CERTIGNA by tessi

DECLARATION DES PRATIQUES DE CERTIFICATION

Edité le :	04/01/2023
Version :	1.0
OID :	1.2.250.1.177.3.2.2
Auteurs :	J. Allemandou
Classification :	Publique

tessi

SOMMAIRE

1 INTRODUCTION

1.1 Présentation générale

Le groupe TESSI s'appuie sur sa filiale CERTIGNA pour se doter de plusieurs autorités de certifications (AC) délivrant des certificats électroniques à des personnes physiques. La présente Déclaration des Pratiques de Certification (DPC) expose les pratiques que CERTIGNA applique dans le cadre de la fourniture de ses services de certification électronique aux usagers en conformité avec sa Politique de Certification (PC) qu'elle s'est engagée à respecter. L'attention du lecteur est attirée sur le fait que la compréhension de la présente DPC suppose qu'il soit familiarisé avec les notions liées à la technologie des Infrastructures de Gestion de Clés (IGC).

La présente DPC vise la conformité aux standards et niveaux de sécurité suivants :

TESSI SIGN CERTIFIED		ETSI	Profil
Signature	1.2.250.1.177.3.2.1	EN 319 411-1 LCP	Particulier

En cas d'incohérence entre cette DPC et ces exigences, ces exigences ont préséance sur cette DPC.

1.2 Nom et identification du document

La présente DPC peut être identifiée par le nom de l'AC racine « Tessi CA » et de l'AC intermédiaire « Tessi Sign Certified », ainsi que par son OID : 1.2.250.1.177.3.2.2. Elle décrit les dispositions mises en œuvre pour répondre aux engagements formulés dans la PC ayant l'OID suivant : 1.2.250.1.177.3.2.1. Les certificats d'AC intermédiaires et finaux délivrés sous cette AC racine disposent également d'un OID permettant d'identifier clairement les pratiques de cette DPC qui lui sont applicables.

1.3 Révision du document

Le tableau ci-dessous présente l'historique de cette DPC.

Ver.	Date	Modifications apportées
1.0	04/01/2023	Création

1.4 Entités intervenant dans l'IGC

1.4.1 Autorité de certification

L'AC a en charge la fourniture des prestations de gestion des certificats tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation, …) et s'appuie pour cela sur une infrastructure technique : une IGC. L'AC est responsable de la mise en application de la PC à l'ensemble de l'IGC qu'elle a mise en place.

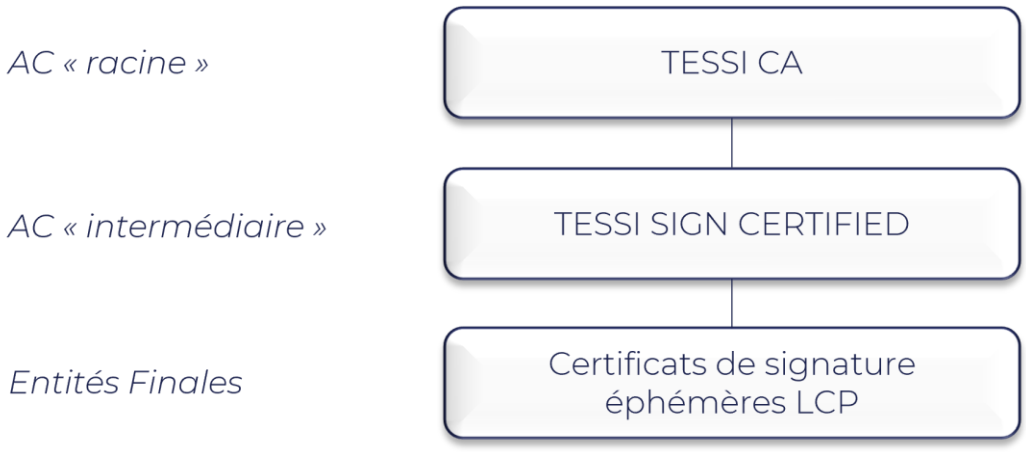
Pour les certificats signés en son nom, l'AC assure les fonctions suivantes :

- Fonctions d'enregistrement et de renouvellement ;
- Fonction de génération des certificats ;
- Fonction de génération d'éléments secrets ;
- Fonction de publication des conditions générales, de la PC, des certificats d'AC et des formulaires de demande de certificat ;
- Fonction de gestion des révocations ;
- Fonction d'information sur l'état des certificats via la liste des certificats révoqués (LCR) mise à jour à intervalles réguliers et selon un mode requête/réponse en temps réel (OCSP) ;
- L'archivage des dossiers de demande de certificat.

L'AC assure ces fonctions directement ou en les sous-traitant, tout ou partie. Dans tous les cas, l'AC en garde la responsabilité. L'AC s'engage à respecter les obligations décrites dans la PC associée. Elle s'engage également à ce que les composants de l'IGC, internes ou externes à l'AC, auxquels elles incombent les respectent aussi.

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

La hiérarchie couverte par la présente PC est la suivante :



1.4.2 Autorité d'enregistrement

L'AE assure les fonctions suivantes déléguées par l'AC, en vertu de la présente DPC :

- La prise en compte et la vérification des informations du futur Porteur et la constitution du dossier d'enregistrement correspondant ;
- L'établissement et la transmission de la demande de certificat à l'AC ;
- La conservation et la protection en confidentialité et intégrité des données personnelles d'authentification du RC, du Porteur ou du Mandataire de Certification (MC) ;
- La vérification des demandes de révocation de certificat.

L'AE assure ces fonctions directement ou en les sous-traitant à des autorités d'enregistrement externes ou à des autorités d'enregistrement déléguées (cf. chapitre 1.4.7 Autres participants). Dans tous les cas, l'AE garde la responsabilité de ces fonctions.

Dans le cas d'une AE externe, les missions de l'AE sont réparties de la manière suivante :

<table>
<tr><th></th><th>CERTIGNA</th><th>AE Externe</th></tr>
<tr><td>Diffusion des CGU aux porteurs</td><td></td><td>AE Externe</td></tr>
<tr><td>Collecte de l'acceptation des CGU</td><td></td><td>AE Externe</td></tr>
<tr><td>Collecte des informations des porteurs</td><td></td><td>AE Externe</td></tr>
<tr><td>Vérification des informations des porteurs</td><td></td><td>AE Externe (opérateur ou vérification automatisée)</td></tr>
<tr><td>Collecte de l'acceptation du certificat</td><td></td><td>AE Externe</td></tr>
<tr><td>Génération de la donnée d'activation</td><td>CERTIGNA ou</td><td>AE Externe</td></tr>
<tr><td>Communication de la donnée d'activation au porteur</td><td>CERTIGNA ou</td><td>AE Externe</td></tr>
<tr><td>Archivage des dossiers d'enregistrement</td><td>CERTIGNA ou</td><td>AE Externe</td></tr>
<tr><td>Collecte des demandes de révocation</td><td colspan="2" rowspan="3">Non applicable
Pas de révocation sur certificats éphémères</td></tr>
<tr><td>Vérification des demandes de révocation</td></tr>
<tr><td>Archivage des demandes de révocation</td></tr>
</table>

Sauf indication contraire, dans le présent document, la mention AE couvre l'autorité d'enregistrement et les autorités d'enregistrement externes et déléguées.

(*) : Pour les certificats destinés aux professionnels, l'AE offre la possibilité à l'entité cliente d'utiliser un Mandataire de Certification (MC) désigné et placé sous sa responsabilité pour effectuer tout ou partie des opérations de vérification des informations. Dans ce cas, l'AE s'assure que les demandes soient complètes et effectuées par un mandataire de certification dûment autorisé.

.

1.4.3 Responsable de certificat ou Porteur

Deux termes différents sont utilisés dans cette DPC lorsqu'il s'agit d'évoquer la personne qui se voit délivrer un certificat et gérer ce dernier :

- On parlera du « Responsable du certificat » (RC) lorsque le certificat délivré est destiné à un service applicatif ou à un serveur, tel qu'un service de cachet ou un serveur web. Le RC est la personne en charge de la gestion du certificat, mais n'est pas désigné explicitement dans ce certificat de personne morale.
- On parlera du « Porteur » lorsque le certificat délivré est destiné à une personne physique, pour signer, s'authentifier ou chiffrer des données. Le porteur est alors la personne physique désignée explicitement dans le certificat.

Le RC ou le Porteur doit respecter les conditions et obligations de cette PC et des CGU.

1.4.3.1 Responsable du certificat d'une AC

Pour l'AC racine et les AC intermédiaires, le RC ne peut être que l'Autorité de Certification CERTIGNA.

1.4.3.2 Porteur d'un certificat de personne physique

LCP	Signature
Un porteur de certificat ne peut être qu'une personne physique, acteur du secteur privé ou du secteur public. Cette personne utilise sa clé privée et le certificat correspondant dans le cadre de ses activités personnelles.	

1.4.4 Utilisateurs de certificats

Les utilisateurs de certificats doivent prendre toutes les précautions décrites dans la PC associée ainsi que dans les CGU.

1.4.5 Certificat d'AC

TESSI CA	*AC racine*
Entité ou personne physique qui utilise un certificat d'autorité racine et qui s'y fie pour vérifier l'origine et la validité d'un certificat émis par cette autorité.	
AC intermédiaires	*AC intermédiaire*
Entité ou personne physique qui utilise un certificat d'autorité intermédiaire et qui s'y fie pour vérifier l'origine et la validité d'un certificat émis par cette autorité.	

1.4.6 Certificat de personne physique

Un utilisateur de certificat de signature peut être notamment :

- 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.

1.4.7 Autres participants

1.4.7.1 Autorité d'enregistrement externe

L'AC peut s'appuyer sur une AE externe qui est autonome pour réaliser les missions de l'AE. Les engagements de l'AE à l'égard de l'AC sont précisés dans un contrat écrit avec cette AE externe. L'AC déterminera si les moyens humains et techniques mis en œuvre par l'AE pour réaliser ses missions d'AE permettent de répondre aux exigences de la PC associée.

1.4.7.2 Autorité d'enregistrement déléguée

L'AE s'appuie également sur des AED pour sous-traiter une partie des fonctions de l'AE. Un opérateur d'AED a le pouvoir :

- De traiter une demande de certificat ou de renouvellement de certificat ;
- De traiter une demande de révocation de certificat.

Il assure pour l'AE, dans le contexte de la délivrance de certificat, la vérification d'identité des futurs Porteurs dans les mêmes conditions et avec le même niveau de sécurité que ceux requis pour l'opérateur d'AE.

Les engagements de l'opérateur d'AED à l'égard de l'AE sont précisés dans un contrat écrit avec l'AC ou l'AE.. L'AED doit effectuer de façon impartiale et scrupuleuse les contrôles d'identité et des éventuels attributs des futurs Porteurs, et respecter les parties de la présente DPC et de la Déclaration des Pratiques de Certification (DPC) lui incombant et notamment les engagements des chapitres 3 et 4.

1.4.7.3 Service clients

Pour assurer un service réactif et conforme aux exigences, Certigna peut recourir à un prestataire spécialisé dans les « Services clients » afin d'assister ses prospects et clients dans leurs demandes relatives aux certificats, A cette fin, les opérateurs de cette entité sont enrôlés en tant qu'opérateur d'AE ou d'AED pour leur permettre d'accéder aux dossiers de demande et d'assister au mieux les Porteurs dans leurs démarches.

Un contrat similaire au contrat avec un AED est établi avec l'entité en charge de ce service. Le prestataire s'engage ainsi à respecter les parties de la PC et de la présente DPC lui incombant, et notamment les engagements des chapitres 3 et 4.

1.4.7.4 Hébergeurs de l'infrastructure technique

Certigna peut recourir à un prestataire pour l'hébergement physique de son infrastructure technique. Un contrat est établi avec le prestataire pour garantir la sécurité des services conformément aux engagements du chapitre 5.1 de la Politique de Certification.

1.5 Usage des certificats

1.5.1 Domaines d'utilisation applicables

LCP
Les certificats électroniques sont utilisés par des applications pour lesquelles les besoins de sécurité sont moyens eu égard aux risques qui les menacent.

1.5.1.1 Certificat d'AC

CERTIGNA ROOT CA	*AC racine*
La bi-clé d'AC racine est utilisée pour la signature des certificats d'AC intermédiaires et des Listes de certificats d'AC Révoqués (LAR).	
TESSI SIGN CERTIFIED	*AC intermédiaire*
La bi-clé d'AC intermédiaire est utilisée pour la signature des certificats finaux et des Listes de Certificats Révoqués (LCR).	

1.5.1.2 Certificat de personne physique

L'utilisation la clé privée est strictement limitée à la création de signatures électroniques avancées au sens du Règlement européen N°910/2014 (eIDAS).

Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.

1.5.2 Domaines d'utilisation interdits

Les usages autres que ceux cités dans le paragraphe précédent sont interdits. L'AC s'engage à respecter ces restrictions et à imposer leur respect par les Porteurs et les utilisateurs de certificats. A cette fin, elle publie à destination des Porteurs et des utilisateurs potentiels des CGU qui peuvent être consultées sur le site https://www.certigna.com ou sur le site de l'AE externe, avant toute demande de certificat ou toute utilisation d'un certificat.

1.6 Gestion de la PC

1.6.1 Entité gérant la PC

L'AC dispose d'un Comité de Sécurité responsable de l'élaboration, du suivi et de la modification de la PC et de la présente Déclaration des Pratiques de Certification (DPC). Il statue sur toute modification nécessaire à apporter à la PC à échéance régulière.

La validation formelle de la PC, de la DPC et des CGU est assurée à minima par une personne dans un rôle de confiance de contrôleur et d'une personne dans un rôle de confiance d'Officier de sécurité.

1.6.2 Point de contact

CERTIGNA
20 allée de la Râperie
Zone de la plaine
59650 Villeneuve d'Ascq
FRANCE

Contact mail : contact@certigna.fr
Téléphone : 0 806 115 115 (Service gratuit)

1.6.3 Entité déterminant la conformité de la DPC avec la PC

Le Comité de Sécurité s'assure de la conformité de la DPC par rapport à la PC. Il peut le cas échéant se faire assister par des experts externes pour s'assurer de cette conformité.

1.6.4 Procédures d'approbation de la conformité de la DPC

La DPC traduit en termes technique, organisationnel et procédural les exigences de la PC en s'appuyant sur la politique de sécurité de l'entreprise. Le Comité de Sécurité s'assure que les moyens mis en œuvre et décrits dans cette DPC répondent à ces exigences selon le processus d'approbation mis en place. Un contrôle de conformité de la DPC par rapport à la PC est effectué lors des audits internes et externes réalisés en vue de la qualification de l'AC.

Toute demande de mise à jour de la DPC suit également ce processus.

Toute nouvelle version approuvée de la DPC est publiée sans délai.

1.7 Définitions et acronymes

1.7.1 Définitions

Les termes utiles à la bonne compréhension de la PC sont les suivants :

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification.

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

Autorité de Certification – 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).

Certificat électronique - Fichier électronique attestant du lien entre une clé publique et l'identité de son propriétaire (personne physique ou service applicatif). Cette attestation prend la forme d'une signature électronique réalisée par un PSCE. Il est délivré par une AC. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

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

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

Dispositif de protection des éléments secrets - Désigne un dispositif de stockage des éléments secrets remis au porteur ou au responsable du certificat (ex. clé privée, code PIN, ...). Il peut prendre la forme d'un module cryptographique, d'une carte à puce, d'une clé USB à capacité cryptographique ou se présenter au format logiciel (ex. fichier PKCS#12).

