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

Déclaration des Pratiques 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 1.3 Diffusion : Publique

TABLE DES MATIERES

1 INTRODUCTION

1.1 Présentation générale

Le présent document constitue la Déclaration des Pratiques de Certification (DPC) des Autorités de Certification émettrices « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » et « *AC CONFIDENTIALITE MEF QUALIFIEE* » des Ministères économiques et financiers (MEF). Ces AC sont portées, à la date à de la rédaction du document par le Ministère de l'Economie, des Finances et de la Relance (MEFR).
A la mise à jour du document, il s'agit du ministère de l'Economie, des Finances et de la Souveraineté Industrielle et Numérique.

Cette DPC réunit l'ensemble des mesures mises en œuvre par les différentes composantes du service d'émission de certificats en lien avec la délivrance et l'usage des certificats électroniques de personnes physiques dans le cadre de leur activité au sein des MEF, conformément aux Politiques de Certification (*Cf. chapitre suivant*) des AC « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » et « *AC CONFIDENTIALITE MEF QUALIFIEE* ».

La présente DPC contient les informations publiques des pratiques des AC. Les informations considérées confidentielles sont portées dans des documents annexes non-communicables au public.

De manière à mettre en exergue les mesures 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

Cette DPC est identifiée par son OID (1.2.250.1.131.1.11.6.4.1.1 et 1.2.250.1.131.1.11.7.4.1.1), son nom et sa version.
Elle est commune aux Autorités de Certification « *AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE* » et « *AC CONFIDENTIALITE MEF QUALIFIEE* » délivrant les certificats suivants :

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	1.2.250.1.131.1.11.7.3.1.1	RGS *

1.3 Définitions et acronymes

Voir PC même chapitre.

1.4 Entités intervenant dans l'infrastructure de gestion de clés

1.4.1 Comité de surveillance du service d'émission de certificats

Voir PC même chapitre.

1.4.2 Autorités de certification

Voir PC même chapitre.

L'AC est en charge des fonctions suivantes au sein du service d'émission de certificats :

- La fonction de publication.
- La fonction d'archivage

1.4.3 Autorité d'enregistrement

Voir PC même chapitre.
Chaque AE est liée contractuellement avec l'AC et s'engage à respecter les exigences de la PC de l'AC à travers le document [MEF – CONVENTION AC-AE].
A ce jour, seules les entités suivantes des MEF sont reconnues comme AE par l'AC :

- La DGDDI,
- L'Administration Centrale.

1.4.4 Porteurs de certificats

Voir PC même chapitre.

1.4.5 Utilisateurs de certificats

Voir PC même chapitre.

1.4.6 Autres participants

1.4.6.1 Composantes du service d'émission de certificats

L'AC délègue les opérations de gestion du service d'émission de certificats à un prestataire appelé « *Opérateur technique* » (*OT*). Le prestataire actuel est la société IN Groupe qui est en charge de :

- Définir l'infrastructure technique du service d'émission de certificats,
- Assurer le paramétrage et l'administration des composants,
- Assurer l'exploitation, le maintien en condition opérationnelle et la supervision des composants.

L'OT est en charge des fonctions suivantes au sein du service d'émission de certificats :

- La fonction de génération des certificats,

- La fonction de génération des éléments secrets du porteur particulièrement pour la génération du code d'authentification à usage unique du porteur lors de son face-à-face avec l'AE,
- La fonction d'information sur l'état des certificats pour le répondeur OCSP,
- La fonction de gestion des recouvrements,
- La fonction de séquestre et recouvrement,
- La fonction de gestion des révocations

Les fonctions de publication et d'archivage sont à la charge des MEF.

1.4.6.2Mandataires de certification

Voir PC même chapitre.

1.5 Usage des certificats

1.5.1 Domaines d'utilisation applicables

1.5.1.1Bi-clés et certificats des porteurs

Voir PC même chapitre.

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

Voir PC même chapitre.

1.5.2 Domaines d'utilisation interdits

Voir PC même chapitre.

1.6 Gestion des politiques de certification

1.6.1 Entité gérant les politiques de certification

La PC est soumise à l'approbation du Comité de Surveillance du service d'émission des certificats notamment pour :

- Valider les usages et restrictions d'usage des certificats émis par l'AC,
- Vérifier sa conformité aux évolutions technologiques et aux exigences fonctionnelles ou légales et réglementaires.

La PC embarque un tableau indiquant les différentes versions de la PC, les dates de révision et les principales modifications apportées par rapport à sa version antérieure.
Les identifiants OID des PC peuvent être incrémentés en cas d'évolution significative, relative notamment à la sécurité du service d'émission de certificats, aux modalités de délivrance des certificats ou aux usages autorisés des certificats. L'incrémentation d'OID est validée en comité de surveillance, à l'occasion de l'approbation de la PC ayant évolué.

1.6.2 Point de contact de la politique de certification

Voir PC même chapitre.

1.6.3 Entité gérant la conformité de la DPC avec les PC

Voir PC même chapitre.

1.6.4 Procédures d'approbation de la conformité de la DPC

La procédure d'approbation de la conformité de la DPC est détaillée dans le document [MEF – COMITE DE SURVEILLANCE].

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

2.1 Entités chargées de la mise à disposition des informations

La mise à disposition des LCR et des LAR est assurée par l'OT.
Le dispositif de publication des LCR et LAR sur les différents points de distribution est détaillée dans le document [OT - DAT] pour la génération de la LCR et sur le document [MEF – PROC-PUB] pour la réplication de la LCR sur les différents points de distribution.

La publication des documents des informations de l'AC (*PC, DPC, CGU, certificats d'AC*) est réalisée sur le site des MEF.
La procédure de publication sur le site des MEF est détaillée dans le document [MEF – PROC-PUB].

2.2 Informations publiées

Les informations sont publiées aux points de distribution suivants :

<table>
<tr><th rowspan="2">Information publiée</th><th colspan="2">Emplacement de publication</th></tr>
<tr><th>AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIEE</th><th>AC CONFIDENTIALITE MEF QUALIFIEE</th></tr>
<tr><td>Politique de Certification</td><td colspan="2">▪ https://igc.finances.gouv.fr/pc-ac-personnes-mef-qualifiees.pdf
▪ https://igc1.finances.gouv.fr/pc-ac-personnes-mef-qualifiees.pdf
▪ https://igc2.finances.gouv.fr/pc-ac-personnes-mef-qualifiees.pdf</td></tr>
<tr><td rowspan="2">Certificat de la chaine de confiance</td><td colspan="2">Pour l'AC AC RACINE MEF QUALIFIEE :
▪ https://igc.finances.gouv.fr/ac-racine-mef-qualifiee.cer
▪ https://igc1.finances.gouv.fr/ac-racine-mef-qualifiee.cer
▪ https://igc2.finances.gouv.fr/ac-racine-mef-qualifiee.cer</td></tr>
<tr><td>Pour l'AC AUTHENTIFICATION ET SIGNATURE MEF QUALIFIE :
▪ https://igc.finances.gouv.fr/ac-authentification-signature-mef-qualifiee.cer
▪ https://igc1.finances.gouv.fr/ac-authentification-signature-mef-qualifiee.cer
▪ https://igc2.finances.gouv.fr/ac-authentification-signature-mef-qualifiee.cer</td><td>Pour l'AC CONFIDENTIALITE MEF QUALIFIEE :
▪ https://igc.finances.gouv.fr/ac-confidentialite-mef-qualifiee.cer
▪ https://igc1.finances.gouv.fr/ac-confidentialite-mef-qualifiee.cer
▪ https://igc2.finances.gouv.fr/ac-confidentialite-mef-qualifiee.cer</td></tr>
</table>

