Politique de Certification

Certigna Racine

(Certification des AC intermédiaires)

OID = 1.2.250.1.177.1.0.1.1

Référence RD-90 Version 1.0

Dhimyotis

Suivi des modifications

Date	Version	Auteur	Evolution du document
03/11/2008	1.0	P. Merlin	Création
28/11/2008	1.0	Comité de sécurité	Validation

Table des matières

Chapitre 1

Introduction

1.1 Présentation générale

L'autorité Certigna Racine constitue l'autorité auto-signée (niveau 0) de l'IGC Certigna détenue par Dhimyotis.

La présente Politique de Certification (PC) expose les engagements de l'AC Certigna Racine concernant les certificats qu'elle émet.

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) et notamment les termes définis au chapitre 1.6 de cette PC.

La présente PC vise la conformité au document « Politique de Référencement Intersectorielle de Sécurité » V2 élaborée conjointement par l'ADAE (Agence pour le Développement de l'Administration Electronique) et la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) et référencé dans la suite du document PRIS V2 . Cette conformité est visée en cohérence avec la certification PRIS qu'ont obtenu plusieurs autorités de certification intermédiaires au sein de l'IGC Certigna.

L'AC Certigna Racine délivre des certificats de signature exclusivement aux autorités intermédiaires de l'IGC Certigna.

1.2 Identification du document

La présente PC est dénommée « Politique de Certification de l'Autorité de Certification Certigna Racine ».
Elle peut être identifiée par son numéro d'OID. Le numéro d'OID du présent document est : 1.2.250.1.177.1.0.1.1

1.3 Entités intervenant dans l'IGC

1.3.1 Autorité de certification

L'AC Certigna Racine 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 publication de la PC, et des certificats d'AC ;
- Fonction de gestion des révocations ;
- Fonction d'information sur l'état des certificats via la liste des certificats révoqués (LAR).

L'AC assure ces fonctions directement et en garde la responsabilité.

L'AC Certigna Racine 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, auxquelles elles incombent les respectent aussi.

1.3.2 Autorité d'enregistrement

L'AE assure les fonctions suivantes qui lui sont déléguées par l'AC, en vertu de la présente PC :
- La prise en compte et la vérification des demandes de certificats pour les autorités intermédiaires (également dites subalternes) ;
- La vérification des demandes de révocation de certificat.

1.3.3 Porteurs de certificat

Dans le cadre de la présente PC, la notion de porteur de certificat n'existe pas.
Les certificats sont délivrés exclusivement aux autorités intermédiaires.

1.3.4 Utilisateurs de certificat

Un utilisateur d'un certificat d'une autorité intermédiaire peut être :
- Un usager destinataire d'un message ou de données (données d'authentification, données de chiffrement ou signature) provenant d'un porteur d'un certificat émis par une autorité intermédiaire de l'IGC Certigna, cet usager souhaitant vérifier la chaîne de certification transmise

1.3.5 Autres participants

Sans objet

1.4 Usage des certificats

1.4.1 Domaines d'utilisation applicables

Bi-clés et certificats des serveurs

Il est expressément entendu qu'une autorité intermédiaire, pour laquelle l'autorité Certigna Racine a délivré un certificat, ne peut user de sa clé privée et de son certificat qu'à des fins de signature exclusivement (signature des certificats des porteurs, signature des listes des certificats révoqués ou LCR).

La présente PC interdit toute utilisation d'un certificat émis par l'autorité Certigna Racine dans un contexte autre que celui de la certification des clés privées de porteurs et la certification de liste de certificats révoqués.

Bi-clés et certificats de composantes

L'AC Certigna Racine dispose d'un seul bi-clé et le certificat (auto-signé) correspondant n'est rattaché à aucune AC de niveau supérieur. L'AC Certigna Racine est une autorité racine, c'est-à-dire l'AC de plus haut niveau. Le bi-clé de l'AC Certigna Racine permet de signer différents types d'objets qu'elle génère : certificats d'autorité intermédiaire et LAR.

