Politique de certification
CERTIGNA IDENTITY CA

OID :	1.2.250.1.177.2.3.1
Version :	1.9
Edité le :	26/02/2019
Auteurs :	J. Allemandou
Classification :	Publique

CERTIGNA est la marque des services de certification électronique de DHIMYOTIS

SOMMAIRE

HISTORIQUE DU DOCUMENT

Date	Version	Auteurs	Evolution du document
05/03/2015	1.0	Y. LEPLARD	Création
28/04/2015	1.1	R. DELVAL	Archivage des réponses OCSP
19/10/2015	1.2	R. DELVAL	Ajout des certificats d'authentification et de signature
16/02/2016	1.3	R. DELVAL	Changement du calcul du « serialNumber » du DN
01/08/2016	1.4	J. ALLEMANDOU	Précisions sur la vérification de l'adresse email (cf. 3.2)
25/10/2016	1.5	J. ALLEMANDOU	Extension « msEFS » dans les certificats de chiffrement
16/12/2016	1.6	J. ALLEMANDOU	Révision de la charte graphique et précisions sur : - le niveau de conformité aux spécifications ETSI (cf. 1.1), - la sémantique du « serialNumber » du DN (cf. 3.1.5), - le retrait de la mention « Certifié conforme » (cf. 3.2.3), - les modalités de renouvellement courant (cf. 3.3.1), - les modalités d'acceptation du certificat (cf. 4.4.1), - le rôle d'officier d'enregistrement (cf. 5.2.1), - la durée minimale d'archivage (cf. 5.5.2), - la transmission des données d'activation (cf. 6.4.1), - les certificats de l'AC émis par deux AC Racine (cf. 7), - les exigences sur la qualification du dispositif (cf. 11.2).
01/09/2017	1.7	J. ALLEMANDOU	Ajout de l'extension « ExpiredCertsOnCRL » (7.3.2)
25/01/2018	1.8	J. ALLEMANDOU	Précisions apportées sur : - l'email de contact de Certigna (cf. 1.6.2), - le formulaire pour signaler un certificat (cf. 2.3), - la périodicité de mise à jour de l'ARL et des LCR (cf. 2.4), - les causes possibles d'une révocation (cf. 4.9.1), - les accès physiques (cf. 5.1.2), - le schéma de la hiérarchie d'AC (cf. 7), - la longueur maximale du numéro de série (cf. 7), - la qualification du module cryptographique de l'AC (cf. 10.2).
20/02/2019	1.9	J. ALLEMANDOU	Précisions apportées sur : - Délai de délivrance des certificats (cf. 4.2.3), - Pratiques de séquestre (cf. 4.12), - La protection des données à caractère personnel (cf. 9.4.1).

1. INTRODUCTION

1.1. Présentation générale

Certigna s'est dotée de l'Autorité de Certification (AC) nommée « Certigna Identity CA » pour délivrer des certificats destinés à des personnes physiques.

La présente Politique de Certification (PC) expose les pratiques que l'AC applique et s'engage à respecter dans le cadre de la fourniture de son service de certification électronique. La PC identifie également les obligations et exigences portant sur les autres intervenants, les utilisateurs de certificat.

L'attention du lecteur est attirée sur le fait que la compréhension de la présente PC suppose qu'il soit familiarisé avec les notions liées à la technologie des Infrastructures de Gestion de Clés (IGC).

La présente PC vise la conformité à :
- La PC Type « *Certificats électroniques de personnes* » pour les usages d'authentification et signature et de chiffrement au niveau * du Référentiel Général de Sécurité (RGS) élaboré par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) ;
- Au règlement européen eIDAS au niveau LCP de l'ETSI EN 319 411-1.

1.2. Identification du document

La présente PC peut être identifiée par le nom de l'AC « Certigna Identity CA » ainsi que par son OID : 1.2.250.1.177.2.3.1

Usage(s)	RGS	ETSI / Niveau	Type	OID
Chiffrement	*	EN 319 411-1 LCP	Particulier	1.2.250.1.177.2.3.1.3.1
Chiffrement	*	EN 319 411-1 LCP	Professionnel	1.2.250.1.177.2.3.1.1.1
Authentification et signature	*	EN 319 411-1 LCP	Particulier	1.2.250.1.177.2.3.1.4.1
Authentification et signature	*	EN 319 411-1 LCP	Professionnel	1.2.250.1.177.2.3.1.2.1

1.3. Définitions et acronymes

1.3.1. Acronymes

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

AA	Autorité Administrative
AAP	Autorité d'Approbation des Politiques
AC	Autorité de Certification
AE	Autorité d'Enregistrement
AED	Autorité d'Enregistrement Déléguée
AH	Autorité d'Horodatage
ANSSI	Agence nationale de la sécurité des systèmes d'information
ANTS	Agence Nationale des Titres Sécurisés
CGU	Conditions Générales d'Utilisation
CNIL	Commission Nationale de l'Informatique et des Libertés
CSR	Certificate Signature Request
DN	Distinguished Name
DNS	Domain Name System
DPC	Déclaration des Pratiques de Certification
ETSI	European Telecommunications Standards Institute
FQDN	Fully Qualified Domain Name
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
LCP	Lightweight Certificate Policy
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
RSA	Rivest Shamir Adleman
SGMAP	Secrétariat Général pour la Modernisation de l'Action Publique
SP	Service de Publication
SSI	Sécurité des Systèmes d'Information
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
UTC	Universal Time Coordinated

1.3.2. Définitions

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

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

Applicatif de vérification de cachet - Il s'agit de l'application mise en œuvre par l'utilisateur pour vérifier le cachet des données reçues à partir de la clé publique du serveur contenue dans le certificat correspondant.

Applications utilisatrices - Services applicatifs exploitant les certificats émis par l'Autorité de Certification pour des besoins de cachet du service auquel le certificat est rattaché.

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).

Autorité d'horodatage - Autorité responsable de la gestion d'un service d'horodatage.

Cachet serveur – Signature numérique effectuée par un serveur applicatif sur des données dans le but de pouvoir être utilisée soit dans le cadre d'un service d'authentification de l'origine des données, soit dans le cadre d'un service de non répudiation.

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 (ex. clé privée, code PIN, …). Il peut prendre la forme 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.

FQDN - Nom de domaine pleinement qualifié indiquant la position absolue d'un nœud dans l'arborescence DNS et précisant les domaines de niveau supérieur jusqu'à la racine.

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 Autorités révoquées - 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.

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 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.

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 ou une valeur d'authentification provenant d'un porteur de certificat ou chiffrer des données à destination d'un porteur de certificat.

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

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).

Chiffrement
- Fonction de gestion des recouvrements ; - Fonction de séquestre et recouvrement.

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 présente PC. 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 certificat et de la gestion des révocations ont une structure documentée qui préserve l'impartialité des opérations.

1.4.2. Autorité d'enregistrement

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

- La prise en compte et la vérification des informations du futur Porteur et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- La prise en compte et la vérification des informations, le cas échéant, du futur mandataire de certification (*) et de son entité de rattachement et la constitution du dossier d'enregistrement correspondant ;
- L'établissement et la transmission de la demande de certificat à l'AC ;
- L'archivage des dossiers de demande de certificat ;
- La conservation et la protection en confidentialité et intégrité des données personnelles d'authentification du Porteur ou du MC ;
- La vérification des demandes de révocation de certificat.

L'AE assure ces fonctions directement ou en les sous-traitant en partie à des autorités d'enregistrement déléguées. Dans tous les cas, l'AE en garde la responsabilité.

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

(*) : L'AE offre la possibilité à l'entité cliente d'utiliser un mandataire de certification 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.

Dans tous les cas l'archivage des pièces du dossier d'enregistrement (sous forme électronique et/ou papier) est de la responsabilité de l'AE.

1.4.3. Porteurs de certificats

Dans le cadre de la présente PC, 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 en relation avec l'entité identifiée dans le certificat et avec laquelle il a un lien contractuel, hiérarchique ou réglementaire.

Le porteur respecte les conditions qui lui incombent, conditions définies dans la PC et dans les CGU.

Dans la suite du document le terme « entité » est utilisé pour désigner une entreprise ou une administration. La dénomination « entreprise » recouvre les entreprises au sens le plus large, à savoir toutes personnes morales de droit privé : sociétés, associations ainsi que les artisans et travailleurs indépendants.

1.4.4. Utilisateurs de certificats

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

Authentification et Signature
- Un service en ligne qui utilise un certificat et un dispositif de vérification d'authentification soit pour valider une demande d'accès faite par le porteur du certificat dans le cadre d'un contrôle d'accès, soit pour authentifier l'origine d'un message ou de données transmises par le porteur du certificat ; - Un 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 destinataire d'un message ou de données et qui utilise un certificat et un dispositif de vérification d'authentification afin d'en authentifier l'origine. - Un 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.

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

1.4.5. Autres participants

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

- D'autoriser, d'effectuer une demande de certificat ou de renouvellement de certificat ;
- D'effectuer une demande de révocation de certificat ;
- Le cas échéant, d'enregistrer les mandataires de certification au sein des entités émettrices de demandes de certificat.

Il assure pour l'AC, 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. Il est pour cela en relation directe avec l'AE.

Les engagements de l'opérateur d'AED à l'égard de l'AC sont précisés dans un contrat écrit avec l'entité responsable de l'opérateur ainsi que dans la lettre d'engagement que doit signer ce dernier. Ces deux documents précisent notamment que l'opérateur d'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 PC et de la DPC lui incombant.

