisateurs de certificats

Sont appelés utilisateurs, les personnes physiques ou services en ligne qui utilisent les certificats émis par les AC des MEF.

Dans le cadre des certificats d'authentification et signature électronique, un utilisateur peut être notamment :

- Un service en ligne qui utilise un certificat et 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,
- Un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification d'authentification afin d'en authentifier l'origine,
- Un service en ligne qui utilise un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le porteur du certificat,
- Un usager qui signe électroniquement un document ou un message,
- Un usager destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par le porteur du certificat sur ce message ou sur ces données.

Dans le cadre des certificats chiffrement, un utilisateur peut être notamment :

- Un service en ligne qui utilise un dispositif de chiffrement pour chiffrer des données ou un message à destination du porteur du certificat,
- Une personne qui émet un message chiffré à l'intention du porteur du certificat électronique.

1.4.6 Autres participants

1.4.6.1 Composantes du service d'émission de certificats

L'AC délègue les prestations techniques de gestion du service d'émission de certificats à un Opérateur technique (OT). Toutefois la fonction publication reste affectée aux MEF

1.4.6.2 Mandataires de certification

Le recours à un mandataire de certification (MC) n'est pas obligatoire pour une entité. Une même entité peut s'appuyer sur un ou plusieurs MC.
Dans le cas où elle y a recours, le MC est nécessairement un agent des MEF et est formellement désigné par un représentant légal de l'entité concernée. Le MC est en relation directe avec l'AE.
Le MC est une personne ayant, directement par la réglementation ou par délégation, le pouvoir d'autoriser une demande de certificat portant le nom de l'entité. Il peut aussi avoir d'autres pouvoirs au nom de l'organisation, comme celui de révocation.
Dans le cadre d'une organisation, un MC peut être désigné pour effectuer les actes nécessaires à l'émission d'un certificat en lieu et place des porteurs.

Le MC doit :

- Être une personne physique dûment autorisée à agir pour le compte d'une organisation,
- 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/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 n'a pas 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 Domaines d'utilisation applicables

1.5.1.1 Bi-clés et certificats des porteurs

Les certificats émis dans le cadre de la présente PC couvrent les usages suivants limités aux activités professionnelles :

Authentification et signature
Les usages sont : • L'authentification des porteurs auprès de serveurs distants ou auprès d'autres personnes (*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*). • La signature électronique de données apportant, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

Confidentialité
Les usages sont : • Déchiffrement : à l'aide de sa clé privée, un porteur déchiffre les données qui lui ont été transmises dans le cadre d'échanges dématérialisés, chiffrées à partir de sa clé publique ; • Chiffrement : à l'aide de la publique du destinataire, une personne chiffre des données.

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

La bi-clé de l'AC est utilisée uniquement pour :

- Signer les certificats de porteurs qu'elle émet,
- Signer les listes de certificats révoqués (LCR) qu'elle émet,
- Signer les certificats des répondeurs OCSP.

1.5.2 Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.5 de la présente PC. Les porteurs et utilisateurs de certificats doivent respecter les conditions d'utilisation de la clé privée et du certificat correspondant.
Les MEF décline toute responsabilité dans l'usage fait d'un certificat dans un cadre autre que l'usage prévu au chapitres 1.5.1.1 et 4.5.

1.6 Gestion des politiques de certification

1.6.1 Entité gérant les politiques de certification

La présente PC est élaborée et mise à jour par les MEF et validée par le Comité de Surveillance du service d'émission de certificats.

1.6.2 Point de contact de la politique de certification

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

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

Contact-igc-mef@finances.gouv.fr

1.6.3 Entité gérant la conformité de la DPC avec les PC

Le Comité de Surveillance du service d'émission de certificats a autorité et la responsabilité finale pour déterminer la conformité des pratiques de certification avec la présente PC.

1.6.4 Procédures d'approbation de la conformité de la DPC

L'AC met en place un processus d'approbation de la conformité des pratiques à la présente PC.
L'AC est responsable de la gestion (*mise à jour, révisions*) de la PC/DPC. Toute demande de mise à jour de la PC/DPC suit le processus d'approbation mis en place.
Elle est présentée en Comité de Surveillance pour être validée ou rejetée. Toute nouvelle version de la PC/DPC est publiée, conformément aux exigences du paragraphe 2.2 sans délai.

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

2.1 Entités chargées de la mise à disposition des informations

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

Pour la mise à disposition de l'information sur l'état des certificats, l'AC s'appuie sur la publication d'une LCR (*Liste des Certificats Révoqués*) et sur un répondeur OCSP.

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

2.2 Informations publiées

L'AC publie sur les sites
https://igc.finances.gouv.fr
https://igc1.finances.gouv.fr
https://igc2.finances.gouv.fr

les informations suivantes à destination des porteurs et des utilisateurs de certificats :

- Les PC applicables,
- Les éléments publics de la DPC,
- Les certificats d'AC,
- Les LCR des AC,
- Les Conditions Générales d'Utilisation correspondant aux « *PKI Disclosure Statement* » (PDS) définis dans la norme ETSI applicable,
- Les formulaires.

Les URLs des éléments publiés sont précisées dans la DPC.
Par ailleurs, les détails de la DPC que l'AC considère comme confidentiels ne sont pas publiés.

2.3 Délais et fréquence de publication

Les informations documentaires de l'AC (*nouvelle PC, conditions générales d'utilisation, …*) sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.

Les certificats d'AC sont diffusés préalablement à toute diffusion de certificats de porteurs et/ou de LCR correspondantes.

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

Les LCR sont mises à jour toutes les 12 heures et sont publiées au maximum dans les 30 minutes qui suivent leur génération.

2.4 Contrôle d'accès aux informations publiées

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

L'accès en modification aux systèmes de publication des informations d'état des certificats (*ajout, suppression, modification des informations publiées*) est strictement limité aux fonctions internes habilitées du service d'émission de certificats.
Les listes de révocation sont générées par IN Groupe et transmises dans la foulée aux MEF pour publication.
Dès que ces fichiers sont reçus ils sont publiés automatiquement par script sur les serveurs de publication IGC1 et IGC2.
Un troisième site récupère directement ces fichiers chez IN Groupe et les met à disposition (IGC).

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

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

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

3.1.2 Nécessité d'utilisation de noms explicites

3.1.2.1 Identités des AC

Les AC émettrices sont identifiées par leur DN, comme suit :

Attribut du DN	Valeur
country (C)	FR
organisationName (O)	MINISTERES ECONOMIQUES ET FINANCIERS
organizationUnitName (OU)	0002 130013345
organizationIdentifier (OrgID)	NTRFR-130013345
commonName (CN)	[Nom de l'AC]

Les AC objet de la présente PC sont les suivantes :

- AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE,
- AC CONFIDENTIALITE MEF QUALIFIEE.

3.1.2.2 Identités des porteurs

Les noms choisis pour désigner les porteurs de certificats sont explicites.
Le DN des porteurs est construit nécessairement à partir des champs suivants :

Attribut du DN	Valeur
Country (C)	Désigne la France.
OrganizationName (O)	Nom complet de l'entité de rattachement du porteur (*Entité des MEF à laquelle est rattaché le porteur*)
OrganizationalUnitName (OU)	Le SIREN de l'entité du porteur précédé de la chaîne « 0002 » (*SIREN de l'entité du MEFR concernée*).
OrganizationIdentifier (OrgID)	Le SIREN de l'entité du porteur précédé de la chaîne « NTRFR- » (*SIREN de l'entité des MEF concernée*).

CommonName (CN)	Le nom complet du porteur tel qu'il apparaît dans le référentiel des agents des MEF ou tel qu'il est transmis, justificatif à l'appui, par le demandeur.
GivenName (GN)	Le prénom du porteur tel qu'il apparaît dans le référentiel des agents des MEF ou tel qu'il est transmis, justificatif à l'appui, par le demandeur.
SurName (SN)	Le nom du porteur tel qu'il apparaît dans le référentiel des agents des MEF ou tel qu'il est transmis, justificatif à l'appui, par le demandeur.
SerialNumber (SNU)	Elément complémentaire permettant de distinguer les homonymes : valeur unique calculée par le CMS permettant de garantir l'unicité du DN du porteur au sein de l'AC.

3.1.2.3 Certificats de test

Les certificats de test sont identifiables par le fait que leur CN contient le mot « TEST », précédant un prénom et un nom. Tous les autres champs (*à l'exception des informations d'AC*) sont susceptibles de différer des profils des certificats porteurs décrits au chapitre 7.1.2.
Ces certificats ne sont pas délivrés à des agents ou des prestataires externes dans le cadre de leurs activités professionnelles et ne doivent en aucun cas être considérés comme tels.

3.1.3 Anonymisation et pseudonymisation des porteurs

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

3.1.4 Règles d'interprétation des différentes formes de noms

Les règles suivantes sont appliquées par les MEF :

- Tous les caractères sont au format UTF8String ou PrintableString ;
- L'attribut CN du DN des certificats émis comporte :
    - Le prénom et le nom du porteur tel qu'ils apparaissent dans le référentiel des agents des MEF, ou,
    - Le premier prénom du porteur suivi d'un espace puis du nom du porteur tel qu'ils apparaissent sur le justificatif d'identité de ce dernier dans le cas d'une identification hors référentiel des agents. Dans ce cas, les prénoms et noms composés utilisent le tiret (*trait d'union "-"*) comme élément séparateur.

3.1.5 Unicité des noms

Le DN du champ « *subject* » de chaque certificat de porteur permet d'identifier de façon unique le porteur correspondant au sein du domaine de l'AC.
L'unicité du DN sur le domaine de l'AC est assurée par l'attribut « SerialNumber » présent dans le DN et contenant un nombre permettant de garantir cette unicité.

3.1.6 Rôle des marques déposées

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

3.2 Validation initiale de l'identité

L'enregistrement d'un porteur peut se faire soit directement auprès de l'AE, soit via un Mandataire de Certification. Dans ce dernier cas, le MC est préalablement enregistré par l'AE.
La vérification et la validation initiale de l'identité d'une entité ou d'une personne physique est ainsi réalisée dans les cas suivants :

- Enregistrement d'un porteur sans MC : validation par l'AE de l'identité « personne morale » de l'entité de rattachement du porteur et de l'identité « personne physique » du futur porteur.
- Enregistrement d'un MC : validation de l'identité « personne morale » de l'entité pour lequel le MC interviendra et de l'identité « personne physique » du futur MC.
- Enregistrement d'un porteur via un MC : validation par le MC de l'identité « personne physique » du futur porteur.