LAR	Pour l'AC AC RACINE MEF QUALIFIEE : ▪ http://crl.igc.finances.gouv.fr/ac-racine-mef-qualifiee.crl ▪ http://crl.igc1.finances.gouv.fr/ac-racine-mef-qualifiee.crl ▪ http://crl.igc2.finances.gouv.fr/ac-racine-mef-qualifiee.crl	
LCR	▪ http://crl.igc.finances.gouv.fr/ac-authentification-signature-mef-qualifiee.crl ▪ http://crl.igc1.finances.gouv.fr/ac-authentification-signature-mef-qualifiee.crl ▪ http://crl.igc2.finances.gouv.fr/ac-authentification-signature-mef-qualifiee.crl	▪ http://crl.igc.finances.gouv.fr/ac-confidentialite-mef-qualifiee.crl ▪ http://crl.igc1.finances.gouv.fr/ac-confidentialite-mef-qualifiee.crl ▪ http://crl.igc2.finances.gouv.fr/ac-confidentialite-mef-qualifiee.crl
Répondeur OCSP	▪ http://ocsp-ac-mef.finances.gouv.fr/ac-online-mef-qualifiees/ ▪ http://ocsp-ac-mef.finances.rie.gouv.fr/ac-online-mef-qualifiees/	
CGU / PDS	Version française : ▪ https://igc.finances.gouv.fr/ac-authentification-signature-mef-qualifiee-cgu.pdf ▪ https://igc1.finances.gouv.fr/ac-authentification-signature-mef-qualifiee-cgu.pdf ▪ https://igc2.finances.gouv.fr/ac-authentification-signature-mef-qualifiee-cgu.pdf Version anglaise : ▪ https://igc.finances.gouv.fr/ac-personnes-mef-qualifiees-cgu-en.pdf ▪ https://igc1.finances.gouv.fr/ac-personnes-mef-qualifiees-cgu-en.pdf ▪ https://igc2.finances.gouv.fr/ac-personnes-mef-qualifiees-cgu-en.pdf	Version française : ▪ https://igc.finances.gouv.fr/ac-confidentialite-mef-qualifiee-cgu.pdf ▪ https://igc1.finances.gouv.fr/ac-confidentialite-mef-qualifiee-cgu.pdf ▪ https://igc2.finances.gouv.fr/ac-confidentialite-mef-qualifiee-cgu.pdf
Formulaires	Disponibles sur les sites de publication igc.finances.gouv.fr, igc1.finances.gouv.fr, igc2.finances.gouv.fr.	

Pour permettre aux utilisateurs de s'assurer de l'origine des informations, les empreintes des certificats sont également publiées sur le site de publication.
Les opérations de publication sont détaillées dans le document [MEF – PROC-PUB].

2.3 Délais et fréquence de publication

Voir PC même chapitre.

2.4 Contrôle d'accès aux informations publiées

Les mécanismes mis en œuvre par l'OT pour contrôler les accès relatifs à la publication des LCR et LAR sont présentés dans le document [OT - DAT].

Les MEF mettent en œuvre un contrôle d'accès pour toute modification des informations publiées sur le site de publication du service d'émission de certificats.
La mise à jour des informations publiées sur ce site est réalisée par du personnel des MEF désigné et spécifiquement autorisé. Toute mise à jour est effectuée sur demande d'une personne préalablement habilitée, par l'AC ou par le comité de surveillance, tel que présenté dans le document [MEF – PROC-PUB].
Pour réaliser la publication des informations, le personnel doit effectuer les opérations suivantes :

- Authentification de l'exploitant sur son poste de travail d'administration sur réseau dédié
- Accès aux serveurs de publication pour y déposer les éléments.

La publication des listes de révocation n'est pas réalisée de la même façon.
En effet, 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).

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de noms

Voir PC même chapitre.

3.1.2 Nécessité d'utilisation de noms explicites

3.1.2.1 Identités des AC

Voir PC même chapitre.

3.1.2.2 Identités des porteurs

Voir PC même chapitre.

3.1.2.3 Certificats de test

Voir PC même chapitre.

3.1.3 Anonymisation et pseudonymisation des porteurs

Voir PC même chapitre.

3.1.4 Règles d'interprétation des différentes formes de noms

Voir PC même chapitre.

3.1.5 Unicité des noms

Voir PC même chapitre.

3.1.6 Rôle des marques déposées

Voir PC même chapitre.

3.2 Validation initiale de l'identité

3.2.1 Méthode pour prouver la possession de la clé privée

Voir PC même chapitre.

3.2.2 Validation de l'identité d'un individu

3.2.2.1 Validation de l'identité d'un porteur sans MC

Pour une carte « *agent* » :

Une carte « *agent* » sans intervention d'un MC est délivrée exclusivement à un agent des MEF présent dans le référentiel applicable des agents des MEF. La vérification de l'identité de l'agent s'appuie notamment sur un annuaire à la main de l'entité concernée.

Pour une carte « temporaire » :
Une carte « temporaire » sans intervention d'un MC est délivrée exclusivement à un agent des MEF présent dans le référentiel applicable des agents des MEF. La vérification de l'identité de l'agent s'appuie notamment sur un annuaire à la main de l'entité concernée.

Pour la DGDDI
Les informations de l'agent sont contenues dans l'annuaire propre à la DGDDI.

Pour l'Administration Centrale
Les informations de l'agent sont contenues dans l'annuaire applicable à **l'Administration Centrale**.

Les informations des agents présentes sur le référentiel applicable des MEF sont collectées quotidiennement par le CMS. Le CMS détecte tout nouvel utilisateur enregistré sur le référentiel applicable des MEF et l'enregistre dans sa base interne.

Les opérations relatives à la validation de l'identité de l'agent et de son entité de rattachement sont décrites dans le document propre à chaque AE.

Ces opérations sont décrites dans le document [MEF – PROC-AE]

3.2.2.2Enregistrement d'un MC

Voir PC même chapitre.
L'ensemble des contrôles réalisés pour la validation du dossier d'enregistrement du MC est décrit dans le document [MEF – PROC-AE].

3.2.2.3Validation de l'identité d'un porteur avec MC

Pour une carte « temporaire » :
L'intervention d'un MC est indispensable pour une carte « temporaire » délivrée :

- A une personne ne figurant pas dans le référentiel des agents des MEF :
  - Agent non encore connu dans ce référentiel
  - Prestataire externe

L'identité du porteur pour une demande de carte « temporaire » est validée par l'AE sur la base d'un dossier d'enregistrement transmis par un agent des MEF enregistré au préalable en tant que MC auprès de l'AC. Les contenus des dossiers d'enregistrement du MC et du porteur sont décrits dans la PC respectivement aux chapitres 3.2.3.2 et 3.2.3.3.

Une fois les éléments du dossier d'enregistrement validés par le MC, le MC transmet le dossier à l'AE qui valide les informations du porteur dans le CMS.

L'ensemble des actions et contrôles réalisés par le MC est décrit dans le document [MEF – PROC-MC]

L'ensemble des contrôles réalisés pour la validation des dossiers d'enregistrement est décrit dans le document [MEF – PROC-AE].

3.2.3 Informations non vérifiées du porteur

Voir PC même chapitre.

3.2.4 Validation de l'autorité du demandeur

Voir PC même chapitre.
Les vérifications sont décrites dans le document [MEF – PROC-AE].