Entité - Désigne une autorité administrative ou une entreprise au sens le plus large, c'est à dire également les personnes morales de droit privé de type associations. Il peut s'agir d'une organisation privée, d'une entité gouvernementale, d'une entité commerciale ou d'une entité non commerciale.

Entité commerciale - Toute entité qui n'est ni une organisation privée, ni une autorité administrative ou une entité non-commerciale. Cette définition couvre par exemple des partenariats généraux, des associations non constituées ainsi que des entreprises individuelles.

Existence légale - Une entité privée, une entité publique, une entité commerciale ou une entité non commerciale a une existence légale si elle a été formellement validée et n'est pas liquidée, dissolue ou abandonnée.

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

Liste des certificats d'AC révoqués - Liste comprenant les numéros de série des certificats des autorités intermédiaires ayant fait l'objet d'une révocation, et signée par l'AC racine.

Liste des Certificats Révoqués - Liste comprenant les numéros de série des certificats ayant fait l'objet d'une révocation, et signée par l'AC émettrice.

Organisation privée - toute entité qui n'est pas une entité publique (cotée ou non en bourse) enregistrée dont l'existence a été créée au travers d'un dépôt (ou d'un acte) auprès d'un organisme d'enregistrement des sociétés au niveau de sa juridiction d'immatriculation. En France, cette immatriculation s'effectue au niveau du registre du commerce et des sociétés.

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

Porteur de certificat – Personne identifiée dans le certificat de personne physique et qui est la détentrice de la clé privée correspondant à la clé publique.

Prestataire de services de certification électronique (PSCE) - Toute personne ou entité qui est responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des porteurs et utilisateurs de ces certificats.

Produit de sécurité - Un dispositif logiciel ou matériel qui met en œuvre des fonctions de sécurité nécessaires à la sécurisation d'une information ou d'un système.

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

Qualification d'un prestataire de services de certification électronique - Le Décret RGS et le Règlement européen eIDAS décrivent les procédures de qualification des PSCO. Un PSCE étant un PSCO particulier, la qualification d'un PSCE est un acte par lequel un organisme de certification atteste de la conformité de tout ou partie de l'offre de certification électronique d'un PSCE (famille de certificats) à certaines exigences d'une PC Type pour un niveau de sécurité donné et correspondant au service visé par les certificats.

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

Représentant légal : Une personne d'une entité privée, d'une entité publique, ou d'une entité commerciale qui en est soit un propriétaire, un associé, un membre de la direction, le directeur ou un responsable, tel qu'identifié dans sa fiche de poste, ou un employé, un contractant, ou un agent autorisé par l'entité pour gérer l'activité en lien avec la demande, la délivrance et l'utilisation des certificats.

Responsable du certificat - Personne en charge et responsable du certificat électronique de service applicatif.

RSA - Algorithme à clés publiques du nom de ses inventeurs (Rivest, Shamir et Adleman).

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

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

Utilisateur de certificat - Entité ou personne physique qui utilise un certificat et qui s'y fie pour vérifier une signature électronique provenant d'un porteur de certificat.

1.7.2 Acronymes

Les acronymes utiles à la bonne compréhension de ce document sont les suivants :

AA	Autorité Administrative
AC	Autorité de Certification
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
CGU	Conditions Générales de Vente et d'Utilisation
CNIL	Commission Nationale de l'Informatique et des Libertés
CSR	Certificate Signing Request
DBA	Doing Business As (Marque)
DN	Distinguished Name
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
ICD	International Code Designator
IGC	Infrastructure de Gestion de Clés (= PKI : Public Key Infrastructure)
INPI	Institut National de la Propriété Industrielle
LAR	Liste des certificats d'AC Révoqués
LCR	Liste des Certificats Révoqués
MC	Mandataire de Certification
OC	Opérateur de Certification
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PC	Politique de Certification
PCA	Plan de Continuité d'Activité
PP	Profil de Protection
PKCS	Public Key Cryptographic Standards
PSCE	Prestataire de Services de Certification Électronique
PSCO	Prestataire de Services de Confiance
RC	Responsable du Certificat Cachet Serveur
RSA	Rivest Shamir Adleman
SSI	Sécurité des Systèmes d'Information
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

2 RESPONSABILITE CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS

2.1 Publication

2.1.1 Entités chargées de la mise à disposition des informations

L'AC met à disposition des utilisateurs et des applications utilisatrices des certificats qu'elle émet des informations sur l'état de révocation des certificats en cours de validité émis par l'AC.

2.1.2 Informations devant être publiées

L'AC publie à destination des Porteurs et des utilisateurs de certificats :
- La PC ;
- La DPC ;
- Les Conditions Générales d'Utilisation liées au service de certification ;
- Les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, ...) ;
- Le certificat d'AC racine et les certificats d'AC intermédiaires en cours de validité ;
- Les listes des certificats révoqués (LAR / LCR).

Remarque : compte tenu de la complexité de lecture d'une DPC pour les personnes non spécialistes du domaine, l'AC publie en dehors des PC et DPC des CGU que le futur Porteur est dans l'obligation de lire et d'accepter lors de toute demande de certificat (demandes initiales et suivantes, en cas de renouvellement) auprès de l'AE.

2.2 Publication de la documentation

2.2.1 Publication de la PC, des conditions générales et des formulaires

La PC, la DPC, les CGU et les différents formulaires nécessaires pour la gestion des certificats sont publiés sous forme électronique à l'adresse http://www.certigna.com. Ces informations sont également publiées à l'adresse http://www.dhimyotis.com.

La diffusion des CGU auprès des futurs Porteurs de certificat peut être sous-traiter à l'AE ou à un AED.

2.2.2 Publication de la DPC

L'AC publie, à destination des Porteurs et des utilisateurs de certificats, sa DPC pour rendre possible l'évaluation de la conformité avec sa PC. Les détails relatifs à ses pratiques ne sont toutefois pas rendus publics.

2.2.3 Publication des certificats d'AC

Les Porteurs et les utilisateurs de certificat peuvent accéder aux certificats d'AC qui sont à l'adresse suivante https://www.certigna.com/autorite-crl ou directement via les adresses listées dans le tableau suivant. Afin de garantir cette disponibilité et une reprise rapide en cas de sinistre, plusieurs sites répliqués ont été mis en place. Afin de détecter et de corriger dans les meilleurs délais tout incident survenant lors de l'exploitation de l'un des sites, les mesures suivantes ont notamment été mises en place :

- Instauration d'astreinte pendant les heures non ouvrées ;
- Souscription d'un service de surveillance de sécurité (24 heures sur 24) ;
- Installation et exploitation d'un logiciel de supervision permettant de surveiller tous les éléments constitutifs de la plate-forme technique et d'émettre en temps réel des alertes en cas de détection d'incident ;
- Développement et mise en place de scripts permettant d'automatiser et de simplifier la répartition de charge d'un site à l'autre.

TESSI CA	
Certificat d'AC	http://autorite.certigna.fr/tessi_ca.der http://autorite.dhimyotis.com/tessi_ca.der
TESSI SIGN CERTIFIED	
Certificat d'AC	http://autorite.certigna.fr/tessi_sign_certified.der http://autorite.dhimyotis.com/tessi_sign_certified.der

2.2.4 Publication de la LAR

La liste des certificats d'autorités de certification révoqués est publiée au format électronique aux adresses du tableau ci-dessus. Ces adresses sont également indiquées dans les certificats.

TESSI CA et AC intermédiaires	
LAR	http://crl.certigna.fr/tessica.crl http://crl.dhimyotis.com/tessica.crl

2.2.5 Publication de la LCR

La liste des certificats finaux révoqués est publiée au format électronique aux adresses du tableau ci-dessus. Ces adresses sont également indiquées dans les certificats émis par l'AC.

TESSI SIGN CERTIFIED	
LCR	http://crl.certigna.fr/tessi_sign_certified.crl http://crl.dhimyotis.com/tessi_sign_certified.crl

2.3 Délais et fréquences de publication

2.3.1 Publication de la documentation

La PC, la DPC, les CGU et les différents formulaires nécessaires pour la gestion des certificats sont mis à jour si nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC. La

fonction de publication de ces informations (hors informations d'état des certificats) est disponible les jours ouvrés.

2.3.2 Publication des certificats d'AC

Les certificats d'AC sont diffusés préalablement à toute diffusion de certificats émis par l'AC et de LCR correspondants. La disponibilité des systèmes publiant les certificats d'AC est garantie 24 heures sur 24, 7 jours sur 7.

2.3.3 Publication de la LAR

La LAR est mise à jour au minimum une fois par an, et à chaque nouvelle révocation.

2.3.4 Publication de la LCR

La LCR est mise à jour au minimum toutes les 24 heures, et à chaque nouvelle révocation.

2.4 Contrôle d'accès aux informations publiées

L'accès aux informations publiées à destination des utilisateurs est libre. L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC.

2.5 Signaler un certificat malveillant ou dangereux

Pour signaler un certificat malveillant ou dangereux (un certificat dont la clé privée est suspectée de compromission, un certificat dont l'usage n'est pas respecté, ou tout autre type de fraude : détournement d'usage, conduite inappropriée, etc.) ou tout autre problème relatif aux certificats, veuillez utiliser le formulaire de contact disponible à l'adresse suivante https://www.certigna.com/contactez-nous/ et sélectionner l'objet « Certificat jugé malveillant ou dangereux ».

3 IDENTIFICATION ET AUTHENTIFICATION

3.1 Nommage

3.1.1 Types de nom

Dans chaque certificat conforme à la norme X.509, l'AC émettrice (correspondant au champ « issuer ») et la personne physique (champ « subject ») sont identifiés par un « Distinguished Name » (DN) répondant aux exigences de la norme X.501.

3.1.2 Nécessité d'utilisation de noms explicites

Le DN du certificat permet d'identifier la personne physique et est construit à partir de l'identité du Porteur telle que figurant sur les justificatifs présentés lors de son enregistrement et son authentification auprès de l'AE.

Le format du DN est défini au chapitre « 7.2 Profils des certificats et des LCR » de cette DPC.

Le DN des certificats des porteurs est constitué des champs suivants :

- SerialNumber (SN) : un numéro de série de caractères constituée en partie d'un aléa, afin de garantir l'unicité du DN ;
- Common Name (CN) : Prénom (à minima le premier prénom) et le nom (à minima le nom patronymique) figurant sur la pièce d'identité du porteur ;
- Given Name (GN) : le premier Prénom figurant sur la pièce d'identité du porteur ;
- Surname (SN) : le nom patronymique figurant sur la pièce d'identité du porteur ;
- Country (C) : le Pays auprès duquel le Porteur est enregistré.

3.1.3 Anonymisation ou pseudonymisation

L'AC n'émet pas de certificat comportant une identité anonyme.

3.1.4 Règles d'interprétation des différentes formes de nom

Aucune interprétation n'est faite sur le nom des certificats.

3.1.5 Unicité des noms

Note : L'attribut « serialNumber » présent dans le champ DN et le champ « serialNumber » du certificat sont des données distinctes. Par défaut, le format du « serialNumber » est défini avec un numéro aléatoire.

3.1.5.1 Certificat d'AC

TESSI CA & AC intermédiaires	*AC racine & intermédiaires*
L'AC garantit que les noms positionnés dans le champ CN des certificats d'AC intermédiaires sont uniques sur le périmètre de l'AC.	

3.1.5.2 Certificat de personne physique

LCP	Signature
La combinaison du pays, du nom et de l'adresse e-mail du Porteur de certificat identifie de manière univoque le titulaire du certificat. L'attribut « *serialNumber* », valeur unique attribuée à chaque certificat émis par l'AC et présente dans le DN, assure également l'unicité du DN. Ce champ est constitué à partir d'un numéro aléatoire unique géré par l'AC précédé de la lette « S » pour « Signature ».	

3.1.6 Identification, authentification et rôle des marques déposées

L'AC est responsable de l'unicité des noms des personnes morales et physiques utilisés dans ses certificats et de la résolution des litiges portant sur la revendication d'utilisation d'un nom. Cet engagement de responsabilité s'appuie sur le niveau de contrôle assuré lors du traitement des demandes de certificats. L'AC peut éventuellement vérifier l'appartenance de la marque auprès de l'INPI.

3.2 Validation initiale de l'identité

L'enregistrement d'un Porteur s'effectue directement auprès de l'AE, d'une AE Externe ou d'un AED.

Lors de la demande de certificat, l'adresse email du Porteur est vérifiée au travers de l'envoi d'un ou plusieurs emails dans le cadre du processus d'enregistrement sur le site de l'AE, de l'AE externe ou de l'AED. D'autres informations du porteur, telles que son numéro de téléphone peuvent être utilisées pour envoyer au Porteur une donnée d'activation lui permettant d'utiliser son certificat.

La demande de certificat est formulée par le Porteur via un moyen mis à disposition par l'AE ou l'AED tel qu'un formulaire sur un site web pour demander l'obtention d'un certificat, qui sera utilisé ensuite pour un service de signature de documents par exemple.

3.2.1 Méthode pour prouver la possession de la clé privée

L'AC assure la génération et la gestion de la bi-clé du Porteur durant toute sa durée de validité.

Une donnée d'activation est mise à la disposition du Porteur (Ex : via l'envoi d'un OTP par SMS sur le numéro de mobile du Porteur), afin de lui permettre d'utiliser à distance sa bi-clé hébergée par l'AC.

3.2.2 Authentification de l'organisation

Sans objet. Les certificats émis par la présente DPC sont destinés aux particuliers.

3.2.3 Authentification de l'identité du Porteur

Pour authentifier l'identité d'un Porteur, la vérification de la photocopie d'une pièce d'identité de l'individu est nécessaire.

La donnée d'activation fournie au Porteur permet également de l'authentifier lors de sa demande de certificat et de l'usage de son certificat. Les opérateurs d'AE et d'AED sont sensibilisés sur les fraudes qui peuvent intervenir sur la délivrance de documents ou copies de documents officiels. Une attention particulière est apportée aux contrôles de validité des pièces fournies (date de validité des pièces d'identité, date des demandes, etc.). Dans le cas de l'utilisation d'un système de contrôle d'identité automatisé, des tests sont réalisés par l'AE pour s'assurer de l'efficacité du système quant à la vérification des pièces d'identité fournies et des informations qui en sont extraites pour la production du certificat.

3.2.3.1 Certificat d'AC

CERTIGNA ROOT CA et AC intermédiaires	*AC racine et intermédiaires*
L'enregistrement d'une nouvelle demande de certificat d'AC est réalisé auprès de l'AE par le responsable de l'Autorité de certification. Cette demande est formalisée au travers du script rempli lors de la cérémonie des clés ayant servi à la génération du certificat.	

3.2.3.2 Certificat de personne physique

LCP	*Signature*
La demande de certificat est réalisée depuis le formulaire en ligne disponible sur le site de CERTIGNA, de l'AE Externe ou de l'AED. Une fois complété, les éléments suivants sont transmis à l'AE : - La demande de certificat produite via le site et désignant le futur Porteur et ses coordonnées, ainsi que les CGU applicables ; - La photocopie numérisée d'un document officiel d'identité en cours de validité du futur Porteur comportant une photographie d'identité (CNI, Passeport ou titre de séjour).	