Dans le cadre de la présente PC, l'AC prévoit de délivrer des certificats sur deux types de carte Rossignol :

- **Sur une carte Rossignol « *agent* » (*nécessitant une personnalisation graphique au préalable*), permanente :**
  - Pour les agents présents sur le référentiel des agents des MEF et ne nécessitant pas l'intervention d'un MC,
- **Sur une carte Rossignol « *temporaire* » (*ne nécessitant pas de personnalisation graphique comme la carte agent*) :**
  - Pour les prestataires externes (par définition inconnus du référentiel des agents des MEF) et nécessitant l'intervention d'un MC,
  - Pour les agents inconnus dans le référentiel des agents des MEF (*ex : cas d'un nouvel arrivant non-inscrit dans le référentiel*) et nécessitant l'intervention d'un MC et la constitution d'un dossier d'enregistrement,
  - Pour les agents présents dans le référentiel des agents des MEF, ayant déjà une carte permanente et ayant besoin d'une carte temporaire.

En synthèse, le tableau ci-dessous présente pour chaque contexte de porteur, le type d'enregistrement et le type de carte fourni au porteur :

Porteur / Contexte	Type d'enregistrement	Type de carte
Agent connu du référentiel des agents des MEF	Via le référentiel des agents des MEF	Carte agent (*si nouvelle carte ou si carte agent perdue ou révoquée*) Carte temporaire

Agent inconnu du référentiel des agents des MEF	Dossier d'enregistrement déposé par un MC	Carte temporaire
Externe	Dossier d'enregistrement déposé par un MC	Carte temporaire

3.2.1 Méthode pour prouver la possession de la clé privée

L'opération de génération de la bi-clé du porteur est réalisée par l'AC ou par l'AE. Cette dernière assure l'attribution au porteur de cette bi-clé en important la clé privée et le certificat de clé publique associé dans le dispositif matériel qui lui sera remis.
La génération de la bi-clé est réalisée en présence du porteur.

Certificat d'authentification et de signature
Pour un certificat double usage d'authentification et signature électronique, la génération de la bi-clé est déclenchée par l'AE en présence du porteur et effectuée directement sur le dispositif matériel du futur porteur.

Certificat de confidentialité (chiffrement)
Pour un certificat de confidentialité, la génération de la bi-clé est déclenchée par l'AE en présence du porteur et est générée par l'AC. L'AC assure l'attribution au porteur de cette bi-clé en important la clé privée et le certificat de clé publique associé dans le dispositif matériel qui lui sera remis.

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 Validation de l'identité d'un porteur sans MC

La validation de l'identité d'un porteur sans MC ne concerne que les agents connus du référentiel des agents des MEF et quel que soit le type de carte délivrée, à savoir :

- Une carte Rossignol « *agent* »,
- Ou une carte Rossignol « *temporaire* ».

La validation de l'identité du porteur est réalisée sur la base :

- D'un enregistrement initial du futur porteur s'appuyant sur le référentiel des agents des MEF qui est réputé fiable. La présence du porteur dans le référentiel des agents des MEF prouve son lien avec les MEF,
- D'une identification du porteur en face-à-face par l'AE lors de la remise de la carte au porteur.

3.2.3.2 Enregistrement d'un MC

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,
- Éventuellement, fourniture d'un certificat au MC pour qu'il puisse signer les dossiers d'enregistrement de porteurs de l'entité qu'il représente et les transmettre sous forme électronique.

Dans le cadre de la présente PC, le MC est nécessairement un agent des MEF.

Le dossier d'enregistrement du MC contient :

- Un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le MC. Ce mandat est signé par le MC pour acceptation, contenant :
  - Un engagement du MC, auprès de l'AC, à effectuer correctement et de façon indépendante les contrôles des dossiers des demandeurs,
  - Un engagement du MC à signaler à l'AE son départ de l'entité,
- Un document officiel d'identité en cours de validité du MC comportant une photographie d'identité (*carte nationale d'identité, passeport, carte de séjour, nouveau permis de conduire ou commission d'emploi de moins de 15 ans*), qui est transmis à l'AE qui en conserve une copie ou les traces.

Le MC est identifié en face-à-face par l'AE ou sous forme dématérialisée à condition que le dossier d'enregistrement du MC soit signé par le MC à l'aide de sa carte Rossignol.

3.2.3.3 Validation de l'identité d'un porteur avec MC

La validation de l'identité d'un porteur avec MC ne concerne que :

- Les agents inconnus du référentiel des agents des MEF,
- Et les prestataires externes.

Pour ces cas, seule une carte Rossignol « *temporaire* » peut être délivrée.

La validation de l'identité du porteur est réalisée sur la base :

- D'un enregistrement initial du futur porteur s'appuyant sur un dossier d'enregistrement constitué et déposé par un MC auprès de l'AE et comprenant :
  - Une demande de certificat co-signée, et datée de moins de 3 mois, par le futur porteur et le MC. De par la signature du MC ce formulaire vaut mandat du responsable légal.
  - Les conditions générales d'utilisation signées par le futur porteur (*qui seront acceptées par le porteur lors de la remise de la carte*),
  - Un document officiel d'identité en cours de validité du porteur comportant une photographie d'identité (*carte nationale d'identité, passeport, carte de séjour, nouveau permis de conduire ou commission d'emploi de moins de 15 ans*), qui est transmis à l'AE qui en conserve une copie ou les traces.

- D’une identification du porteur en face-à-face par l’AE lors de la remise de la carte au porteur.

L’existence de l'entité de rattachement et son numéro SIREN, tel qu’il figurera dans le certificat, est établie pour l’entité des MEF à l’origine de la demande du certificat. Le dossier d’enregistrement ne nécessite pas de pièce particulière attestant de l’existence de l’entité des MEF compte-tenu de son contexte d’émission exclusivement interne (*pour les agents et les prestataires externes intervenant au sein des MEF*).

Le porteur est systématiquement identifié en face-à-face par l’AE lors de la remise de sa carte.

3.2.4 Informations non vérifiées du porteur

Les certificats émis sous la présente PC et délivrés pour des agents s’appuient sur les informations des annuaires de référence des entités des MEF, synchronisés de manière fiable avec le référentiel des agents des MEF, et ne comportent ainsi aucune information non vérifiée.
L’UPN (User Principal Name), le login et l’adresse email professionnelle du porteur sont également issus d’annuaires de référence des entités des MEF et sont donc fiables.
Ces informations sont insérées dans l’extension « SubjectAlternativeName » (SAN) du certificat du porteur.

Les certificats émis sous la présente PC et délivrés pour des agents inconnus dans les annuaires ou pour des prestataires externes ne comportent aucune information non vérifiée.
Dans ces deux cas, ces informations (*y compris l’UPN, le login et l’adresse email professionnelle du porteur*) sont renseignées dans le dossier d’enregistrement du porteur et sont vérifiées et validées par le MC.
Ces informations sont insérées dans l’extension « SubjectAlternativeName » (SAN) du certificat du porteur.

3.2.5 Validation de l’autorité du demandeur

Cette étape est effectuée en même temps que la validation de l’identité de la personne physique.

3.2.6 Critères d’interopérabilité, certification croisée d’AC

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

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

Le renouvellement de la bi-clé d'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

Lors du premier renouvellement, la vérification de l'identité du sujet est optionnelle. S'il n'y a aucune modification portant sur les identités identifiées, la liste des documents à fournir est allégée.
Lors du renouvellement suivant, l'AE, saisie de la demande, identifie le sujet selon la même procédure que pour l'enregistrement initial.

La DPC contenant les informations non-diffusables précise les modalités de renouvellement.

3.3.2 Identification et validation pour un renouvellement des clés 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 est identique à la procédure d'enregistrement initiale.

3.4 Identification et validation d'une demande de révocation

Dans le cadre de la présente PC, le demandeur de la révocation d'un certificat peut être :

- Le porteur lui-même,
- Un MC ou un représentant légal ou une personne autorisée,
- L'AE,
- L'AC.

Dans tous les cas, le demandeur est formellement authentifié par la vérification de son identité et de son autorité par rapport au certificat à révoquer.

La demande de révocation peut être effectuée :

- Sur Internet si le porteur dispose d'un moyen d'authentification au portail Self-service,
- En face-à-face entre le porteur et l'AE au cours duquel le porteur présente un document officiel d'identité (*carte nationale d'identité, passeport, carte de séjour, nouveau permis de conduire ou commission d'emploi de moins de 15 ans*),
- Via un centre d'appel en fonction de l'AE,
- Par courriel ou par courrier (*en fonction de l'AE*), la demande doit être signée par le demandeur. Ci-dessous les adresses de chaque direction endossant le rôle d'AE dans le cadre de la présente PC :

Direction des MEF	Contacts
DGDDI	**Par courriel :** *revocation-dgddi.ac-mef@douane.finances.gouv.fr* **Par courrier :** *Direction générale des douanes et droits indirects*

	SDSI / Bureau SI2 *11 RUE DES DEUX COMMUNES* *93558 MONTREUIL*
Administration Centrale	**Centre de service**

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DE CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

Une demande de certificat ne peut être effectuée que par un des acteurs ci-dessous :

- Le futur porteur,
- Un MC,
- L'AE,

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

Dans tous les cas ci-après, les informations suivantes font partie de la demande de certificat :

- Le nom du porteur à utiliser dans le certificat,
- Les données personnelles d'identification du porteur,
- Les données de l'entité du porteur (*entité des MEF à laquelle est rattaché le porteur*).

Pour une carte « *agent* » délivrée à un agent connu dans le référentiel des agents des MEF:

La demande de certificat est effectuée en ligne par le porteur lui-même ou par l'AE.
Dans ce cas, les informations de la demande proviennent du référentiel des agents des MEF.

Pour une carte « *temporaire* » délivrée à un agent connu dans le référentiel des agents des MEF :

La demande de certificat est effectuée en ligne par l'AE.
Dans ce cas, les informations de la demande proviennent du référentiel des agents des MEF.

Pour une carte « *temporaire* » délivrée à :

- **Un agent inconnu dans le référentiel des agents des MEF,**
- **Un prestataire externe** (ne figurant pas dans le référentiel des agents des MEF et pouvant être connu dans un annuaire de référence d'une entité des MEF).