3.2.5 Critères d'interopérabilité, certification croisée d'AC

Sans objet.

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

3.3.1 Identification et validation pour un renouvellement courant

Les dispositifs matériels utilisés pour les porteurs sont des dispositifs de création de signature qualifiés (QSCD) et disposent de 4 emplacements par type de certificat :

- 4 emplacements pour les certificats Authentification & Signature,
- 4 emplacements pour les certificats Confidentialité.

Ces emplacements permettent de supporter les différents renouvellements qui interviendront au cours de la vie des AC Emettrices concernées par la présente DPC.

Conformément à la PC associée à la présente DPC, seul le 1er renouvellement peut être réalisé sur la même carte (*exclusivement pour les cartes agent*). Le 2ème renouvellement doit être réalisé sur une nouvelle carte.

Le 3ème renouvellement ne pourra être réalisé à partir des AC Emettrices de la présente DPC étant donné que celles-ci ne peuvent émettre de certificats dont la date de fin serait postérieure à la date d'expiration des certificats correspondants des AC Emettrices.

L'AC effectue une veille sécuritaire et réglementaire pour suivre le maintien des qualifications des produits utilisés dans le cadre de Rossignol. En cas de perte de qualification d'un dispositif matériel utilisé dans le cadre de Rossignol, celui-ci est retiré de la liste des dispositifs matériels supportés par le service empêchant ainsi toute génération sur un dispositif matériel non-qualifié.
Dans tous les cas, le renouvellement de certificats ne peut être réalisé que sur un QSCD valide.

Pour une carte « agent » :
Le porteur est alerté par email 60 jours avant l'expiration de son certificat.
Pour le premier renouvellement, le porteur peut réaliser l'opération seul en "self-service". A cette occasion, le porteur s'authentifie avec l'ancien certificat toujours en cours de validité et déclenche la génération de son nouveau certificat.
Les échanges quotidiens entre le CMS et le référentiel des agents des MEF, via l'annuaire de référence de la direction ou du service concerné, permettent de valider que l'agent est toujours habilité à recevoir une carte et que les informations du porteur sont toujours cohérentes avec celles des certificats à renouveler.
Pour ce premier renouvellement, le porteur peut également se rapprocher d'une AE pour réaliser l'opération.

Les opérations relatives au renouvellement sont décrites dans le document [MEF – PROC-AE].

Pour le second renouvellement, le porteur doit suivre la même procédure que pour la demande initiale. A cette occasion, une nouvelle carte lui sera délivrée.

Pour une carte « temporaire » :
Le porteur est alerté par email 60 jours avant l'expiration de son certificat.
Le porteur doit suivre la même procédure que pour la demande initiale. A cette occasion, une nouvelle carte lui sera délivrée.

3.3.2 Identification et validation pour un renouvellement des clés après révocation

Voir PC même chapitre.

3.4 Identification et validation d'une demande de révocation

Voir PC même chapitre.
Les opérations relatives à la gestion des révocations sont décrites dans le document [MEF – PROC-AE].

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DE CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

La procédure de demande de certificat est décrite dans le document [MEF – PROC-AE].

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

Pour une carte « agent » - Cas de l'agent connu du référentiel applicable des agents des MEF :

Le CMS interroge régulièrement le référentiel applicable des agents des MEF et alimente sa base interne avec les informations des agents collectées.

Les mécanismes d'alimentation des informations des agents sont décrits dans le document [MEF – PROC-AE].

Le demandeur habilité se connecte sur le portail et effectue une demande de certificat pour lui-même (*cas du porteur*) ou pour un agent de son périmètre (*cas de l'opérateur de l'AE*).

- Le porteur (*agent connu sur le référentiel des agents des MEF*) peut effectuer sa demande de certificat en se connectant sur le portail « self-service » et démarrer le processus de demande de carte.
- L'opérateur de l'AE se connecte sur le CMS, sélectionne l'utilisateur rattaché à son périmètre puis démarre le processus de demande de carte.

Dans les deux cas, l'émission des certificats et la remise de la carte sont des opérations réalisées par l'opérateur de l'AE en présence du porteur.

Ces pratiques sont détaillées dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

Pour une carte « temporaire » - Cas de l'agent connu du référentiel applicable des agents des MEF :

Pour un agent connu du référentiel des agents des MEF, l'opérateur de l'AE se connecte sur le CMS, sélectionne l'utilisateur rattaché à son périmètre puis démarre le processus de demande de carte.

L'émission des certificats et la remise de la carte sont des opérations réalisées par l'opérateur de l'AE en présence du porteur.

Ces pratiques sont détaillées dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

Pour une carte « temporaire » :

- **Cas de l'agent inconnu du référentiel des agents des MEF**,
- **Cas du prestataire externe** (par définition inconnu du référentiel des agents des MEF)**.**

Dans les deux cas, l'intervention d'un MC est nécessaire. Ce dernier constitue un dossier d'enregistrement avec le futur porteur qu'il rencontre pour vérifier son identité.

Une fois complet, le dossier d'enregistrement est déposé auprès de l'AE par voie électronique ou par voie papier.
Après validation de la demande, l'émission des certificats et la remise de la carte sont des opérations réalisées par l'opérateur de l'AE en présence du porteur.

Ces pratiques sont détaillées dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

4.2 Traitement d'une demande de certificat

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

Dès lors que la demande est validée par l'opérateur de l'AE, un email est transmis au porteur l'invitant à venir récupérer sa carte auprès de son AE.
Cet email contient notamment un code d'authentification à usage unique et un lien permettant de consulter les CGU.
Ce code est généré aléatoirement par le CMS et permet notamment au porteur de s'authentifier lors du face-à-face avec l'opérateur de l'AE.

Lorsque le porteur se présente auprès de l'AE pour récupérer son certificat :

- L'opérateur de l'AE vérifie l'identité du porteur.
- L'opérateur de l'AE s'authentifie sur le CMS et insère la carte du porteur.
- Le numéro de série de la carte insérée par l'opérateur de l'AE et destinée au porteur est vérifié par le CMS (*celui-ci doit correspondre à celui affecté lors de la validation de la demande*).
- L'opérateur de l'AE lance le processus de personnalisation de la carte au cours duquel le code d'authentification à usage unique est demandé et est saisi par le porteur,

Le détail des traitements effectués par l'AE est décrit dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

4.2.2 Acceptation ou rejet de la demande

En cas de rejet de la demande, un email est envoyé à l'agent pour l'informer du rejet. Le processus d'attribution de carte pour l'agent est ainsi arrêté.

Le détail des traitements effectués par l'AE est décrit dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

4.2.3 Durée d'établissement du certificat

Voir PC même chapitre.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Voir PC même chapitre.
La délivrance des certificats est réalisée par l'opérateur de l'AE en face-à-face avec le porteur. Cette opération est réalisée dans les locaux de l'AE.

Le détail des traitements effectués par l'AE est décrit dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

Pour la DGDDI
Dans certains cas, l'opérateur de l'AE peut être amené à se déplacer sur le lieu du porteur pour effectuer les opérations de délivrance des certificats.

Pour l'Administration Centrale
Il n'est pas prévu que l'AE se déplace sur le lieu du porteur.

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

Voir PC même chapitre.

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

Préalablement au face-à-face, le porteur reçoit un email contenant un code d'authentification à usage unique généré aléatoirement par le CMS et permettant :

- Au porteur de s'authentifier lors du face-à-face avec l'opérateur de l'AE,
- De sécuriser l'initialisation de la carte et la délivrance des certificats (*nécessaire pour lancer les opérations d'initialisation de la carte et d'émission du certificat*),
- D'accepter les Conditions Générales d'Utilisation des certificats délivrés : la saisie de l'OTP (*ou la fourniture de l'OTP à l'opérateur de l'AE*) et la case cochée à l'issue de la session valent acceptation des CGU.