L'AC offre la possibilité à l'entité cliente de désigner un ou plusieurs mandataires de certification (MC). Ce mandataire a, par la loi ou par délégation, le pouvoir :
- D'autoriser, d'effectuer une demande de certificat ou de renouvellement de certificat portant le nom de l'entité ;
- D'effectuer une demande de révocation de certificat portant le nom de l'entité.

Le mandataire de certification peut être un représentant légal ou toute personne que ce dernier aura formellement désignée. Il assure pour l'AC, 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. Il est pour cela en relation directe avec l'Autorité d'Enregistrement.

Les engagements du mandataire à l'égard de l'AC sont précisés dans un contrat écrit avec l'entité responsable du MC ainsi que dans la lettre d'engagement que doit signer le mandataire. Ces deux documents précisent notamment que le MC doit effectuer de façon impartiale et scrupuleuse les contrôles d'identité et des éventuels attributs des futurs Porteurs, et respecter les parties de la PC et de la DPC lui incombant.

L'entité doit signaler sans délai à l'AC le départ du MC de ses fonctions et lui désigner éventuellement un successeur. Le MC ne doit pas avoir accès aux données d'activation de la clé privée associée au certificat délivré au Porteur.

1.5. Usage des certificats

1.5.1. Domaines d'utilisation applicables

Bi-clés et certificats des porteurs

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

Authentification et Signature
- Authentification des porteurs auprès de serveurs distants ou auprès d'autres personnes. Il peut s'agir d'authentification dans le cadre d'un contrôle d'accès à un serveur ou une application, ou de l'authentification de l'origine de données dans le cadre de la messagerie électronique. - Signature électronique de données. 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.

Les certificats électroniques sont utilisés par des applications pour lesquelles les besoins de sécurité sont moyens eu égard aux risques élevés qui les menacent (usurpation d'identité, …).

Bi-clés et certificats d'AC et de composantes

L'AC dispose d'un seul bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur (AC Racine). La bi-clé de l'AC permet de signer et de vérifier les différents types d'objets qu'elle génère : certificats des porteurs, certificat OCSP de l'AC, LCR.

Les opérateurs de l'IGC disposent de certificats permettant de s'authentifier sur cette IGC. Pour les opérateurs d'AE (les opérateurs d'AED n'étant pas concernés), ce certificat permet de signer les demandes de certificats et de révocation avant leur transmission à l'AC. Ces certificats sont émis par une IGC distincte, interne à Certigna, et dont le niveau de sécurité est adapté à celui requis pour l'AC.

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, MC et utilisateurs potentiels des CGU qui peuvent être consultées sur le site https://www.certigna.fr 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 présidé par le responsable Sécurité.

Ce comité est responsable de l'élaboration, du suivi, de la modification et de la validation de la présente PC. Il statue sur toute modification nécessaire à apporter à la PC à échéance régulière.

1.6.2. Point de contact

Dhimyotis - Certigna
20 allée de la Râperie
Zone de la plaine
59650 Villeneuve d'Ascq
FRANCE

Contact mail **:** contact@certigna.fr

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'information » de l'entreprise. Le Comité de Sécurité s'assure que les moyens mis en œuvre et décrits dans la 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.

2. RESPONSABILITE CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS

2.1. Entités chargées de la mise à disposition des informations

Dhimyotis 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. Ces informations sont publiées au travers de plusieurs serveurs :

- Serveurs Web :
    - http://crl.certigna.fr/identityca.crl
    - http://crl.dhimyotis.com/identityca.crl
- Serveurs OCSP :
    - http://identityca.ocsp.certigna.fr
    - http://identityca.ocsp.dhimyotis.com

2.2. Informations devant être publiées

L'AC publie à destination des Porteurs et utilisateurs de certificats :

- La PC ;
- 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 le certificat d'AC intermédiaire en cours de validité ;
- La liste des certificats révoqués (LAR / LCR) ;
- La DPC sur demande expresse auprès de Dhimyotis.

Remarque : compte tenu de la complexité de lecture d'une PC pour les Porteurs ou les utilisateurs de certificats non spécialistes du domaine, l'AC publie en dehors des PC et DPC des CGU que le futur Porteurs 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.

2.2.1. Publication de la documentation

Publication de la PC, des conditions générales et des formulaires

La PC, les conditions générales d'utilisation et les différents formulaires nécessaires pour la gestion des certificats sont publiés sous forme électronique à l'adresse https://www.certigna.fr

La PC est également publiée à l'adresse https://www.dhimyotis.com.

Publication de la DPC

L'AC publie, à destination des Porteurs et utilisateurs de certificats, et sur leur demande, sa DPC pour rendre possible l'évaluation de la conformité avec sa politique de certification. Les

détails relatifs à ses pratiques ne sont toutefois pas rendus publics.

Publication des certificats d'AC

Les Porteurs et les utilisateurs de certificat peuvent accéder aux certificats d'AC qui sont publiés aux adresses suivantes :
- https://www.certigna.fr/autorites,
- https://www.dhimyotis.com/autorites.

2.2.2. Publication de la LCR

La liste des certificats révoqués est publiée au format électronique aux adresses décrites dans le chapitre 2.1 ci-dessus. Ces adresses sont également indiquées dans les certificats émis par l'AC.

2.2.3. Publication de la LAR

La liste des certificats d'autorité intermédiaire révoqués est publiée sous format électronique aux adresses décrites dans le chapitre 2.1 ci-dessus. Ces adresses sont également indiquées dans les certificats émis par l'AC racine.

2.3. 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 : compromission, 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.fr/contact.xhtml et sélectionner l'objet « Certificat jugé malveillant ou dangereux ».

2.4. Délais et fréquences de publication

2.4.1. Publication de la documentation

La PC, 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.

2.4.2. 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.

2.4.3. Publication de la LCR

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

2.4.4. Publication de la LAR

La LAR est mise à jour au minimum tous les ans, et à chaque nouvelle révocation.

2.5. 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, au travers d'un contrôle d'accès fort, basé sur une authentification à deux facteurs.

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 le porteur (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 le porteur du certificat. Il est construit à partir des prénom et nom de son état civil porté sur le document d'identité présenté lors de son enregistrement auprès de l'AE ou du MC.

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

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

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 d'une ou plusieurs lettres indiquant le(s) usage(s) du certificat :

- "I" pour « Authentification » et « Signature »,
- "C" pour "Chiffrement" uniquement,

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.

3.1.6. Identification, authentification et rôle des marques déposées

L'AC est responsable de l'unicité des noms des porteurs 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 peut se faire soit directement auprès de l'AE (ou d'un AED), soit via un mandataire de certification de l'entité. Dans ce dernier cas, le mandataire de certification doit être préalablement enregistré auprès de l'AE.

Lors de la demande de certificat, l'adresse email du Porteur est vérifiée au travers de l'envoi de plusieurs emails qui permettent au Porteur d'accéder à son compte client Certigna et à certaines données d'activation lui permettant ainsi de récupérer et d'utiliser son certificat.

3.2.1. Méthode pour prouver la possession de la clé privée

L'AC s'assure de la détention de la clé privée par le Porteur avant de certifier la clé publique. Pour cela, l'AE génère la bi-clé sur un dispositif conforme aux exigences du chapitre 11, et fournit à l'AC une preuve de possession de sa clé privée en signant sa demande de certificat (Certificate Signing Request au format PKCS#10).

3.2.2. Validation de l'identité d'un organisme

Cf. chapitre 3.2.3

3.2.3. Validation de l'identité d'un individu

L'enregistrement d'un Porteur peut se faire soit directement auprès de l'AE, soit via un mandataire de certification de l'entité. Dans ce dernier cas, le MC doit être préalablement enregistré par l'AE.

L'enregistrement du futur Porteur nécessite la validation :

- de l'identité du futur Porteur [Particulier] [Entreprise] [Administration]
- de l'identité "personne morale" de l'entité **[Entreprise] [Administration]**
- du rattachement du futur porteur à cette entité **[Entreprise] [Administration]**

Enregistrement d'un Porteur [Particulier] sans MC

Le dossier de demande de certificat est à compléter depuis les formulaires disponibles sur le site de Certigna. Une fois complétés, les éléments suivants doivent être transmis à l'AE :

Formulaire de demande du certificat	
Objet	Désignation du futur Porteur habilité et de ses coordonnées
	Désignation des CGU applicables (Incluant l'obligation du porteur sur l'utilisation d'un dispositif conforme aux exigences du chapitre 11)
Date	Signature du formulaire de moins de 3 mois
Signature	Signature du futur Porteur pour accepter le rôle de Porteur et les CGU

Pièce d'identité officielle du Porteur	
Objet	La photocopie d'un document officiel d'identité en cours de validité du futur Porteur comportant une photographie d'identité. *Exemple : carte nationale d'identité, passeport ou carte de séjour*
Date	Pièce valide au moment de l'enregistrement

L'authentification du futur porteur par l'AE (opérateur d'AE ou opérateur d'AED) est réalisée par l'envoi du dossier soit par courrier postal, soit sous forme dématérialisée (dossier scanné puis transmis par courrier électronique).

Le Porteur est informé que les informations personnelles d'identité pourront être utilisées comme données d'authentification lors d'une éventuelle demande de révocation.