Les opérateurs de l'IGC disposent de certificats permettant de s'authentifier sur cette IGC. Pour les opérateurs d'AE, ce certificat permet de signer les demandes de certificats et de révocation avant leur transmission à l'AC.

1.4.2 Domaines d'utilisation interdits

Les restrictions d'utilisation des bi-clés et des certificats sont définies au chapitre 4.5 ci-dessous.

1.5 Gestion de la PC

1.5.1 Entité gérant la PC

L'AC Certigna Racine est responsable de l'élaboration, du suivi, de la modification et de la validation de la présente PC. Elle statue sur toute modification nécessaire à apporter à la PC à échéance régulière. Le chapitre 9.12 de la présente PC précise les procédures applicables pour l'administration de la PC.

1.5.2 Point de contact

Sans objet

1.5.3 Entité déterminant la conformité de la DPC avec la PC

L'AAP (Autorité d'Approbation des Politiques) 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. L'AAP est constituée par le comité de sécurité de Dhimyotis.

1.5.4 Procédures d'approbation de la conformité de la DPC

La DPC traduit en termes technique, organisationnel et procédural les exigences de la PC en s'appuyant sur la politique de sécurité de l'entreprise. L'AAP doit s'assurer que les moyens mis en œuvre et décrits dans la DPC répondent à ces exigences. Le traitement des modifications est décrit dans le chapitre 9.12.1. Procédures d'amendements.

Un contrôle de conformité de la DPC par rapport à la PC peut être également être effectué par le cabinet d'audit externe dans le contexte du programme d'audit annuel.

1.6 Niveau d'assurance sécurité de l'AC Certigna Racine

L'AC Certigna Racine a pour vocation de certifier les clés publiques des autorités intermédiaires, dont font partie notamment des autorités certifiées PRIS niveau ***. A ce titre, l'AC Certigna Racine , et plus particulièrement la clé privée de signature (des certificats des AC intermédiaires et des LAR), s'engage à répondre a minima aux exigences formulées dans les PC type PRIS ***.
Ces exigences concernent :

- La génération du bi-clé (exigence sur la taille, l'algorithme de signature, etc.)
- Le profil du certificat d'AC
- La protection de la clé privée (utilisation d'un module cryptographique) Dhimyotis s'engage à répondre à ces exigences et a notamment pris les mesures suivantes pour renforcer la sécurité de cette autorité :
- L'AC Certigna Racine est maintenue hors-tension et hors-ligne en dehors de toute opération de certification (traitements requérant la mise en œuvre de sa clé privée pour la signature des clés publiques des AC intermédiaires et des liste des autorités révoquées)
- La génération du bi-clé de l'AC Certigna Racine a été effectuée lors d'une cérémonie de clé et la protection de la clé privée est assurée par un module cryptographique répondant aux exigences exprimées au chapitre 10.

1.7 Définitions et acronymes

1.7.1 Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

AAP Autorité d'Approbation des Politiques

AC Autorité de Certification

AE Autorité d'Enregistrement

CNIL Commission Nationale de l'Informatique et des Libertés

CS Certificate Signature Request

DN Distinguished Name

DPC Déclaration des Pratiques de Certification

FQDN Fully Qualified Domain Name

ICD International Code Designator

IGC Infrastructure de Gestion de Clés

INPI Institut National de la Propriété Industrielle

LAR Liste des Autorités Révoquées

LCP Lightweight Certificate Policy

LCR Liste des Certificats Révoqués

OCSP Online Certificate Status Protocol

OID Object Identifier

PC Politique de Certification

PCA Plan de Continuité d'Activité

PRIS Politique de Référencement Intersectorielle de Sécurité

PKCS Public Key Cryptographic Standards

1.7.2 Définitions

Autorité de Certification (AC) : cf. chapitre 1.3.1

Autorité d'Enregistrement (AE) : cf. chapitre 1.3.2

Certificat électronique : Fichier électronique attestant qu'un bi-clé appartient à la personne physique ou morale ou à l'élément matériel ou logiciel identifié dans le certificat. Il est délivré par une autorité de certification. En signant le certificat, l'AC valide le lien entre l'identité de la personne physique ou morale ou l'élément matériel ou logiciel et le bi-clé. Le certificat est valide pendant une durée donnée précisée dans celui-ci.