La liste précise des pièces d'identité recevables est définie dans les procédures de l'AE, et le contrat reliant l'AC et l'AE Externe, le cas échéant. Cette liste est présentée aux futurs porteurs sur le site de l'AC ou de l'AE permettant de formuler la demande de certificat.

3.2.4 Informations non vérifiées du RC ou Porteur

Sans objet.

3.2.5 Validation de l'autorité du Porteur et des signatures

Cette étape est effectuée en même temps que la validation de l'identité du Porteur (directement par l'AE, l'AE Externe ou l'AED).

3.2.6 Critères d'interopérabilité ou de certification

L'AC divulgue tous les certificats croisés qui identifient l'AC en tant que sujet, à condition que l'AC ait organisé ou accepté l'établissement de la relation de confiance (c'est-à-dire le certificat croisé en cause).

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

3.3.1 Identification et authentification d'une demande de renouvellement courant

L'AC n'émet pas de nouveau certificat pour une bi-clé précédemment émise. Le renouvellement passe par la génération d'une nouvelle bi-clé et d'une nouvelle demande de certificat.

3.3.1.1 Certificat d'AC

L'identification et l'authentification d'une demande de renouvellement courant de certificat d'AC sont identiques à la demande initiale.

3.3.1.2 Certificat de personne physique

LCP	*Signature*
Non applicable. Les certificats éphémères ne font pas l'objet d'un renouvellement.	

3.3.2 Identification et authentification pour un renouvellement après révocation

LCP	*Signature*
Non applicable. Les certificats de signature éphémères des Porteurs ne font pas l'objet de révocation.	

3.4 Identification et authentification d'une demande de révocation

3.4.1 Certificat d'AC

La révocation d'un certificat d'AC ne peut être décidée que par l'entité responsable de l'AC, ou par les autorités judiciaires via une décision de justice. La révocation des autres certificats de composantes est décidée par l'entité opérant la composante concernée qui doit en informer l'AC sans délai.

3.4.2 Certificat de personne physique

LCP	*Signature*
Non applicable. Les certificats éphémères ne font pas l'objet de révocation.	

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

4.1.1.1 Certificat d'AC

La demande de certificat doit émaner d'un représentant légal de l'AC.

4.1.1.2 Certificat de personne physique

La demande de certificat est établie via un service en ligne mis en œuvre par l'AE, l'AE Externe ou l'AED pour l'enregistrement du Porteur.

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

4.1.2.1 Certificat d'AC

Le dossier de demande est établi directement par le responsable de l'AC lors de la Cérémonie des clés.

4.1.2.2 Certificat de personne physique

La demande de certificat est établie via un service en ligne mis en œuvre par l'AE, l'AE Externe ou l'AED pour l'enregistrement du Porteur.

Lors de l'enregistrement du futur Porteur, ce dernier doit fournir une adresse email qui permet à l'AE de prendre contact avec le Porteur pour toute question relative à son enregistrement.

4.2 Traitement d'une demande de certificat

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

4.2.1.1 Certificat d'AC

La demande est validée par l'ensemble des témoins présents lors de la cérémonie des clés parmi lesquels figurent obligatoirement un administrateur de l'AE.

4.2.1.2 Certificat de personne physique

L'AE effectue les opérations suivantes lors du traitement d'une demande de certificat qui lui a été transmise :

- Validation de l'identité du Porteur ;
- Validation du dossier et de la cohérence des justificatifs présentés ;
- Assurance que le futur Porteur a pris connaissance des modalités applicables pour l'utilisation du certificat.

Toutes les opérations citées ci-dessus sont réalisées par l'AE. L'identité du futur Porteur est approuvée si les pièces justificatives fournies sont valides à la date de réception.

Un dossier de demande de certificat (dossier d'enregistrement) du porteur se compose des informations d'identité du Porteur et des preuves d'acceptation des CGU et du contenu prévu ou placé dans son certificat. Le dossier peut inclure la copie de la pièce d'identité ayant servi à l'authentification et l'identification du porteur, ou bien uniquement certaines informations constitutives de cette pièce d'identité (Ex : Numéro d'identification de la pièce d'identité, nom et prénom y figurant, date d'expiration, type, etc.).

Le dossier d'enregistrement du futur Porteur est conservé selon les modalités définies dans la convention entre l'AC et l'AE :
- Soit par l'AE Externe pendant au moins 7 après la fin de validité du certificat ;
- Soit par l'AC après avoir été transmis par l'AE ou l'AE Externe pour archivage.

4.2.2 Acceptation ou rejet de la demande de certificat

Après traitement de la demande, l'AE notifie le rejet éventuel de la demande au Porteur.

La justification d'un éventuel refus est effectuée par l'AE en précisant la cause (Ex : justificatif invalide).

En cas de validation par l'AE, de la demande de certificat, l'AE opère une demande à l'AC de génération de la bi-clé et du certificat du futur Porteur. LAE assure la présentation des informations prévues ou contenues dans le certificat au futur Porteur.

4.2.3 Durée d'établissement du certificat

4.2.3.1 Certificat d'AC

La demande de certificat d'AC étant formellement établie lors de la cérémonie des clés, le certificat concerné est généré dans les heures qui suivent la demande.

4.2.3.2 Certificat de personne physique

Le certificat est établi après la réception par l'AC du dossier complet du porteur validé et envoyé par l'AE.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

4.3.1.1 Certificat d'AC

Les bi-clés et certificats de l'AC racine et les AC intermédiaires sont générées lors de cérémonie des clés. Les opérations de génération et de signature des certificats émis par l'AC racine sont effectuées dans les mêmes circonstances contrôlées que la génération des bi-clés d'AC (cf. 6.1.1), en présence de personnes dans des rôles de confiance autorisées par l'AC et dans le cadre de « cérémonies de clés ». L'administrateur d'AC effectue les commandes de génération et de signature des certificats par l'AC racine en présence des rôles de confiance qui s'assurent de la conformité des pratiques avec les exigences de sécurité et le script défini.

4.3.1.2 Certificat de personne physique

Suite à la validation de la demande de certificat par l'AE, l'AC déclenche le processus de génération du certificat destiné au Porteur. 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

4.3.2.1 Certificat d'AC

La remise du certificat d'AC est réalisée lors de la cérémonie des clés, auprès d'un administrateur de l'AC habilité par l'AC en charge de son exploitation et de sa diffusion.

4.3.2.2 Certificat de personne physique

Le certificat complet et exact est conservé par l'AC, et envoyé à l'AE.

Dans le cas où le certificat est utilisé par le Porteur pour signer des documents électroniques par exemple, le Porteur pourra accéder au certificat dans la signature électronique des documents en question (sous réserve que ces documents soient mis à la disposition du Porteur par l'AE ou l'AED).

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

4.4.1.1 Certificat d'AC

Le représentant de l'autorité et les différents témoins, présents lors la cérémonie, contrôlent que le contenu du certificat est conforme à la demande. L'acceptation est formalisée au travers du procès-verbal de la cérémonie des clés.

4.4.1.2 Certificat de personne physique

L'AE doit présenter au Porteur les informations prévues ou contenues dans le certificat avant sa première utilisation. L'utilisation du certificat par son Porteur vaut acceptation tacite du certificat.

En cas de détection d'incohérence entre les informations prévues ou figurant dans le certificat ou dans l'accord contractuel, le Porteur ne doit pas accepter la génération ou l'utilisation du certificat avant son expiration.

4.4.2 Publication du certificat

4.4.2.1 Certificat d'AC

Les certificats d'AC Racine et d'AC intermédiaires sont publiés par l'AC. Cf. chapitre 2.

4.4.2.2 Certificat de personne physique

Aucune publication du certificat du Porteur n'est effectuée par l'AC dans le cadre du processus de délivrance de certificat.

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

L'AE est informée de la génération du certificat par l'AC qui est responsable de la gestion du certificat généré.

4.5 Usages de la bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat

Le Porteur doit respecter strictement les usages autorisés des bi-clés et des certificats décrits au chapitre 1.5.1. Dans le cas contraire, sa responsabilité pourrait être engagée.

L'usage autorisé de la bi-clé et du certificat associé est indiqué dans le certificat lui-même, via l'extension Key Usage le cas échéant.

Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du Porteur par l'AE avant la délivrance du certificat. Elles sont consultables préalablement à toute demande de certificat en ligne et sont accessibles sur le site https://www.certigna.com.

Les CGU acceptées lors de la demande de certificat restent applicables pendant toute la durée de vie du certificat.

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

Les utilisateurs de certificats doivent respecter strictement les usages autorisés des certificats et cités au chapitre 1.5.1. Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6 Renouvellement d'un certificat

L'AC n'émet pas de nouveau certificat pour une bi-clé précédemment émise. Le renouvellement passe par la génération d'une nouvelle bi-clé et une nouvelle demande de certificat (cf. chapitre 4.1).

4.6.1 Circonstance pour le renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification de la délivrance d'un nouveau certificat

Sans objet.

4.6.5 Modalité d'acceptation d'un nouveau certificat

Sans objet.

4.6.6 Publication du renouvellement du certificat par l'AC

Sans objet.

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

Sans objet.

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

4.7.1 Causes possibles de changement d'un bi-clé

4.7.1.1 Certificat d'AC

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des AC et les certificats correspondants, sont renouvelés régulièrement (cf. période de validité chapitre 6.3.2). Par ailleurs, une bi-clé et un certificat peuvent être renouvelés par anticipation, suite à la révocation du certificat.

4.7.1.2 Certificat de personne physique

LCP	*Signature*
Non applicable. Les certificats de signature éphémères des Porteurs ne font pas l'objet de renouvellement	

4.7.2 Origine d'une demande d'un nouveau certificat

4.7.2.1 Certificat d'AC

La demande de certificat doit émaner d'un représentant légal de l'AC.

4.7.2.2 Certificat de personne physique

LCP	*Signature*
Non applicable. Les certificats de signature éphémères des Porteurs ne font pas l'objet de renouvellement	

4.7.3 Traitement d'une demande de changement de clé

Cf. chapitre 4.2.1

4.7.4 Notification de la délivrance d'un nouveau certificat

Cf. chapitre 4.3.2.

4.7.5 Modalité d'acceptation d'un nouveau certificat

Cf. chapitre 4.4.1.

4.7.6 Publication du renouvellement du certificat par l'AC

Cf. chapitre 4.4.2.

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

Cf. chapitre 4.4.3.

4.8 Modification du certificat

La modification des certificats d'AC ou de Porteur n'est pas autorisée. En cas de nécessité de changement d'informations présentes dans le certificat (principalement le DN), un nouveau certificat doit être délivré après révocation de l'ancien.

4.8.1 Circonstance pour la modification d'un certificat

Sans objet.

4.8.2 Origine d'une demande de modification de certificat

Sans objet.

4.8.3 Traitement d'une demande de modification de certificat

Sans objet.

4.8.4 Notification de la délivrance d'un nouveau certificat

Sans objet.

4.8.5 Modalité d'acceptation d'un certificat modifié

Sans objet.

4.8.6 Publication du certificat modifié par l'AC

Sans objet.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

4.9.1.1 Raisons pour révoquer un certificat d'AC

Une ou plusieurs des circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'AC racine ou d'AC intermédiaire sous 7 jours :

- L'AC demande la révocation du certificat ;
- L'AC notifie l'AC émettrice que la demande de certificat originale n'était pas autorisée et n'accorde pas d'autorisation rétroactive ;
- L'AC obtient la preuve que la clé privée de l'AC correspondant à la clé publique dans le certificat est compromise ou n'est plus conforme avec les exigences des chapitres 6.1.5 et 6.1.6 ;
- L'AC obtient la preuve que l'usage du certificat d'AC est détourné ;
- L'AC est informée que le certificat d'AC n'a pas été émis en conformité avec les exigences et pratiques formulées dans la PC ou la présente DPC ;
- L'AC détermine que les informations apparaissant dans le certificat d'AC sont inexactes ou trompeuses ;
- L'AC cesse toute activité pour une raison quelconque.

4.9.1.2 Raisons pour révoquer un certificat de personne morale ou physique

LCP	*Signature*
Non applicable. Les certificats de signature éphémères des Porteurs ne font pas l'objet de révocation.	

4.9.2 Origine d'une demande de révocation

4.9.2.1 Certificat d'AC

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

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

4.9.2.2 Certificat de personne physique

LCP	*Signature*
Non applicable. Les certificats de signature éphémères des Porteurs ne font pas l'objet de révocation.	

4.9.3 Procédure de traitement d'une demande de révocation

4.9.3.1 Certificat d'AC

Dans le cas où l'AC Racine décide de révoquer un certificat de l'AC (à la suite de la compromission d'une des clés privées), cette dernière informe par mail l'ensemble des Porteurs que leurs certificats ne sont plus valides car l'un des certificats de la chaîne de certification n'est plus valide.

Le contact identifié sur le site de l'ANSSI (https://www.ssi.gouv.fr) est immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification.

Le mécanisme de révocation est décrit dans la « Procédure opérationnelle de demande de révocation ». Le processus est détaillé dans la « Procédure de gestion des clés cryptographiques » et dans la « Procédure de gestion des certificats de composante ».

4.9.3.2 Certificat de personne physique

LCP	*Signature*
Non applicable. Les certificats de signature éphémères des Porteurs ne font pas l'objet de révocation.	

4.9.4 Délai accordé pour formuler la demande de révocation

4.9.4.1 Certificats d'AC

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

4.9.4.2 Certificat de personne physique

LCP	*Signature*
Sans objet. Les certificats de signature éphémères des Porteurs ne font pas l'objet de révocation.	

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

4.9.5.1 Certificats d'AC

La révocation d'un certificat d'AC est effectuée dès la détection d'un événement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat de signature de l'AC (signature de certificats/LCR) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

L'organisation et les moyens mis en œuvre en cas de révocation d'un certificat d'une composante de l'IGC sont décrits dans la « Procédure de gestion des clés cryptographiques » et dans la « Procédure de gestion des certificats de composante ».

4.9.5.2 Certificat de personne physique

LCP	*Signature*
Sans objet. Les certificats de signature éphémères des Porteurs ne font pas l'objet de révocation.	

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

L'utilisateur d'un certificat de Porteur est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée (LCR ou OCSP) est à l'appréciation de l'utilisateur selon leur disponibilité et les contraintes liées à son application.

4.9.7 Fréquence d'établissement des LAR/LCR

La LAR est émise au minimum tous les ans. En outre, une nouvelle LAR est systématiquement et immédiatement publiée après la révocation d'un certificat d'AC.

La LCR d'une AC intermédiaire est émise au minimum toutes les 24 heures. En outre, une nouvelle LCR est systématiquement et immédiatement publiée après la révocation d'un certificat.

4.9.8 Délai maximum de publication d'une LAR/LCR

Une LAR ou une LCR est publiée dans un délai maximum de 30 minutes suivant sa génération.

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

En complément de la publication des LCR sur les sites en ligne, l'AC met à disposition un répondeur OCSP conforme à la RFC 6960 et/ou à la RFC 5019. Le répondeur OCSP répond aux exigences d'intégrité, de disponibilité et de délai pour la publication décrite dans cette PC. Les réponses OCSP sont signées par un répondeur OCSP dont le certificat est signé par l'AC qui délivre le certificat dont l'état de révocation est vérifié.