Enregistrement d'un Porteur [Entreprise][Administration] sans MC

Le dossier de demande de certificat est à compléter depuis les formulaires disponibles sur le site de Certigna. Une fois complétés, les éléments suivants doivent être transmis à l'AE :

Formulaire de demande du certificat	
Objet	Désignation du futur Porteur habilité et de ses coordonnées
	Désignation des CGU applicables (Incluant l'obligation du Porteur sur l'utilisation d'un dispositif conforme aux exigences du chapitre 11)
	Désignation de l'identité de l'entité à laquelle est rattaché le Porteur
	Désignation d'un représentant légal de l'entité et de ses coordonnées
Date	Signature du formulaire de moins de 3 mois
Signature	Signature du futur Porteur pour accepter le rôle de Porteur et les CGU
	Signature d'un représentant légal de l'entité pour habiliter le futur Porteur

Pièce d'identité officielle du Porteur	
Objet	La photocopie d'un document officiel d'identité en cours de validité du futur Porteur ou d'une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintient un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent.
Date	Pièce valide au moment de l'enregistrement

Pièce d'identité officielle du Représentant légal	
Objet	La photocopie d'un document officiel d'identité en cours de validité du représentant légal ou d'une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintient un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent.
Date	Pièce valide au moment de l'enregistrement

Justificatif attestant de la qualité du Représentant légal	
Objet	**[Entreprise]** Tout document attestant de la qualité du représentant légal de l'entité reconnu à l'échelle nationale. *Ex : un exemplaire des statuts de l'entreprise, en cours de validité, portant signature de ses représentants.* **[Administration]** Une pièce portant délégation ou subdélégation de l'autorité responsable de la structure administrative reconnue à l'échelle nationale.
Date	Justificatif valide au moment de l'enregistrement

Justificatif portant le numéro de SIREN de l'entité	
Objet	**[Entreprise]** Toute pièce portant le numéro SIREN de l'entreprise ou, à défaut, une autre pièce valide attestant l'identification unique de l'entreprise qui figurera dans le certificat. *Ex : extrait KBIS ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements*

Date	Justificatif valide au moment de l'enregistrement

L'authentification du futur porteur par l'AE (opérateur d'AE ou opérateur d'AED) est réalisée par l'envoi du dossier soit par courrier postal, soit sous forme dématérialisée (dossier scanné puis transmis par courrier électronique).

Le Porteur est informé que les informations personnelles d'identité pourront être utilisées comme données d'authentification lors d'une éventuelle demande de révocation.

Enregistrement du mandataire de certification (MC) [Entreprise][Administration]

Le mandataire de certification (MC) doit s'enregistrer auprès de l'AE pour pouvoir se substituer à l'AE dans le processus d'enregistrement des demandeurs de certificats.

L'enregistrement d'un MC nécessite la validation de l'identité "personne morale" de l'entité pour laquelle le MC interviendra, de l'identité "personne physique" du futur MC, et du rattachement du futur MC à cette entité. Le dossier d'enregistrement d'un mandataire de certification est à compléter depuis les formulaires disponibles sur le site de Certigna. Le dossier transmis à l'AE doit comprendre les éléments suivants :

Formulaire de demande d'enregistrement d'un mandataire	
Objet	Désignation d'un représentant légal de l'entité et de ses coordonnées
	Désignation du futur MC habilité et de ses coordonnées
	Désignation de l'identité de l'entité à laquelle est rattaché le MC
Date	Signature du formulaire de moins de 3 mois
Signature	Signature d'un représentant légal de l'entité pour habiliter le futur MC Signature du futur MC pour accepter ce rôle

Lettre d'engagement du mandataire	
Objet	Désignation du futur mandataire habilité et de ses coordonnées
	Désignation du rôle et des responsabilités du mandataire dont notamment : - Effectuer de façon impartiale et scrupuleuse les contrôles d'identité des futurs Porteurs tels que définis dans la PC ; - Informer l'AE en cas de départ de l'entité.
Date	Signature du formulaire de moins de 3 mois
Signature	Signature du futur MC pour s'engager à respecter ces responsabilités

Pièce d'identité officielle du mandataire	
Objet	La photocopie d'un document officiel d'identité en cours de validité du mandataire ou d'une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintient un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent.
Date	Pièce valide au moment de l'enregistrement

Justificatif attestant de la qualité du Représentant légal	
Objet	**[Entreprise]** Tout document attestant de la qualité du représentant légal de l'entité reconnu à l'échelle nationale. *Ex : un exemplaire des statuts de l'entreprise, en cours de validité, portant signature de ses représentants.* **[Administration]** Une pièce portant délégation ou subdélégation de l'autorité responsable de la structure administrative reconnue à l'échelle nationale.
Date	Justificatif valide au moment de l'enregistrement

Justificatif portant le numéro de SIREN de l'entité	
Objet	**[Entreprise]** Toute pièce portant le numéro SIREN de l'entreprise ou, à défaut, une autre pièce valide attestant l'identification unique de l'entreprise qui figurera dans le certificat. *Ex : extrait KBIS ou Certificat d'Identification au Répertoire National des Entreprises et de leurs Etablissements*
Date	Justificatif valide au moment de l'enregistrement

L'authentification du MC par l'AE s'effectue via l'envoi du dossier papier par courrier accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, MC).

Cette authentification peut également se faire sous forme dématérialisée à condition que les différentes pièces justificatives du dossier soient signées à l'aide d'un procédé de signature électronique conforme aux exigences du niveau * et que la signature soit vérifiée et valide au moment de l'enregistrement. Si le mandataire n'est pas équipé d'un certificat de niveau * ou supérieur, les dossiers ne pourront être envoyés sous forme dématérialisée. Dans ce cas, chaque dossier ne sera validé qu'après réception des documents originaux par courrier.

Le mandataire de certification est informé que les informations personnelles d'identité pourront être utilisées comme données d'authentification lors d'une éventuelle demande de révocation.

Enregistrement d'un Porteur via un MC [Entreprise][Administration]

L'enregistrement d'un Porteur via un MC nécessite la validation par le MC de l'identité "personne physique" du futur Porteur et de son rattachement à l'entité pour laquelle le MC intervient. Le dossier de demande de certificat est à compléter depuis les formulaires disponibles sur le site de Certigna. Le dossier transmis à l'AE doit comprendre les éléments suivants :

Formulaire de demande du certificat	
Objet	Désignation du futur Porteur habilité et de ses coordonnées
	Désignation des CGU applicables (Incluant l'obligation du Porteur sur l'utilisation d'un dispositif conforme aux exigences du chapitre 11)
	Désignation de l'identité de l'entité à laquelle est rattaché le Porteur
	Désignation d'un MC de l'entité et de ses coordonnées
Date	Signature du formulaire de moins de 3 mois
Signature	Signature du futur Porteur pour accepter le rôle de Porteur et les CGU
	Signature du MC de l'entité pour habiliter le futur Porteur

Pièce d'identité officielle du Porteur	
Objet	La photocopie d'un document officiel d'identité en cours de validité du futur Porteur ou d'une carte professionnelle délivrée par une autorité administrative (dans le cas où cette autorité maintient un registre des identités garantissant le lien entre l'agent et la carte professionnelle), comportant une photographie d'identité (notamment carte nationale d'identité, passeport ou carte de séjour) ou une référence au dossier administratif de l'agent.
Date	Pièce valide au moment de l'enregistrement

L'authentification du porteur par le MC peut se faire par l'envoi du dossier papier par courrier accompagné d'une photocopie des documents d'identité de chacun des signataires des pièces du dossier (représentant légal, [porteur/MC]). Cette authentification peut également se faire sous forme dématérialisée à condition que les différentes pièces justificatives du dossier soient signées à l'aide d'un procédé de signature électronique conforme aux exigences du niveau (*) décrites dans le document [RGS_A1] et que la signature soit vérifiée et valide au moment de l'enregistrement.

Lors de la transmission des dossiers de porteurs par le MC, celui-ci doit s'authentifier auprès de l'AE par le paraphe du MC apposé sur les différentes pages du dossier de demande, complété par sa signature sur les principales pages.

3.2.4. Informations non vérifiées du Porteur

Sans objet.

3.2.5. Validation de l'autorité du demandeur

Cette étape est effectuée en même temps que la validation de l'identité de la personne physique (directement par l'AE ou par le MC).

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

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. Identification et validation pour un renouvellement courant

Lors du premier renouvellement, la vérification de l'identité du porteur est optionnelle. Elle est laissée à l'appréciation de l'AC qui engage sa responsabilité quant à la validité des informations contenues dans le certificat renouvelé. Lors du renouvellement suivant, l'AE identifie le porteur selon la même procédure que pour l'enregistrement initial.

3.3.2. Identification et validation pour un renouvellement après révocation

La vérification de l'identité du Porteur est identique à la demande initiale.

3.4. Identification et validation d'une demande de révocation

La demande de révocation du certificat par le Porteur, un représentant légal de l'entité, un opérateur d'AED, ou le cas échéant un MC, peut s'effectuer par l'un des moyens suivants :

- Courrier : demande remplie et signée à partir du formulaire de révocation d'un certificat disponible sur le site de Certigna https://www.certigna.fr. Le demandeur s'authentifie en joignant la photocopie de sa pièce d'identité au courrier envoyé.
- Depuis l'espace client du site Certigna https://www.certigna.fr en sélectionnant le certificat à révoquer.