La demande de certificat est effectuée par un MC qui constitue un dossier d'enregistrement et le dépose auprès de l'AE :

- **Soit au format papier :** dans ce cas le dossier contient les paraphes du MC et sa signature sur les pages principales de manière à l'authentifier auprès de l'AE (*un face-à-à-face entre le MC et l'AE est nécessaire si celui-ci n'a pas encore eu lieu au moment de la demande*).

- **Soit au format électronique :** dans ce cas, le dossier doit être signé par le MC avec sa carte Rossignol de manière à l'authentifier auprès de l'AE.

Dans ce cas, les informations de la demande proviennent du dossier déposé par le MC.

Le dossier de demande contient les éléments listés au chapitre 3.2.3.3.

Dans tous les cas cités ci-dessus, le séquestre de la clé privée pour le certificat de chiffrement est demandé systématiquement, et le porteur est informé de ce séquestre lors de la remise du certificat et à travers les Conditions Générales d'Utilisation qu'il accepte.

4.2 Traitement d'une demande de certificat

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

Les opérations d'identification et de validation suivantes sont réalisées par l'AE lors de la remise en face-à-face du dispositif matériel au porteur :

- La validation de l'identité du porteur sur présentation d'un document officiel d'identité en cours de validité du futur porteur comportant une photographie d'identité (*notamment carte nationale d'identité, passeport, carte de séjour, nouveau permis de conduire ou commission d'emploi de moins de 15 ans*),
- La vérification de la cohérence des justificatifs présentés : notamment entre les informations du porteur contenues dans la demande et les informations du document officiel d'identité.
- L'authentification du porteur via un code d'authentification qu'il est seul à avoir en sa possession,
- La vérification que le futur porteur a pris connaissance des modalités applicables pour l'utilisation du certificat. (*voir les Conditions Générales d'Utilisation*).

Le porteur est ensuite authentifié par un code d'authentification qu'il est seul à avoir en sa possession.

Concernant les agents, le numéro de la pièce d'identité présentée est noté et conservé dans l'interface opérateur du système.

Concernant les prestataires externes, pour lesquels l'intervention d'un mandataire de certification est nécessaire, il est conservé une trace des justificatifs d'identité présentés :

- Pour les pièces au format papier, sous la forme d'une photocopie signée à la fois par le futur porteur et par le MC ;
- Pour les pièces au format électronique, celles-ci sont conservées sous une forme ayant valeur légale (*copie du justificatif d'identité du porteur signée électroniquement par le porteur et par le MC*).

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

Une fois la demande de certificat validée, le certificat est émis dans les meilleurs délais.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération et de préparation des différents éléments destinés au porteur en présence de ce dernier :

- Le certificat du porteur,
- La bi-clé du porteur (*exclusivement dans le cas du certificat de chiffrement*)

Certificats d'authentification signature sur QSCD pour des personnes physiques
Pour le certificat d'authentification et de signature électronique, les opérations suivantes sont réalisées : • L'AE insère le dispositif matériel du porteur sur son poste de personnalisation, • L'AE déclenche la génération de la bi-clé, • Le dispositif matériel génère la bi-clé et transmet la CSR à l'AC, • L'AC génère le certificat et le retourne au poste de personnalisation qui l'insère dans le dispositif matériel du porteur.

Certificats de chiffrement sur QSCD pour des personnes physiques
Pour le certificat de chiffrement, les opérations suivantes sont réalisées : • L'AE insère le dispositif matériel du porteur sur son poste de personnalisation, • L'AE déclenche la génération de la bi-clé, • L'AC génère la bi-clé et la CSR, • L'AC génère le certificat et retourne la bi-clé et le certificat au poste de personnalisation de manière sécurisée qui l'insère dans le dispositif matériel du porteur.

A l'issue de la génération des certificats, les opérations suivantes sont réalisées :

- L'AC génère un code de déblocage,
- Le code d'activation est initialisé par le porteur lui-même et le code de déblocage du dispositif matériel du porteur est modifié.

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

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

La remise du certificat au porteur se fait en face-à-face par l'AE quel que soit le type de carte (*carte « agent » ou carte « temporaire »*).

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

L'opération de personnalisation du dispositif matériel du porteur est réalisée par l'AE en présence du porteur. L'acceptation des Conditions Générales d'Utilisation (*CGU*) de chaque AC par le porteur est collectée lors de cette rencontre :

- Via la fourniture d'un code OTP à usage unique reçu par le porteur et renseigné par ce dernier après avoir pris connaissance des CGU,
- Et par une case à cocher à la fin de l'opération de personnalisation du dispositif matériel du porteur.

Les certificats générés (*authentification & signature, confidentialité*) à l'issue de la personnalisation du dispositif matériel sont présentés au porteur pour validation.
L'acceptation des certificats par le porteur est collectée par une case à cocher.

4.4.2 Publication du certificat

Certificats d'authentification signature sur QSCD pour des personnes physiques
Les certificats d'authentification et signature sont publiés en interne pour une utilisation en interne exclusivement.

Certificats de chiffrement sur QSCD pour des personnes physiques
Les certificats de chiffrement ne sont pas publiés au sens du RGS. Ils sont publiés en interne pour une utilisation en interne exclusivement.

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

L'AE étant en charge de la personnalisation du dispositif matériel du porteur et de sa remise est alors systématiquement notifiée par l'AC.

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 à la fonction de sécurité concernée (*cf. chapitre 1.5.1.1*).
Les porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.
Les usages autorisés de la bi-clé et du certificat associé sont indiqués dans le certificat lui-même, via les extensions concernant les usages des clés (*« Key Usage » et « Extended Key Usage »*).

Authentification et signature
Au-delà de l'usage précisé au chapitre 1.5.1.1, les certificats d'authentification et signature sont utilisés pour : • L'authentification client SSL, • L'ouverture de session par carte à puce,

- La protection des courriels (*origine*).

Ces usages sont précisés dans l'extension « *Extended Key Usage* » du certificat (*cf. détails du profil au chapitre 7.1.2*).

Confidentialité
Au-delà de l'usage précisé au chapitre 1.5.1.1, les certificats de confidentialité sont utilisés pour : • La protection des courriels (*confidentialité*) Ces usages sont précisés dans l'extension « *Extended Key Usage* » du certificat (*cf. détails du profil au chapitre 7.1.2*).

L'utilisation de la clé privée du porteur et du certificat associé est strictement limitée au service défini par l'OID de sa politique (cf. chapitre 1.5.1.1).

A l'issue de la personnalisation de son dispositif matériel, le porteur accepte les Conditions Générales d'Utilisation de l'AC dans lesquelles sont rappelés les usages de la clé privée.

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

Cf. chapitre précédent et chapitre 1.5.
Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats. Dans le cas contraire, leur responsabilité pourrait être engagée.

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

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

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

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

4.7.1 Causes possibles de changement d'une bi-clé

Les bi-clés sont périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des porteurs, et les certificats correspondants, sont renouvelés au minimum tous les trois ans.
Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat (*cf. chapitre 4.9*).

4.7.2 Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat au porteur se fait à l'initiative du porteur.
Le processus de renouvellement ne concerne que la carte « *agent* » et non la carte « *temporaire* » qui doit suivre le même processus qu'une demande initiale.

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.

Pour les actions de l'AC, cf. chapitre 4.3.1.

4.7.4 Notification au porteur de l'établissement du nouveau certificat

Cf. chapitre 4.3.2.

4.7.5 Démarche d'acceptation du nouveau certificat

Cf. chapitre 4.4.1.

4.7.6 Publication du nouveau certificat

Cf. chapitre 4.4.2.

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

Cf. chapitre 4.4.3.

4.8 Modification d'un certificat

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

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

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificat de porteur

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 changement du nom de famille suite à un mariage*), 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 dispositif matériel*),
- Le départ du porteur de l'entité duesMEF à laquelle est rattaché,
- Le décès du porteur ou la cessation d'activité de l'entité du porteur.

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 est révoqué.

4.9.1.2 Certificat d'une composante du service

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante du service d'émission de certificats (*y compris un certificat d'AC, un certificat d'AC pour la génération de certificats et de LCR, un certificat d'opérateur de l'AE, un certificat de répondeur OCSP*) :

- Suspicion de compromission, compromission, perte ou vol de la clé privée de la composante,
- Décision de changement de composante du service d'émission de certificats 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 Certificat de porteur

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

- Le porteur,
- Le MC ou le représentant légal de l'entité,
- L'AC émettrice, ou
- Le personnel de l'AE qui a enregistré la demande du porteur.

Le porteur est informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son certificat dans les Conditions Générales d'Utilisation.

4.9.2.2 Certificat d'une composante du service

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 responsable de l'AC ou de l'AE selon le certificat de composante concerné.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Certificat de porteur

À la réception d'une demande de révocation, l'AE vérifie l'identité du demandeur et la validité de la demande, selon les exigences décrites au paragraphe 3.4.

La demande de révocation comporte au moins les informations suivantes :

- L'identité du porteur figurant dans le certificat (*nom et prénom*),
- Le nom du demandeur de la révocation,
- Une information permettant de retrouver rapidement et sans erreur le certificat à révoquer (*par défaut le n° de série*),
- Eventuellement, la cause de révocation.

Une demande de révocation peut être déposée par le porteur, le MC le cas échéant ou le représentant légal :

- En face-à-face avec l'AE,
- En ligne sur le portail,
- Par courriel ou courrier via un formulaire envoyé à l'AE.

D'autres points d'accès sont définis en fonction de l'entité des MEF (AE) qui reçoit la demande de révocation.

Une fois la demande authentifiée et contrôlée, la fonction de gestion des révocations révoque le certificat correspondant en changeant son statut, puis communique ce nouveau statut à la fonction d'information sur l'état des certificats.

L'information de révocation est diffusée :

- Via une LCR signée par l'AC elle-même,
- Via un service OCSP dont la réponse est signée par un certificat de répondeur OCSP lui-même signé par l'AC ayant émis le certificat à révoquer.

Quelle que soit la cause ayant entraîné la révocation d'un certificat, le porteur est informé par une notification de la révocation de son certificat. Le MC peut également être notifié. Cette notification prend la forme d'un courrier électronique et indique la date à laquelle la révocation du certificat a pris effet.

L'ensemble des opérations et des mesures prises par l'AC est consigné et sauvegardé.

Les procédures de révocation sont détaillées dans la DPC contenant les informations non-diffusables.

4.9.3.2 Certificat d'une composante du service

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe 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, le service d'émission de certificats pourra par exemple envoyer des récépissés aux 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.