4.9.10 Exigences sur la vérification en ligne de la révocation

Le répondeur OCSP opéré par l'AC supporte la méthode http GET, telle que décrite dans la RFC 6960 et/ou la RFC 5019. En complément de la publication des LCR sur les sites en ligne, l'AC met à disposition un répondeur OCSP accessible aux adresses suivantes :

TESSI SIGN CERTIFIED	
OCSP	URL=http://tessisigncertified.ocsp.certigna.fr URL=http://tessisigncertified.ocsp.dhimyotis.com

Le répondeur OCSP répond aux exigences d'intégrité, de disponibilité et de délai de publication décrites dans cette PC. Le répondeur OCSP supporté la méthode « http GET », telle que décrite dans la RFC 6960 et/ou la RFC 5019. Les informations fournies par le répondeur OCSP pour les certificats sont mises à jour tous les 4 jours au maximum, et les réponses OCSP ont une durée de validité de 7 jours. Les certificats révoqués et expirés sont maintenus dans les CRL et répondeurs OCSP.

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

4.9.12.1 Certificats d'AC

Pour les certificats d'AC, outre les exigences du chapitre 4.9.3 ci-dessus, la révocation suite à une compromission de la clé privée fait l'objet d'une information clairement diffusée au moins sur le site de Certigna et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

Les mesures mises en œuvre sont cadrées par la « Procédure de gestion des clés cryptographiques » et dans la « Procédure de gestion des certificats de composante ».

4.9.12.2 Certificat de personne physique

Le Porteur doit interrompre immédiatement et définitivement l'usage de sa clé privée et du certificat associé s'il a connaissance de la compromission de sa clé privée.

4.9.13 Suspension de certificat

Les certificats émis par les AC couvertes par cette PC ne peuvent pas être suspendus.

4.9.14 Origine d'une demande de suspension

Non applicable.

4.9.15 Procédure d'une demande de suspension

Non applicable.

4.9.16 Limites de la période de suspension

Non applicable.

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. La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LCR/LAR. Ces LCR/LAR sont des LCR au format V2, publiées sur le site http://www.certigna.com (accessible avec le protocole HTTP).

Les activités relatives au service de publication sont définies dans la « Procédure de gestion du service publication ».

4.10.2 Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24 heures/24, 7 jours/7.

La durée maximale d'indisponibilité de la fonction d'information d'état des certificats est :
- Par interruption (panne ou maintenance) de 4 heures (jours ouvrés) ;
- Par mois de 32 heures (jours ouvrés).

En cas de vérification en ligne du statut d'un certificat, le temps de réponse du serveur OCSP à la requête reçue est au maximum de 10 secondes. Il s'agit de la durée mesurée au niveau du serveur (requête reçue par le serveur et réponse au départ de ce dernier). La réplication des services sur plusieurs systèmes d'information permet d'assurer automatiquement une continuité des services en cas de sinistre. L'AC s'appuie également sur les astreintes de son personnel aux heures non-ouvrées pour assurer la supervision des alertes de disponibilités de ces fonctions.

4.10.3 Autres caractéristiques

Sans objet.

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

En cas de fin de relation contractuelle ou réglementaire entre l'AC et l'AE externe ou l'entité de rattachement du Porteur avant la fin de validité du certificat, l'AC laisse expirer le certificat du Porteur, sans permettre l'utilisation de la clé privée associée.

4.12 Séquestre de clé et recouvrement

Aucun séquestre des clés privées des Porteurs n'est réalisé par l'AC sous la forme d'une copie des clés privées. La clé privée du Porteur initiale est hébergée par l'AC, et n'est utilisable que sous le seul contrôle du Porteur et aucune copie n'est réalisée. La clé privée du porteur est supprimée dans l'heure qui suit l'expiration du certificat associé.

5 MESURES DE SECURITE NON TECHNIQUES

RAPPEL - L'AC a mené une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Sa DPC a été élaborée en fonction de cette analyse. La gestion des risques de sécurité de l'information est décrite dans la « Procédure de gestion des risques SI » ainsi que dans le formulaire « Gestion des risques SI ».

5.1 Mesures de sécurité physique

5.1.1 Situation géographique et construction des sites

Les systèmes d'information utilisés pour les fonctions de l'AC sont hébergés dans plusieurs centres de production présentant les mêmes caractéristiques en matière de sécurité. La localisation des sites ne présente pas de risques majeurs. Les risques sont identifiés dans le document « Gestion des risques SI ».

5.1.2 Accès physique

Un contrôle strict d'accès physique aux composants de l'IGC est effectué, avec journalisation des accès et vidéo-surveillance : le périmètre de sécurité défini autour des machines hébergeant les composantes de l'IGC n'est accessible qu'aux personnes disposant d'un rôle de confiance.

En dehors des heures ouvrables, la mise en œuvre de moyens de détection d'intrusion physique et logique renforce la sécurité de l'IGC. En outre, toute personne (prestataire externe, etc.) entrant dans ces zones physiquement sécurisées ne peut pas être laissée sans la surveillance d'une personne autorisée.

Les accès physiques aux centres de production de l'AC sont restreints au travers de mesures de contrôle d'accès physique. Les mesures mises en œuvre sont décrites dans la « Politique de sûreté ».

5.1.3 Alimentation électrique et climatisation

Des mesures concernant la fourniture d'énergie électrique et de climatisation sont prises pour répondre aux engagements de l'AC sur la garantie du niveau de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et les fonctions d'information sur l'état des certificats.

Les centres de production de l'AC sont équipés d'onduleurs et de groupes électrogènes. Les mesures mises en œuvre sont décrites dans la « Politique de sûreté ».

5.1.4 Vulnérabilité aux dégâts des eaux

Des mesures concernant la protection contre les dégâts des eaux sont prises pour répondre aux engagements de l'AC sur la garantie du niveau de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et les fonctions d'information sur l'état des certificats.

Des moyens pour la détection des fuites d'eaux sont positionnés dans les centres de production de l'AC. Les mesures mises en œuvre sont décrites dans la « Politique de sûreté ».

5.1.5 Prévention et protection incendie

Des mesures concernant la prévention et la protection contre les incendies sont prises pour répondre aux engagements de l'AC sur la garantie du niveau de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et les fonctions d'information sur l'état des certificats.

Les salles informatiques des centres de production de l'AC sont équipées de systèmes d'extinction automatique par gaz inerte. Les mesures mises en œuvre sont décrites dans la « Politique de sûreté ».

5.1.6 Conservation des supports

Les informations et leurs actifs supports intervenant dans les activités de l'IGC sont identifiés, inventoriés et leurs besoins de sécurité définis en disponibilité, intégrité et confidentialité.

Les actifs de l'AC sont listés dans le document « Inventaire des actifs », et les besoins de sécurité dans le formulaire de « Gestion des risques SI ».

Des mesures sont mises en place pour éviter la compromission et le vol de ces informations. Les supports correspondant à ces informations sont gérés selon des procédures conformes à ces besoins de sécurité. En particulier, ils sont manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.

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

Les mesures mises en œuvre permettent de couvrir les risques identifiés dans le formulaire de « Gestion des risques SI ».

La « Politique de sûreté », la « Procédure de gestion des actifs » et la « Procédure de gestion des matériels » décrivent plus en détails les dispositions mises en œuvre par l'AC.

5.1.7 Mise hors service des supports

Les mesures prises pour la mise hors service des supports d'informations sont en conformité avec le niveau de confidentialité des informations correspondantes.

La « Politique de sûreté », la « Procédure de gestion des actifs » et la « Procédure de gestion des matériels » décrivent plus en détails les dispositions mises en œuvre par l'AC.

5.1.8 Sauvegardes hors site

Des sauvegardes externalisées sont mises en œuvre et organisées de façon à assurer une reprise des fonctions de l'IGC après incident le plus rapidement possible, et conformément aux engagements en matière de disponibilité et de protection en confidentialité et en intégrité des informations sauvegardées.

La « Procédure de sauvegarde », la « Procédure de gestion des actifs » et la « Procédure de gestion des matériels » décrivent plus en détails les dispositions mises en œuvre par l'AC.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Chaque composante de l'IGC distingue 7 rôles fonctionnels de confiance :

- Responsable de sécurité : Le responsable de sécurité est chargé de la mise en œuvre et du contrôle de la politique de sécurité des composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes des composantes. Il est habilité à prendre connaissance des archives et des journaux d'évènements. Il est responsable des opérations de génération et de révocation des certificats qui sont implémentées par les Officiers d'enregistrement.
- Responsable d'application : Le responsable d'application est chargé, au sein de la composante à laquelle il est rattaché, de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'IGC au niveau de l'application dont il est responsable. Sa responsabilité couvre l'ensemble des fonctions rendues par cette application et des performances correspondantes.
- Administrateur système : Il est chargé de la mise en route, de la configuration, de l'installation et de la maintenance technique des équipements informatiques de l'AC pour l'enregistrement, la génération des certificats, et la gestion des révocations. Il assure l'administration technique des systèmes et des réseaux de la composante.
- Opérateur : Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante.
- Contrôleur : Personne désignée par une autorité compétente et dont le rôle est de procéder de manière régulière à des contrôles de conformité de la mise en œuvre des fonctions fournies par la composante par rapport aux politiques de certification, aux déclarations des pratiques de certification de l'IGC et aux politiques de sécurité de la composante.
- Officier d'enregistrement : Il est en charge de l'approbation des actions de génération et de révocation des certificats des services, serveurs et Porteurs.
- Porteur de part de secret : Il a la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui lui sont confiées.

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

Le document « Rôles, responsabilités et autorités », la « Procédure de gestion du personnel » et le document de « Suivi du personnel » décrivent plus en détails les dispositions mises en œuvre par l'AC.

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

La « Politique de sûreté », la « Procédure de gestion des actifs » et la « Procédure de gestion des matériels » décrivent plus en détails les dispositions mises en œuvre par l'AC.

5.2.2 Nombre de personnes requises par tâche

Pour des raisons de disponibilité, chaque tâche doit pouvoir être effectuée par au moins deux personnes. Pour certaines tâches sensibles telles que les opérations sur les HSM (par exemple la cérémonie des clés), plusieurs personnes sont requises pour des raisons de sécurité et de « dual control ».

Le document « Rôles, responsabilités et autorités », la « Procédure de gestion du personnel » et le document de « Suivi du personnel » décrivent plus en détails les dispositions mises en œuvre par l'AC.

5.2.3 Identification et authentification pour chaque rôle

Chaque attribution de rôle à un membre du personnel de l'IGC est acceptée formellement. L'AC fait vérifier l'identité et les autorisations de tout membre de son personnel avant l'attribution des privilèges relatifs à ses fonctions. L'attribution d'un rôle à un membre du personnel de l'IGC suit une procédure stricte avec signature de procès-verbaux pour l'attribution de tous les éléments nécessaires à l'exécution de ce rôle dans l'IGC (clés, codes d'accès, clés cryptographiques, etc.).

Le document « Rôles, responsabilités et autorités », la « Procédure de gestion du personnel » et le document de « Suivi du personnel » décrivent plus en détails les dispositions mises en œuvre par l'AC.

5.2.4 Rôle exigeant une séparation des attributions

Concernant les rôles de confiance, les cumuls suivants sont interdits au sein de l'IGC :
- Responsable de sécurité et administrateur système/opérateur ;
- Contrôleur et tout autre rôle ;
- Administrateur système et opérateur.

Le document « Rôles, responsabilités et autorités », la « Procédure de gestion du personnel » et le document de « Suivi du personnel » décrivent plus en détails les dispositions mises en œuvre par l'AC.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC sont soumis à une clause de confidentialité vis-à-vis de l'employeur. L'adéquation des compétences professionnelles des personnels intervenant dans l'IGC est vérifiée en cohérence avec les attributions. Le personnel d'encadrement, le responsable sécurité, les administrateurs système, disposent des expertises nécessaires à l'exécution de leur rôle respectif et sont familiers aux procédures de sécurité appliquées à l'exploitation de l'IGC.

L'AC informe tout employé intervenant dans des rôles de confiance de l'IGC de ses responsabilités relatives aux services de l'IGC et des procédures liées à la sécurité du système et au contrôle du personnel.

Les compétences professionnelles sont déterminées lors du recrutement et chaque année par les responsables sécurité. Le document « Rôles, responsabilités et autorités », la « Procédure de gestion du personnel » et le document de « Suivi du personnel » décrivent plus en détails les dispositions mises en œuvre par l'AC.

5.3.2 Procédures de vérification des antécédents

L'AC s'assure que tout employé intervenant sur l'IGC n'a pas subi de condamnation de justice en contradiction avec ses attributions. Les employés fournissent une copie du bulletin n°3 de leur casier judiciaire préalablement à leur affectation. Cette vérification est renouvelée périodiquement (au minimum tous les 3 ans). De plus, l'AC s'assure que les personnels ne souffrent pas de conflits d'intérêts préjudiciables à l'impartialité de leurs tâches.

L'AC peut décider en cas de refus du personnel de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions du personnel, de lui retirer ces attributions.

Le document « Rôles, responsabilités et autorités », la « Procédure de gestion du personnel » et le document de « Suivi du personnel » décrivent plus en détails les dispositions mises en œuvre par l'AC.

5.3.3 Exigences en matière de formation initiale

Une formation initiale aux logiciels, matériels et procédures internes de fonctionnement et de sécurité est dispensée aux employés, formation en adéquation avec le rôle que l'AC leur attribue. Une sensibilisation sur les implications des opérations dont ils ont la responsabilité est également opérée.

Le document « Rôles, responsabilités et autorités », la « Procédure de gestion du personnel » et le document de « Suivi du personnel » décrivent plus en détails les dispositions mises en œuvre par l'AC.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation.

Le document « Rôles, responsabilités et autorités », la « Procédure de gestion du personnel » et le document de « Suivi du personnel » décrivent plus en détails les dispositions mises en œuvre par l'AC.

5.3.5 Fréquence et séquence de rotation entre différentes attributions

Sans objet.

5.3.6 Sanctions en cas d'actions non autorisées

Tout membre du personnel de l'AC agissant en contradiction avec les politiques et les procédures établies et les processus et procédures internes de l'IGC, soit par négligence, soit par malveillance, verra ses privilèges révoqués et fera l'objet de sanctions administratives, voire de poursuites judiciaires.

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

Le personnel des prestataires externes intervenant dans les locaux et/ou sur les composantes de l'IGC doit également respecter les exigences du chapitre 5.3. Ceci est traduit en clauses adéquates dans les contrats avec ces prestataires. Le cas échéant, si le niveau d'intervention le requiert, il peut être demandé au prestataire de signer la charte informatique et/ou de fournir des éléments de vérification d'antécédents.

5.3.8 Documentation fournie au personnel

Chaque membre du personnel dispose de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en œuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, l'AC lui remet les politiques de sécurité l'impactant. Les opérateurs disposent notamment des manuels d'opérateurs correspondant aux composantes sur lesquelles ils interviennent.

Le document « Rôles, responsabilités et autorités », la « Procédure de gestion du personnel » et le document de « Suivi du personnel » décrivent les mesures mises en œuvre en matière de sensibilisation et formations sur les documentations et le document « Procédure de gestion documentaire » cadre la gestion de ces documentations.

5.4 Procédures de constitution des données d'audit

Les événements pertinents intervenant dans la gestion et l'exploitation de l'IGC sont enregistrés sous forme manuscrite ou sous forme électronique (par saisie ou par génération automatique) et ce, à des fins d'audit.