A l'issue de la génération, les informations des certificats sont affichées sur l'écran du poste de l'opérateur de l'AE et présentées au porteur.
Si les informations du certificat sont jugées correctes par le porteur, alors ce dernier coche la case d'acceptation des certificats qui s'affiche à l'écran.

La carte est ensuite remise en mains propres au porteur par l'opérateur de l'AE.

Le détail de l'acceptation du certificat est décrit dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

4.4.2 Publication du certificat

Voir PC même chapitre.

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

Voir PC même chapitre.

4.5 Usages de la bi-clé et du certificat

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

Voir PC même chapitre.

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

Voir PC même chapitre.

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

Sans objet.

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

Voir PC même chapitre.

4.7.2 Origine d'une demande d'un nouveau certificat

Voir PC même chapitre.

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

Sans objet.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificat de porteur

Voir PC même chapitre.

4.9.1.2 Certificat d'une composante du service

Voir PC même chapitre.

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificat de porteur

Voir PC même chapitre.

4.9.2.2 Certificat d'une composante du service

La révocation des certificats suivants est décidée par l'entité responsable de l'AC :

- Les certificats du répondeur OCSP délivrés par chaque AC Emettrice,
- Les certificats d'authentification serveur délivrés par une AC publique référencée dans les navigateurs pour le portail des opérateurs et pour le portail des porteurs (*portail self-service*),
- Le certificat de chiffrement des informations stockées en base et délivré par une AC technique de la PKI,
- Les certificats des AC Emettrices.

La révocation des certificats suivants peut être décidée par l'entité responsable de l'AE ou de l'AC :

- Les certificats des opérateurs de l'AE qui sont les certificats du service d'émission de certificats des MEF ou d'autres certificats reconnus par le CMS.

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Certificat de porteur

Une demande de révocation peut être déposée en utilisant l'un des moyens suivants :

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

Le traitement d'une demande de révocation est décrit dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

4.9.3.2Certificat d'une composante du service

Pour les certificats de la chaine de confiance, le certificat du répondeur OCSP, les certificats d'authentification serveur et le certificat de chiffrement des informations en base, la décision de révoquer le certificat est prise par le comité de surveillance.

En cas de révocation d'un certificat de la chaine de confiance :

- Tous les certificats émis par l'AC et en cours de validité sont révoqués et inclus dans la LCR,
- L'ensemble des porteurs concernés sont informés dans les plus brefs délais que leurs certificats ne sont plus valides,
- Le point de contact identifié de l'ANSSI est informé dans les plus brefs délais,
- Une demande de révocation pour le certificat de l'AC concernée est transmise à l'AC Racine à laquelle l'AC est subordonnée. Le traitement d'une révocation d'un certificat d'AC Subordonnée est détaillé dans la Politique de Certification de l'AC Racine,
- Le numéro de série du certificat de l'AC est inclus dans la LAR émise par l'AC Racine,
- Une opération de destruction des clés de l'AC révoquée est réalisée conformément au document [MEF - PAA].

Pour le certificat d'un opérateur de l'AE, la demande de révocation est réalisée si nécessaire par un opérateur habilité des MEF ou de l'entité des MEF concernée.
Le traitement d'une demande de révocation du certificat d'un opérateur de l'AE est décrit dans la procédure opérationnelle [MEF – PAA].

4.9.4 Délai accordé au porteur pour formuler la demande de révocation

Voir PC même chapitre.

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

4.9.5.1Certificat de porteur

Voir PC même chapitre.

4.9.5.2Disponibilité du système de traitement des demandes de révocation

Voir PC même chapitre.

4.9.5.3Certificat d'une composante du service

Voir PC même chapitre.

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

Voir PC même chapitre.

4.9.7 Fréquence d'établissement des LCR

Voir PC même chapitre.

4.9.8 Délai maximum de publication d'une LCR

Voir PC même chapitre.

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

Voir PC même chapitre.

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 demandeurs autorisés à effectuer une demande de révocation sont tenus de le faire sans délais après avoir eu connaissance de la compromission de la clé privée.

Pour un certificat d'AC, la procédure de révocation est détaillée dans le document [MEF - PAA].

4.9.13 Causes possibles d'une suspension

Sans objet.

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

Voir PC même chapitre.

Le répondeur OCSP mis à disposition des utilisateurs de certificats s'appuie sur la LCR de chaque AC Emettrice.

4.10.2 Disponibilité de la fonction

Voir PC même chapitre.

4.10.3 Dispositifs optionnels

Sans objet.

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

Voir PC même chapitre.

4.12 Séquestre de clé et recouvrement

4.12.1 Politiques et pratiques de recouvrement par séquestre des clés

4.12.1.1 Demande de séquestre

Le porteur reçoit en début de processus de délivrance préalablement au face-à-face ou à l'occasion du face à face pour une carte temporaire, un email contenant un code d'authentification à usage unique et un lien permettant de consulter les CGU.
A travers celles-ci, le porteur est informé en début de processus du séquestre qui sera réalisé pour la clé de déchiffrement qui sera générée. La saisie de l'OTP par le porteur et la case cochée en fin de session valent acceptation des CGU et donc de l'opération de séquestre qui sera réalisée.

4.12.1.2 Traitement d'une demande de séquestre

La bi-clé de chiffrement/déchiffrement est générée par un HSM puis transférée vers la base de données de l'IGC où elle est stockée sous forme de P12 chiffré. Le chiffrement est réalisé avec une clé de chiffrement/déchiffrement de l'IGC mise en œuvre dans un HSM.

4.12.1.3 Origine d'une demande de recouvrement

Voir PC même chapitre.
Une demande de recouvrement de clé est traitée de manière concomitante à une demande de personnalisation d'une nouvelle carte.

Le détail des traitements effectués par l'AE est décrit dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

4.12.1.4 Identification et validation d'une demande de recouvrement

Le recouvrement d'une clé de déchiffrement est réalisé lors de la personnalisation d'une nouvelle carte qui s'appuie sur les processus d'identification du porteur et de délivrance initiaux.

Le porteur reçoit donc en début de processus de délivrance, un email contenant un code d'authentification à usage unique et un lien permettant de consulter les CGU.
A travers celles-ci, le porteur est informé en début de processus du recouvrement qui sera réalisé pour ses clés de déchiffrement existantes. La fourniture de l'OTP par le porteur vaut acceptation des CGU et donc de l'opération de recouvrement qui sera réalisée.

Le détail des traitements effectués par l'AE est décrit dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

4.12.1.5 Traitement d'une demande de recouvrement

Les dispositifs matériels utilisés pour les porteurs disposent de 4 emplacements pour les certificats Confidentialité.
La fonction de séquestre et de recouvrement ne peut recouvrer au maximum que les trois (3) bi-clés les plus récentes sur le dispositif matériel du porteur.
Le dernier emplacement doit être libre afin d'accueillir le nouveau certificat de Confidentialité qui doit être généré.

Le détail des traitements effectués par l'AE est décrit dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

Pour toute demande de recouvrement sur requête judiciaire, l'AC met à disposition une procédure exceptionnelle détaillée dans le document [MEF – PROC EXCEPTIONNELLE DE RECOUVREMENT]

4.12.1.6 Destruction des clés séquestrées

A l'issue de la période de séquestre, la bi-clé séquestrée est supprimée de la base de données de l'IGC.