La révocation du certificat de l'AC, est facilitée par la signature d'une Liste des Autorités Révoquées (LAR) par l'autorité de certificat racine.

Le point de contact identifié sur le site http ://ssi.gouv.fr est immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification.

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

Dès que le porteur (*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 Certificat de porteur

Par nature une demande de révocation est traitée en urgence.

4.9.5.2 Disponibilité du système de traitement des demandes de révocation

La fonction de gestion des révocations est disponible 24h/24 7j/7.
Cette fonction a une durée maximale d'indisponibilité par interruption de service (*panne ou maintenance*) de 2h et une durée maximale totale d'indisponibilité par mois de 8h.
Toute demande de révocation d'un certificat est traitée dans un délai inférieur à 24h, 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.

4.9.5.3 Certificat d'une composante du service

La révocation d'un certificat d'une composante du service d'émission de certificats est effectuée dès la détection d'un évènement 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.
La révocation d'un certificat de signature de l'AC (*signature de certificats, de LCR / LAR*) est 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'AC met à disposition des utilisateurs de certificats un répondeur OCSP, des listes de certificats révoqués (LCR) et des listes d'autorités révoquées (LAR) tous précisés au chapitre 2.1.

Avant toute utilisation de certificats, notamment lorsque les dits certificats créent des effets juridiques, le tiers utilisateur doit impérativement :

- Vérifier l'état des certificats de l'ensemble de la chaîne de certification correspondante. Le choix de la méthode utilisée (*LCR, OCSP*) est à l'appréciation de l'utilisateur.
- Contrôler la validité intrinsèque de l'ensemble de la chaîne de certification, en particulier leur signature, et la validité du certificat de l'émetteur.

4.9.7 Fréquence d'établissement des LCR

La fréquence de publication des LCR est de 12 heures.

4.9.8 Délai maximum de publication d'une LCR

La LCR est publiée dans un délai maximum de 30 minutes.

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

Un service de vérification en ligne du statut des certificats (OCSP) est mis à disposition des utilisateurs. Ses caractéristiques en termes d'intégrité, de disponibilité et de délai de publication sont les mêmes que celles du service de publication de LCR.
En cas d'indisponibilité du service OCSP, les utilisateurs peuvent consulter le statut des certificats à partir des points de distribution de la LCR.

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

Cf. chapitre 4.9.6.

4.9.11 Autres moyens disponibles d'information sur les révocations

Sans objet.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

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

Pour les certificats d'AC, la révocation suite à une compromission de la clé privée fait l'objet d'une information diffusée sur le site web de l'AC a minima.
La procédure de révocation d'une AC est réalisée par une opération de cérémonie de clé, détaillée dans la DPC contenant les informations non-diffusables.

4.9.13 Causes possibles d'une suspension

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

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

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

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

L'AC met également à disposition des utilisateurs de certificats un répondeur OCSP pour vérifier le statut d'un certificat.

4.10.2 Disponibilité de la fonction

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

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

Pour la fonction de vérification en ligne du statut d'un certificat (OCSP), le temps de réponse du serveur à la requête reçue est au maximum de 10 secondes.

4.10.3 Dispositifs optionnels

Sans objet.

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

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

4.12 Séquestre de clé et recouvrement

Dans le cadre de la présente PC :

- Les clés privées de signature des porteurs ne sont pas séquestrées,
- Les clés privées de chiffrement/déchiffrement des porteurs sont séquestrées par l'AC à la demande explicite faite par le porteur dans son dossier de demande.

4.12.1 Politiques et pratiques de recouvrement par séquestre des clés

4.12.1.1 Demande de séquestre

Toute demande de certificat de chiffrement intègre systématiquement un séquestre de la clé privée.
La demande intègre systématiquement les informations relatives au séquestre qui est obligatoire pour le certificat de chiffrement dans le cadre de la présente PC.
La durée de conservation de la clé privée correspondante au certificat de chiffrement est de dix ans à compter de sa génération.
Le porteur est informé du séquestre de la clé privée correspondante au certificat sur lequel porte sa demande ainsi que de sa durée de conservation à travers les Conditions Générales d'Utilisation qu'il accepte.

4.12.1.2 Traitement d'une demande de séquestre

Lorsque l'AE déclenche le processus d'émission du certificat, la bi-clé et le certificat sont générés par l'AC. La clé privée correspondante au certificat émis par l'AC fait systématiquement l'objet d'un séquestre suite à sa génération.
La clé privée est conservée par la fonction de séquestre et de recouvrement de l'AC sous forme chiffrée pour une durée de dix ans et est recouvrable sur cette période même si le certificat associé est expiré ou révoqué.
La clé privée conservée au sein de la fonction de séquestre et de recouvrement de l'AC est identifiée avec le numéro de série du certificat associé.
Les conditions de séquestre sont détaillées dans la DPC contenant les informations non-diffusables.

4.12.1.3 Origine d'une demande de recouvrement

Un porteur pourra demander l'émission d'une nouvelle carte en cours de validité comme décrit au chapitre 3.3. Après contrôle et validation de la demande, un opérateur de recouvrement de l'AE personnalisera une nouvelle carte dont le certificat de chiffrement et sa bi-clé seront ceux de la carte devant être renouvelée.

Sur demande judiciaire, ou en cas d'indisponibilité prolongée du porteur, le représentant légal de l'entité du porteur ou un représentant dument accrédité pourra demander à l'AC de lui fournir la bi-clé de chiffrement.

Une demande de recouvrement de clé privée d'un porteur peut alors être effectuée par :

- Le porteur lui-même,
- Un représentant légal de l'entité du porteur,
- Un représentant dument accrédité
- Toute entité autorisée par la loi.

4.12.1.4 Identification et validation d'une demande de recouvrement

Dans le cadre d'un renouvellement de certificats nécessitant un changement de carte et donc le recouvrement de la clé privée de la carte à renouveler, la validation de l'identité du demandeur est réalisée dans les mêmes conditions qu'une demande initiale.

L'identité du demandeur d'un recouvrement d'une clé séquestrée est vérifiée, sauf cas particulier des entités autorisées par la loi, par la fonction de gestion des recouvrements suivant les mêmes exigences que la validation initiale de l'identité d'un demandeur d'un certificat définies au chapitre 3.2.

La demande de recouvrement comporte à minima :

- Le motif du recouvrement de la clé privée,
- Les informations permettant d'identifier la clé privée à recouvrer (*n° de série du certificat associé, nom du porteur associé*).

Une fois l'identité du demandeur validée et la clé à recouvrer identifiée, la fonction de gestion des recouvrements s'assure que le demandeur est bien l'une des personnes autorisées à demander le recouvrement de la clé concernée.

4.12.1.5 Traitement d'une demande de recouvrement

Suite à l'identification et la validation de la demande de recouvrement, le service de gestion des recouvrements émet la demande auprès de la fonction de séquestre et recouvrement de l'AC. La demande est protégée en intégrité et en confidentialité.

Au moins un opérateur habilité au recouvrement est saisi pour le recouvrement de la clé privée du porteur. Cet opérateur est authentifié par la fonction de séquestre et recouvrement préalablement à l'opération de recouvrement.

La fonction de séquestre et recouvrement remet ensuite de manière sécurisée la clé privée recouvrée au demandeur du recouvrement. Cette remise s'effectue avec une sécurité équivalente à la remise de la clé privée lors de la génération du certificat du porteur.

La fonction de gestion des recouvrements a la responsabilité de l'archivage des pièces du dossier de demande de recouvrement (*ou de l'envoi vers la composante chargée de l'archivage*), l'archivage des informations liées à l'opération de recouvrement étant du ressort de la fonction de séquestre et recouvrement au titre de l'archivage des journaux d'évènements correspondants.

4.12.1.6 Destruction des clés séquestrées

Dès la fin de la période de conservation d'une clé séquestrée, tout exemplaire de cette clé détenue par l'AC est détruit de manière fiable afin de ne pouvoir ni recouvrer ni reconstituer la clé.

4.12.1.7 Disponibilité des fonctions liées au séquestre et au recouvrement

La fonction de séquestre et de recouvrement est disponible aux jours ouvrés.

Le délai de traitement d'une demande de recouvrement est de deux jours ouvrés à compter de la réception d'une demande de recouvrement authentifiée jusqu'à la remise de la clé privée recouvrée au demandeur.

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

Sans objet

5 MESURES DE SECURITE NON TECHNIQUES

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

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

5.1.2 Accès physiques

Afin d'éviter toute perte, dommage et compromission des ressources du service d'émission de certificats et l'interruption des services de l'AC, les accès aux locaux des différentes composantes du service d'émission de certificats sont contrôlés.
L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.
Afin d'assurer la disponibilité des systèmes, l'accès aux machines (*ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisés pour la mise en œuvre de ces fonctions*) est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

5.1.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements du service d'émission de certificats telles que fixées par leurs fournisseurs.
Elles permettent également de respecter les exigences de la présente PC, ainsi que les engagements pris par l'AC dans sa DPC, 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 permettent de respecter les exigences de la présente PC, ainsi que les engagements pris par l'AC dans sa DPC, 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 permettent de respecter les exigences de la présente PC, ainsi que les engagements pris par l'AC dans sa DPC, 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 du service d'émission de certificats ont été identifiées dans le cadre de l'analyse de risque, et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).
Les supports (*papier, disque dur, disquette, CD, etc.*) correspondant à ces informations sont traités et conservés conformément à ces besoins de sécurité.

5.1.7 Mise hors service des supports

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

5.1.8 Sauvegardes hors site

En complément de sauvegardes sur sites, les composantes du service d'émission de certificats mettent en œuvre des sauvegardes hors sites de leurs applications et de leurs informations. Ces sauvegardes sont organisées de façon à assurer une reprise des fonctions du service d'émission de certificats après incident le plus rapidement possible, et conforme aux exigences de la présente PC et aux engagements de l'AC dans sa DPC en matière de disponibilité, en particulier pour les fonctions de gestion des révocations et d'information sur l'état des certificats (*Cf. chapitres 4.9.5.1 et 4.10.2*).

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

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

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

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

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

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

responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.

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

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

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

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

5.2.2 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.
Pour des raisons de sécurité, les fonctions sensibles sont réparties sur plusieurs personnes. La présente PC définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques du service d'émission de certificats (*Cf. chapitre 6*).
La partie de la DPC contenant les informations non-diffusables précise les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter.