5.4.1 Type d'événements à enregistrer

Les systèmes d'exploitation des serveurs de l'IGC journalisent les événements suivants, automatiquement dès leur démarrage et sous forme électronique (liste non exhaustive) :

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

D'autres événements sont aussi recueillis. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques :

- Les accès physiques (enregistrés électroniquement) ;
- Les accès logiques aux systèmes ;
- Les actions de maintenance et de changement de la configuration des systèmes enregistrés manuellement ;
- Les changements apportés au personnel ;
- Les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels des RC et Porteurs).

Des événements spécifiques aux différentes fonctions de l'IGC sont également journalisés :

- Evénements liés aux clés de signature et aux certificats d'AC ou aux données d'activation (génération, sauvegarde et récupération, révocation, destruction, destruction des supports, ...) ;
- Réception d'une demande de certificat (initiale et renouvellement) ;
- Validation d'une demande de certificat ;
- Génération des certificats des services, serveurs et Porteurs ;
- Transmission des certificats aux Porteurs et, selon les cas, acceptations / rejets explicites par les Porteurs ;
- Publication et mise à jour des informations liées à l'AC (PC/DPC, certificats d'AC, CGU, etc.)
- Réception d'une demande de révocation ;
- Validation / rejet d'une demande de révocation ;
- Génération puis publication des LCR.

Le processus de journalisation permet un enregistrement en temps réel des opérations effectuées. Chaque enregistrement d'un événement dans un journal contient au minimum les champs suivants :

- Le type d'événement ;
- La date et heure de l'événement (l'heure exacte des événements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat est enregistrée) ;
- Le nom de l'exécutant ou la référence du système ayant déclenché l'événement (pour imputabilité) ;
- Le résultat de l'événement (réussite ou échec).

En fonction du type d'événement, on trouve également les champs suivants :

- Le destinataire de l'opération ;
- Le nom du demandeur de l'opération ou la référence du système ayant effectué la demande ;
- Le nom des personnes présentes (pour les opérations nécessitant plusieurs personnes) ;
- La cause de l'événement ;
- Toute information caractérisant l'événement (par exemple : n° de série du certificat émis ou révoqué).

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

Les évènements et données spécifiques à journaliser sont documentés par l'AC. Les pratiques mises en œuvre sont décrites plus en détails dans la « Procédure de journalisation » et la « Procédure d'archivage ».

5.4.2 Fréquence de traitement des journaux d'événements

Cf. chapitre 5.4.8

5.4.3 Période de conservation des journaux d'événements

Le délai de conservation des journaux d'événements sur site est de 1 mois. L'archivage des journaux d'événements est effectué au plus tard 1 mois après leur génération.

5.4.4 Protection des journaux d'événements

Seuls les membres dédiés de l'AC sont autorisés à traiter ces fichiers.

L'accès en écriture à ces fichiers est protégé au travers de contrôles d'accès logiques et physiques décrit plus en détail dans la « Procédure de journalisation », la « Politique de contrôle d'accès logiques » et la « Politique de sûreté ».

Les systèmes générant les journaux d'événements (exceptés les systèmes de contrôle d'accès physique) sont synchronisés quotidiennement sur une source fiable de temps UTC (cf. 6.8. Horodatage / système de datation).

La « Procédure de synchronisation des horloges » décrit les mesures mises en œuvre par l'AC.

5.4.5 Procédure de sauvegarde des journaux d'événements

Des mesures de sécurité sont mises en place par chaque entité opérant une composante de l'IGC afin de garantir l'intégrité et la disponibilité des journaux d'événements pour la composante considérée, conformément aux exigences de la présente PC. Une sauvegarde est effectuée à fréquence élevée afin d'assurer la disponibilité de ces informations.

5.4.6 Système de collecte des journaux d'événements

Les journaux d'événements sont centralisés dans un concentrateur. La consolidation obtenue est accessible par le personnel Certigna. La protection de la confidentialité et de l'intégrité des journaux d'événements est assurée par le contrôle d'accès logique ainsi que par l'utilisation d'outil de scellement des fichiers.

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

Sans objet.

5.5 Archivage des données

5.5.1 Types de données à archiver

L'AC archive :

- Les journaux d'événement des différentes composantes de l'IGC ;
- La PC ;
- La DPC ;
- Les demandes de certificats électroniques ;
- Les dossiers d'enregistrement des MC ;
- Les dossiers d'enregistrement des opérateurs d'AED ;
- Les dossiers de demande de certificat, avec les informations d'identité ;
- Les certificats émis ;
- Les demandes de révocation ;
- Les LCR émises ;
- Les réponses OCSP.

5.5.2 Période de conservation des archives

5.5.2.1 Dossiers de demande de certificat

Un dossier de demande de certificat se compose des informations d'identité du Porteur et des preuves d'acceptation des CGU et du contenu prévu ou placé dans son certificat. Le dossier peut inclure la copie de la pièce d'identité ayant servi à l'authentification et l'identification du porteur, ou bien uniquement certaines informations constitutives de cette pièce d'identité (Ex : Numéro d'identification de la pièce d'identité, nom et prénom y figurant, date d'expiration, type, etc.).

Tout dossier de demande de certificat accepté est archivé à minima sept ans à compter de l'expiration du certificat, et aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable, en particulier à l'article 6-II du décret d'application n°2001-272 du 30 mars 2001. En l'occurrence, il est archivé pendant au moins sept ans à compter de l'expiration du certificat. Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat peut être présenté par l'AC lors de toute sollicitation par les autorités habilitées. Ce dossier, complété par les mentions consignées par l'AE, doit permettre de retrouver l'identité réelle du Porteur responsable à un instant "t" du certificat émis par l'AC.

5.5.2.2 Certificats, LCR / LAR et réponses OCSP émis par l'AC

Les certificats de clés de serveurs et d'AC, ainsi que les LCR / LAR produites (respectivement par cette AC et l'AC Racine), sont archivés pendant au moins sept ans après leur expiration.

Les réponses OCSP produites sont archivées pendant au moins deux ans après leur expiration.

Les réponses sont détruites automatiquement après cette durée.

5.5.2.3 Journaux d'événements

Les journaux d'événements traités au chapitre 5.4 sont archivés pendant au moins sept ans après l'expiration des certificats associés.

Les archives sont conservées en plusieurs exemplaires grâce au processus de réplication entre les centres de production de l'AC, ce qui assure la protection et la disponibilité des informations. Les archives électroniques sont effacées (Processus périodique) une fois leur période de conservation passée.

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives sont protégées en intégrité. Elles peuvent être relues et exploitées par les membres dédiés de l'AC. L'accès en écriture à ces fichiers est protégé (gestion des droits). L'accès en lecture à ces journaux n'est possible qu'à partir d'une machine identifiée et autorisée des réseaux internes.

5.5.4 Procédure de sauvegarde des archives

Le procédé de « réplication » (automatique ou manuel en cas de reprise) garantit l'existence d'une copie de secours de l'ensemble des archives.

Pour pallier l'impossibilité de réplication entre les sites de production, des sauvegardes quotidiennes sont réalisées afin de garantir l'existence d'une copie des données enregistrées.

5.5.5 Exigences d'horodatage des données

Les données sont datées conformément au chapitre 6.8.

5.5.6 Système de collecte des archives

L'archivage est réalisé sur des serveurs d'archivage qui assurent la disponibilité, l'intégrité et la confidentialité des archives.

La « Procédure de sauvegarde » et la « Procédure d'archivage » décrivent les mesures mises en œuvre par l'AC.

5.5.7 Procédures de récupération et de vérification des archives

Les archives peuvent être récupérées uniquement par les membres dédiés de l'AC autorisés à traiter ces fichiers dans un délai maximal de deux jours ouvrés.

Les données concernant les contractants peuvent être récupérées à leur demande.

5.6 Renouvellement d'une clé de composante de l'IGC

5.6.1 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 du certificat de l'AC doit être supérieure à celle des certificats qu'elle signe. Au regard de la date de fin de validité de ce certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée 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.

L'IGC CERTIGNA communiquera en temps utiles sur son site en cas de génération d'un nouveau certificat pour cette AC ou l'AC Racine, en invitant les utilisateurs à télécharger la nouvelle chaîne de certification.

La « Procédure de gestion des clés cryptographiques » et le document de « Suivi des clés » décrivent les mesures mises en œuvre par l'AC.

5.6.2 Clés des autres composantes

Les bi-clés et certificats associés des composantes de l'IGC sont renouvelés soit dans les trois mois précédant leur expiration ou après révocation du certificat en cours de validité.

5.7 Reprise suite à compromission et sinistre

L'AC établit des procédures visant à assurer le maintien, dans la mesure du possible, des activités et décrit, dans ces procédures, les étapes prévues en cas de corruption ou de perte de ressources informatiques, de logiciels et de données.

Ces procédures sont formalisées dans le cadre de la mise en place des Plans de Continuité d'Activité. En particulier pour les risques majeurs identifiés, ces plans abordent le traitement immédiat dans le cas de contraintes fortes de disponibilité de service exigées par la PC. L'exploitation d'un moniteur de supervision garantit une détection et une prise en compte en temps réel des incidents sur les deux sites de production.

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

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée de l'AC, l'événement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement l'AC.

Le cas de l'incident majeur est impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, sera faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé, etc.).

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

- Informera tous les RC et Porteurs et les tiers utilisateurs de certificats avec lesquels l'AC a passé des accords ou à d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;
- Révoquera tout certificat concerné.

La « Procédure de gestion des incidents » et les « Plans de continuité d'activité » décrivent les mesures mises en œuvre par l'AC.

5.7.2 Procédures de reprise en cas de corruption des ressources informatiques

Chaque composante de l'IGC est intégrée dans le plan de continuité d'activité (PCA) de la société afin de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant des engagements de l'AC et des résultats de l'analyse de risque de l'IGC, notamment en ce qui concerne les fonctions liées à la publication et/ou liées à la révocation des certificats.

Ce plan est testé au minimum une fois tous les trois ans.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité d'activité de la composante en tant que sinistre (cf. chapitre 5.7.2). Dans le cas de compromission d'une clé d'AC, le certificat correspondant sera immédiatement révoqué. De même, tous les certificats serveurs en cours de validité émis par cette AC seront révoqués.

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

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

Remarque : Dans le cas de l'AC Racine, le certificat de signature n'étant pas révocable, ce sont les certificats des autorités intermédiaires qui sont révoqués en cas de compromission de la clé privée de l'AC Racine.

La « Procédure de gestion des clés cryptographiques », la « Procédure de gestion des incidents » et les « Plans de continuité d'activité » décrivent les mesures mises en œuvre par l'AC.

5.7.4 Capacité de continuité d'activité suite à un sinistre

Les différentes composantes de l'IGC disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la PC de l'AC.

L'AC s'appuie sur la redondance de ses systèmes d'informations sur plusieurs sites et ses plans de continuité d'activité pour assurer la continuité des services.

Les mesures sont décrites dans les « Plans de continuité d'activité ».

5.8 Fin de vie de l'IGC

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à la transférer à une autre entité. Le transfert d'activité est défini comme :

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

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

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

Une ou plusieurs composantes de l'IGC peuvent être amenées à cesser leur activité ou à les transférer à une autre entité. Afin d'assurer un niveau de confiance constant pendant et après de tels événements, l'AC prend les mesures suivantes :

- Elle assure la continuité du service d'archivage, en particulier des certificats et des dossiers d'enregistrement ;
- Elle assure la continuité du service de révocation, conformément aux exigences de disponibilité pour ses fonctions définies dans la présente PC ;
- Elle communique aux responsables d'applications les principes du plan d'action destinés à faire face à la cessation d'activité ou à organiser le transfert d'activité ;
- Elle effectue une information auprès des autorités administratives. En particulier le contact de l'ANSSI est averti (http://www.ssi.gouv.fr). L'AC l'informera notamment de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus de transfert ou de cessation d'activité.

La « Procédure de gestion des incidents » et les « Plans de continuité d'activité » décrivent en détails les dispositions mises en œuvre par l'AC.

5.8.1.2 Cessation d'activité affectant l'AC

Dans l'hypothèse d'une cessation d'activité totale, avant que l'AC ne mette un terme à ses services, elle effectue les procédures suivantes :

- Elle informe les composantes de l'IGC et les tiers par mail de la cessation d'activité. Cette information sera relayée également directement auprès des entités ;
- Elle révoque tous les certificats qu'elle a signés et qui sont encore valides ;
- Elle révoque son certificat ;

- Elle détruit la clé privée stockée dans le module cryptographique, ainsi que le contexte du module. Les porteurs de secret (clé privée et contexte) sont convoqués et détruisent leur(s) part(s) de secret. L'AC s'interdit en outre de transmettre sa clé à des tiers.

Si l'AC est en faillite, c'est au tribunal de commerce de décider de la suite à donner aux activités de l'entreprise. Néanmoins, le cas échéant, l'AC s'engage à accompagner le tribunal de commerce dans les conditions suivantes : avant une faillite, il y a une période préalable, générée la plupart de temps soit par plusieurs procédures d'alerte du commissaire aux comptes soit par un redressement judiciaire ; pendant cette période, l'AC s'engage à préparer pour le tribunal de commerce, le cas échéant, une proposition de transfert des certificats numériques vers une autre autorité disposant d'une certification d'un niveau au moins égal au sien.

Le contact identifié sur le site de l'ANSSI (http://www.ssi.gouv.fr) est immédiatement informé en cas de cessation d'activité de l'AC.

La « Procédure de gestion des incidents » et les « Plans de continuité d'activité » décrivent en détails les dispositions mises en œuvre par l'AC.

6 MESURES DE SECURITE TECHNIQUES

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

6.1.1.1 Génération des bi-clés d'AC

Ce chapitre décrit le contexte de génération de la bi-clé de l'AC Racine et des AC intermédiaires.

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 10.

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnes dans des rôles de confiance, dans le cadre de « cérémonies de clés ».

La cérémonie se déroule suivant un script préalablement défini :
- Elle se déroule sous le contrôle d'au moins une personne ayant un rôle de confiance au sein de l'IGC et en présence de plusieurs témoins ;
- Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

La génération des clés de signature d'AC s'accompagne de la génération de parts de secrets. Les parts de secret d'IGC 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 ces dernières. Ces secrets sont des parties de la clé privée de l'AC décomposée suivant un schéma à seuil de Shamir.

Suite à leur génération, les parts de secrets sont remises à leurs porteurs désignés au préalable et habilités à ce rôle de confiance par l'AC. Les parts de secret sont placées dans des enveloppes scellées, placées elles-mêmes dans des coffres.

Les scripts de cérémonie des clés ainsi que la répartition des parts de secrets sont suivis et documentés. La « Procédure de gestion des clés cryptographiques » et la « Procédure de gestion des HSM » décrivent les mesures mises en œuvre.

6.1.1.2 Génération des bi-clés d'AE

Sans objet.

Note : L'AE utilise tant que possible les certificats finaux délivrés par les AC couvertes par cette DPC pour authentifier son personnel et sécuriser ses services.

6.1.1.3 Génération des bi-clés de personne morale ou physique

L'AC génère les bi-clés des Porteurs dans un environnement ou dispositif sécurisé conforme aux exigences du chapitre 11.

6.1.2 Transmission de la clé privée à son propriétaire

L'AC génère la clé privée au nom du Porteur et l'authentification du Porteur par l'AE est réalisée préalablement à la génération de la bi-clé.

La clé privée est conservée par l'AC et protégée par une donnée d'activation remise au Porteur par l'AE ou l'AC (Ex : par mail ou par SMS). Cette donnée d'activation, qui n'est connue que du Porteur permet à lui seul d'activer sa clé privée.