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

Porteur de certificat : cf. chapitre 1.3.3 Infrastructure de Gestion de Clés (IGC) : Ensemble de composantes, fonctions et procédures dédiées à la gestion de clés cryptographiques et de leurs certificats utilisés par des services de confiance. Une IGC peut être composée d'une autorité de certification, d'un opérateur de certification, d'une autorité d'enregistrement centralisée et/ou locale, de mandataires de certification, d'une entité d'archivage, d'une entité de publication, ...

Liste des Autorités révoquées (LAR) : 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 (LCR) : Liste comprenant les numéros de série des certificats ayant fait l'objet d'une révocation, et signée par l'AC émettrice.

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

RSA : Algorithme à clés publiques du nom de ses inventeurs (Rivest, Shamir et Adleman).
Utilisateur de certificat : cf. chapitre 1.3.4

Chapitre 2

Responsabilité concernant la mise à disposition des informations devant être publiées

2.1 Entités chargées de la mise à disposition des informations

L'IGC met à disposition des utilisateurs des certificats qu'elle émet des informations sur l'état de révocation des certificats en cours de validité émis par l'AC Certigna Racine . Ces informations sont publiées au travers de plusieurs serveurs :

- Serveur Web (2) :
  http://www.certigna.fr/crl/certigna.crl
  http://www.dhimyotis.com/crl/certigna.crl

2.2 Informations devant être publiées

L'AC Certigna Racine publie à destination des utilisateurs de certificats :
- La PC ;
- Le certificat d'AC Certigna Racine ;
- La liste des certificats révoqués (LAR).

2.2.1 Publication de la documentation

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

La PC est publiée sous format électronique à l'adresse http ://www.certigna.fr et également à l'adresse http ://www.dhimyotis.com à destination des utilisateurs de certificats Certigna.
Aucune condition générale n'est publiée.
Aucun formulaire n'est publié (cf. réservée usage interne à l'IGC Certigna).

Publication de la DPC

La DPC n'est pas publiée.

Publication des certificats d'AC

Les porteurs de certificats et les utilisateurs de certificat peuvent accéder aux certificats d'AC qui sont publiés aux adresses :
– http ://www.certigna.fr/chaine_certification.php
– http ://www.dhimyotis.com

NB : suivant le système d'exploitation et/ou le navigateur utilisé par l'utilisateur le certificat de l'AC Certigna Racine peut être automatiquement installé dans les magasins de certificats des autorités de confiance grâce aux mécanismes de mise à jour (pour les éditeurs ayant reconnu l'autorité Certigna comme autorité de confiance)

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.

2.3 Délais et fréquences de publication

2.3.1 Publication de la documentation

La PC est mise à jour si nécessaire afin de refléter les engagements, moyens et procédures effectifs de l'AC.

2.3.2 Publication du certificat de l'AC Certigna Racine

Le certificat de l'AC Certigna Racine a été diffusé préalablement à toute diffusion de certificats d'AC intermédiaires. La disponibilité des systèmes publiant le certificat de l'AC Certigna Racine est garantie 24 heures sur 24, 7 jours sur 7. La durée maximale d'indisponibilité par interruption (panne ou maintenance) des systèmes publiant le certificat de l'AC Certigna Racine est de 1 heure. La durée totale d'indisponibilité par mois des systèmes publiant le certificat de l'AC Certigna Racine est de 4 heures. La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de publication est de 8 heures (jours ouvrés). La durée maximale totale d'indisponibilité par mois de la fonction de publication est de 32 heures (jours ouvrés).