4.12.1.7 Disponibilité des fonctions liées au séquestre et au recouvrement

Voir PC même chapitre.

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

Sans objet

4.13 Certificats de test

Les modalités d'émission d'un certificat de test sont décrites dans le document [MEF – PROC-AE].

5 MESURES DE SECURITE NON TECHNIQUES

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

OT :
Le service d'émission de certificats des MEF est hébergé par l'OT sur des sites distincts.

Les sites d'hébergement de l'OT respectent les règlements et normes en vigueur et leur installation permet de répondre aux besoins de sécurité des MEF.

AC :
Les locaux de l'entité responsable de l'AC respectent les règlements et normes en vigueur.

AE (entités des MEF) :
Les opérateurs de l'AE se trouvent dans les locaux de chaque entité des MEF désignée comme AE par l'AC.

Pour la DGDDI
Les AE sont présentes sur plusieurs sites de la DGDDI au niveau national.

Pour l'Administration Centrale
Les AE sont présentes sur plusieurs sites au niveau national.

5.1.2 Accès physiques

OT :
L'accès physique au site de l'hébergeur, aux salles de production et de cérémonie de clés est contrôlé par des dispositifs de sécurité spécifiques décrits dans le document de référence de l'OT [OT – CONTROLE ACCES].

AC :
L'accès physique au site de l'entité responsable de l'AC est contrôlé par des dispositifs de sécurité décrits dans le document de l'AC [MEF - CONTROLE ACCES].

AE (entités des MEF) :
L'accès physique aux locaux de l'AE est contrôlé par des dispositifs de sécurité respectant la politique de sécurité physique de l'AE concernée.

La politique de sécurité physique de l'AE s'appuie sur le document [MEF - CONTROLE ACCES].

5.1.3 Alimentation électrique et climatisation

Le site d'hébergement dispose d'un système d'alimentation secourue : onduleurs et groupes électrogènes. Toutes les salles de production de l'hébergeur sont équipées d'un système de conditionnement d'air. Les exigences sont décrites dans le document [OT - SECURITE PHYSIQUE].

5.1.4 Vulnérabilité aux dégâts des eaux

Le site d'hébergement est protégé contre les risques d'inondation et de dégâts des eaux. Les exigences sont décrites dans le document [OT – SECURITE PHYSIQUE].

5.1.5 Prévention et protection incendie

Des procédures spécifiques sont prévues notamment en matière de protection incendie sur le site d'hébergement.
Les exigences sont décrites dans le document [OT - SECURITE PHYSIQUE].

5.1.6 Conservation des supports

Les opérations effectuées par les opérateurs de l'AE sont automatiquement enregistrées dans le journal d'audit du service. Par conséquent, elles sont archivées par l'AC.
Les médias stockés par l'hébergeur (*bandes magnétiques,* …) sont protégés contre tout excès de température, d'humidité et de rayonnement magnétique. Les mesures prises sont décrites dans le document [OT – GESTION DES SUPPORTS].

5.1.7 Mise hors service des supports

Tous les supports servant au stockage des informations sensibles de l'AC sont effacés ou détruits avant leur mise au rebut. Les mesures prises sont décrites dans le document [OT – GESTION DES SUPPORTS].

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Les rôles de confiance de l'AC sont détaillés dans le document [MEF - RÔLES].

Les rôles de confiance de l'OT sont détaillés dans le document [OT - RÔLES].

5.2.2 Nombre de personnes requises par tâches

OT :
Ci-dessous la matrice des personnes requises pour les tâches sensibles :

Opération	**Acteur de l'opération**	**Entité bénéficiaire de l'opération**	**Autorisations requises**			
			Porteurs de secrets AC	**Porteurs de secrets OT**	**Nombre d'Opérateurs**	**Nombre d'Admin**
	AC RACINE	AC	3	1	1	2

Opération	Acteur de l'opération	Entité bénéficiaire de l'opération	Autorisations requises			
			Porteurs de secrets AC	Porteurs de secrets OT	Nombre d'Opérateurs	Nombre d'Admin
Génération de bi-clé et certificat	AC	AE	3	1	1	1
	AC	UF	0	0	1	0
Modification configuration des profils de l'AC	AC	AC, UF	0	0	0	2
Stockage et restauration de clé privée	AC	AC	3	0	0	2
Révocation de certificat	AC RACINE	AC	0	0	0	2
	AC	AE	0	0	1	1
	AC	UF	0	0	1	0
Recouvrement de clé	AC	UF	0	0	1	0
Contrôle des journaux d'événements	AC	*	0	0	0	1

AC : Autorité de Certification
AE : Autorité d'Enregistrement
UF : Utilisateur Final

5.2.3 Identification et authentification pour chaque rôle

OT :
Chaque attribution d'un rôle est notifiée par écrit au personnel concerné. Ce dernier s'engage explicitement à endosser le rôle.
La procédure d'attribution de rôle est détaillée dans le document [OT – ROLES].

AC/AE :
Chaque attribution d'un rôle est notifiée par écrit au personnel concerné. Ce dernier s'engage explicitement à endosser le rôle.
La procédure d'attribution de rôle est détaillée dans le document [MEF – ROLES].

5.2.4 Rôles exigeant une séparation des attributions

Voir PC même chapitre.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

OT :

La qualification et l'expérience des personnes qui possèdent un rôle de confiance sont contrôlées. Les contrôles effectués à l'embauche et à la prise d'un rôle de confiance sont décrits dans le document [OT - ROLES].

AC :
La qualification et l'expérience des personnes qui possèdent un rôle de confiance sont contrôlées. Les contrôles effectués à l'embauche et à la prise d'un rôle de confiance sont décrits dans le document [MEF – ROLES].

AE (entités des MEF) :
La qualification et l'expérience des personnes qui possèdent un rôle de confiance sont contrôlées.
Les contrôles effectués à l'embauche et à la prise d'un rôle de confiance s'appuient sur le document [MEF - ROLES].

5.3.2 Procédures de vérification des antécédents

OT :
Les antécédents des personnels de l'OT, recrutés et intervenant dans le cadre du service d'émission de certificats des MEF, sont vérifiés au moins à travers le bulletin n°3 de leur casier judiciaire.
Ces vérifications sont réalisées avant d'affecter un rôle de confiance et sont revues à minima tous les 3 ans.

AC :
Les antécédents de tout personnel de l'AC sont vérifiés à travers différents moyens détaillés dans le document [MEF – ROLES].
L'AC met en place des vérifications régulières des antécédents applicables aux agents des MEF endossant un rôle de confiance.

AE (entités des MEF) :
Les antécédents de tout personnel de l'AE sont vérifiés à travers différents moyens détaillés dans le document [MEF – ROLES].

5.3.3 Exigences en matière de formation initiale

Les personnes amenées à détenir un rôle de confiance font l'objet d'une formation spécifique en fonction du rôle.

OT :
Tout nouvel employé de l'OT suit une formation initiale adaptée au métier qu'il devra exercer au sein de l'OT. Il suit une formation générique sur la politique de sécurité interne et la gestion de la sécurité au quotidien.

AC/AE :
Tout employé affecté à une composante du service suit une formation initiale adaptée au métier qu'il devra exercer au sein de la composante. Il suit une formation générique sur la politique de sécurité interne et la gestion de la sécurité au quotidien.

Les opérateurs de l'AE suivent une formation particulière aux tâches liées à la gestion des certificats suivant le document propre à AE.
Ces formations s'appuient sur la procédure opérationnelle de l'AE [MEF – PROC-AE].