L'adresse postale du service de révocation est disponible sur le site de Certigna https://www.certigna.fr

La demande papier doit comporter les éléments suivants :

- Le prénom et le nom du Porteur ;
- L'adresse e-mail du Porteur ;
- La raison de la révocation.

Si le Porteur n'est pas le demandeur :

- Le prénom et le nom du demandeur ;
- La qualité du demandeur (responsable légal, opérateur d'AED, MC) ;
- Le numéro de téléphone du demandeur.

Le formulaire papier peut également être transmis sous format électronique. La demande électronique peut être effectuée par une personne habilitée munie d'un certificat de même niveau ou supérieur (un opérateur d'AED ou le cas échéant un MC). La demande sera alors signée électroniquement avec ce certificat de même niveau ou supérieur.

4. EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1. Demande de certificat

4.1.1. Origine d'une demande de certificat

Pour [Entreprise] et [Administration] la demande de certificat doit émaner d'un représentant légal de l'entité ou d'un MC dûment mandaté pour cette entité, avec un consentement préalable du futur Porteur.

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

Le dossier de demande est établi soit directement par le futur Porteur à partir des éléments fournis par son entité, soit par son entité et signé par le futur Porteur. Le dossier est transmis directement à l'AE si l'entité n'a pas mis en place de MC. Le dossier est remis à ce dernier dans le cas contraire. Lors de l'enregistrement du futur Porteur, ce dernier doit fournir une adresse mail qui permet à l'AE de prendre contact pour toute question relative à son enregistrement. Le MC doit également fournir une adresse mail lors de son enregistrement, pour que l'AE puisse prendre contact avec ce dernier pour toute question relative à l'enregistrement des Porteurs. Le dossier de demande de certificat doit contenir les éléments décrits au chapitre 3.2.3.

4.2. Traitement d'une demande de certificat

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

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

- Validation de l'identité du futur porteur ;
- [Entreprise][Administration] Validation de l'identité de l'entité ;
- Validation de l'identité des signataires de la demande (Porteur, représentant légal) ;
- 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.

L'identité du futur Porteur et du représentant légal est approuvée si les pièces justificatives fournies sont valides à la date de réception.

Dans le cas d'une demande via un opérateur d'AED, ce dernier retransmet le dossier à l'AE après avoir effectué les opérations ci-dessus. L'AE s'assure alors que la demande correspond au mandat de l'opérateur d'AED.

Dans le cas d'une demande via un MC, ce dernier retransmet le dossier à l'AE après avoir effectué en partie les opérations ci-dessus (validation de l'identité du futur Porteur, validation

du dossier, assurance de la prise de connaissance des conditions générales). L'AE s'assure alors que la demande correspond au mandat du MC. Dans tous les cas, le dossier de demande est archivé par l'AE.

4.2.2. Acceptation ou rejet de la demande

Après traitement de la demande, l'AE notifie le rejet éventuel de la demande au Porteur, le cas échéant à l'opérateur d'AED, ou au MC.

La justification d'un éventuel refus est effectuée par l'AE en précisant la cause :
- Le dossier de demande est incomplet (pièce manquante) ;
- Une des pièces du dossier est non valide (date de signature supérieure à 3 mois, date de validité de la pièce est dépassée, etc.) ;
- La demande ne correspond pas au mandat de l'opérateur d'AED ou du MC ;

En cas d'acceptation par l'AE, après génération du certificat par l'AC, l'AE envoie un mail au Porteur pour effectuer l'importation du certificat.

4.2.3. Durée d'établissement du certificat

A compter de la réception du dossier d'enregistrement complet et de la demande électronique (CSR), le certificat est établi dans un délai de 30 jours.

4.3. Délivrance du certificat

4.3.1. Actions de l'AC concernant la délivrance du certificat

Suite à la validation 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

Le certificat complet et exact est mis à disposition de son Porteur (depuis l'espace client). Le Porteur s'authentifie sur son espace client pour accepter son certificat ou remplit un formulaire au format Papier.

4.4. Acceptation du certificat

4.4.1. Démarche d'acceptation du certificat

L'acceptation peut être réalisée de deux façons :
- Soit, lors de l'installation du certificat, le Porteur choisit explicitement d'accepter ou non le certificat depuis son espace client. La notification d'acceptation ou de refus est transmise automatiquement à l'AC.
- Soit le Porteur notifie explicitement l'acceptation ou non du certificat en complétant un formulaire papier qui sera envoyé par courrier ou remis lors d'un face à face.

En cas de détection d'incohérence entre les informations figurant dans l'accord contractuel et le contenu du certificat, le Porteur doit refuser le certificat, ce qui aura pour conséquence sa révocation.

4.4.2. Publication du certificat

Aucune publication n'est effectuée après l'acceptation du certificat par son porteur.

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 délivrance, au Porteur, du certificat généré.

4.5. Usages de la bi-clé et du certificat

4.5.1. Utilisation de la clé privée et du certificat par le Porteur

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

Faisant partie du dossier d'enregistrement, les conditions générales sont portées à la connaissance du Porteur ou du MC par l'AC avant d'entrer en relation contractuelle. Elles sont consultables préalablement à toute demande de certificat en ligne. Elles sont accessibles sur le site https://www.certigna.fr.

Les conditions acceptées par le Porteur lors de la demande de certificat restent applicables pendant toute la durée de vie du certificat, ou le cas échéant jusqu'à l'acceptation et la signature par le Porteur de nouvelles conditions générales émises et portées à sa connaissance par l'AC via le site https://www.certigna.fr. Les nouvelles conditions signées doivent être transmises par le Porteur à l'AC pour être applicables.

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).

Dans le cas où le Porteur génère la bi-clé, il s'engage en acceptant les Conditions Générales d'Utilisation, à générer une nouvelle bi-clé à chaque demande.

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

4.7.1. Causes possibles de changement d'un bi-clé

Les bi-clés doivent être périodiquement renouvelées afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des Porteurs, et les certificats correspondants, sont renouvelés (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 du Porteur.

4.7.2. Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat est à l'initiative du Porteur (pas d'existence de processus automatisé). L'entité, via son MC le cas échéant, peut également être à l'initiative d'une demande de fourniture d'un nouveau certificat pour un porteur qui lui est rattaché.

4.8. Modification du certificat

La modification des certificats de Porteurs 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.

4.9. Révocation et suspension des certificats

4.9.1. Causes possibles d'une révocation

Certificats des porteurs

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

- Les informations du Porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat (par exemple, modification de l'identité), ceci avant l'expiration normale du certificat ;
- Le Porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le Porteur, l'entité, le cas échéant le MC ou l'opérateur d'AED, n'a pas respecté ses obligations découlant de la PC ou de la DPC ;
- Le Porteur, le représentant légal de l'entité à laquelle il appartient, le cas échéant le MC, ou l'opérateur d'AED demande la révocation du certificat (notamment dans le cas d'une destruction ou altération de la clé privée du porteur et/ou de son support) ;
- Le représentant légal de l'entité à laquelle appartient le porteur informe l'AC que la demande de certificat originale n'était pas autorisée et n'accorde pas d'autorisation rétroactive ;
- Le porteur n'a pas respecté les Conditions Générales d'Utilisation du certificat ou l'AC obtient la preuve que l'usage du certificat est détourné ;
- L'AC est informée que le porteur a violé une ou plusieurs de ses obligations en vertu des Conditions Générales d'Utilisation ;

- L'AC est informée de toute circonstance indiquant que l'utilisation d'une information dans le certificat n'est plus autorisée légalement ;
- Les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- L'AC détecte que les informations apparaissant dans le certificat sont inexactes ou trompeuses ;
- L'AC cesse ses activités pour quelque raison que ce soit et n'a pas pris de dispositions pour qu'une autre AC assure le relai en cas de révocation du certificat ;
- Le droit de l'AC pour émettre des certificats sous ces exigences expire ou est révoqué ou est terminé, à moins que l'AC n'ait pris des dispositions pour maintenir la publication des CRL/OCSP ;
- Le certificat de signature de l'AC est révoqué (ce qui entraîne la révocation de tous les certificats en cours de validité signés par la clé privée correspondante) ;
- Le contenu ou le format des certificats présente un risque inacceptable pour les fournisseurs de logiciels applicatifs ou les utilisateurs ;
- Le décès du Porteur ou la cessation d'activité de l'entité du Porteur ;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement ;
- La clé privée du serveur est suspectée de compromission, est compromise, est perdue ou volée (ou éventuellement les données d'activation associées à la clé privée) ;
- Pour des raisons techniques (échec de l'envoi du certificat, …).

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance, le certificat concerné est révoqué.

Certificats d'une composante de l'IGC

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat d'une composante de l'IGC :
- Suspicion de compromission, compromission, perte ou vol de la clé privée ;
- Décision de changement de composante de l'IGC suite à la détection d'une non-conformité des procédures appliquées au sein de la composante avec celles annoncées dans la présente PC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

4.9.2. Origine d'une demande de révocation

Certificats des porteurs

Les personnes ou entités qui peuvent demander la révocation d'un certificat sont les suivantes:
- Le Porteur ;
- Un représentant légal de l'entité à laquelle est rattaché le porteur ;
- Le cas échéant le MC ;
- L'AC ;
- L'AE ou AED.

Le Porteur est informé, en particulier par le biais des CGU qu'il a acceptées, des personnes ou

entités susceptibles d'effectuer une demande de révocation pour le certificat dont il a la responsabilité.