5.2.3 Identification et authentification pour chaque rôle

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

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

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

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.
Concernant les rôles de confiance, les cumuls suivants sont interdits :

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

Les attributions associées à chaque rôle sont décrites dans la DPC contenant les informations non-diffusables.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

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

5.3.2 Procédures de vérification des antécédents

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

5.3.3 Exigences en matière de formation initiale

« Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité. »
Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité correspondants à la composante au sein de laquelle il opère.

5.3.4 Exigences et fréquence en matière de formation continue

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

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

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

5.3.7 Exigences vis-à-vis du personnel des prestataires

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

5.3.8 Documentation fournie au personnel

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

5.4 Procédures de constitution des données d'audit

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

5.4.1 Type d'évènements à enregistrer

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

- Création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.),
- Démarrage et arrêt des systèmes informatiques et des applications,
- Traces d'activité (logs) des pare-feux et des routeurs,
- Evénements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à la défaillance de la fonction de journalisation, pannes logicielles et matérielles,
- Connexion / déconnexion des Utilisateurs ayant des rôles de confiance, et des tentatives non réussies correspondantes,

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

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

- Les changements apportés au personnel,
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (*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 du service d'émission de certificats, des évènements spécifiques aux différentes fonctions du service d'émission de certificats sont journalisés, notamment :

- Réception d'une demande de certificat (*initiale et renouvellement*),
- Validation / rejet d'une demande de certificat,
- Evénements liés aux clés de signature et aux certificats d'AC (*génération, sauvegarde / récupération, destruction, …*),
- Génération des bi-clés des porteurs,
- Personnalisation des codes d'activation et génération des codes de déblocage,
- Génération des certificats des porteurs,
- Remise du QSCD et des certificats au porteur,
- Acceptation ou rejet explicite par le porteur,
- Publication et mise à jour des informations liées aux AC (*PC, certificats d'AC, CGU, …*)
- Réception d'une demande de révocation,
- Validation / rejet d'une demande de révocation,
- Génération puis publication des LCR,
- Requêtes et réponses OCSP.

Mais également les journaux relatifs au cycle de vie des certificats de chiffrement :

- Séquestre d'une clé privée de porteur,
- Réception d'une demande de recouvrement,
- Validation / rejet d'une demande de recouvrement,
- Recouvrement d'une clé privée,
- Remise d'une clé privée recouvrée au demandeur du recouvrement.

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

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

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

- Destinataire de l'opération,
- Nom ou identifiant du demandeur de l'opération ou référence du système effectuant la demande,

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

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

5.4.2 Fréquence de traitement des journaux d'évènements

Voir chapitre 5.4.8.

5.4.3 Période de conservation des journaux d'évènements

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

5.4.4 Protection des journaux d'évènements

La journalisation est conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité permettent de détecter toute modification, volontaire ou accidentelle, de ces journaux.
Les journaux d'évènements sont protégés en disponibilité (*contre la perte et la destruction partielle ou totale, volontaire ou non*).
Les systèmes générant les journaux d'événements sont synchronisés sur une source fiable de temps détaillée au chapitre 6.8.

5.4.5 Procédure de sauvegarde des journaux d'évènements

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

5.4.6 Système de collecte des journaux d'évènements

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

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

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

5.4.8 Évaluation des vulnérabilités

Chaque entité opérant une composante du service d'émission de certificats est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.
Les journaux d'évènements sont contrôlés au moins 1 fois par jour ouvré, afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité 1 fois par semaine et dès la détection d'une anomalie. Cette analyse donne lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.
Un rapprochement entre les différents journaux d'évènements de fonctions qui interagissent entre elles (*AE et fonction de génération, fonction de gestion des révocations et fonction d'information sur l'état des certificats, etc.)* est effectué au moins 1 fois par mois, ceci afin de vérifier la concordance entre évènements dépendants et contribuer ainsi à révéler toute anomalie.

5.5 Archivage des données

5.5.1 Types de données à archiver

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

- Les logiciels (*exécutables*) et les fichiers de configuration des équipements informatiques,
- Les PC,
- Les DPC contenant les informations non-diffusables,
- Les Conditions Générales d'Utilisation,
- Les accords contractuels avec d'autres AC ;
- Les certificats et LCR tels qu'émis ou publiés,
- Les récépissés ou notifications (*à titre informatif*),
- Les engagements signés des MC,
- Les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement,
- Les journaux d'évènements des différentes entités du service d'émission de certificats.

5.5.2 Période de conservation des archives

Dossier de demande de certificat
Tout dossier de demande de certificat accepté est archivé 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.

Tout dossier de demande de recouvrement accepté est archivé pendant au moins cinq (5) ans à compter de la fin du séquestre par l'AC de la clé privée correspondante.

A l'expiration de la durée d'archivage, tout dossier et pièces justificatives font l'objet d'une destruction.

Certificats, LCR et réponses OCSP émis par l'AC
Les certificats des porteurs et d'AC, ainsi que les LCR / LAR produites, sont archivés pendant au moins cinq (5) ans après leur expiration.

Les réponses OCSP produites sont archivées pendant au moins trois mois après leur expiration.
A l'expiration de la durée d'archivage, les LCR / LAR et réponses OCSP font l'objet d'une destruction.

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

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

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives :

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

Les moyens mis en œuvre sont précisés dans la DPC contenant les informations non-diffusables.

5.5.4 Procédure de sauvegarde des archives

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

5.5.5 Exigences d'horodatage des données

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

5.5.6 Système de collecte des archives

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

5.5.7 Procédures de récupération et de vérification des archives

Les archives (*papier et électroniques*) sont récupérables dans un délai inférieur à 2 jours ouvrés, sachant que seule l'AC peut accéder à toutes les archives (*par opposition à une entité opérant une composante du service d'émission de certificats qui ne peut récupérer et consulter que les archives de la composante considérée*).

5.6 Changement de clé d'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC.
Pour cela la période de validité de ce certificat de l'AC est supérieure à celle des certificats qu'elle signe.
Au regard de la date de fin de validité de ce certificat, son renouvellement est demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée est utilisée pour signer des certificats.
Le certificat précédent reste utilisable pour valider les certificats émis sous cette clé et ce jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7 Reprise suite à compromission ou sinistre

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

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

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

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

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

Chaque composante du service d'émission de certificats dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions du service d'émission de certificats découlant de la présente PC, notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats.

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

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

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

- Arrêter immédiatement l'utilisation de la clé de la composante compromise,
- Informer sans délai tous les porteurs, MC, les tiers utilisateurs et les AE,

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

5.7.4 Capacités de continuité d'activité suite à un sinistre

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

5.8 Fin de vie du service

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

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

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

- Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (*notamment, archivage des certificats des porteurs et des informations relatives aux certificats, archivage de séquestre*),
- Assure la continuité de la révocation (*prise en compte d'une demande de révocation et publication des LCR*), conformément aux exigences de disponibilité pour ses fonctions définies dans la PC,
- 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 les en avise aussitôt que nécessaire sous un délai d'un (1) mois,
- L'AC communique au point de contact identifié sur le site https://ssi.gouv.fr les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (*clés et informations relatives aux certificats*) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans la PC. L'AC communiquera à l'ANSSI, selon les différentes composantes du service d'émission de certificats concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences

(*juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.*) de cet évènement. Elle présentera ’n plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les porteurs et les utilisateurs de certificats,

- L’AC tient informée l’ANSSI de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus.

5.8.2 Cessation d’activité affectant l’AC

La cessation d’activité peut être totale ou partielle (*par exemple : cessation d’activité pour une famille de certificats donnée seulement*). La cessation partielle d’activité est progressive de telle sorte que seules les obligations visées ci-dessous soient à exécuter par l’AC, ou une entité tierce qui reprend les activités, lors de l’expiration du dernier certificat émis par elle.

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

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

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

Lors de l'arrêt du service, l'AC :

- Informe tous les MC et/ou porteurs des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.
- Révoque tous les certificats qu’elle a signés et qui seraient encore en cours de validité,
- Génère une dernière LCR couvrant la révocation des certificats cités plus-haut et signée par la clé privée de l’AC. La valeur de l’extension nextUpdate de la dernière LCR alors émise est alors « *99991231235959Z* »,
- Génère pour chaque certificat émis, une dernière réponse OCSP dont la fin de validité est positionnée au 31 décembre 9999, 23h59m59s (*« 99991231235959Z »*),
- S’interdit de transmettre la clé privée lui ayant permis d’émettre des certificats,
- Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante, Révoque son certificat.

6 MESURES DE SECURITE TECHNIQUES

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'AC

La génération des clés de signature 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 du service d'émission de certificats et/ou la génération des clés de signature d'AC s'accompagne de la génération de parts de secrets d'AC. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signature d'AC.
Ces parts de secrets sont générées suivant un schéma à seuil de Shamir (*n parties parmi m sont nécessaires et suffisantes pour reconstituer le secret*), Ce secret permet de déclencher le chargement sécurisé, dans un nouveau module cryptographique, de la (ou des) clé(s) privée(s) d'AC sauvegardée(s) lors de la cérémonie de clés.

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

6.1.1.2 Clés porteurs générées par l'AC

Certificats d'authentification signature sur QSCD pour des personnes physiques
Dans le cas d'une demande initiale, la bi-clé du porteur est générée par l'AE directement dans le dispositif matériel du porteur conforme aux exigences du chapitre 12 et en présence du porteur.

Certificats de chiffrement sur QSCD pour des personnes physiques

Dans le cas d'une demande initiale, la bi-clé du porteur est générée dans le module cryptographique de l'AC conforme aux exigences du chapitre 11 puis est transférée vers le dispositif matériel du porteur de manière sécurisée.
Ces opérations sont réalisées au cours du face-à-face entre l'AE et le porteur.

La clé privée générée fait l'objet d'un séquestre par l'AC.

6.1.1.3 Clés porteurs générées par le porteur

Certificats d'authentification signature sur QSCD pour des personnes physiques
Dans le cas du premier renouvellement courant (*Cf. chapitre 3.3*), la génération de la bi-clé du porteur est déclenchée par le porteur lui-même directement dans son dispositif matériel conforme aux exigences du chapitre 12. Lors du renouvellement suivant, la génération de la bi-clé est effectuée selon la même procédure que pour la demande initiale (*Cf. chapitre 6.1.1.2*).