2.3.3 Publication de la LCR

Sans objet

2.3.4 Publication de la LAR

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

2.4 Contrôle d'accès aux informations publiées

2.4.1 Contrôle d'accès à la documentation

La PC de l'autorité Certigna Racine sont libres d'accès en lecture.

2.4.2 Contrôle d'accès aux certificat d'AC

Le certificat d'AC Certigna Racine et les certificat d'AC intermédiaires sont libres d'accès en lecture.

2.4.3 Contrôle d'accès à la LCR / LAR

Sans objet pour la LCR. La liste des autorités révoquées (LAR) est libre d'accès en lecture. 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.

Chapitre 3

Identification et Authentification

3.1 Nommage

3.1.1 Types de noms

Dans chaque certificat, l'AC émettrice (correspondant au champ « issuer ») et l'AC intermédiaire (champ « subject ») sont identifiés par un « Distinguished Name » DN de type X.501.

3.1.2 Nécessité d'utilisation de noms explicites

Le DN du certificat permet d'identifier l'autorité intermédiaire (à qui est émis le certificat). Il est construit à partir du nom de cette autorité (nom commercial).

Le DN a la forme suivante :

{
    serialNumber = Numéro de série du certificat,
    CN = Nom de l'autorité intermédiaire,
    O = Nom de l'organisation (Dhimyotis),
    OU = Unité organisationnelle (0002 481463081),
    C = Code pays (FR)
}

3.1.3 Anonymisation ou pseudonymisation des porteurs

Sans objet

3.1.4 Unicité des noms

La combinaison du numéro de série et du nom de l'autorité identifie de manière univoque le titulaire du certificat.

3.1.5 Identification, authentification et rôle des marques déposées

L'AC Certigna Racine est responsable de l'unicité des noms des autorités intermédiaires pour lesquelles elle délivre des certificats. Ces autorités sont exclusivement internes à l'IGC Certigna. Par conséquent les noms des autorités utilisent la marque Certigna dont Dhimyotis est propriétaire. Il ne peut donc avoir aucun litige portant sur la revendication d'utilisation d'un nom.

Les utilisateurs de l'IGC Certigna engagent leur responsabilité en s'appuyant sur le niveau de contrôle assuré lors du traitement des demandes de certificats et la garantie d'unicité du DN construit pour chaque autorité.

3.2 Validation initiale de l'identité

La création d'une nouvelle autorité intermédiaire Certigna est un processus réalisé intégralement au sein de l'IGC Certigna, ce qui garantit une maîtrise complète de ce processus.

3.2.1 Validation de l'identité d'un organisme

Sans objet

3.2.2 Validation de l'identité d'un individu

Sans objet

3.2.3 Validation de l'autorité du demandeur

Sans objet

3.2.4 Critères d'interopérabilité

En cas de demande de certification croisée avec l'AC Certigna Racine , que cette demande émane de cette dernière ou de l'autorité tierce, l'AAP de l'AC Certigna Racine s'engage à effectuer une étude préalable d'impact.

Cette étude comprend :

- L'analyse de la Politique de Certification de l'AC tierce et l'assurance d'un niveau d'exigence équivalent à la sienne ;
- L'analyse des contraintes d'exploitation de l'AC tierce et l'assurance d'un niveau de continuité équivalent au sien ;
- Un audit du site d'exploitation de l'AC tierce.

Tout accord contractuel de reconnaissance mutuelle précisera les limites de responsabilités respectives de chaque autorité.

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

L'AC n'émet pas de nouveau certificat pour un bi-clé précédemment émis. Le renouvellement passe par la génération d'un nouveau bi-clé et d'une nouvelle demande de certificat (cf. chapitre 4.6).

3.3.1 Identification et validation pour un renouvellement courant

Sans objet

3.3.2 Identification et validation pour un renouvellement après révocation

Sans objet

3.4 Identification et validation d'une demande de révocation

La révocation d'un certificat d'une autorité intermédiaire Certigna est décidée par les gestionnaires de l'IGC Certigna. La demande est intrinsèquement identifiée et validée.