6.1.3 Transmission de la clé publique à l'AC

L'AC assure la génération de la bi-clé du Porteur.

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

La délivrance de la clé publique de l'AC, qui permet à tous ceux qui en ont besoin de valider un certificat émis par l'AC en vertu de cette DPC, est effectuée par un moyen garantissant intégrité et authentification de cette clé publique.

La clé publique d'une AC intermédiaire est diffusée dans un certificat lui-même signé par l'AC Racine. La clé publique de l'AC Racine est diffusée dans un certificat auto-signé. Ces clés publiques d'AC, ainsi que leurs valeurs de contrôle, sont diffusées et récupérées par les systèmes d'information de tous les accepteurs de certificats par l'intermédiaire du site de CERTIGNA à l'adresse https://www.certigna.com. Cf. chapitre 2.2.1.2.

6.1.5 Type d'algorithme et taille des clés

6.1.5.1 Certificat d'AC racine

- Algorithme de hachage : SHA-256,
- Taille modulus RSA (bits) : 4096

6.1.5.2 Certificat d'AC intermédiaire

- Algorithme de hachage : SHA-256,
- Taille modulus RSA (bits) : 4096

6.1.5.3 Certificat de personne physique

- Algorithme de hachage : SHA-256,
- Taille modulus RSA (bits) : 3072

6.1.6 Vérification de la génération des paramètres des clés publiques et de leur qualité

Les paramètres et les algorithmes de signature mis en œuvre dans les boîtiers cryptographiques, les supports matériels et logiciels sont documentés par l'AC.

L'AC confirme que la valeur de l'exposant public est un nombre impair supérieur à 3 et compris entre $2^{16}+1$ et $2^{256}-1$

6.1.6.1 Clé d'AC

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

6.1.6.2 Clé de personne physique

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

6.1.7 Objectifs d'usage de la clé

6.1.7.1 Clé d'AC

La clé privée de l'AC racine est utilisée pour signer le certificat de l'AC racine, les LAR et les certificats d'AC intermédiaires.

La clé privée d'une AC intermédiaire est utilisée pour signer les certificats de personne morale ou physique, les LCR, ainsi que le certificat du répondeur OCSP.

6.1.7.2 Clé de personne physique

Les Porteurs doivent respecter strictement les usages autorisés des bi-clés et des certificats cités au chapitre 1.5.1. Dans le cas contraire, leur responsabilité pourrait être engagée.

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 Racine et les AC intermédiaires pour la génération et la mise en œuvre de leurs clés de signature sont conformes aux exigences du chapitre 10. Ces boitiers sont des ressources exclusivement accessibles aux serveurs d'AC via un VLAN dédié. La « Procédure de gestion des HSM » décrit plus en détails les dispositions mises en œuvre par l'AC. L'AC met en œuvre des protections physiques et logiques pour empêcher de la délivrance non autorisée de certificats.

6.2.1.2 Dispositifs de protection des clés privées de personne morale ou physique

Le dispositif utilisé par l'AC pour protéger la clé privée des Porteurs est conforme avec les exigences du chapitre 11.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Le contrôle des clés privées de signature de l'AC est assuré par du personnel de confiance et via un outil mettant en œuvre le partage des secrets (systèmes où n exploitants parmi m doivent s'authentifier, avec n au moins égal à 2). La « Procédure de gestion des HSM » et la « Procédure de gestion des clés cryptographiques » décrivent les mesures mises en œuvre.

6.2.3 Séquestre de la clé privée

6.2.3.1 Clés d'AC

Les clés privées d'AC ne sont jamais séquestrées.

6.2.3.2 Clés de personne morale ou physique

Le séquestre des clés privées des Porteurs est interdit.

6.2.4 Copie de secours de la clé privée

6.2.4.1 Clé privée d'AC

La clé privée de l'AC fait l'objet de copies de secours :

- Dans un ou plusieurs modules cryptographiques conformes aux exigences du chapitre 10.
- En dehors du module cryptographique sous la forme de parts de secret chiffrées par le module cryptographique et réparties entre plusieurs porteurs de secrets.

6.2.4.2 Clé privée de personne physique

Les clés privées des Porteurs ne font pas l'objet de copies de secours.

6.2.5 Archivage de la clé privée

6.2.5.1 Clé privée d'AC

La clé privée d'une AC n'est en aucun cas archivée.

6.2.5.2 Clé privée de personne physique

La clé privée du Porteur n'est en aucun cas archivée.

6.2.6 Transfert de la clé privée avec le module cryptographique

6.2.6.1 Clé privée d'AC

La clé privée d'une AC est générée dans le module cryptographique conforme aux exigences du chapitre 10. Comme décrit en 6.2.4, la clé n'est exportable/importable du module que sous forme chiffrée.

6.2.6.2 Clé privée de personne physique

La clé privée du Porteur est générée sous la responsabilité de l'AC.

6.2.7 Stockage de la clé privée dans un module cryptographique

6.2.7.1 Clé privée d'AC

La clé privée de l'AC racine est générée dans un module cryptographique décrit au chapitre 6.2.1 et est exportée conformément aux exigences du chapitre 6.2.4 afin de continuellement la maintenir hors ligne. La clé est reconstituée dans le module cryptographique pour permettre la génération annuelle des LAR ou la création d'une nouvelle autorité intermédiaire, puis supprimée du module une fois l'opération terminée.

La « Procédure de gestion des HSM » et la « Procédure de gestion des clés cryptographiques » décrivent plus en détails les dispositions mises en œuvre par l'AC.

6.2.7.2 Clé privée de personne physique

La clé privée du Porteur est générée et stockée dans un dispositif conforme aux exigences du chapitre 11, le cas échéant.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clé privée d'AC

L'activation de la clé privée d'une AC dans le module cryptographique est contrôlée via des données d'activation (cf. chapitre 6.4) et fait intervenir deux personnes ayant un rôle de confiance au sein de l'IGC. La « Procédure de gestion des HSM » et la « Procédure de gestion des clés cryptographiques » décrivent plus en détails les dispositions mises en œuvre par l'AC.

6.2.8.2 Clé privée de personne physique

L'activation des clés privées est contrôlée via des données d'activation (Cf. chapitre 6.4) qui sont utilisées par le dispositif utilisé le cas échéant.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clé privée d'AC

Le module cryptographique résiste aux attaques physiques, par effacement des clés privées d'AC. Le module est apte à détecter les attaques physiques suivantes : ouverture du dispositif, retrait ou forçage.

6.2.9.2 Clé privée de personne physique

La clé privée d'un porteur n'est activée que sur sa demande. La bi-clé est supprimée après l'expiration du certificat associé..

6.2.10 Méthode de destruction de la clé privée

6.2.10.1 Clé privée d'AC

En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), la clé est systématiquement détruite, ainsi que les parts de secrets permettant de la reconstituer. Un procès-verbal de destruction de la clé et des parts de secret est établi à l'issue de cette procédure. Les mesures mises en œuvre sont décrites dans la « Procédure de gestion des clés cryptographiques ».

6.2.10.2 Clé privée de personne physique

La bi-clé est supprimée automatiquement dans les 30 minutes qui suivent l'expiration du certificat associé.

6.2.11 Niveau d'évaluation sécurité du module cryptographique

6.2.11.1 Clé d'AC

Le niveau d'évaluation du module cryptographique de l'AC est précisé au chapitre 10.

6.2.11.2 Clé de personne physique

Le niveau d'évaluation du dispositif utilisé par l'AC pour la clé du Porteur est précisé au chapitre 11.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

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

6.3.2 Durées de vie des bi-clés et des certificats

6.3.2.1 Bi-clé et certificat d'AC

Pour l'IGC Certigna, la durée de validité du certificat de l'AC Racine est de 20 ans, et celle des certificats intermédiaires d'AC est de 15 ans.

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

6.3.2.2 Bi-clé et certificat de personne physique

Le certificat du Porteur a une durée de vie de 30 minutes. Après l'expiration du certificat du Porteur, la clé privée associée est supprimée automatiquement.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

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

La génération et l'installation des données d'activation du module cryptographique de l'AC s'effectuent lors de la phase d'initialisation et de personnalisation de ce module (cf. chapitre 6.1.1). La « Procédure de gestion des HSM » et la « Procédure de gestion des clés cryptographiques » décrivent plus en détails les dispositions mises en œuvre par l'AC.

6.4.1.2 Génération et installation des données d'activation correspondant à la clé privée de la personne physique

L'AC génère la bi-clé du Porteur et communique la donnée d'activation au Porteur (Ex : par mail ou SMS) L'AC peut sous-traiter à l'AE la génération et la communication de la donnée d'activation au Porteur.

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 sont directement remises aux Porteurs de secrets lors des cérémonies des clés. Leurs conditions de stockage assurent leur disponibilité, leur intégrité et leur confidentialité. Les secrets sont stockés dans des dispositifs à l'accès limité, dans des enveloppes sécurisées permettant de détecter toute ouverture non autorisée et tracée. La « Procédure de gestion des HSM » et la « Procédure de gestion des matériels » décrivent les mesures mises en œuvre par l'AC.

6.4.2.2 Protection des données d'activation correspondant à la clé privée de la personne physique

La donnée d'activation de la bi-clé du Porteur est générée et communiquée par l'AC ou l'AE au Porteur via l'un des moyens décrits au chapitre 6.4.1.

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

Un niveau minimal d'assurance de la sécurité sur les systèmes informatiques des personnes occupant un rôle de confiance est assuré par :

- Identification et authentification forte des utilisateurs pour l'accès au système (contrôle d'accès physique pour entrer dans la salle + contrôle logique par identifiant / mot de passe ou par certificat pour accéder au système) ;
- Gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur) ;
- 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) ;
- Protection contre les virus informatiques et toutes formes de logiciel compromettant ou non autorisé et mises à jour des logiciels à l'aide du firewall ;
- 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 via le firewall ;
- Communication sécurisée inter-sites (tunnel VPN IP Sec) ;
- Fonctions d'audit (non-répudiation et nature des actions effectuées).

Des dispositifs de surveillance et des procédures d'audit des paramétrages du système, notamment des éléments de routage, sont mis en place. La « Politique de sûreté », la « Politique de contrôle d'accès logiques », la « Charte de sécurité », la « Procédure de gestion des firewalls » décrivent les mesures mises en œuvre par l'AC.

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Sans objet.

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

La configuration des systèmes de l'AC ainsi que toute modification et mise à niveau sont documentées. Le développement est effectué dans un environnement contrôlé et sécurisé.

Afin de permettre à ses prospects ou futurs clients de tester ou d'évaluer certaines de leurs applications d'échange dématérialisé, l'AC a mise en place une AC de test émettant des certificats en tous points identiques aux certificats de production (seul l'émetteur du certificat diffère). Cette AC de test dispose d'une clé privée qui lui est propre. Le certificat de clé publique est auto-signé. Les certificats émis ont une utilisation restreinte à des fins de test exclusivement.

Les solutions Certigna sont testées en premier lieu au sein d'un environnement de développement/test avant d'être utilisées dans l'environnement de production. Les environnements de production et de développement sont dissociés.

La description du contexte d'évolution de l'IGC est définie dans la « Procédure de mise à jour de la plate-forme technique ». Les développements des modules liés à l'exploitation des composantes de l'IGC sont effectués en respectant les règles et consignes édictées dans le « Guide de développement ».

6.6.2 Mesures liées à la gestion de la sécurité

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

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.

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.

La « Procédure de gestion des firewalls », la « Procédure de gestion de la supervision » et la « Politique de contrôle d'accès logiques » décrivent en détails les dispositions mises en œuvre par l'AC.

6.8 Horodatage et Système de datation

Afin d'assurer une synchronisation entre les différentes datations d'événements, les différentes composantes de l'IGC synchronisent leurs horloges systèmes par rapport à une source fiable de temps UTC. La « Procédure de synchronisation des horloges » décrit les mesures mises en œuvre par l'AC.

7 PROFIL DES CERTIFICATS ET DES LCR

Les certificats et les LCR produits par l'AC sont conformes au standard ITU-T Recommandation X.509 version 3, à la RFC 5280 et aux spécifications ETSI EN 319 412 applicables.

7.1 Hiérarchie de confiance

La hiérarchie de confiance est composée des autorités et certificats suivants :

7.2 Profil du certificat d'AC racine

7.2.1 Champs de base

Champs	Tessi CA
Version	V3
Serial Number	1E10ED5EB137C3B966F335D8B514889A
Signature	SHA-256 RSA 4096
Subject Public Key Info	RSA 4096 bits
Validity	Du 01/06/2018 au 01/06/2038
Issuer DN	CN = Tessi CA OU = 0002 48146308100036 O = DHIMYOTIS C = FR
Subject DN	CN = Tessi CA OU = 0002 48146308100036 O = DHIMYOTIS C = FR

7.2.2 Extensions

Extensions	Critique	Tessi CA
SKI	Non	Identifiant de la clé publique de l'autorité
AKI	Non	Identifiant de la clé publique de l'autorité Racine
Certificate Policies	Non	CPS=https://www.certigna.fr/autorites/
CRL Distribution Points	Non	URL=http://crl.certigna.fr/tessica.crl URL=http://crl.dhimyotis.com/tessica.crl
Basic Constraints	Oui	cA = TRUE
Key Usage	Oui	Signature de certificat Signature de CRL

7.3 Profil du certificat de l'AC intermédiaire

7.3.1 Champs de base

Champs	Signé par « Tessi CA »
Version	V3
Serial Number	29a4aa2451a49ab771a8fa8077a2b80fc2b18b13
Signature	Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096
Subject Public Key Info	RSA 4096 bits
Validity	Du 07/11/2022 au 07/11/2037
Issuer DN	CN = Tessi CA OU = 0002 48146308100036 O = DHIMYOTIS C = FR
Subject DN	CN = Tessi Sign Certified O = DHIMYOTIS C = FR

7.3.2 Extensions

Extensions	Critique	Description
Subject Key Identifier	Non	Identifiant de la clé publique de l'autorité
Authority Key Identifier	Non	Identifiant de la clé publique de l'autorité Racine
Certificate Policies	Non	OID= 1.2.250.1.177.3.2.1 CPS=https://www.certigna.fr/autorites/
Authority Information Access	Non	calssuers= http://autorite.certigna.fr/tessica.der calssuers= http://autorite.dhimyotis.com/tessica.der
CRL Distribution Points	Non	URL=http://crl.certigna.fr/tessica.crl URL=http://crl.dhimyotis.com/tessica.crl
Basic Constraints	Oui	cA = TRUE PathLengthConstraint = 0
Key Usage	Oui	Signature de certificat Signature de CRL

7.4 Profils des certificats de Porteur LCP

7.4.1 Champs de base

Champs	Signé par « Tessi Sign Certified »
Version	V3
Serial Number	Numéro de série unique délivré par un CSPRNG (Cryptographically secure pseudorandom number generator) Entre 128 et 160 bits
Signature	Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096
Subject Public Key Info	RSA 3072 bits
Validity	30 minutes
Issuer DN	CN = Tessi Sign Certified O = DHIMYOTIS C = FR
Subject DN	SN[1] = Série de caractères constituée en partie d'un aléa CN = <Prénom>[3] <NOM>[4] GN = <Prénom>[3] SN[2] = <NOM>[4] C = Pays auprès duquel le Porteur est enregistré

[1] Champ Serial Number
[2] Champ Surname
[3] À minima le premier prénom
[4] À minima le nom patronymique