Certificats d'une composante de l'IGC

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

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

4.9.3. Procédure de traitement d'une demande de révocation

Certificat des porteurs

La demande de révocation est effectuée auprès de l'AE, d'un MC ou de l'AC.

Pour une demande effectuée depuis l'espace client, l'utilisateur s'authentifie avec son compte client et sélectionne le certificat à révoquer.

Pour une demande par courrier, les informations suivantes doivent figurer dans la demande de révocation de certificat (formulaire à télécharger sur le site de Certigna) :
- L'identité du Porteur ;
- L'adresse email du Porteur ;
- La raison de la révocation ;

Si le Porteur n'est pas le demandeur :
- Le prénom et le nom du demandeur ;
- La qualité du demandeur (responsable légal, le cas échéant opérateur d'AED ou MC) ;
- Le numéro de téléphone du demandeur.

Si la demande est transmise par courrier, cette dernière doit être signée par le demandeur.
Si la demande est effectuée en ligne, l'habilitation de la personne à effectuer cette demande est vérifiée. En l'occurrence la personne à l'origine de la demande peut être :
- Le porteur lui-même ;
- Le cas échéant un MC ;
- Un opérateur d'AED ;
- Le responsable légal de l'entité.

Les étapes sont les suivantes :
- Le demandeur de la révocation transmet sa demande à l'AE, par courrier ou en ligne ;
- L'AE authentifie et valide la demande de révocation selon les exigences décrites au chapitre 3.4 ;
- Le numéro de série du certificat est inscrit dans la LCR ;
- Dans tous les cas, le Porteur est informé de la révocation par mail ;
- L'opération est enregistrée dans les journaux d'événements avec, le cas échéant, suffisamment d'informations sur les causes initiales ayant entraîné la révocation du certificat ;
- L'AC ne publie pas dans la LCR les causes de révocation des certificats.

Certificats d'une composante de l'IGC

Dans le cas où l'AC Racine décide de révoquer le certificat d'AC intermédiaire (suite à la compromission de la clé privée de l'AC ou de l'AC Certigna Root CA), 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. Cette information sera relayée également directement auprès des entités et le cas échéant de leur MC.

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.

4.9.4. Délai accordé au Porteur pour formuler la demande de révocation

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

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

Certificats des porteurs

La fonction de gestion des révocations est disponible les heures ouvrées pour les révocations en ligne. Dans tous les cas, le délai maximum de traitement d'une demande de révocation est de 24 heures. Ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès des utilisateurs.

La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations est de 2 heures (jours ouvrés).

La durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations est de 16 heures (jours ouvrés).

Certificats d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC 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/réponses OCSP) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

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

L'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 LCR

La LCR est émise au moins 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 LCR

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

4.9.9. Exigences sur 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 accessible aux adresses suivantes :
- http://identityca.ocsp.certigna.fr
- http://identityca.ocsp.dhimyotis.com

Le répondeur OCSP répond aux exigences d'intégrité, de disponibilité et de délai de publication décrites dans cette PC.

4.9.10. Autres moyens disponibles d'information sur les révocations

Sans objet

4.9.11. Exigences spécifiques en cas de compromission de la clé privée

Le Porteur est tenu d'effectuer une demande de révocation dans les meilleurs délais après avoir eu connaissance de la compromission de la clé privée. Pour les certificats d'AC, outre les exigences du chapitre 4.9.3 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.).

En cas de compromission de sa clé privée ou de connaissance de la compromission de la clé privée de l'AC ayant émis son certificat, le Porteur s'oblige à interrompre immédiatement et définitivement l'usage du certificat et de la clé privée qui lui est associée. Pour rappel, cet engagement est pris lors de l'acceptation des CGU.

4.9.12. Suspension de certificat

Les certificats émis par l'AC ne peuvent pas être suspendus.

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 Certigna Root CA.

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 Web de publication (accessible avec le protocole HTTP).

4.10.2. Disponibilité de la fonction

La fonction d'information sur l'état des certificats est disponible 24 heures sur 24, 7 jours sur 7. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 4 heures (jours ouvrés) et une durée maximale totale d'indisponibilité par mois de 32 heures (jours ouvrés).

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).

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'entité de rattachement du Porteur avant la fin de validité du certificat, le certificat est révoqué.

4.12. Séquestre de clé et recouvrement

Chiffrement
Les clés privées des porteurs sont séquestrées.

Authentification et Signature
Le séquestre des clés privées des Porteurs par l'AC est interdit.

4.12.1. Politique de recouvrement par séquestre des clés

Demande de séquestre

Chiffrement
Le séquestre du certificat et la bi-clé sont opérés automatiquement et pour une durée de dix (10) ans à partir de la date d'émission du certificat. Le porteur, peut demander, lors de la commande à faire évoluer la durée de rétention ou bien à ne pas bénéficier du séquestre.

Traitement d'une demande de séquestre

Chiffrement
Le certificat de chiffrement et la clé privée associée font l'objet d'un séquestre permettant leur recouvrement en cas de perte. La durée du séquestre est de dix (10) ans à partir de la date d'émission du certificat sauf demande explicite du porteur lors de la commande du certificat. Chaque clé privée séquestrée est identifiée de manière unique et non équivoque par le numéro de série du certificat correspondant.

Origine d'une demande de recouvrement

Chiffrement
Outre le porteur et les entités autorisées par la loi à accéder aux clés privées séquestrées par une AC, seul le représentant légal de l'entité ou une personne explicitement désignée (nominativement ou par sa fonction) par le représentant légal de l'entité peut demander le recouvrement d'une clé privé d'un porteur donné.

4.12.2. Identification et validation d'une demande de recouvrement

Chiffrement
L'identité du demandeur d'un recouvrement doit être validée, sauf cas particulier des entités autorisées par la loi, par l'AE suivant les mêmes exigences que la validation initiale de l'identité d'un demandeur de certificat (cf. 3.2). La demande de recouvrement doit comporter au moins le motif du recouvrement de la clé privée et les informations permettant d'identifier la clé privée à recouvrer. L'AE s'assure que le demandeur est bien l'une des personnes autorisées à demander le recouvrement de la clé concernée.

Traitement d'une demande de recouvrement

Chiffrement
Suite à l'identification et la validation de la demande de recouvrement, un opérateur d'AE procède à la remise de la clé privée au demandeur, avec une sécurité équivalente à la remise de la clé privée lors de la génération du certificat du porteur. Les pièces du dossier de recouvrement sont archivées par l'AE.

Destruction des clés séquestrées

Chiffrement
Dès la fin de la période de conservation d'une clé séquestrée, tout exemplaire de cette clé détenu par l'AC est détruit de manière fiable.

Disponibilité des fonctions liées au séquestre et au recouvrement

Chiffrement
La fonction de gestion des recouvrements est disponible aux heures ouvrées. Dans tous les cas, le délai maximum de traitement d'une demande de recouvrement est de 72 heures. Ce délai s'entend entre la réception de la demande de recouvrement authentifiée et la mise à disposition de la clé privée auprès du demandeur.

5. Mesures de sécurité 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.

5.1. Mesures de sécurité physique

5.1.1. Situation géographique et construction des sites

Ces informations sont précisées dans la DPC.

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.

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 décrits dans la présente PC 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.

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 décrits dans la présente PC 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.

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 décrits dans cette PC 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.

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.

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.

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.

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 de la présente PC notamment en matière de disponibilité et de protection en confidentialité et en intégrité des informations sauvegardées.

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 porteurs et responsables de certificats.
- **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.

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

5.2.2. Nombre de personnes requises par tâche

Pour des raisons de disponibilité, chaque tâche doit pouvoir être effectuée par au moins deux personnes. Au minimum, chacune des tâches suivantes est affectée sur deux personnes distinctes :
- Administrateur système ;
- Opérateur.

Pour certaines tâches sensibles (par exemple la cérémonie des clés), plusieurs personnes sont requises pour des raisons de sécurité et de « dual control ».

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.).

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.

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.

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.

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.

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.

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 interne de sécurité 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.

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 sur les 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 / rejet d'une demande de certificat ;
- Génération des certificats des 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 ;
- Destruction des supports contenant des renseignements personnels sur les porteurs.
- Le processus de journalisation permet un enregistrement en temps réel des opérations effectuées.

Chiffrement
- Le séquestre d'une clé privée de porteur ; - La réception d'une demande de recouvrement ; - La validation/rejet d'une demande de recouvrement ; - Le recouvrement d'une clé privée ; - La remise d'une clé privée recouvrée au demandeur du recouvrement.

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.

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.

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

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

Des détails sont donnés dans la DPC.

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

Sans objet.

5.4.8. Evaluation des vulnérabilités

Les journaux d'événements sont contrôlés une fois par jour ouvré pour identifier des anomalies liées à des tentatives en échec (accès ou opération).

Les journaux sont analysés dans leur totalité à la fréquence d'au moins 1 fois toutes les 2 semaines et dès la détection d'une anomalie. Un résumé d'analyse est produit à cette occasion.

Un rapprochement entre les différents journaux d'événements de fonctions qui interagissent entre-elles est effectué à la fréquence d'au moins 1 fois par mois et ce, afin de vérifier la

concordance entre événements dépendants et contribuer ainsi à révéler toute anomalie. Le contrôleur se fait assister si besoin par une personne disposant des compétences liées aux différents environnements utilisés.