Chapitre 4

Exigences opérationnelles sur le cycle de vie des certificats

4.1 Demande de certificat

4.1.1 Origine d'une demande de certificat

La demande de certificat est effectuée lors de la création d'une nouvelle autorité intermédiaire au sein de l'IGC Certigna. Cette demande exclusivement émane d'une personne disposant d'un rôle de confiance au sein de l'IGC Certigna.

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

La demande de certificat se réduit à :
- La génération du bi-clé et de la CSR par l'opérateur système responsable de la création de l'AC intermédiaire Certigna. La CSR est ensuite importée sur l'AE de Certigna Racine .

4.2 Traitement d'une demande de certificat

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

Les demandes de certificats sont traitées exclusivement dans le cadre d'une cérémonie de clé (les demandes sont intrinsèquement identifiées et validées dans ce processus).

4.2.2 Acceptation ou rejet de la demande

La demande est implicitement acceptée. Cette phase fait partie intégrante de la procédure de cérémonie de clé.

4.2.3 Durée d'établissement du certificat

Le certificat est immédiatement généré par l'AC Certigna Racine après génération de la demande par l'autorité intermédiaire tel que décrit dans la procédure de cérémonie de clé.

4.3 Délivrance du certificat

4.3.1 Actions de l'AC concernant la délivrance du certificat

Le certificat est délivré immédiatement par la composante AC de l'AC Certigna Racine tel que décrit dans la procédure de cérémonie de clé.

4.3.2 Notification par l'AC de la délivrance du certificat

Sans objet

4.4 Acceptation du certificat

4.4.1 Démarche d'acceptation du certificat

L'acceptation par l'autorité intermédiaire est implicite.

4.4.2 Publication du certificat

Le certificat de l'AC intermédiaire est publié avant toute émission de certificats par cette dernière. Cette publication a pour objectif de permettre aux utilisateurs des certificats émis par l'autorité intermédiaire d'en vérifier la chaîne de certification. C'est le service de publication de l'IGC Certigna qui est responsable de cette publication.

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

Sans objet

4.5 Usages du bi-clé et du certificat

4.5.1 Utilisation de la clé privée et du certificat par le

L'autorité intermédiaire détentrice du certificat est configurée pour n'utiliser ce dernier qu'à des fins de signature (signature des certificats des porteurs, signature des LCR).

L'usage autorisé du bi-clé et du certificat associé est indiqué dans le certificat lui-même, via l'extension Key Usage qui intègre les rôles suivants :

– Signature du certificat
– Signature de la liste de révocation de certificats hors connexion
– Signature de la liste de révocation de certificats

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 émis par l'autorité Certigna Racine , à savoir :
– La vérification de la chaîne de certification des certificats émis par les autorités intermédiaires Certigna (certificats porteurs, certificat OCSP)
– La vérification des LCR émises par les autorités intermédiaires Certigna
Dans le cas contraire, leur responsabilité pourrait être engagée.

4.6 Renouvellement d'un certificat

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

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 renouvelés afin de minimiser les possibilités d'attaques cryptographiques. Ainsi les bi-clés des autorités intermédiaires, et les certificats correspondants, sont renouvelés au minimum tous les 10 ans (le renouvellement peut être anticipé en cas de compromission, ou risque ou suspicion de compromission).

4.7.2 Origine d'une demande d'un nouveau certificat

Le déclenchement de la fourniture d'un nouveau certificat est à l'initiative de l'autorité intermédiaire Certigna (pas d'existence de processus automatisé).

La génération de la CSR est effectuée sous le contrôle de l'opérateur système intervenant lors de la cérémonie de clé.

4.8 Modification du certificat

La modification de certificats Certigna Racine 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 et l'ancien révoqué.