7.4.2 Extensions

Extensions	Critique	Description
Authority Key Identifier	Non	Identifiant de la clé publique de l'AC
Subject Key Identifier	Non	Identifiant de la clé publique du Porteur
Subject Alt. Name	Non	Nom RFC822 = Adresse e-mail du Porteur
Key Usage	Oui	Non répudiation
Extended Key Usage	Non	Email Protection
Certificate Policies	Non	OID= 1.2.250.1.177.3.2.1.1.1 OID= 0.4.0.2042.1.3 (LCP ETSI) CPS=https://www.certigna.fr/autorites/
CRL Distribution Points	Non	URL=http://crl.certigna.fr/tessisigncertified.crl URL=http://crl.dhimyotis.com/tessisigncertified.crl
Authority Information Access	Non	calssuers= http://autorite.certigna.fr/tessisigncertified.der calssuers= http://autorite.dhimyotis.com/tessisigncertified.der URL=http://tessisigncertified.ocsp.certigna.fr URL=http://tessisigncertified.ocsp.dhimyotis.com
Basic Constraints	Non	cA = FALSE
valassured-ST-certs	Non	NULL

7.5 Profils du certificat du répondeur OCSP

7.5.1 Champs de base

Champs	Signé par « Tessi Sign Certified »
Version	V3
Serial Number	Numéro de série unique délivré par un CSPRNG (Cryptographically secure pseudorandom number generator) Entre 128 et 160 bits
Signature	Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096
Subject Public Key Info	RSA 3072 bits
Validity	3 ans
Issuer DN	CN = Tessi Sign Certified O = DHIMYOTIS C = FR
Subject DN	CN = OCSP Tessi Sign Certified OU = 0002 48146308100036 O = DHIMYOTIS C = FR

[1] Champ Serial Number [2] Champ Surname

7.5.2 Extensions

Extensions	Critique	Description
Authority Key Identifier	Non	Identifiant de la clé publique de l'AC
Subject Key Identifier	Non	Identifiant de la clé publique du répondeur OCSP
Key Usage	Oui	Digital Signature, Non répudiation,
Extended Key Usage	Non	Signature OCSP (1.3.6.1.5.5.7.3.9)
CRL Distribution Points	Non	URL=http://crl.certigna.fr/tessisigncertified.crl URL=http://crl.dhimyotis.com/tessisigncertified.crl
Authority Information Access	Non	calssuers= http://autorite.certigna.fr/tessisigncertified.der calssuers= http://autorite.dhimyotis.com/tessisigncertified.der URL=http://tessisigncertified.ocsp.certigna.fr URL=http://tessisigncertified.ocsp.dhimyotis.com
OCSP No Check	Non	
Basic Constraints	Non	cA = FALSE

7.6 Profils des LAR de l'AC racine

Champs		Description
Version		V2
Signature		Identifiant de l'algorithme de signature de l'AC. SHA-256 RSA 4096
Issuer DN	CN =	Tessi CA
	OU =	0002 48146308100036
	O =	DHIMYOTIS
	C =	FR
This Update		Date de génération de la LAR
Next Update		Date de prochaine mise à jour de la LCR [1 an maximum]
Revoked certificates		Liste des n° de série des certificats d'AC révoqués : - Numéro de série - Date de révocation - Cause de révocation
Extensions	**Crit.**	**Description**
AKI	Non	Identifiant de la clé publique de l'AC
CRL Nb	Non	Contient le numéro de série de la LAR
Expired CertsOnCRL	Non	Date depuis laquelle les certificats révoqués et expirés sont maintenus dans la LAR.

7.7 Profils des LCR

Champs		Description
Version		V2
Signature		Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096
Issuer		CN = Tessi Sign Certified O = DHIMYOTIS C = FR
This Update		Date de génération de la LCR
Next Update		Date de prochaine mise à jour de la LCR [6 jours maximum]
Revoked certificates		Liste des n° de série des certificats révoqués
Extensions	**Critique**	**Description**
Authority Key Identifier	Non	Identifiant de la clé publique de l'AC
CRL Number	Non	Contient le numéro de série de la LCR
ExpiredCertsOnCRL	Non	Date depuis laquelle les certificats révoqués et expirés sont maintenus dans la CRL.

7.8 Traitement des extensions de certificats par les applications

Les extensions définies pour les certificats X509 V3 permettent d'associer des informations complémentaires à une clé publique, relatives au serveur ou à l'AC.

7.8.1 Criticité

Le caractère de criticité doit se traiter de la façon suivante selon que l'extension est critique ou non :

- Si l'extension est non-critique, alors :
- Si l'application ne reconnaît pas l'OID, l'extension est abandonnée mais le certificat est accepté ;
- Si l'application reconnaît l'OID, alors :
  - Si l'extension est conforme à l'usage que l'application veut en faire, l'extension est traitée.
  - Si l'extension n'est pas conforme à l'usage que l'application veut en faire, l'extension est abandonnée, mais le certificat est accepté.
- Si l'extension est critique, alors :
- Si l'application ne reconnaît pas l'OID, le certificat est rejeté ;
- Si l'application reconnaît l'OID, alors :
  - Si l'extension est conforme à l'usage que l'application veut en faire, l'extension est traitée.
  - Si l'extension n'est pas conforme à l'usage que l'application veut en faire, le certificat est rejeté.

7.8.2 Description des extensions

AuthorityKeyIdentifier : Cette extension identifie la clé publique utilisée pour vérifier la signature sur un certificat. Elle permet de différencier les différentes clés utilisées par l'AC lorsque celle-ci dispose de plusieurs clés de signature. Il contient un identifiant unique (keyIdentifier). Cet identifiant de clé d'AC a la même valeur que le champ subject-KeyIdentifier du certificat de l'AC. Les champs authorityCertIssuer et authorityCertSerialNumber ne sont pas renseignés.

Subject Key Identifier : Cette extension identifie la clé publique du serveur associée au certificat. Elle permet de distinguer les différentes clés utilisées par le Porteur. Sa valeur est la valeur contenue dans le champ keyIdentifier.

Key Usage : Cette extension définit l'utilisation prévue de la clé contenue dans le certificat. L'AC Indique l'usage prévu de la clé et gère la criticité comme défini au 7.2.

Extended Key Usage : Cette extension définit l'utilisation avancée de la clé.

Certificate Policies : Cette extension définit les politiques de certification que le certificat reconnaît supporter et suivant lesquelles il a été créé. Ce champ est traité pendant la validation de la chaîne de certification. L'AC inclut le champ policyInformation en renseignant le champ policyIdentifier avec l'OID de la PC.

CRL Distribution Points : Cette extension identifie l'emplacement où l'utilisateur peut trouver la LCR indiquant si le certificat a été révoqué. L'AC remplit autant de champs distributionPoint, qu'elle offre de mode d'accès à la LCR. Chacun de ces champs comporte l'uniformRessourceIdentifier de la LCR.

Authority Information Access : Cette extension identifie (avec Method=OCSP) l'emplacement du(des) serveur(s) OCSP fournissant des informations sur le statut des certificats serveurs, ainsi que sur l'AC émettrice en fournissant un lien vers son certificat.

Basic Constraints : Cette extension indique si le certificat est un certificat d'entité finale ou un certificat d'autorité.

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits et les évaluations concernent, d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification au sens de l'Ordonnance n° 2005-1516 du 8 décembre 2005 et du règlement européen eIDAS et, d'autre part, ceux que réalise ou fait réaliser l'AC afin de s'assurer que l'ensemble de son IGC est bien conforme à ses engagements affichés dans cette PC et aux pratiques identifiées dans la DPC correspondante.

Les chapitres suivants ne concernent que les audits et évaluations de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

L'AC peut réaliser des audits auprès des opérateurs d'AE Externe et des opérateurs d'AED au même titre que le personnel de son IGC. Il s'assure entre autres que ces opérateurs ou les systèmes de contrôle d'identité automatisés respectent les engagements vis-à-vis de cette DPC et les pratiques correspondantes.

8.1 Fréquences et/ou circonstances des évaluations

Un contrôle de conformité de l'AC a été effectué avant la première mise en service par rapport aux moyens et règles mentionnées dans la PC et dans la DPC.

Ce contrôle est également effectué par l'AC à minima une fois par an.

8.2 Identités/qualifications des évaluateurs

Le contrôle 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. Les audits annuels de qualifications sont réalisés par des auditeurs qualifiés.

8.3 Relations entre évaluateurs et entités évaluées

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

8.4 Sujets couverts par les évaluations

Les contrôles de conformité visent à vérifier le respect des engagements et pratiques définies dans la PC de l'AC et dans la DPC qui y répond, ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, ...).

L'AC contrôle la qualité du service des certificats délivrés ou contenant des informations vérifiées par un tiers délégué en demandant à un spécialiste de la validation employé par l'AC d'effectuer des vérifications périodiques.

L'autorité de certification examinera les pratiques et les procédures de chaque tiers délégué afin de s'assurer que le tiers délégué est en conformité avec les exigences de cette PC et de la DPC associée.

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 : « Amélioration », « remarque », « écart mineur », « écart majeur ».

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

- En cas d'amélioration, et selon l'importance de l'amélioration, l'équipe d'audit émet des recommandations à l'AC pour améliorer son fonctionnement. Les améliorations sont laissées à l'appréciation de l'AC qui décide ou non de les mettre en place.
- En cas de résultat « remarque » ou « écart mineur », l'AC remet à la composante un avis précisant sous quel délai les non-conformités doivent être levées. Puis, un contrôle de confirmation permettra de vérifier que tous les points critiques ont bien été résolus.
- En cas d'écart majeur, 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.

Chaque session d'audit permet de consulter les avis émis par l'équipe d'audit. Un contrôle de confirmation permettra de vérifier que tous les points critiques ont bien été résolus dans les délais.

8.6 Communication des résultats

Les résultats des audits de conformité effectués par l'équipe d'audit sont tenus à la disposition de l'organisme 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 des certificats

Les informations d'état et de révocation des certificats sont libres d'accès.

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

La société mère du Groupe Tessi auquel l'AC appartient a souscrit pour elle-même et pour l'ensemble de ses filiales dont Certigna, notamment un contrat « responsabilité civile garantissant les dommages directs matériels ou immatériels consécutifs causés dans l'exercice de son activité professionnelle couvrant notamment la responsabilité civile après livraison.
L'AC s'assure que les entités intervenant dans le service (1.4.7) le cas échéant ont également souscrit à un contrat d'assurance adéquat.

9.2.2 Autres ressources

Sans objet.

9.2.3 Couverture et garantie concernant les entités utilisatrices

La société mère du Groupe Tessi auquel l'AC appartient a souscrit pour elle-même et pour l'ensemble de ses filiales dont Certigna, notamment un contrat « responsabilité civile garantissant les dommages directs matériels ou immatériels consécutifs causés dans

l'exercice de son activité professionnelle couvrant notamment la responsabilité civile après livraison.
L'AC s'assure que les entités intervenant dans le service (1.4.7) le cas échéant ont également souscrit à un contrat d'assurance adéquat.

9.3 Confidentialité des données professionnelles

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :
- La partie non-publique de la DPC de l'AC ;
- Les clés privées de l'AC, des composantes et des serveurs ;
- Les données d'activation associées aux clés privées d'AC et des serveurs ;
- Tous les secrets de l'IGC ;
- Les journaux d'événements des composantes de l'IGC ;
- Les dossiers d'enregistrement des Porteurs ;
- Les causes de révocation des certificats.

9.3.2 Informations hors du périmètre des informations confidentielles

Sans objet.

9.3.3 Responsabilités en termes de protection des informations confidentielles

De manière générale les informations confidentielles ne sont accessibles qu'aux personnes concernées par de telles informations ou qui ont l'obligation de conserver et/ou traiter de telles informations.

En particulier, Certigna peut devoir mettre à disposition les données dont il dispose à des tiers dans le cadre de procédures légales et doit également donner l'accès à ces informations à ses clients.

Dès lors que les informations confidentielles sont soumises à un régime particulier régi par un texte législatif et réglementaire, le traitement, l'accès, la modification de ces informations sont effectués conformément aux dispositions des textes en vigueur.

L'AC applique des procédures de sécurité pour garantir la confidentialité des informations caractérisées comme telles au 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage. De plus, lorsque ces données sont échangées, l'AC en garantit l'intégrité.

L'AC est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elle peut devoir mettre à disposition les dossiers d'enregistrement des Porteurs à des tiers dans le cadre de procédures légales. Elle donne également accès à ces informations au Porteur et le cas échéant à l'opérateur d'AE ou d'AED en relation avec le Porteur.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

En acceptant les CGU, le Porteur reconnaît avoir pris connaissance de la Politique d'utilisation des Données Personnelles de CERTIGNA disponible sur le Site https://www.certigna.com/politique-dutilisation-des-donnees-personnelles/.

Les données fournies par le Porteur lors de son inscription sur le Site de l'AC, de l'AE ou de l'AED lors de sa demande de certificats sont des Données Personnelles dont la collecte et le traitement sont régis par la Politique d'utilisation des Données Personnelles susvisée.

Les dossiers de demande de certificat électronique comportant les données personnelles sont archivés par l'AC en tant que prestataire de service de confiance ou l'AE à minima sept ans après l'expiration des certificats associés et aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable. Les informations personnelles d'identité peuvent être utilisées comme données d'authentification lors d'une éventuelle demande de révocation ou d'informations.

Les journaux applicatifs liés au cycle de vie des certificats et comportant les données personnelles sont archivés à minima sept ans après leur génération et aussi longtemps que nécessaire pour les besoins de fourniture de la preuve de la certification dans des procédures légales, conformément à la loi applicable.

Par ailleurs, CERTIGNA conserve les données à caractère personnel pendant une durée de trois ans à compter de la fin des relations commerciales avec le client et 3 ans à compter du dernier contact émanant avec le prospect. Le délai commence à partir de la dernière connexion au compte client ou du dernier envoi d'un courriel au service client, ou d'un clic sur un lien hypertexte d'un courriel adressé par CERTIGNA, ou d'une réponse positive à un courriel demandant si le client souhaite continuer à recevoir de la prospection commerciale à l'échéance du délai de trois ans.

Afin de suivre la qualité de nos services, les appels réalisés auprès de notre service client sont susceptibles d'être enregistrés et conservés durant une période de 30 jours.

Conformément à la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée et au règlement européen « 2016/679/ UE du 27 Avril 2016 » relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, vous bénéficiez d'un droit d'accès, d'opposition, de rectification, de suppression et de portabilité de vos données personnelles. Vous pouvez exercer votre droit en vous adressant par e-mail à : privacy@certigna.com, ou par courrier à l'adresse suivante :

CERTIGNA, Service du DPO,
20 Allée de Râperie, 59 650 Villeneuve d'Ascq, France

Votre demande devra indiquer votre nom et prénom, adresse e-mail ou postale, être datée, signée et accompagnée d'un justificatif d'identité en cours de validité.

9.4.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au minimum les suivantes :
- Les causes de révocation des certificats des services, des serveurs et des Porteurs ;
- Les dossiers d'enregistrement des Porteurs et des opérateurs d'AE ou d'AED.

9.4.3 Informations à caractère non personnel

Sans objet.

9.4.4 Responsabilité en termes de protection des données personnelles

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

9.4.5 Notification et consentement d'utilisation des données personnelles

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les Porteurs à l'AC ne doivent pas 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

La divulgation des informations confidentielles n'est effectuée qu'aux autorités judiciaires ou administratives habilitées officiellement et exclusivement sur leur demande expresse en conformité avec la législation française.