5.3.4 Exigences et fréquence en matière de formation continue

OT :
Le personnel de l'OT est formé en continue en fonction des évolutions des procédures.

AC/AE :
Les opérateurs de l'AE sont formés à chaque évolution significative du logiciel d'enregistrement ou de la PC/DPC impliquant une modification sensible de la procédure d'enregistrement.
Le cas échéant, la formation est réalisée en s'appuyant sur le document propre à chaque entité qui est mis à jour le cas échéant.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

OT :
Des avertissements ou des sanctions peuvent être pris envers les personnels ne respectant pas les procédures internes ou les consignes de sécurité mises en place. Ces sanctions sont décrites dans le document [OT – CHARTE-SECURITE].

AC :
Des avertissements ou des sanctions peuvent être pris envers les personnels ne respectant pas les procédures internes ou les consignes de sécurité mises en place. Ces sanctions sont décrites dans le document [MEF – CHARTE-SECURITE].

AE (entités des MEF) :
Des avertissements ou des sanctions peuvent être pris envers les personnels ne respectant pas les procédures internes ou les consignes de sécurité mises en place.
Ces sanctions sont décrites dans le document [MEF – CHARTE-SECURITE].

5.3.7 Exigences vis-à-vis du personnel des prestataires

Les exigences applicables au personnel des prestataires sont précisées dans les contrats.

OT :
Les exigences sont précisées dans le document [OT – PLAN D'ASSURANCE SECURITE] de l'OT.

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*).

OT :
Les personnels de l'OT qui occupent un rôle de confiance possèdent la documentation relative à la mise en œuvre des fonctions qui leur incombent dans le cadre de l'exploitation du service d'émission des certificats des MEF.

AC/AE :
Les personnels de l'AC et de l'AE qui occupent un rôle de confiance possèdent la documentation relative à la mise en œuvre des fonctions qui leur incombent dans le cadre des services de l'AC.
Cette documentation est fournie pendant les formations et est disponible dans le système documentaire de chaque composante. Le document 'Manuel Utilisateur' détaille l'ensemble des procédures du système de gestion des cartes et certificats (CMS).

5.4 Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer de façon manuelle ou automatique.

5.4.1 Type d'évènements à enregistrer

5.4.1.1 Evénements enregistrés par l'AE

Les évènements enregistrés par l'AE sont décrits dans les documents [MEF – TRACES].

5.4.1.2 Evénements enregistrés par l'AC

Les événements sont enregistrés suivant les procédures de l'OT. Les évènements enregistrés par l'AC sont décrits dans le document [OT - TRACES] et [MEF - TRACES].

5.4.1.3 Evénements divers

L'environnement d'exploitation fait l'objet d'une journalisation des événements :

- Les accès physiques aux locaux,
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (*clés, données d'activation, …*),
- Changements apportés au personnel.

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'évènement générés sur les systèmes des AC, conservés pendant un mois, sont transférés de manière hebdomadaire de l'OT vers l'AC pour que cette dernière puisse réaliser les opérations de rapprochement des journaux.

5.4.4 Protection des journaux d'évènements

Les mesures de protection des journaux présents sur les systèmes des AC sont détaillées dans le document [OT – PSSI].

Les mesures de protection des journaux gérés ou réceptionnés par l'AC ou l'AE sont détaillées dans les documents [[MEF- ARCHIVAGE], [MEF – CONTROLE D'ACCES] et [MEF – PSSI].

5.4.5 Procédure de sauvegarde des journaux d'évènements

Les modalités de sauvegarde des journaux de l'AC et de l'AE sont précisées, selon le cas, dans les documents [OT – DAT] et [MEF – ARCHIVAGE].

5.4.6 Système de collecte des journaux d'évènements

Le document [MEF – TRACES] détaille les modalités de collecte des journaux et traces auprès de l'OT et l'AE.

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

Sans objet.

5.4.8 Évaluation des vulnérabilités

Les journaux d'évènement sont analysés tous les jours par l'OT. Le résultat de ces analyses fait l'objet d'un rapport synthétisant les éléments analysés et les anomalies identifiées.

Par ailleurs, l'AE dresse un rapport synthétisant les journaux d'évènements dont elle dispose (*ex : dossier d'enregistrement,* …) et le transmet à l'AC sur une base hebdomadaire.
Les caractéristiques du rapport sont décrites dans le document [MEF – TRACES].
L'AE assure toutefois la conservation des journaux d'évènements dont elle dispose.

L'AC effectue mensuellement un rapprochement des journaux d'évènements sur la base des rapports d'analyse et des journaux transmis par l'OT et l'AE.
Ce rapprochement des journaux a pour objectif de vérifier la cohérence des évènements entre différentes fonctions du service et d'identifier toute anomalie.
Les modalités de rapprochement sont détaillées dans le document [MEF - TRACES].

5.5 Archivage des données

5.5.1 Types de données à archiver

AC :
L'archivage incluant les données transmises par l'OT est réalisé conformément au document [MEF - ARCHIVAGE].

AE :
L'archivage est réalisé conformément au document [MEF – ARCHIVAGE].

5.5.2 Période de conservation des archives

Voir PC même chapitre.

5.5.3 Protection des archives

AC :
Les mesures de protection des archives sont décrites dans le document [MEF - ARCHIVAGE].

AE :
Les mesures de protection des archives sont décrites dans le document [MEF - ARCHIVAGE].

5.5.4 Procédure de sauvegarde des archives

Les journaux d'évènements archivés par l'AC sont maintenus sur les systèmes de l'AC opérés par l'OT, pendant la durée courante d'un mois.

Conformément au chapitre 5.4.5, les journaux de l'AE font l'objet d'une sauvegarde avant archivage. Ces modalités sont précisées dans le document [MEF – ARCHIVAGE].

5.5.5 Exigences d'horodatage des données

Voir chapitre 6.8.

5.5.6 Système de collecte des archives

L'archivage des données informatiques de l'AC sera effectué conformément au document [MEF - ARCHIVAGE].

5.5.7 Procédures de récupération et de vérification des archives

Les archives sont récupérées conformément au document [MEF - ARCHIVAGE].

5.6 Changement de clé d'AC

Le changement de clé d'AC est traité par l'OT comme l'initialisation d'une nouvelle AC. Une cérémonie des clés est donc organisée à ces fins.
Les MEF communiquent par la suite :

- Le nouveau certificat de l'AC sur son site de publication,
- La nouvelle PC de l'AC sur son site de publication,
- Les informations du changement au contact identifié de l'ANSSI.

5.7 Reprise suite à compromission ou sinistre

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

OT :

Dans le cas où l'OT constate un incident majeur lié à la clé privée de l'AC, ce dernier applique la procédure de remontée et de traitement des incidents conformément au document [MEF – GESTION DES INCIDENTS].

AC :

La procédure de gestion des incidents est décrite dans le document [MEF – GESTION DES INCIDENTS] et est applicable aux personnels de l'AC et de l'AE.
Cette procédure précise notamment :

- Les acteurs participant à la résolution des incidents,
- Les moyens permettant de tracer et gérer les incidents,
- Les détails du processus de gestion des incidents,
- Les conditions de remontée de l'incident auprès du contact identifié de l'ANSSI, en particulier dans le cas d'un incident majeur ou bloquant.

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

L'AC dispose de procédures de reprise dans son Plan de Continuité d'Activité détaillé dans le document [MEFR - PCA] qui inclut notamment les actions attendues de l'OT.