4.9 Révocation et suspension des certificats

4.9.1 Causes possibles d'une révocation

Certificats d'autorité intermédiaire

Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat Certigna Racine :
- L'autorité intermédiaire (son représentant) demande la révocation du certificat pour cause de compromission ou suspicion de compromission de la clé privée ;
- De par la taille insuffisante de la clé privée, le risque de compromission de cette dernière est élevé.

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 de la composante ;
- Décision de changement de composante de l'IGC suite à la détection d'une non conformité des procédures appliquées au sein de la composante avec celles annoncées dans la présente PC (par exemple, suite à un audit de conformité négatif) ;
- Cessation d'activité de l'entité opérant la composante.

4.9.2 Origine d'une demande de révocation

Certificats d'autorité intermédiaire

Les personnes ou entités qui peuvent demander la révocation d'un certificat émis par l'autorité Certigna Racine sont les suivantes :
- L'autorité intermédiaire détentrice du certificat (son représentant) ;
- L'AC ;
- L'AE.

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. Ces certificats sont émis par une autorité tierce.

4.9.3 Procédure de traitement d'une demande de révocation

Certificat ded'autorité intermédiaire

La demande de révocation est effectuée auprès de l'AE.
Cette demande étant générée en interne, elle est présentée et validée lors d'un comité de direction ou de sécurité. S'agissant d'un certificat de la chaîne de certification, l'IGC informe dans les plus brefs délais et par tout moyen l'ensemble des porteurs concernés que leurs certificats ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE et aux MC. Ces derniers devront informer les porteurs de certificats en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

Le contact identifié sur le site du DGME/SDAE (http ://www.synergies-publiques.fr) est immédiatement informé en cas de révocation d'un des certificats de la chaîne de certification. Le DGME/SDAE se réserve le droit de diffuser par tout moyen l'information auprès des promoteurs d'application au sein des autorités administratives et auprès des usagers.

4.9.4 Délai accordé aux autorités intermédiaires pour formuler la demande de révocation

Dès que l'autorité intermédiaire a connaissance qu'une des causes possibles de révocation est effective, elle doit en informer sans délai le comité de direction ou de sécurité.

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

Certificats d'autorité intermédiaire

Une fois la décision de révocation prise par le comité de direction ou de sécurité, le traitement de cette révocation est immédiat.

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/LAR) est effectuée immédiatement, particulièrement dans le cas de la compromission de la clé.

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

L'utilisateur d'un certificat d'une autorité intermédiaire est tenu de vérifier, avant son utilisation, l'état de révocation de ce dernier. Le moyen mis à disposition des utilisateurs est la liste d'autorités révoquées (LAR). Etant donné la gravité d'un événement de révocation d'un certificat d'autorité, cette information est relayée par tout autre moyen dont dispose de l'IGC (sites Web, publication dans des journaux, etc.)

4.9.7 Fréquence d'établissement des LAR

La durée de validité de la LCR est d'un an. En outre, une nouvelle LAR sera systématiquement et immédiatement publiée après révocation d'un certificat d'autorité intermédiaire Certigna.

4.9.8 Délai maximum de publication d'une LAR

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

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

Il n'y a pas de serveur OCSP offrant un service en ligne d'état de révocation des autorités intermédiaires Certigna.

4.9.10 Exigences spécifiques en cas de compromission de la clé privée

Pour les certificats d'AC (AC Certigna Racine et AC intermédiaires), 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 Internet de l'IGC et éventuellement relayée par d'autres moyens (autres sites Internet institutionnels, journaux, etc.).

4.9.11 Suspension de certificat

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

4.10 Fonction d'information sur l'état des certificats

4.10.1 Caractéristiques opérationnelles

L'AC Certigna Racine fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat d'AC intermédiaire, c'est à dire de vérifier les signatures des certificats de la chaîne, les signatures garantissant l'origine et l'intégrité des LAR.
La fonction d'information sur l'état des certificats met à la disposition des utilisateurs de certificats un mécanisme de consultation libre de LAR. Cette LAR est une 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 et 7 jours sur 7. Cette fonction a une durée maximale d'indisponibilité par interruption de service (panne ou maintenance) de 1 heure et une durée maximale totale d'indisponibilité par mois de 4 heures.