9.4.7 Autres circonstances de divulgation d'informations personnelles

Sans objet.

9.5 Droits sur la propriété intellectuelle et industrielle

La marque « Certigna » est protégée par le code de la propriété industrielle. Par conséquent, toute reproduction et/ou représentation, et tout usage de cette marque est prohibée sauf autorisation écrite et préalable de Certigna.

Ces stipulations ne font pas obstacle au droit du Porteur de reproduire le(s) document(s) signé(s) avec le Certificat, si la production de ce(s) Document(s) était strictement nécessaire à des fins de conservation chez un tiers archiveur à sa charge ou afin de valoir preuve, notamment pour production devant un juge le cas échéant.

9.6 Interprétations contractuelles et garanties

Les obligations communes aux composantes de l'IGC sont les suivantes :

- Protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées ;
- N'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent ;
- Respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante) ;
- Se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre 8) et l'organisme de qualification ;
- Respecter les accords ou contrats qui les lient entre elles ou à l'entité ;
- 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 s'engage à :
- Pouvoir démontrer, aux utilisateurs de ses certificats, qu'elle a émis un certificat pour un Porteur donné et que le Porteur correspondant a accepté le certificat, conformément aux exigences du chapitre 4.4 ;
- Garantir et maintenir la cohérence de sa DPC avec sa PC ;
- Prendre toutes les mesures raisonnables pour s'assurer que les Porteurs sont au courant de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'IGC.
- Fournir un service de consultation en ligne sur le site de l'AC permettant à tout moment aux tiers de vérifier la validité du certificat émis par l'AC ;
- Mettre à disposition du public 24h/24, 7j/7 les informations sur l'état (valide ou révoqué) des certificats non expirés ;
- Réaliser toute collecte et tout usage de données à caractère personnel dans le strict respect de la législation et de la réglementation en vigueur sur le territoire français, et de la Politique d'utilisation des données personnelles disponible sur le Site de l'AC ;Mettre en œuvre et suivre, lors de l'émission d'un certificat, les exigences décrites au chapitre 3.2 et 3.3 pour vérifier que les informations contenues dans le certificat sont exactes ;
- Mettre en œuvre et suivre, lors de l'émission d'un certificat, les exigences décrites au chapitre 3.2 et 3.3 pour vérifier l'identité du Porteur désigné.
- Si l'AC et l'organisation qui demande le certificat ne sont pas affiliées, ces parties s'engagent sur un accord de souscription juridiquement valide et exécutoire.

L'AC assume toute conséquence dommageable résultant du non-respect de sa PC par elle-même ou l'une de ses composantes. Elle a pris les dispositions nécessaires pour couvrir ses responsabilités liées à ses opérations et/ou activités et posséder la stabilité financière et les ressources exigées pour fonctionner en conformité avec la présente politique. De plus, l'AC reconnaît engager sa responsabilité en cas de faute ou de négligence, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des Porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des certificats de l'AC.

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

9.6.2 Service d'enregistrement

Le service d'enregistrement s'engage à vérifier et à valider les dossiers de demande de certificats.

9.6.3 Porteur

Le Porteur a le devoir de :

- Effectuer sa DEMANDE DE CERTIFICAT en suivant toutes les étapes de la procédure figurant sur le Site de CERTIGNA, de l'AE Externe ou de l'AED ;
- Communiquer des informations exactes, complètes et à jour pour la demande de certificat ;
- Transmettre à l'AE, le cas échéant à l'AED, les informations requises pour la demande de certificat en ligne sur le Site de l'AC ou sur le site de l'AE ou de l'AED le cas échéant, ainsi que les pièces justificatives.
- Informer l'AE en cas de non-réception d'un e-mail ou SMS contenant la donnée d'activation de la clé privée associée à son certificat ;
- Accepter explicitement le CERTIFICAT avant ou après sa génération et depuis son compte client CERTIGNA ou celui de l'AE Externe ou de l'AED le cas échéant. Cette acceptation peut également être tacite via la première utilisation du certificat.
- Protéger ses données d'activation et, le cas échéant, les mettre en œuvre ;
- Respecter les conditions d'usages du certificat et de la clé privée associée citées au chapitre 4.5 ;
- Ne plus utiliser un CERTIFICAT et la bi-clé associée à la suite de l'expiration ou la REVOCATION de ce CERTIFICAT ;
- Ne pas accepter la génération ou l'utilisation du certificat avant son expiration en cas de détection d'incohérence entre les informations prévues ou figurant dans le certificat ou dans l'accord contractuel ;
- Vérifier l'adéquation à son besoin du certificat et de ses caractéristiques ;
- S'assurer que les prérequis matériels et/ou logiciels préconisés par l'AC sont remplis en vue de l'utilisation du certificat ;
- Disposer de toutes les compétences et moyens nécessaires pour utiliser les certificats ;
- Prévenir sans délai la personne en charge de la sécurité des systèmes d'information de son entité (exemple : RSSI) en cas de perte ou de vol de la donnée d'activation ;
- Pour les applications jugées les plus critiques au niveau métier, mettre en place des mesures permettant de détecter des transactions potentiellement frauduleuses (incohérence des données métiers signés, etc.) et de prévoir, le cas échéant, une procédure alternative.

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 sans pour autant créer de relation contractuelle entre eux. Ces informations s'appliquent également aux opérateurs d'AE et d'AED.

9.6.4 Utilisateurs de certificats

Les tiers utilisateurs doivent :

- Vérifier et respecter l'usage pour lequel un certificat a été émis ;
- Pour chaque certificat de la chaîne de certification, du certificat d'entité finale jusqu'à l'AC racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (date de validité, statut de révocation) ;
- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.

9.6.5 Autres participants

Sans objet.

9.6.6 Résiliation

Sans objet.

9.7 Livraison et garantie

Le Porteur doit vérifier que les informations prévues ou contenues dans le certificat sont exactes. A défaut, le Porteur doit prendre contact avec un membre du personnel de l'AC, de l'AE ou de l'AED. S'il s'agit de l'AC, soit par téléphone au 0 806 115 115 (service gratuit coût d'un appel local), soit par email à l'adresse suivante : contact@certigna.fr. Le support téléphonique est disponible du lundi au vendredi, sauf jours fériés, de 9h à 18h sans interruption. Le Porteur est conscient qu'en cas d'erreur lors de la commande dans la nature même du certificat, aucune modification ne pourra être faite par l'AC et une nouvelle demande de certificat devra être réalisée par le Porteur.

Une fois la demande de certificat validée, le certificat est généré. A ce stade, aucune modification des informations ne peut être effectuée par l'AC. Il est donc de la responsabilité du Porteur de bien vérifier l'exactitude de ses informations la première fois que cela lui est demandé. A défaut, le Porteur devra faire une nouvelle demande de certificat via le site de l'AC, de l'AE ou de l'AED et le certificat généré ne donnera lieu à aucun remboursement.

Une fois le certificat accepté, celui-ci est mis à la disposition du RC ou du Porteur soit depuis son espace client, soit sur un support cryptographique. L'utilisation du certificat se fait sous la seule responsabilité du Porteur à l'aide de la donnée d'activation mise à sa disposition. En cas de difficulté quelconque pendant cette dernière phase, le Porteur peut contacter l'AE, l'AED ou l'AC au numéro de téléphone et l'adresse email de l'AC indiqués précédemment ou aux coordonnées disponibles sur le site de l'AE ou de l'AED. L'AC ne garantit pas le fonctionnement du certificat dans le cas d'une utilisation en dehors des usages prévus au chapitre 1.5 de la présente PC.

La garantie est valable pour le monde entier hors USA et Canada.

9.8 Limite de responsabilité

L'AC est soumise à une obligation générale de moyens. L'AC ne pourra voir sa responsabilité engagée à l'égard du Porteur que pour les dommages directs qui pourraient lui être imputés au titre des prestations qui lui sont confiées dans le cadre de la présente PC et des CGU associées.

La responsabilité de l'AC ne pourra pas être recherchée pour tout préjudice indirect, tel que notamment, la perte de chiffre d'affaires, la perte de bénéfice, la perte de commandes, la perte de données, la perte d'une chance, le trouble à l'image ou tout autre dommage spécial ou évènements en dehors de son contrôle ou de tout fait ne lui étant pas imputable.

L'AC n'est responsable que des tâches expressément mises à sa charge. L'AC ne saurait être tenue responsable de quelque manière que ce soit de l'utilisation faite par le Porteur du certificat, ni du contenu des documents et des données qui lui sont remis par le Porteur.

En aucun cas, la responsabilité de l'AC ne saurait être recherchée pour :
- Faute, négligence, omission ou défaillance de l'AC, qui constituerait la cause exclusive de survenance du dommage,
- Dysfonctionnement ou d'indisponibilité d'un bien matériel ou immatériel dans le cas où celui-ci a été fourni par le Porteur,
- Retard dans la fourniture des données à traiter dû au Porteur ;
- Perte de la qualification d'un tiers prestataire qui est indépendant de la volonté de CERTIGNA (Ex : le fournisseur du support cryptographique du certificat).

De convention expresse entre l'AC et le Porteur, la responsabilité de l'AC est limitée, tous préjudices confondus, à la somme de deux (2) fois le montant réglé par certificat par le tiers qui a contracté avec Certigna pour la fourniture de certificat aux porteurs dans le cadre de ses services (Ex : service de signature électronique de document avec les certificats).

9.9 Indemnités

9.9.1 Indemnisation par le CM ou le Porteur

Sans objet.

9.9.2 Indemnisation par un tiers

Sans objet.

9.10 Durée et fin anticipée de validité de la PC

9.10.1 Durée de validité

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

9.10.2 Fin anticipée de validité

La publication d'une nouvelle version des documents cités au chapitre 1.1 peut entraîner, en fonction des évolutions apportées, la nécessité pour l'AC de faire évoluer sa PC correspondante. Dans ce cas, cette mise en conformité n'imposera pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

Enfin, la validité de la PC peut arriver à terme prématurément en cas de cessation d'activité de l'AC (cf. chapitre 5.8).

9.10.3 Effets de la fin de validité et clauses restant applicables

La fin de validité de la PC met également fin à toutes les clauses qui la composent.

9.11 Notifications individuelles et communications entre les participants

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

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

9.12 Amendements à la PC

9.12.1 Procédures d'amendements

L'AC procède à toute modification des spécifications stipulées dans la PC et la DPC et/ou des composantes de l'AC qui lui apparaît nécessaire pour l'amélioration de la qualité des services de certification et de la sécurité des processus, en restant toutefois conforme aux exigences citées au chapitre 1.1.

L'AC procède également à toute modification des spécifications stipulées dans la PC et la DPC et/ou des composantes de l'AC qui est rendue nécessaire par une législation, réglementation en vigueur ou par les résultats des Contrôles. Une révision et mise à jour si nécessaire de la PC et DPC sont effectuées à minima 1 fois par an.

9.12.2 Mécanisme et période d'information sur les amendements

L'AC communique via son site Internet http://www.certigna.com l'évolution de la PC au fur et à mesure de ses amendements.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

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

Lorsque la modification de la PC est de nature typographique ou lorsque la modification de la PC n'impacte pas le niveau de qualité et de sécurité des fonctions de l'AC et de l'AE les OID de la DPC et de la PC correspondante ne sont pas modifiés.

9.13 Dispositions concernant la résolution de conflits

La validité de la présente DPC et toute autre question ou litiges relatifs à son interprétation, à son exécution ou à sa résiliation seront régis par le droit français.

L'AC et le Porteur s'engagent à consacrer leurs meilleurs efforts à la résolution amiable de toutes les questions ou de tous les litiges qui pourraient les diviser, préalablement à la saisie de la juridiction ci-après désignée.

9.14 Juridictions compétentes

L'AC et le Porteur conviennent, pour le cas où un accord amiable serait impossible à arrêter, que les juridictions de Lille auront compétences exclusives pour connaître de tout différend résultant de la validité, de l'interprétation, de l'exécution ou de la résiliation des présentes, et plus généralement de tout litige procédant des présentes qui pourrait les diviser, nonobstant pluralités des défendeurs ou appel en garantie.

9.15 Conformité aux législations et réglementations

La présente PC est soumise au droit français et aux textes législatifs applicables à la présente PC.

Les pratiques de services de confiance en vertu desquelles l'AC opère sont non-discriminatoires.

9.16 Dispositions diverses

9.16.1 Accord global

Le présent document contient l'intégralité des clauses régissant l'IGC.

9.16.2 Transfert d'activités

Cf. chapitre 5.8.

9.16.3 Conséquences d'une clause non valide

En cas d'une clause non valide, les autres clauses ne sont pas remises en question.

En cas de conflit entre les exigences de cette DPC et une loi, un règlement ou une ordonnance gouvernementale (ci-après la « Loi ») de toute juridiction dans laquelle l'AC exploite ou émet des certificats, l'AC peut modifier toute exigence contradictoire dans la mesure du possible afin que l'exigence soit valide et légale dans la juridiction. Cela s'applique uniquement aux opérations ou aux émissions de certificats qui sont assujetties à cette Loi. Dans un tel cas, l'AC inclura immédiatement dans cette section (et avant de délivrer un certificat en vertu de l'exigence modifiée) une référence détaillée à la Loi exigeant une

modification des exigences et les modifications spécifiques apportées à ces exigences par l'AC.

9.16.4 Application et renonciation

Aucune renonciation à se prévaloir de l'un de ses droits ne saurait intervenir tacitement. Pour être opposable à l'AC une renonciation doit avoir été formulée par écrit. Une telle renonciation ne saurait constituer une renonciation pour l'avenir aux dits droits.

9.16.5 Force majeure

L'AC ne pourra être tenue pour responsable de tout retard ou manquement dans l'exécution de l'une quelconque de ses obligations au titre de la présente DPC, si ledit retard ou manquement est dû à la survenance d'un cas de force majeure habituellement reconnu par la jurisprudence des cours et tribunaux français, notamment le cas d'un événement irrésistible, insurmontable et imprévisible.

9.17 Autres dispositions

Sans objet.

10 ANNEXE 1 : EXIGENCE DE SECURITE DU MODULE CRYPTOGRAPHIQUE DE L'AC

10.1 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 et des réponses OCSP), répond aux exigences de sécurité suivantes :

- Assurer la confidentialité et l'intégrité des clés privées de signature de l'AC durant tout leur cycle de vie, et assurer leur destruction sûre en fin de vie ;
- Etre capable d'identifier et d'authentifier ses utilisateurs ;
- Limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- Etre capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- Permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas les clés privées de l'AC et qui ne peut pas être falsifiée sans la connaissance de ces clés privées ;
- Créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- Si une fonction de sauvegarde et de restauration des clés 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.

10.2 Exigences sur la qualification

Le module cryptographique utilisé par l'AC doit être certifié Critères Communs au niveau EAL4+ ou FIPS 140-2 Level 3.

11 ANNEXE 2 : EXIGENCES DE SÉCURITÉ DU DISPOSITIF UTILISÉ POUR LE PORTEUR

11.1 Exigences sur les objectifs de sécurité

Le dispositif utilisé pour stocker et mettre en œuvre la clé privée du Porteur 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 ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Garantir la confidentialité et l'intégrité de la clé privée ;
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif ;

11.2 Exigences sur la qualification

Aucune exigence.

CERTIGNA
by tessi

www.certigna.com