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

Dans le cas d'une compromission de la clé privée de l'AC, le MEF applique sa procédure de reprise conformément au document [MEF - PCA] qui inclut les actions attendues de l'OT.

Cette procédure précise notamment :

- L'entité responsable de la prise de décision pour la révocation de l'AC,
- Les moyens de communication pour informer les porteurs et MC mais aussi les applications utilisatrices ainsi que le contact identifié auprès de l'ANSSI,
- Les modalités de révocation de l'ensemble des certificats émis par l'AC,
- Les modalités de révocation du certificat de l'AC compromise,
- Les modalités de publication des LCR et LAR.

Dans le cas d'une compromission de la clé privée d'un opérateur de l'AE, le certificat est systématiquement révoqué.

5.7.4 Capacités de continuité d'activité suite à un sinistre

Les MEF disposent de procédures de continuité détaillées dans le document [MEF - PCA] et s'appuie sur l'OT qui dispose de son côté de procédures de continuité détaillées dans le document [OT - CONTINUITE].

5.8 Fin de vie du service

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

En cas de cessation d'activité de l'OT ou de changement d'OT par l'AC, l'arrêt d'activité est traduit en fin de contrat.

5.8.2 Cessation d'activité affectant l'AC

Dans le cas d'une cessation d'activité affectant l'AC, les MEF réalisent les opérations de cessation conformément au document [MEF - PAA].

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

Voir PC même chapitre.
Les clés des AC sont générées sur un équipement cryptographique sécurisé qualifié au minimum au niveau standard par l'ANSSI
La génération des clés d'AC est réalisée suivant le script de cérémonie [MEF – CEREMONIE DES CLES].

6.1.1.2 Clés porteurs générées par l'AC

Le modèle de QSCD utilisé par les porteurs est précisé au chapitre 6.2.1.2.

Certificat d'authentification et de signature
Les clés du porteur sont générées directement dans le QSCD du porteur par les opérateurs de l'AE et en présence du porteur. Le QSCD est ensuite remis en face-à-face au porteur permettant ainsi à ce dernier d'avoir le contrôle exclusif de sa clé privée.

Certificat de chiffrement
Les clés des porteurs sont générées par l'AC dans un environnement sécurisé par un module cryptographique, puis transférées vers la base de données de l'IGC où elles sont stockées sous forme de P12 chiffré.

Les clés sont ensuite transférées dans le QSCD du porteur à travers la connexion HTTPS avec authentification mutuelle entre le système de l'IGC (CMS) et le poste de l'opérateur de l'AE ou du porteur (*cas du 1er renouvellement*). Ces opérations sont réalisées au cours du face-à-face entre l'AE et le porteur.

Les opérations de génération sont détaillées dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

6.1.1.3Clés porteurs générées par le porteur

Dans le cadre du premier renouvellement, le porteur a la possibilité de renouveler lui-même ses certificats.

Certificat d'authentification et de signature
Les clés des porteurs sont générées directement dans le QSCD par le porteur lui-même.

Certificat de chiffrement
Le porteur déclenche la génération des clés qui sont générées par l'AC dans un environnement sécurisé par un module cryptographique, puis transférées de manière sécurisée dans son QSCD.

Les conditions de génération des clés sont détaillées dans le guide de l'AE.

Les opérations de génération sont détaillées dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

6.1.2 Transmission de la clé privée à son propriétaire

Voir PC même chapitre.

6.1.3 Transmission de la clé publique à l'AC

Voir PC même chapitre.

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

Voir PC même chapitre.

6.1.5 Taille des clés

Voir PC même chapitre.

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

Voir PC même chapitre.

6.1.7 Objectifs d'usage de la clé

Voir PC même chapitre.

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

L'équipement cryptographique utilisé pour l'AC est un équipement Proteccio qualifié au minimum au niveau standard par l'ANSSI.

6.2.1.2 Dispositifs de création de signature des porteurs

Le QSCD utilisé par les porteurs est de type NXP Semiconductor - Chipdoc V2 on JCOP3 P60

6.2.2 Contrôles de la clé privée par plusieurs personnes

Le partage de secrets mis en œuvre pour le contrôle des clés d'AC est détaillé dans le document de cérémonie des clés [MEF – CEREMONIE DES CLES].

A l'issue de la cérémonie des clés, les secrets sont remis à des porteurs de secrets formellement identifiés dans le document détaillant les rôles de confiance et les habilitations de chacun :

- Pour l'AC : voir document [MEF - RÔLES],
- Pour l'OT : voir document [OT - RÔLES].

6.2.3 Séquestre de la clé privée

Voir chapitre 4.12.

6.2.4 Copies de secours de la clé privée

Des copies de secours des bi-clés des AC sont réalisées à des fins de disponibilité. Ces copies sont faites lors de la cérémonie de clés et sont identifiées comme secret de l'AC. Les opérations liées aux copies de secours sont détaillées dans le document [MEF – CEREMONIE DES CLES].

6.2.5 Archivage de la clé privée

Sans objet.

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

6.2.6.1 Clés privées d'AC

Voir PC même chapitre.
Voir document [MEF – CEREMONIE DES CLES]

6.2.6.2Clés privées des porteurs

Voir le chapitre 6.1.1.2 pour le transfert de la bi-clé de chiffrement/déchiffrement vers le QSCD du porteur.

6.2.7 Stockage de la clé privée dans un module cryptographique

Voir PC même chapitre.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1Clés privées d'AC

Voir PC même chapitre.
L'activation de la bi-clé de l'AC est détaillée dans le document [MEF – CEREMONIE DES CLES]

6.2.8.2Clés privées des porteurs

La clé privée d'un porteur est activable à l'aide d'un code PIN. L'usage du code PIN est nécessaire à chaque utilisation de la clé privée.
Le code PIN est sous la maîtrise du porteur puisqu'il est personnalisé par le porteur lui-même lors de la personnalisation de la carte conformément au guide de l'AE.
Les règles de constitution du code PIN sont précisées dans le manuel de l'utilisateur de l'AE [MEF – PROC – AE]

Les opérations de personnalisation de la carte sont détaillées dans la procédure opérationnelle de l'AE [MEF – PROC-AE].

Un blocage de la carte est systématique suite à plusieurs tentatives de renseignement de code PIN erroné.
Le déblocage de la carte peut être déclenché par un utilisateur habilité par l'application et suite à une authentification du porteur par OTP.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1Clés privées d'AC

La désactivation de la clé privée d'une AC correspond à l'effacement des clés contenues dans le module cryptographique ou à l'arrêt du module cryptographique.
La désactivation de la clé privée est effectuée manuellement à l'aide de l'outil d'administration du HSM.

6.2.9.2Clés privées des porteurs

La désactivation de la clé privée d'un porteur correspond au retrait (déconnexion) du dispositif matériel du porteur.

6.2.10 Méthode de destruction de la clé privée

6.2.10.1 Clés privées d'AC

La destruction d'une clé privée d'AC revient à :

- Détruire la clé privée contenue dans le module cryptographique par effacement à l'aide des fonctions du module cryptographique
- Détruire toutes les copies de secours de la clé privée
- Faire un PV de destruction.

6.2.10.2 Clés privées des porteurs

La destruction de la clé privée du porteur est effectuée à l'aide du dispositif matériel en utilisant les fonctions logiques d'effacement de la bi-clé du middleware ou en détruisant physiquement le dispositif matériel.