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

Sans objet

4.12 Séquestre de clé et recouvrement

Les clés d'AC intermédiaires ne sont en aucun cas séquestrées.

Chapitre 5

Mesures de sécurité non techniques

RAPPEL (cf. chapitre 1.3.1) - 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 sur cette IGC.

En dehors des heures ouvrables, la mise en œuvre de moyens de détection d'intrusion physique et logique renforce la sécurité de l'IGC.

5.1.3 Alimentation électrique et climatisation

Des moyens concernant la fourniture d'énergie électrique et de climatisation sont pris 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 moyens concernant la protection contre les dégâts des eaux sont pris 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 moyens concernant la prévention et la protection contre les incendies sont pris 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

Des moyens concernant la protection des informations intervenant dans l'activité de l'IGC sont pris pour répondre aux besoins de sécurité identifiés dans l'analyse de risque.

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

L'IGC met en œuvre du mirroring entre le site principal et le site de secours assurant une sauvegarde des applications et des informations des composantes de l'IGC. Ce mirroring permet une continuité de l'activité en cas d'interruption de service sur le site principal et permet à l'IGC de respecter ses engagements en termes de disponibilité.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Chaque composante de l'IGC distingue 5 rôles fonctionnels de confiance :

1. **Responsable de sécurité** – Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'événements afin de détecter tout incident, anomalie, tentative de compromission, etc. Il est également chargé d'approuver (de contrôler dans le cas de l'AC Certigna Racine) la génération/révocation de certificats.
2. **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.
3. **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.

4. **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.
5. **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.

Un sixième rôle, lié au partage du secret de l'AC, est également défini :

Porteur de part de secret – Il a la responsabilité d'assurer la confidentialité, l'intégrité et la disponibilité des parts qui lui sont confiées.

5.2.2 Nombre de personnes requises par tâches

Pour des raisons de disponibilité, chaque tâche doit pouvoir être effectuée par au moins deux personnes.

Au minimum, les tâches suivantes sont affectées 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

Les membres du personnel de l'AC Certigna Racine se voient attribuer les rôles de confiance dans des documents internes.

L'AC Certigna Racine 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 en particulier 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 ingénieur système/opérateur ;
– contrôleur et tout autre rôle.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétences et habilitations requises

Tous les personnels amenés à travailler au sein de composantes de l'IGC doivent signer la charte de sécurité interne. L'adéquation des compétences des personnels intervenant dans l'IGC est vérifiée par rapport à ses attributions sur les composantes de cette dernière.
Le personnel d'encadrement, le responsable sécurité, les ingénieurs 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. L'employé doit à cet effet fournir une copie du bulletin n°3 de son casier judiciaire. Cette vérification est renouvelée périodiquement (au minimum tous les 3 ans).

De plus, l'AC s'assure que l'employé ne souffre pas de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

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 Certigna Racine agissant en contradiction avec les politiques et les procédures établies ici 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 présent 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 employé 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.

Les opérateurs disposent notamment des manuels d'opérateurs correspondant aux composantes sur lesquelles ils interviennent (Autorité d'Enregistrement, Autorité de Certification).

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 fin d'audit.
Notamment la génération de certificats d'autorités intermédiaires est consignée dans un procès verbal de « Cérémonie de clé ». Ces générations sont effectuées pour rappel en présence de personnes disposant de rôles au sein de l'IGC et également en présence de témoins (le nombre dépend de la qualification de l'AC pour laquelle le certificat est généré).

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 / suppression de comptes utilisateur ;
- Démarrage et arrêt des systèmes informatiques et des applications ;
- Connexion / déconnexion des utilisateurs ayant des rôles de confiance, ...