5.5. Archivage des données

5.5.1. Types de données à archiver

L'AC archive :
- Les logiciels (exécutables) constitutifs de l'IGC ;
- Les fichiers de configuration des équipements informatiques ;
- 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 justificatifs d'identité ;
- Les certificats émis ;
- Les demandes de révocation ;
- Les LCR émises ;
- Les réponses OCSP.

5.5.2. Période de conservation des archives

Dossiers de demande de certificat

Tout dossier de demande de certificat accepté est archivé à minima sept ans 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'acceptation du certificat par le Porteur. 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 ou le MC, doit permettre de retrouver l'identité réelle du Porteur désigné dans le certificat émis par l'AC à un instant "t".

Chiffrement
Les dossiers de demande de recouvrement d'une clé privée sont archivés par l'AC jusqu'à la date 't' = 't_0' + 10 ans, avec 't_0' date d'archivage du dossier de demande de certificat associé à la clé privée recouvrée.

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

Les certificats de clés des Porteurs 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 trois mois après leur expiration.

Journaux d'événements

Les journaux d'événements traités au chapitre 5.4 sont archivés pendant au moins sept ans après leur génération.

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.

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.

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.

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.

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 porteurs devient insuffisant pour son utilisation prévue restante, alors l'AC :

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

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 3 ans.

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

Le cas de compromission d'une clé d'infrastructure ou de contrôle d'une composante est traité dans le plan de continuité 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 des porteurs 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, MC et les autres entités avec lesquelles l'AC a passé des accords ou a d'autres formes de relations établies, parmi lesquelles des tiers utilisateurs et d'autres AC. En complément, cette information 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.

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.

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.

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 prévient les Porteurs dans le cas où les changements envisagés peuvent avoir des répercussions sur les engagements pris et ce, au moins sous le délai de 1 mois ;
- 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 (https://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.

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 tous les Porteurs, les autres composantes de l'IGC et les tiers par mail de la cessation d'activité. Cette information sera relayée également directement auprès des entités et le cas échéant de leur MC ;
- 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 (https://www.ssi.gouv.fr) est immédiatement informé en cas de cessation d'activité de l'AC.

6. Mesures de sécurité techniques

6.1. Génération et installation de bi-clés

6.1.1. Génération des bi-clés

Clés d'AC

Ce chapitre décrit le contexte de génération de la bi-clé de l'AC.

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé (cf. chapitre 5). Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique conforme aux exigences du chapitre 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. Un porteur ne peut détenir qu'une seule part d'un même secret. Les parts de secret sont placées dans des enveloppes scellées, placées elles-mêmes dans des coffres.

Clés générées par le porteur de certificat

Dans ce cas, le Porteur s'engage de manière contractuelle, en acceptant les conditions générales d'utilisation, à :
- Générer la clé privée dans un dispositif conforme aux exigences du chapitre 11.
- Respecter les exigences quant au dispositif qu'il utilise pour générer et stocker sa clé privée, si ce dernier n'est pas fourni par l'AE.

L'AC prendra le cas échéant les mesures nécessaires pour obtenir les informations techniques

sur le dispositif et se réserve le droit de refuser la demande de certificat s'il était avéré que ce dispositif ne réponde pas à ces exigences.

Clés des porteurs générées par l'AC

La génération des clés des Porteurs s'effectue dans un dispositif conforme aux exigences du chapitre 11.

6.1.2. Transmission de la clé privée à son propriétaire

Dans le cas où la clé privée est générée par l'AE, celle-ci est transmise de manière sécurisée. La clé privée est protégée par une donnée d'activation transmise au porteur qu'il changera lors de l'acceptation du certificat.

Une fois le certificat délivré, l'AC ne duplique ni ne conserve la clé privée.

6.1.3. Transmission de la clé publique à l'AC

Si la bi-clé n'est pas générée par l'AC, la demande de certificat (format PKCS#10), contenant la clé du Porteur, est transmise à l'AC par le Porteur. Cette demande est signée avec la clé privée du Porteur, ce qui permet à l'AE d'en vérifier l'intégrité et de s'assurer que le Porteur possède la clé privée associée à la clé publique transmise dans cette demande. Une fois ces vérifications effectuées, l'AE signe la demande puis la transmet à l'AC.

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 PC, est effectuée par un moyen garantissant intégrité et authentification de cette clé publique.

La clé publique de l'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.fr.

6.1.5. Taille des clés

Clés d'AC

- AC Racine : bi-clé RSA 4096 bits / Algorithme de hachage SHA-256 (256 bits)
- AC Intermédiaire : bi-clé RSA 4096 bits / Algorithme de hachage SHA-256 (256 bits)

Clés des porteurs

Bi-clé RSA 2048 bits / Algorithme de hachage SHA-256 (256 bits)

6.1.6. Vérification de la génération des paramètres des bi-clés 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.

Clés d'AC

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

Clés des porteurs

L'équipement de génération de bi-clés employé par le Porteur 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

Clés d'AC

L'utilisation de la clé privée de l'AC et du certificat associé est exclusivement limitée à la signature de certificats et de LCR (cf. chapitre 1.5.1).

Clés des porteurs

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

Modules cryptographiques de l'AC

Les modules cryptographiques utilisés par l'AC Racine et l'AC 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.

Dispositifs de protection des clés privées des porteurs

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

Dans le cas où l'AC fournit le dispositif au Porteur, directement ou indirectement, l'AC s'assure que :
- La préparation du dispositif est contrôlée de façon sécurisée ;
- Le dispositif est stocké et distribué de façon sécurisée ;
- La désactivation et réactivation du dispositif est contrôlée de façon sécurisée.

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).

6.2.3. Séquestre de la clé privée

Clés d'AC

Les clés privées d'AC ne sont jamais séquestrées.

Clés des porteurs

Chiffrement
Les clés privées des porteurs font l'objet d'un séquestre.

6.2.4. Copie de secours de la clé privée

Clé d'AC

La clé privée de l'AC fait l'objet de copies de secours :
- Dans un second module cryptographique conforme 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.

Clés des porteurs

Chiffrement
Les clés privées des porteurs séquestrées font l'objet de copies de secours moyennant le respect des exigences de sécurité pour le séquestre des clés.

6.2.5. Archivage de la clé privée

Clé d'AC

La clé privée de l'AC n'est en aucun cas archivée.

Clés des porteurs

Les clés privées de Porteurs ne sont en aucun cas archivées.

Pour les clés privées générées dans un module cryptographique, il est techniquement impossible d'effectuer une copie de ces clés hors HSM.

6.2.6. Transfert de la clé privée avec le module cryptographique

Pour rappel, la clé privée du porteur est générée sous la responsabilité de l'opérateur d'AE, d'AED, du MC ou du Porteur.

Les clés privées d'AC sont générées dans le module cryptographique. Comme décrit en 6.2.4,

ces clés ne sont exportables/importables du module que sous forme chiffrée.

6.2.7. Stockage de la clé privée dans un module cryptographique

Les clés privées d'AC sont générées et stockées dans un module cryptographique décrit au chapitre 6.2.1 conformément aux exigences du chapitre 6.2.4.

6.2.8. Méthode d'activation de la clé privée

Clés d'AC

L'activation des clés privées d'AC dans le module cryptographique est contrôlée via des données d'activation (cf. chapitre 6.4) et fait intervenir deux personnes ayant un rôle de confiance au sein de l'IGC.

Clés des porteurs

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

6.2.9. Méthode de désactivation de la clé privée

Clés 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.

Clés des porteurs

La méthode de désactivation de la clé privée dépend du module cryptographique utilisé par le Porteur.

6.2.10. Méthode de destruction des clés privées

Clés 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.

Clés des porteurs

Le Porteur étant l'unique détenteur de sa clé privée, il est le seul à pouvoir la détruire (effacement de la clé ou destruction physique du dispositif).

Chiffrement
Lorsque la clé privée d'un porteur n'est plus nécessaire, la méthode de destruction de cette clé privée permet de répondre aux exigences définies dans le chapitre 11 pour le niveau de

sécurité considéré.

À la fin de la période de validité d'un certificat, le passage à une nouvelle clé privée peut se faire au niveau du porteur :
- Soit en conservant l'ancienne et la nouvelle clé privée, afin que le porteur continue à accéder aux données précédemment chiffrées avec son ancienne clé privée,
- Soit en procédant à un transchiffrement de l'ancienne clé privée vers la nouvelle, dans ce cas l'ancienne clé n'a pas à être conservée.

6.2.11. Niveau d'évaluation sécurité du module cryptographique

Le niveau d'évaluation du module cryptographique de l'AC est précisé au chapitre 10.
Le niveau d'évaluation du dispositif 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 Porteurs sont archivées dans le cadre de l'archivage des certificats correspondants.

6.3.2. Durées de vie des bi-clés et des certificats

Les bi-clés et les certificats des porteurs ont une durée de validité de 5 ans maximum pour un [Particulier] et de 3 ans maximum [Entreprise][Administration] en fonction du contrat souscrit.

Pour l'IGC Certigna, la durée de validité du certificat de l'AC Racine est de 20 ans, et celle du certificat de l'AC est de 18 ans.

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

6.4. Données d'activation

6.4.1. Génération et installation des données d'activation

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).

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

Dans le cas où l'AC génère la bi-clé, les données d'activation sont préalablement personnalisées par le Porteur depuis l'espace client. Ces données ne sont pas conservées par l'AC.