Certificats de chiffrement sur QSCD pour des personnes physiques
Dans le cas du premier renouvellement courant (*Cf. chapitre 3.3*), la génération de la bi-clé du porteur est déclenchée par le porteur lui-même directement dans le module cryptographique de l'AC conforme aux exigences du chapitre 11 puis est transférée vers le dispositif matériel du porteur de manière sécurisée. La clé privée générée fait l'objet d'un séquestre par l'AC. Lors du renouvellement suivant, la génération de la bi-clé est effectuée selon la même procédure que pour la demande initiale (*Cf. chapitre 6.1.1.2*).

6.1.2 Transmission de la clé privée à son propriétaire

Le dispositif matériel contenant la clé privée générée par l'AC est remis au porteur en face-à-face par l'AE.

6.1.3 Transmission de la clé publique à l'AC

Certificats d'authentification signature sur QSCD pour des personnes physiques
Dans le cas du premier renouvellement courant (*Cf. chapitre 3.3*), les requêtes de demande de certificat du porteur sont transmises à l'AC au format PKCS#10, ce qui permet de garantir l'intégrité de la clé et d'authentifier l'origine.

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

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

6.1.5 Taille des clés

L'AC racine dispose d'une clé RSA de 4096 bits.
Les AC émettrices disposent d'une clé RSA de 4096 bits.
Les **porteurs** disposent d'une clé RSA d'une longueur supérieure ou égale à 2048 bits.
Ces exigences sont revues à mesure de l'évolution de l'état de l'art technique et/ou de la législation.

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

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

6.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats, de LCR / LAR (*Cf. chapitre 1.5.1.2*).

L'utilisation de la clé privée du répondeur OCSP et du certificat associé est strictement limitée à la signature réponses OCSP.

L'utilisation de la clé privée et du certificat émis associé est strictement limitée aux usages définis dans les chapitres 1.5.1.1 et 4.5.

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

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'AC

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

Les modules cryptographiques, utilisés par l'AC, pour la génération des clés des porteurs, sont des modules cryptographiques répondant au minimum aux exigences du chapitre 11 ci-dessous pour le niveau de sécurité considéré.

6.2.1.2 Dispositifs de création de signature des porteurs

L'AC fournit au porteur le dispositif matériel.
Celui-ci est préparé, stocké, distribué, déverrouillé le cas échéant, de façon sécurisée.
Les dispositifs matériels des porteurs respectent les exigences du chapitre 12 pour le niveau de sécurité considéré.
Les dispositifs matériels utilisés pour les porteurs sont des dispositifs de création de signature qualifiés (QSCD).

6.2.2 Contrôles de la clé privée par plusieurs personnes

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

6.2.3 Séquestre de la clé privée

Seules les clés privées associées aux certificats électroniques dont l'usage est la confidentialité (*chiffrement*) peuvent être séquestrées, conformément aux dispositions prévues dans la PC et la DPC de l'AC (*Cf. chapitre 4.12*).

6.2.4 Copies de secours de la clé privée

Hormis les clés privées à usage de confidentialité, les clés privées des porteurs 'e font ''objet d'aucune copie de secours par l'AC.
Les clés privées des AC font l'objet d'une copie de secours bénéficiant du même niveau de sécurité que les clés originales.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC ne sont en aucun cas archivées.
Les clés privées des porteurs ne sont en aucun cas archivées, ni par l'AC ni par aucune des composantes du service d'émission de certificats.

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

6.2.6.1 Clés privées d'AC

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

6.2.6.2 Clés privées des porteurs

Certificats de chiffrement sur QSCD pour des personnes physiques
Les clés privées de chiffrement sont générées par l'AC sur un module cryptographique répondant aux exigences du chapitre 11 puis sont transférées de manière sécurisée vers le dispositif matériel du porteur conformément au chapitre 6.1.1.2.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC sont stockées dans un module cryptographique répondant aux exigences du chapitre 11 pour le niveau de sécurité considéré.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'AC

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

L'activation est précisée au niveau de la DPC contenant les informations non-diffusables.

6.2.8.2 Clés privées des porteurs

La méthode d'activation des clés privées des porteurs dans un dispositif matériel de type QSCD permet de répondre aux exigences définies dans le chapitre 12 pour le niveau de sécurité considéré.

L'activation des clés privées des porteurs nécessite la saisie du code PIN du dispositif matériel, sous le contrôle exclusif du porteur et permet de répondre aux exigences définies dans le chapitre 12 pour le niveau de sécurité considéré.

Par ailleurs, l'AC propose un service de déblocage aux porteurs pour que ces derniers aient la possibilité de débloquer leur dispositif matériel de type QSCD si celui-ci est bloqué suite à plusieurs tentatives successives erronées de saisie du code PIN.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'AC

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

La désactivation est précisée au niveau de la DPC contenant les informations non-diffusables.

6.2.9.2 Clés privées des porteurs

En cas de délai d'inactivité prolongé ou en cas de retrait de la carte, la clé privée est désactivée.
La méthode de désactivation de la clé privée du porteur est celle du dispositif matériel du porteur et permet de répondre aux exigences définies dans le chapitre 12 pour le niveau de sécurité considéré.

6.2.10 Méthode de destruction de la clé privée

6.2.10.1 Clés privées d'AC

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

En fin de vie d'une clé privée d'AC, 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

Dès lors que la clé privée a été remise au porteur, sa destruction est sous sa responsabilité.

La méthode de destruction de la clé privée du porteur est celle du dispositif matériel du porteur et permet de répondre aux exigences définies dans le chapitre 12 pour le niveau de sécurité considéré.

Certificats de chiffrement sur QSCD pour des personnes physiques
À la fin de la période de validité d'un certificat de chiffrement, le passage à une nouvelle clé privée se fait au niveau du porteur en conservant l'ancienne et la nouvelle clé privée, afin que le porteur continue à accéder aux données précédemment chiffrées avec son ancienne clé privée, Les dispositifs matériels des porteurs disposent de 4 emplacements pour accueillir des certificats de chiffrement.

6.2.11 Niveau d'évaluation sécurité des modules cryptographiques

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

Les dispositifs matériels des porteurs répondent aux exigences du chapitre 12.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

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

6.3.2 Durée de vie des bi-clés et des certificats

Les certificats et bi-clés des porteurs ont la même durée de vie.
Cette durée de vie est inférieure ou égale à 3 ans pour les certificats de porteurs.

La fin de vie d'un certificat d'AC est postérieure à la fin de vie des certificats qu'elle émet.
Les certificats et bi-clés des AC émettrices ont la même durée de vie.
Cette durée de vie est inférieure ou égale à 10 ans .

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

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

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

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

Les clés privées du porteur générées par l'AC sont transmises de manière sécurisée vers le dispositif matériel du porteur. Les codes d'activation sont choisis directement par le porteur. Toutes ces opérations sont réalisées lors de la remise du dispositif matériel au porteur en face-à-face avec l'AE.

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 du service d'émission de certificats sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

6.4.2.2 Protection des données d'activation correspondant à la clé privée du porteur

Les codes d'activation des porteurs sont des codes PIN et sont personnalisés directement par le porteur.

6.4.3 Autres aspects liés aux données d'activation

Sans objet.

6.5 Mesures de sécurité des systèmes informatiques

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Les systèmes informatiques du service d'émission de certificats offrent un niveau de sécurité décrit précisément dans la DPC contenant les informations non-diffusables et qui couvre notamment les points suivants pour assurer la protection des échanges d'information entre les différentes composantes de l'IGC :

- Identification et authentification forte des utilisateurs pour l'accès au système (*authentification à deux facteurs, de nature physique et/ou logique*),

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

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

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Le module cryptographique de l'AC et les dispositifs matériels des porteurs sont qualifiés par l'ANSSI au minimum au niveau standard.

6.6 Mesure de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurités liées au développement des systèmes

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

6.6.2 Mesures liées à la gestion de la sécurité

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

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

Sans objet.

6.7 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement souhaité par l'AC et pour contrer les attaques de type déni de service ou les intrusions. En l'occurrence, le réseau est équipé de routeurs, firewalls avec système de détection des intrusions IPS avec émission d'alertes

L'AC garantit que les composants du réseau local 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.

Le réseau d'administration des systèmes informatiques est logiquement séparé du réseau d'exploitation.

6.8 Horodatage / Système de datation

Il n'y a pas d'horodatage utilisé par l'AC mais une datation des évènements qui permet à l'AC de séquencer les événements à partir de l'heure système du service d'émission de certificats.

Des procédures automatiques ou manuelles sont utilisées pour synchroniser les horloges des systèmes du service d'émission du certificat entre elles, au minimum à la minute près, et par rapport à une source fiable de temps UTC, au minimum à la seconde près.

7 PROFILS DES CERTIFICATS ET DES LCR / LAR

7.1 Profils de certificats

7.1.1 Profil des certificats d'AC

Les Autorités de Certification portées par la présente PC sont les suivantes :

- AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE
- AC CONFIDENTIALITE MEF QUALIFIEE

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

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

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

Extensions	**Criticité**	**Valeur**	
KeyUsage	***O***	• KeyCertSign • crlSigning	
Certificate Policies	***N***		
PolicyIdentifier		2.5.29.32.0 (anyPolicy)	
policyQualifierId		CPS	
Qualifier		URL des points de publication de la PC de l'AC RACINE MEF QUALIFIEE	
CRL Distribution Point	***N***	Points de distribution de la LAR	
AuthorityKeyIdentifier	***N***		
KeyIdentifier		Identifiant de la clé publique de l'AC RACINE MEF QUALIFIEE	
SubjectKeyIdentifier	***N***	**AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE**	**AC CONFIDENTIALITE MEF QUALIFIEE**

KeyIdentifier		Identifiant de la clé publique de l'AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE	Identifiant de la clé publique de l'AC Confidentialité MEFR
BasicConstraints	***O***		
CA		Vrai	
pathLenConstraint		0	

7.1.2 Profil des certificats de porteur

Les Autorités de Certification portées par la présente PC délivrent respectivement les certificats de porteurs suivants :

- Certificat double usage « *authentification et signature* » délivré par l'AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE
- Certificat « *confidentialité* » délivré par l'AC CONFIDENTIALITE MEF QUALIFIEE