6.2.11 Niveau d'évaluation sécurité des modules cryptographiques

Les modules cryptographiques de l'AC sont évalués au niveau EAL4+ selon les Critères Communs et qualifiés au minimum au niveau standard par l'ANSSI.

Les dispositifs matériels des porteurs sont qualifiés au minimum au niveau standard par l'ANSSI.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Voir PC même chapitre.

6.3.2 Durée de vie des bi-clés et des certificats

Voir PC même chapitre.

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 relatives aux clés d'AC sont détaillées dans le document de cérémonie des clés [MEF – CEREMONIE DES CLES].

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

Le code PIN est sous la maîtrise du porteur puisqu'il est personnalisé par le porteur lui-même lors de la personnalisation de la carte conformément au guide de l'AE.

Les opérations de personnalisation de la carte sont détaillées dans la procédure opérationnelle de l'AE [MEF – PROC-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

A l'issue de la cérémonie des clés, les données d'activation sont remises entre plusieurs porteurs de secrets qui ont la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.
Cette remise des données d'activation est détaillée dans le document de cérémonie [MEF – CEREMONIE DES CLES].

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

Le porteur personnalise son code PIN lors de l'initialisation de son dispositif matériel. L'AC n'a pas connaissance du code PIN du porteur.
Le porteur s'assure que la donnée d'activation de la clé privée est protégée en confidentialité de telle sorte qu'il soit le seul à pouvoir activer la clé privée contenue sur son support matériel.

L'AC met à disposition du porteur une fonction de déblocage du dispositif matériel.
Le fonctionnement du dispositif de déblocage du dispositif matériel est précisé dans le document [MEF – PROC-AE].

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

Le système d'information de l'AC opéré par l'OT est mis en œuvre conformément aux exigences de [OT - PSSI].

Les dispositifs de surveillance mis en place et des procédures d'audit des paramétrages du système sont précisés dans le document [OT - SUPERVISION] et dans le [OT – DAT].

Le système d'information de l'AE est mis en œuvre conformément aux exigences de la politique de sécurité des systèmes d'information et des standards sécurité associés du ministère [MEF - PSSI].

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Voir PC même chapitre.

6.6 Mesure de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurités liées au développement des systèmes

Le service d'émission de certificats s'appuie sur la suite logicielle de l'OT et qui est développée suivant une politique de développement sécurisée [OT – DEV-SEC].

6.6.2 Mesures liées à la gestion de la sécurité

La configuration et les mises à jour du système sont réalisées par l'OT conformément à ses pratiques de gestion du changement détaillées dans le document [OT - CHANGEMENT].

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

Sans objet.

6.7 Mesures de sécurité réseau

Les mesures de sécurité réseau sont détaillées dans le document [OT – SEC-RESEAU] et dans [OT - DAT].

6.8 Horodatage / Système de datation

Le dispositif de synchronisation des horloges des serveurs est décrit dans le document [OT - DAT].

7 PROFILS DES CERTIFICATS ET DES LCR / LAR

Voir PC même chapitre.

8 AUDITS DE CONFORMITE ET AUTRES EVALUATIONS

Voir PC même chapitre.
Le document [MEF – PROC AUDIT INTERNE] liste les sujets couverts lors de l'audit interne.

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

Voir PC même chapitre.

10 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 Règlementation

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

10.2 Documents techniques

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

10.3 Documents de référence

Documents AC	
MEF - Organisation du comité de surveillance v0.1	Document détaillant l'organisation pour gouvernance de l'AC.
[MEF – PROC-PUB]	Document détaillant les modalités de publication des informations de l'AC
[MEF - PAA]	Document détaillant les modalités d'arrêt d'activité de l'AC.
[MEF - CONTROLE ACCES]	Document(s) décrivant les principes de gestion des accès logiques
[MEF - CGU]	Conditions Générales d'Utilisation
[MEF - RÔLES]	Document(s) définissant les rôles et le mode d'attribution des rôles (*notamment les contrôles des antécédents réalisés*)
[MEF – CONVENTION AC-AE]	Document contractuel entre l'AC et l'AE
[MEF – PROC-AE]	Documents détaillant les procédures opérationnelles appliquées par l'AE
[MEF – PROC-MC]	Document détaillant les procédures opérationnelles appliquées par le MC
[MEF - PROC EXCEPTIONNELLE DE RECOUVREMENT]	Document détaillant la procédure exceptionnelle de recouvrement de clé de chiffrement sur requête judiciaire
[MEF – CHARTE-SECURITE]	Charte de sécurité de l'AC
[MEF - TRACES]	Document(s) détaillant la gestion des journaux (*collecte, analyse, archivage*)
[MEF - ARCHIVAGE]	Document(s) détaillant les modalités d'archivage de l'AC
[MEF – GESTION DES INCIDENTS]	Document détaillant les modalités de gestion des incidents
[MEF - PCA]	Document détaillant les modalités de continuité et de reprise d'activité
[MEF – CEREMONIE DES CLES]	Script de cérémonie des clés

[MEF – PROC AUDIT INTERNE]	Document détaillant les modalités de gestion des audits internes
[MEF - PSSI]	Référentiel sécurité des MEF (*PSSIE, PSSI des MEF, standards de sécurité, …*)

Documents OSC	
[OT - DAT]	Document d'architecture technique décrivant la structure générale du SI.
[OT- CONTROLE ACCES]	Document(s) décrivant les principes de gestion des accès logiques
[OT – GESTION DES SUPPORTS]	Document détaillant la procédure de gestion des supports durant leur cycle de vie
[OT - RÔLES]	Document(s) définissant les rôles et le mode d'attribution des rôles (*notamment les contrôles des antécédents réalisés*)
[OT – DEV-SEC]	Document(s) décrivant le cadre et les règles de développement sécurisé des composantes du service et respectant dans la mesure du possible des normes de modélisation et d'implémentation.
[OT - CHANGEMENT]	Document(s) définissant les modalités de gestion des changements pour les applications et services de production administrés et exploités par l'OT
[OT – SEC-RESEAU]	Document(s) décrivant les mesures de sécurité réseau mises en œuvre sur l'infra des MEF opérée par l'OT (*ex : cloisonnement du réseau d'administration, mise en œuvre de mécanismes cryptographiques, ...*).
[OT - SUPERVISION]	Document(s) détaillant les outils permettant de monitorer le service notamment : la mise en œuvre d'alertes de supervision, la détection et la remontée des anomalies.
[OT – CHARTE-SECURITE]	Règlement intérieur et/ou charte de sécurité

[OT - TRACES]	Document(s) détaillant la gestion des journaux (*collecte, analyse, archivage*)
[OT - ARCHIVAGE]	Document(s) détaillant les modalités d'archivage de l'OC
[OT - CONTINUITE]	Document détaillant les procédures de continuité et de reprise d'activité appliquées pour le service d'émission de certificats des MEF.
[OT - PSSI]	Politique de Sécurité des Systèmes d'Information de l'OC
[OT – PLAN D'ASSURANCE SECURITE]	Document(s) contenant les mesures de sécurité mises en œuvre sur la(les) composante(s) opérée(s) par l'OT

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

11.1 Exigences sur les objectifs de sécurité

Voir PC même chapitre.

11.2 Exigences sur la qualification

Voir PC même chapitre.

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 RGS
V1.2	01/08/2023	Mise à jour du document suite à l'intégration de l'Administration Centrale en tant qu'AE (§ 1.4.2, 3.2.2.1, 4.3.1 et 5.1.1)
V1.3	25/10/2023	Prise en compte des remarques de l'auditeur lors de l'audit de qualification RGS (§1.4.1 et 1.4.3)

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