6.4.2. Protection des données d'activation

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

Les données d'activation sont directement remises aux porteurs lors des cérémonies des clés. Leurs conditions de stockage assurent leur disponibilité, leur intégrité et leur confidentialité.

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

Si la bi-clé est générée par l'AE, elle génère également les données d'activation qui sont envoyées par les moyens décrit au chapitre 6.4.1. Ces données d'activation ne sont pas sauvegardées par l'AE et sont modifiées par le porteur lors de l'acceptation du certificat.

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 à l'aide du 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.

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

Conformément à l'analyse de risque menée, lors de la conception de tout nouveau projet de développement, une analyse sur le plan de la sécurité est réalisée et approuvée par le Comité de Sécurité de l'AC.

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 exigeant un niveau élevé d'autorisation.

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.

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.

6.8. Horodatage et Système de datation

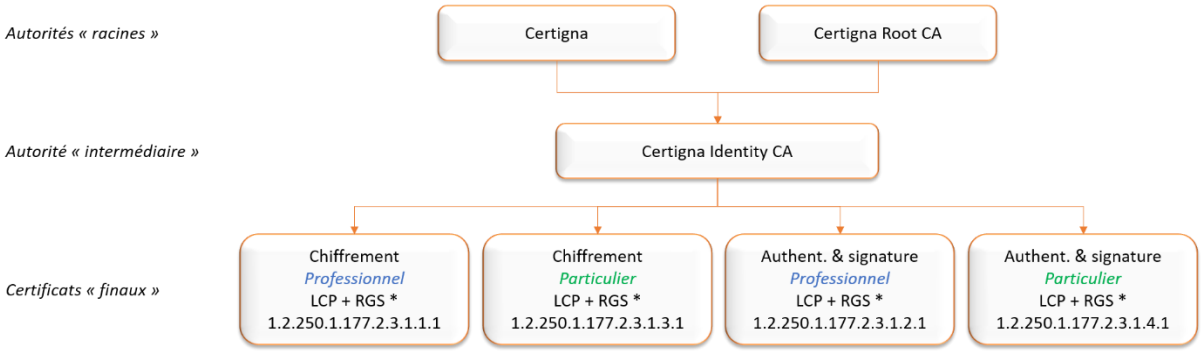
Afin d'assurer une synchronisation entre les différentes datations d'événements, les différentes composantes de l'IGC synchronisent leurs horloges systèmes par rapport à une source fiable de temps UTC.

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.

7.1. Hiérarchie de confiance

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



7.2. Profils des certificats des Autorités Racines

Ces profils sont décrits dans les Politiques de Certification associées aux Autorités Racines et disponibles à l'adresse suivante : https://www.certigna.fr/autorites/

7.3. Profil du certificat de l'Autorité intermédiaire

Deux certificats d'AC ont été émis pour cette Autorité de Certification : l'un signé par l'ancienne AC Racine « Certigna », l'autre par la nouvelle AC Racine « Certigna Root CA ».

7.3.1. Champs de base

Champs	Signé par « Certigna »	Signé par « Certigna Root CA »
Version	V3	
Serial Number	41 12 0D 20 00 2E 4B 6F 9F 47 D3 55 73 E7 8A 77	59 44 CB 2D BE 6A DE A5 13 4E 9A 32 19 41 0C AE
Signature	Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096	
Subject Public Key Info	RSA 4096 bits	
Validity	Dates et heures d'activation et d'expiration du Certificat	
Issuer DN	CN = Certigna O = Dhimyotis C = FR	CN = Certigna Root CA OU = 0002 48146308100036 O = Dhimyotis C = FR
Subject DN	CN = Certigna Identity CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 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=**1.2.250.1.177.2.0.1.1 **CPS**=https://www.certigna.fr/autorites/
Authority Information Access	Non	**caIssuers**=http://autorite.certigna.fr/certignarootca.der **caIssuers**= http://autorite.dhimyotis.com/certignarootca.der
CRL Distribution Points	Non	**URL**=http://crl.certigna.fr/certignarootca.crl **URL**=http://crl.dhimyotis.com/certignarootca.crl
Basic Constraints	**Oui**	**cA** = TRUE **PathLengthConstraint** = 0
Key Usage	**Oui**	Signature de certificat Signature de CRL

7.4. Profil des certificats

7.4.1. Chiffrement * [Particulier]

Champs	Description	
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	
SubjectPublicKeyInfo	RSA 2048	
Validity	Dates et heures d'activation et d'expiration du Certificat [5 ans maximum]	
Issuer DN	CN = Certigna Identity CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR	
Subject DN	CN = <Prénom> <NOM> **CHIF** GN= <Prénom> SN= <NOM> C = Pays de l'autorité compétente auprès de laquelle le porteur est officiellement enregistrée SN= Série de caractères constitué en partie d'un aléa pour l'unicité	
Extensions	**Crit.**	**Description**
Authority Key Identifier	Non	Identifiant de la clé publique de l'AC
Subject Key Identifier	Non	Identifiant de la clé publique du Porteur
SubjectAlternativeName	Non	Nom RFC822=Adresse e-mail du Porteur
Key Usage	**Oui**	keyEncipherment
Extended Key Usage	Non	Email Protection / msEFS
Certificate Policies	Non	**OID=**1.2.250.1.177.2.3.1.3.1 **CPS**= https://www.certigna.fr/autorites/
CRL Distribution Points	Non	**URL**=http://crl.certigna.fr/identityca.crl **URL**=http://crl.dhimyotis.com/identityca.crl
Authority Information Access	Non	**caIssuers**=http://autorite.certigna.fr/identityca.der **caIssuers**=http://autorite.dhimyotis.com/identityca.der **URL**=http://identityca.ocsp.certigna.fr **URL**=http://identityca.ocsp.dhimyotis.com
Basic Constraints	Non	**cA** = FALSE

7.4.2. Chiffrement * [Entreprise][Administration]

Champs	Description	
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	
SubjectPublicKeyInfo	RSA 2048	
Validity	Dates et heures d'activation et d'expiration du Certificat [3 ans maximum]	
Issuer DN	CN = Certigna Identity CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR	
Subject DN	CN = <Prénom> <NOM> **CHIF** GN= <Prénom> SN= <NOM> OU = ICD + identifiant de l'entité à laquelle appartient le porteur enregistré conformément à la législation et aux réglementations en vigueur OI = Informations sur le justificatif d'identité de l'entité O = Nom de l'entité à laquelle le porteur est rattaché C = Pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée SN= Série de caractères constitué en partie d'un aléa pour l'unicité	
Extensions	**Crit.**	**Description**
Authority Key Identifier	Non	Identifiant de la clé publique de l'AC
Subject Key Identifier	Non	Identifiant de la clé publique du Porteur
SubjectAlternativeName	Non	Nom RFC822=Adresse e-mail du Porteur
Key Usage	**Oui**	keyEncipherment
Extended Key Usage	Non	Email Protection / msEFS
Certificate Policies	Non	**OID=**1.2.250.1.177.2.3.1.1.1 **CPS**= https://www.certigna.fr/autorites/
CRL Distribution Points	Non	**URL**=http://crl.certigna.fr/identityca.crl **URL**=http://crl.dhimyotis.com/identityca.crl
Authority Information Access	Non	**caIssuers**=http://autorite.certigna.fr/identityca.der **caIssuers**=http://autorite.dhimyotis.com/identityca.der **URL**=http://identityca.ocsp.certigna.fr **URL**=http://identityca.ocsp.dhimyotis.com
Basic Constraints	Non	**cA** = FALSE

7.4.3. Authentification et signature * [Particulier]

Champs	Description	
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	
SubjectPublicKeyInfo	RSA 2048	
Validity	Dates et heures d'activation et d'expiration du Certificat [5 ans maximum]	
Issuer DN	CN = Certigna Identity CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR	
Subject DN	CN = <Prénom> <NOM> **ID** GN= <Prénom> SN= <NOM> C = Pays de l'autorité compétente auprès de laquelle le porteur est officiellement enregistrée SN= Série de caractères constitué en partie d'un aléa pour l'unicité	
Extensions	**Crit.**	**Description**
Authority Key Identifier	Non	Identifiant de la clé publique de l'AC
Subject Key Identifier	Non	Identifiant de la clé publique du Porteur
SubjectAlternativeName	Non	Nom RFC822=Adresse e-mail du Porteur
Key Usage	**Oui**	Digital signature / Non repudiation
Extended Key Usage	Non	Client Auth / Email Protection
Certificate Policies	Non	**OID=**1.2.250.1.177.2.2.1.4.1 **CPS**= https://www.certigna.fr/autorites/
CRL Distribution Points	Non	**URL**=http://crl.certigna.fr/identityca.crl **URL**=http://crl.dhimyotis.com/identityca.crl
Authority Information Access	Non	**caIssuers**=http://autorite.certigna.fr/identityca.der **caIssuers**=http://autorite.dhimyotis.com/identityca.der **URL**=http://identityca.ocsp.certigna.fr **URL**=http://identityca.ocsp.dhimyotis.com
Basic Constraints	Non	**cA** = FALSE