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

Certificat de porteur		
Champs	**Valeur**	
Version	2 (=version 3)	
SerialNumber	Fourni par le service (*unique et généré de manière aléatoire*)	
SignatureAlgorithm	sha256WithRSAEncryption	
	AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE	**AC CONFIDENTIALITE MEF QUALIFIEE**
Issuer	CN = AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE OrgID = NTRFR-130013345 OU = 0002 130013345 O = MINISTERES ECONOMIQUES ET FINANCIERS C = FR	CN = AC CONFIDENTIALITE MEF QUALIFIEE OrgID = NTRFR-130013345 OU = 0002 130013345 O = MINISTERES ECONOMIQUES ET FINANCIERS C = FR
Validity	3 ans	
NotBefore	Date de la génération de la bi-clé	
NotAfter	Date de la génération de la bi-clé + 3 ans	
SubjectPublicKeyInfo	La clé publique du porteur avec une longueur de 2048 bits (RSA)	
Subject	Voir chapitre 3.1.2.2	

Le tableau suivant présente les extensions d'un certificat de porteur :

Extensions	**Criticité**	**Valeur**	
Certificate Policies	***N***	**AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE**	**AC CONFIDENTIALITE MEF QUALIFIEE**
PolicyIdentifier		OID de la PC de l'AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE	OID de la PC de l'AC CONFIDENTIALITE MEF QUALIFIEE
policyQualifierId		CPS	CPS
Qualifier		URL des points de publication de la PC de l'AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE	URL des points de publication de la PC de l'AC CONFIDENTIALITE MEF QUALIFIEE
CRL Distribution Point	***N***	Points de distribution de la LCR de l'AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE	Points de distribution de la LCR de l'AC CONFIDENTIALITE MEF QUALIFIEE

Authority Information Access	***N***	Points de publication du certificat de l'AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE Point d'accès au service OCSP de l'AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE	Points de publication du certificat de l'AC CONFIDENTIALITE MEF QUALIFIEE Point d'accès au service OCSP de l'AC CONFIDENTIALITE MEF QUALIFIEE
AuthorityKeyIdentifier	***N***		
KeyIdentifier		Identifiant de la clé publique de l'AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE	Identifiant de la clé publique de l'AC CONFIDENTIALITE MEF QUALIFIEE
SubjectKeyIdentifier	***N***		
KeyIdentifier		Identifiant de la clé publique du porteur	
BasicConstraints	***N***		
CA		Faux	
pathLenConstraint		Aucun	
Subject Alternative Name	***N***		
otherName (UPN)		L'UPN tel qu'il est dans l'annuaire	
Directory Name		Login = [Login]	
rfc822Name		Adresse email du porteur	
		AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE	**AC CONFIDENTIALITE MEF QUALIFIEE**
KeyUsage	***O***	• digitalSignature • nonRepudiation	• keyEncipherment
ExtendedKeyUsage		• id-kp-clientAuth • id-ms-smartcardlogon • id-kp-emailProtection	• id-kp-emailProtection
QcCompliance		id-etsi-qcs 1	Non-utilisé
QcSSCD		id-etsi-qcs 4	Non-utilisé
QcType		id-etsi-qct-esign	Non-utilisé
QcPDS		URL vers les CGU en anglais (PDS)	Non-utilisé

7.2 Profil des LCR

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

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

LCR	
Champs	**Valeur**
Version	1 (=version 2)
SerialNumber	Fourni par le service
SignatureAlgorithm	sha256WithRSAEncryption
Issuer	DN de l'AC Emettrice (*Cf. chapitre 7.1.1*)
This Update	Date d'émission de la LCR
Next Update	Date limite d'émission de la prochaine LCR (*This update + 6 jours*)
Revoked certificates	Liste des numéros de série des certificats révoqués

Le tableau suivant présente les extensions d'une LCR :

Extensions	**Criticité**	**Valeur**
AuthorityKeyIdentifier	***N***	
KeyIdentifier		Identifiant de la clé publique de l'AC Emettrice
CRL Number	***N***	Numéro de série de la LCR

ExpiredCertOnCRL	***N***	Indique que la LCR contient également les numéros de série des certificats arrivés à expiration après leur révocation

7.3 Protocole OCSP

Chaque AC dispose d'un répondeur OCSP permettant à tout utilisateur de vérifier en ligne l'état des certificats émis.
La réponse OCSP est signée par le répondeur OCSP dont le certificat est émis par l'AC Emettrice du certificat vérifié.

Afin d'assurer la disponibilité du statut de révocation à tout moment et au-delà de la période de validité du certificat, les réponses OCSP contiennent l'extension « *id-pkix-ocsp-archive-cutoff* » conformément à la RFC 6960 contenant la date de début de validité de l'AC émettrice.

7.3.1 Profil des certificats OCSP

Le tableau suivant présente les champs de base d'un certificat de répondeur OCSP :

Certificat OCSP		
Champs	**Valeur**	
Version	2 (=version 3)	
SerialNumber	Fourni par le service	
SignatureAlgorithm	sha256WithRSAEncryption	
	AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE	**AC CONFIDENTIALITE MEF QUALIFIEE**
Issuer	CN = AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE OrgID = NTRFR-130013345 OU = 0002 130013345 O = MINISTERES ECONOMIQUES ET FINANCIERS C = FR	CN = AC CONFIDENTIALITE MEF QUALIFIEE OrgID = NTRFR-130013345 OU = 0002 130013345 O = MINISTERES ECONOMIQUES ET FINANCIERS C = FR
Validity	1 an	
NotBefore	Date de la génération de la bi-clé	
NotAfter	Date de la génération de la bi-clé + 1 an	
SubjectPublicKeyInfo	La clé publique avec une longueur de 2048 bits (RSA)	
Subject	CN = [Nom du service OCSP] OrgID = NTRFR-130013345 OU = 0002 130013345 O = MINISTERES ECONOMIQUES ET FINANCIERS C = FR	

Le tableau suivant présente les extensions d'un certificat de répondeur OCSP :

Extensions	**Criticité**	**Valeur**	
Certificate Policies	***N***	**AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE**	**AC CONFIDENTIALITE MEF QUALIFIEE**
PolicyIdentifier		OID de la PC de l'AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE	OID de la PC de l'AC CONFIDENTIALITE MEF QUALIFIEE
policyQualifierId		CPS	CPS
Qualifier		URL des points de publication de la PC de l'AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE	URL des points de publication de la PC de l'AC CONFIDENTIALITE MEF QUALIFIEE

AuthorityKeyIdentifier	***N***		
KeyIdentifier		Identifiant de la clé publique de l'AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE	Identifiant de la clé publique de l'AC CONFIDENTIALITE MEF QUALIFIEE
SubjectKeyIdentifier	***N***		
KeyIdentifier		Identifiant de la clé publique du répondeur OCSP	
BasicConstraints	***N***		
CA		Faux	
pathLenConstraint		Aucun	
KeyUsage	***O***	digitalSignature	
ExtendedKeyUsage		OCSP Signing with no-check	

8 AUDITS DE CONFORMITE ET AUTRES EVALUATIONS

8.1 Fréquence et circonstances des évaluations

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

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

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

8.2 Identité et qualification des évaluateurs

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

8.3 Relations entre évaluateurs et entités évaluées

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

8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une composante du service d'émission de certificats (*contrôles ponctuels*) ou sur l'ensemble de l'architecture du service d'émission de certificats (*contrôles périodiques*) et visent à vérifier le respect des engagements et pratiques définis dans la présente PC et dans la DPC qui y répond ainsi que des éléments qui en découlent (*procédures opérationnelles, ressources mises en œuvre, etc.*).
L'audit technique sera le moyen privilégié pour justifier que les mesures nécessaires ont été prises pour assurer la protection des échanges d'informations entre les composantes de l'IGC.

8.5 Actions prises suite aux conclusions des évaluations

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

- « *réussite* »,
- « *échec* »,
- « *à confirmer* ».

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

- En cas d'échec, et selon l'importance des non-conformités, l'équipe d'audit émet des recommandations à l'AC qui peuvent être la cessation (*temporaire ou définitive*) d'activité, la révocation du certificat de la composante, la révocation de l'ensemble des certificats émis depuis le dernier contrôle positif, etc. Le choix de la mesure à appliquer est effectué par l'AC et doit respecter ses politiques de sécurité internes.
- En cas de résultat « *A confirmer* », l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être réparées. Puis, un contrôle de « *confirmation* » permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas de réussite, l'AC confirme à la composante contrôlée la conformité aux exigences de la présente PC et la DPC associée contenant les informations non-diffusables.

8.6 Communication des résultats

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

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Sans objet.

9.1.2 Tarifs pour accéder aux certificats

Sans objet.

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

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

9.1.4 Tarifs pour d'autres services

Sans objet.

9.1.5 Politique de remboursement

Sans objet.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

L'Etat est son propre assureur.

9.2.2 Autres ressources

Sans objet.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

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

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

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

9.3.2 Informations hors du périmètre des informations confidentielles

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

9.3.3 Responsabilité en termes de protection des informations confidentielles

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

L'AC peut mettre à disposition les dossiers d'enregistrement des porteurs à des tiers dans le cadre de procédures légales. Ces dossiers sont aussi accessibles au porteur et au MC conformément au chapitre 9.4.1.

9.4 Protection des données à caractère personnel

9.4.1 Politique de protection des données à caractère personnel

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

9.4.2 Données à caractère personnel

Les données suivantes sont considérées à caractère personnel :

- Toutes les données nominatives des porteurs, représentants légaux et mandataires de certification enregistrées par le service d'émission de certificats (*prénom, nom, adresse email, …*),
- Les causes de révocation des certificats des porteurs (*qui sont considérées comme confidentielles sauf accord explicite du porteur*),

9.4.3 Données à caractère non personnel

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

9.4.4 Responsabilité en termes de protection des données à caractère personnel

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

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

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

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

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

9.4.7 Autres circonstances de divulgation de données personnelles

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

9.5 Droits de propriété intellectuelle et industrielle

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

9.6 Interprétations contractuelles et garanties

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

- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- N'utiliser leurs clés cryptographiques (*publiques, privées et/ou secrètes*) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la 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 et l'organisme de qualification et remédier aux non-conformités qu'ils révéleraient
- 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 est responsable vis-à-vis de ses porteurs, mandataires de certification et tiers utilisateurs des opérations relatives aux services de certification réalisées par l'une quelconque des composantes du service d'émission de certificats. Elle garantit le lien qui existe entre une entité identifiée et une bi-clé.

L'AC garantit et maintient la cohérence de sa DPC avec sa PC conformément au chapitre 1.6 de la présente PC.

L'AC veille à ce que les AE qui agissent en son nom se conforment à toutes les modalités pertinentes de la présente Politique de Certification, concernant le fonctionnement des AE.

L'AC veille à ce que les mandataires de certification aient connaissance et approuvé des obligations et responsabilités endossées dans le cadre de leurs fonctions.
L'AC et le responsable de l'AC se conforment à toutes les exigences de la présente Politique de Certification et de la DPC associée contenant les informations non-diffusables.

L'AC et le personnel de l'AC doivent respecter les droits des porteurs et tiers utilisateurs de certificats, eu égard aux lois et règlements en vigueur.

L'AC informe les tiers utilisateurs de la révocation du certificat d'un porteur ou d'une composante du service d'émission de certificats en transmettant dans les plus brefs délais la révocation du certificat auprès du service d'émission de certificats qui a en charge de publier les Listes de Certificats Révoqués.

L'AC est responsable de la transmission de l'information au service d'émission de certificats pour ses mandataires de certification et ses porteurs des procédures à suivre au cours du cycle de vie des certificats ; cela concerne, notamment, l'émission, la révocation, le retrait des certificats. Ainsi, l'AC s'engage à faire connaître aux composantes concernées (l'AE) les procédures d'exploitation pour tout le cycle de vie des certificats.

L'AC valide la génération des certificats, transmet les informations concernant la révocation des certificats et transmet les informations nécessaires au renouvellement des certificats au bénéfice des utilisateurs.

Le personnel de l'AC, ainsi que l'ensemble du personnel des AE, doit se conformer à toutes les exigences pertinentes de la présente Politique de Certification et de la DPC associée contenant les informations non-diffusables. Il doit respecter les droits des porteurs et des tiers utilisateurs de certificats eu égard aux lois et règlements en vigueur et doit informer l'AC de tout problème constaté.

Les membres du personnel de l'AC, et des AE, à qui sont assignés des rôles relatifs au service d'émission de certificats (*responsable de l'AC, responsable de la sécurité de l'AC*...) doivent être personnellement responsables de leurs actes. L'expression « *personnellement responsable* » signifie que l'on puisse prouver qu'une telle personne a bel et bien fait une telle action.

9.6.2 Service d'enregistrement

Une AE se conforme à toutes les exigences de la présente politique de certification et de la DPC associée contenant les informations non-diffusables. En outre, une AE :

- Traite les demandes de certificat, de révocation, et de renouvellement,

- Vérifie les données personnelles d'identification et les données contenues dans le certificat,
- Transmet à l'AC les demandes de génération, révocation, renouvellement des certificats qu'elle aurait traité favorablement,
- Transmet à l'AC une trace imputable de la validité de cette vérification,
- Transmet en toute confidentialité des supports physiques, et
- Conserve et protège en confidentialité et en intégrité toutes les données à caractère personnel et d'identification collectées lors des procédures d'enregistrement.

L'AE se soumet à tout contrôle technique et audit de qualité des procédures que pourrait demander l'AC.

9.6.3 Porteurs de certificats

Les obligations des porteurs sont les suivantes :

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

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

9.6.4 Mandataire de certification

Les obligations du porteur précisées au chapitre 9.6.3 sont applicables au mandataire de certification.

Le mandataire de certification doit se conformer à toutes les exigences de la présente Politique de Certification.

Il doit respecter ses obligations précisées dans le formulaire d'engagement qui le lie à l'AC.

Il garantit que les informations qu'il fournit à l'AC ou à une AE, pour l'identification de l'entité identifiée ou du porteur, sont exactes, complètes et que les documents transmis ou présentés sont valides.

S'il soupçonne la compromission d'une clé privée, il est tenu d'en aviser l'AC dans les plus brefs délais et selon les instructions données par celle-ci.

Il doit protéger en confidentialité et en intégrité ses clés privées, ses codes d'activation ou d'accès. Il doit prendre toutes les mesures raisonnables pour en éviter la perte, la divulgation, la compromission, la modification ou l'utilisation non autorisée.

9.6.5 Utilisateurs de certificats

Les obligations de l'Utilisateur de la sphère publique sont les suivantes :

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

9.6.6 Autres participants

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

9.7 Limite de garantie

Sous réserve des dispositions d'ordre public applicables, le Ministère de l'Economie, des Finances et de la Relance ne pourra pas être tenu responsable d'une utilisation non autorisée ou non conforme des certificats, des clés privées associées et des données d'activation, des LAR et des LCR ainsi que de tout autre équipement ou logiciel mis à disposition.

Le Ministère de l'Economie, des Finances et de la Relance décline en particulier sa responsabilité pour tout dommage résultant :

- D'un emploi des bi-clés pour un usage autre que ceux prévus,
- De l'usage de certificats révoqués ou expirés,
- De l'absence de demande de révocation d'un certificat entraînant l'utilisation du certificat et de la bi-clé par un tiers non autorisé,
- D'un cas de force majeure tel que défini par les tribunaux français.

Le Ministère de l'Economie, des Finances et de la Relance décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations contenues dans les certificats, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées.

9.8 Limite de responsabilités

Sans objet.

9.9 Indemnités

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

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

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

9.10.2 Fin anticipée de validité

La publication d'une nouvelle version de la présente PC peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa DPC correspondante, contenant les informations non-diffusables.

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

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

9.10.3 Effets de la fin de validité et clauses restant applicables

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

9.11 Notifications individuelles et communication entre les participants

En cas de changement de toute nature intervenant dans la composition du service d'émission de certificats, l'AC devra :

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

9.12 Amendements de la PC

9.12.1 Procédures d'amendement

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

9.12.2 Mécanisme et période d'information sur les amendements

Sans objet.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

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

9.13 Dispositions concernant la résolution de conflits

L'AC propose le traitement à l'amiable des litiges ou conflits portés à sa connaissance (par le porteur, par le service d'assistance par exemple).

9.14 A défaut d'une résolution à l'amiable, les conflits seront résolus par les tribunaux compétents.Juridictions compétentes

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

9.15 Conformité aux législations et réglementations

La politique et les pratiques de l'AC sont non-discriminatoires.
Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre 10 ci-dessous.
L'AC est notamment soumise aux dispositions prévues par l'article 31 de la [LSQ] concernant la remise des clés privées des porteurs séquestrées.

9.16 Dispositions diverses

9.16.1 Accord global

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

9.16.2 Transfert d'activités

Cf. chapitre 5.8

9.16.3 Conséquences d'une clause non valide

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

9.16.4 Application et renonciation

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

9.16.5 Force majeure

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

9.17 Autres dispositions

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

10 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 Règlementation

[CNIL]	Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles puis par ordonnance n°2018-1125 du 12 décembre 2018
[DIRSIG]	Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.
[LCEN]	Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.
[ORDONNANCE]	Ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives modifiée par ordonnance n°2017-1426 du 4 octobre 2017.
[PSCO_QUALIF]	Prestataires de services de confiance qualifiés - Critères d'évaluation de la conformité au règlement eIDAS, version en vigueur.
[PSCE_RGS_EIDAS]	Services de délivrance de certificats qualifiés de signature électronique, de cachet électronique et d'authentification de site internet - Modalités de qualification selon le règlement eIDAS des services qualifiés selon le RGS, version en vigueur.
[DEC_EXEC_1506]	Décision d'exécution (UE) 2015/1506 de la Commission du 8 septembre 2015 établissant les spécifications relatives aux formats des signatures électroniques avancées et des cachets électroniques avancés devant être reconnus par les organismes du secteur public visés à l'article 27, paragraphe 5, et à l'article 37, paragraphe 5, du règlement [eIDAS].
[eIDAS]	Règlement n° 910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive n°1999/93/CE.
[DécretRGS]	Décret pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005
[LSQ]	Loi n°2001-1062 du 15 novembre 2001 relative à la sécurité quotidienne.

[SIG]	Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.

10.2 Documents techniques

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

	(complétée par les correctifs techniques Corrigendum 1 de janvier 2007et Corrigendum 2 de novembre 2008)
[TS_119_312]	ETSI TS 119 312 V1.1.1 (2014-11) : Electronic Signatures and Infrastructures (ESI); Cryptographic Suites.

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

11.1 Exigences sur les objectifs de sécurité

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

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

11.2 Exigences sur la qualification

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

12 ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF DE PROTECTION DES ELEMENTS SECRETS

12.1 Exigences sur les objectifs de sécurité

Le dispositif de protection des éléments secrets du porteur, utilisé par le porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer sa bi-clé, doit répondre aux exigences de sécurité suivantes :

- Si la bi-clé 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 des clés privées ;
- Garantir la confidentialité et l'intégrité des clés privées ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Générer une fonction de sécurité qui ne peut être falsifiée sans la connaissance de la clé privée ;
- Assurer la fonction de sécurité 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.
- Assurer la fonction de déchiffrement, de clés symétriques de fichier ou de message, 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 symétrique de fichier ou de message, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données ;
- Le cas échéant, permettre de garantir la confidentialité, l'authenticité et l'intégrité de la clé privée lors de son export hors du dispositif, à destination d'une fonction de séquestre ou d'archivage des clés privées.

12.2 Exigences sur la qualification

Le dispositif de création de signature utilisé par le porteur doit être qualifié au minimum au niveau standard par l'ANSSI,

13 HISTORIQUE DES PRINCIPALES MODIFICATIONS

V1.0	14/02/2022	Document initial validé en comité de surveillance le 14/02/2022
V1.1	22/04/2022	Prise en compte des remarques de l'auditeur lors de l'audit de qualification • Ajout dans la présentation des fonctions des fonctions nécessaires pour les certificats de confidentialité (§ 1.4) • Précisions sur l'identification, authentification et rôle des marques déposées (§ 3.1.6) • Précision sur le déblocage du dispositif matériel du porteur (QSCD) (§ 6.2.8.2) Adaptation de l'extension 'certificate Policies' du gabarit des certificats des porteurs (retrait du champ UserNotice).
V1.2	05/12/2022	Ajout d'une nouvelle pièce d'identité, le nouveau permis de conduire.
V1.3	20/01/2023	Ajout d'une nouvelle pièce d'identité, la commission d'emploi de moins de 15 ans.
V1.4	01/08/2023	Mise à jour du document suite à l'intégration de l'Administration Centrale en tant qu'AE (§ 1.4.2 et 3.4)
V1.5	25/10/2023	Prise en compte des remarques de l'auditeur lors de l'audit de qualification Administration Centrale (§ 1.4.1, 1.4.3 et 1.6)
V1.6	21/05/2024	Prise en compte des remarques de l'auditeur de l'audit de renouvellement de la qualification du service

Contact : contact-igc-mef@finances.gouv.fr