7.4.4. Authentification et signature * [Entreprise][Administration]

Champs	Description	
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	
SubjectPublicKeyInfo	RSA 2048	
Validity	Dates et heures d'activation et d'expiration du Certificat [3 ans maximum]	
Issuer DN	CN = Certigna Identity CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR	
Subject DN	CN = <Prénom> <NOM> **ID** GN= <Prénom> SN= <NOM> OU = ICD + identifiant de l'entité à laquelle appartient le porteur enregistré conformément à la législation et aux réglementations en vigueur OI = Informations sur le justificatif d'identité de l'entité O = Nom de l'entité à laquelle le porteur est rattaché C = Pays de l'autorité compétente auprès de laquelle l'entité est officiellement enregistrée SN= Série de caractères constitué en partie d'un aléa pour l'unicité	
Extensions	**Crit.**	**Description**
Authority Key Identifier	Non	Identifiant de la clé publique de l'AC
Subject Key Identifier	Non	Identifiant de la clé publique du Porteur
SubjectAlternativeName	Non	Nom RFC822=Adresse e-mail du Porteur
Key Usage	**Oui**	Digital signature / Non repudiation
Extended Key Usage	Non	Client Auth / Email Protection
Certificate Policies	Non	**OID=**1.2.250.1.177.2.3.1.2.1 **CPS**= https://www.certigna.fr/autorites/
CRL Distribution Points	Non	**URL**=http://crl.certigna.fr/identityca.crl **URL**=http://crl.dhimyotis.com/identityca.crl
Authority Information Access	Non	**caIssuers**=http://autorite.certigna.fr/identityca.der **caIssuers**=http://autorite.dhimyotis.com/identityca.der **URL**=http://identityca.ocsp.certigna.fr **URL**=http://identityca.ocsp.dhimyotis.com
Basic Constraints	Non	**cA** = FALSE

7.5. Profil des LCR

7.5.1. Champs de base

Champs	Description
Version	V2
Signature	Identifiant de l'algorithme de signature de l'AC SHA-256 RSA 4096
Issuer	CN = Certigna Identity CA OU = 0002 48146308100036 OI = NTRFR-48146308100036 O = Dhimyotis C = FR
This Update	Date de génération de la LCR
Next Update	Date de prochaine mise à jour de la LCR [7 jours maximum]
Revoked certificates	Liste des n° de série des certificats révoqués

7.5.2. Extensions

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.

7.6. 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 porteur ou à l'AC.

7.6.1. 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.

7.6.2. 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 porteur 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 chapitre 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 porteur, 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 conformité et autres évaluations

Les audits et les évaluations concernent, d'une part, ceux réalisés en vue de la délivrance d'une attestation de qualification au sens de l'Ordonnance 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'AED ou des mandataires de certification au même titre que le personnel de son IGC. Il s'assure entre autres que les opérateurs d'AED ou les MC respectent les engagements vis-à-vis de cette PC 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 tous les 3 ans.

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.

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, …).

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 problématiques métiers et légales

9.1. Tarifs

9.1.1. Tarifs pour la fourniture ou le renouvellement de certificats

La délivrance de certificats aux Porteurs est facturée selon les tarifs affichés sur le site internet ou sur le formulaire de commande.

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

D'autres prestations pourront être facturées. Dans ce cas, les tarifs seront portés à la connaissance des personnes auxquelles ils s'appliquent et seront disponibles auprès de l'AC.

9.1.5. Politique de remboursement

La commande de certificats ne peut être annulée dès lors que le dossier est en cours de traitement. Tout certificat émis ne peut faire l'objet d'une demande de remboursement.

9.2. Responsabilité financière

9.2.1. Couverture par les assurances

Dhimyotis a souscrit un contrat d'assurance responsabilité civile adapté aux technologies de l'information.

9.2.2. Autres ressources

Sans objet.

9.2.3. Couverture et garantie concernant les entités utilisatrices

Cf. chapitre 9.9.

9.3. Confidentialité des données professionnelles

9.3.1. Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :
- La partie non-publique de la DPC de l'AC ;
- Les clés privées de l'AC, des composantes et des Porteurs ;
- Les données d'activation associées aux clés privées d'AC et des Porteurs ;
- 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.

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, MC et le cas échéant à l'opérateur d'AED en relation avec le Porteur.

9.4. Protection des données personnelles

9.4.1. Politique de protection des données personnelles

Les dossiers de demande de certificat électronique comportant les données personnelles sont archivés à minima sept ans 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.

Par ailleurs, DHIMYOTIS 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 DHIMYOTIS, 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 suivre la qualité de nos services, les appels réalisés auprès de notre service clients 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@dhimyotis.com, ou par courrier à l'adresse suivante :

DHIMYOTIS, 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 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 les suivantes :
- Les causes de révocation des certificats des Porteurs ;
- Les dossiers d'enregistrement des Porteurs, des opérateurs d'AED et des MC.

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. L'utilisation de cette marque par l'entité est autorisée uniquement dans le cadre du contrat d'abonnement.

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. La relation entre un Porteur et l'AC est formalisée par un lien contractuel / réglementaire précisant les droits et obligations des parties et notamment les garanties apportées par l'AC.

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 et de révocation de certificat.

9.6.3. Porteur

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

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.
Ces informations s'appliquent également aux opérateurs d'AED et aux MC.

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 du Porteur jusqu'à l'AC racine, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (date de validité, statut de révocation) ;

- Vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente PC.
- Contrôler que le certificat émis par l'AC est référencé au niveau de sécurité et pour le service de confiance requis par l'application.

9.6.5. Autres participants

Sans objet.

9.7. Limite de garantie

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

9.8. Limite de responsabilité

Il est expressément entendu que l'AC ne saurait être tenue pour responsable, ni d'un dommage résultant d'une faute ou négligence d'un accepteur et/ou des Porteurs, ni d'un dommage causé par un fait extérieur, notamment en cas de :

- Utilisation d'un certificat pour une autre application que les applications définies au chapitre 1.5.1 de la présente PC ;
- Utilisation d'un certificat pour garantir un autre objet que l'identité du Porteur pour lequel le certificat a été émis ;
- Utilisation d'un certificat révoqué ;
- Utilisation d'un certificat au-delà de sa limite de validité ;
- Non-respect par les entités concernées des obligations définies aux chapitres 9.6.3 et 9.6.4 de la présente PC ;
- Faits extérieurs à l'émission du certificat tels qu'une défaillance de l'application pour laquelle il peut être utilisé ;
- Force majeure comme définie par les tribunaux français.

9.9. Indemnités

Dhimyotis a notamment souscrit un contrat « Responsabilité civile après livraison ».

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 du RGS et des documents complémentaires à ce dernier.

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.

9.12.2. Mécanisme et période d'information sur les amendements

L'AC communique via son site Internet https://www.certigna.fr 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 PC et de la DPC correspondante ne sont pas modifiés.

9.13. Dispositions concernant la résolution de conflits

Il est rappelé que les conditions d'utilisation des certificats émis par l'AC sont définies par la présente PC et/ou par le contrat d'abonnement aux services de certification définissant les relations entre Certigna d'une part et les Porteurs d'autre part.

Les parties s'engagent à tenter de résoudre à l'amiable tout différend susceptible d'intervenir entre elles, soit directement, soit via un médiateur, dans les 2 mois de la réception du courrier avec accusé réception informant du différend. Les éventuels frais de médiation seront supportés par moitié par chacune des parties. Le cas échéant, l'affaire sera portée devant le tribunal de commerce de Lille.

9.14. Juridictions compétentes

Tout litige relatif à la validité, l'interprétation, l'exécution de la présente PC sera soumis aux tribunaux de Lille.

9.15. Conformité aux législations et réglementations

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

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.

9.16.4. Application et renonciation

Sans objet.

9.16.5. Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un événement irrésistible, insurmontable et imprévisible.

9.17. Autres dispositions

Sans objet.

10. Annexe 1 : exigence de sécurité 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 est :

- Qualifié au niveau « renforcé » par l'ANSSI selon le processus décrit dans le RGS ;
- Certifié Critères Communs au niveau EAL4+ ou FIPS 140-2 Level 3.

11. Annexe 2 : exigences de sécurité du dispositif utilisé par le Porteur

11.1. Exigences sur les objectifs de sécurité

Le dispositif utilisé par le Porteur pour stocker et mettre en œuvre sa clé privée et, le cas échéant, générer son bi-clé, doit répondre aux exigences de sécurité suivantes :

- Si la bi-clé du Porteur est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée ;
- Détecter les défauts lors des phases d'initialisation, de personnalisation et d'opération et disposer de techniques sûres de destruction de la clé privée en cas de régénération de la clé privée ;
- Garantir la confidentialité et l'intégrité de la clé privée ;
- Assurer la correspondance entre la clé privée et la clé publique ;
- Générer une fonction de sécurité qui ne peut être falsifié sans la connaissance de la clé privée ;
- Assurer la fonction de sécurité pour le Porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ;
- Permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

Chiffrement
Le dispositif de protection des clés privées doit aussi répondre aux exigences suivantes : - Assurer la fonction de déchiffrement, de clés symétriques de fichier ou de message, pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers ; - Permettre de garantir l'authenticité et l'intégrité de la clé symétrique de fichier ou de message, une fois déchiffrée, lors de son export hors du dispositif à destination de l'application de déchiffrement des données ; - Le cas échéant, permettre de garantir la confidentialité, l'authenticité et l'intégrité de la clé privée lors de son export hors du dispositif, à destination d'une fonction de séquestre ou d'archivage des clés privées.

11.2. Exigences sur la qualification

Niveau *
Le dispositif de protection des clés privées fourni par l'AC ou utilisé par le Porteur est : - Qualifié au minimum au niveau « Elémentaire » par l'ANSSI.