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 actions de maintenance et de changement de la configuration des systèmes enregistrés manuellement ;
- Les changements apportés au personnel enregistré.

Des événements spécifiques aux différentes fonctions de l'IGC sont également journalisés :
- Evénements liés aux clés de signature et aux certificats d'AC (génération, sauvegarde et récupération, révocation, destruction,...) ;
- Réception d'une demande de certificat ;
- Validation / rejet d'une demande de certificat ;
- Génération des certificats ;

– Réception d'une demande de révocation ;
– Validation / rejet d'une demande de révocation ;
– Génération des LAR.
Le processus de journalisation permet un enregistrement en temps réel des opérations effectuées. En cas de saisie manuelle, l'écriture est faite sauf exception le même jour ouvré que l'événement.

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.
Lors de l'exploitation du serveur (hébergeant les composantes de l'AC), exploitation nécessitant son démarrage et sa connexion au réseau de l'IGC, les journaux résultant sont stockés sur le serveur d'archivage avec réplication immédiate sur le second site (par mirroring).

5.4.4 Protection des journaux d'événements

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

En dehors de toute exploitation courante, le serveur est pour rappel hors tension. La synchronisation automatique sur une source fiable de temps UTC (cf. 6.8. Horodatage / système de datation) est par conséquent effective lors des opérations d'exploitation du serveur.

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 tous les mois pour identifier des anomalies liées à des utilisations illicites ou abusives.

Le système hébergeant les composants de l'autorité Certigna Racine étant hors tension en dehors des cérémonies de clés et des générations des LAR, les menaces de tentatives d'intrusion sont inexistantes et justifient l'espacement des contrôles dans le temps.
L'auditeur des journaux se fait assister 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 Certigna Racine 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 certificats émis ;
- Les demandes de révocation ;
- Les LAR émises.

5.5.2 Période de conservation des archives

Dossiers de demande de certificat Sans objet

Certificats et LAR émis par l'AC Les certificats de clés des autorités intermédiaires, ainsi que les LAR produites, sont archivés pendant au moins cinq ans après l'expiration de ces certificats.

Journaux d'événements Les journaux d'événements traités au chapitre 5.4 sont archivés pendant cinq 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 Certigna Racine . L'accès en écriture à ces fichiers est protégé (gestion des droits). L'accès en lecture à ces journaux (stockés sur les serveurs NetApp) n'est possible qu'à partir une machine identifiée et autorisée des réseaux internes (réseau internal ou DMZ1 du site principal ou secondaire).

5.5.4 Procédure de sauvegarde des archives

Le procédé de mirroring (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

Pas de procédure particulière. La sauvegarde et l'archivage sont réalisés sur les deux serveurs d'archivage (par réplication et consolidation).

5.5.7 Procédures de récupération et de vérification des archives

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

5.6 Changement de clé d'AC

L'AC Certigna Racine 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'un nouveau bi-clé d'AC est généré, seule la nouvelle clé privée est utilisée pour signer des certificats d'autorité intermédiaire ou des LAR.

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.

Pour rappel :
Suivant le système d'exploitation et/ou le navigateur utilisé par l'utilisateur le nouveau certificat de l'AC Certigna Racine peut être automatiquement installé dans les magasins de certificats des autorités de confiance grâce aux mécanismes de mise à jour (pour les éditeurs ayant reconnu l'autorité Certigna comme autorité de confiance).

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

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 cette information, 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.).

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 par an (niveau d'exigence imposé par la PRIS ***).

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 (cf. chapitre 5.7.2). Dans le cas de compromission d'une clé d'AC, le certificat correspondant sera immédiatement révoqué (cf. chapitre 4.9), excepté pour la clé de l'AC Certigna Racine . Cette dernière ne pouvant être révoquée, ce sont les certificats des autorités intermédiaires délivrés par l'AC Certigna Racine qui sont révoqués et renouvelés.

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 (cf. chapitre 5.7.2).

L'existence de deux sites redondants (site principal et site secondaire), de liens de communication redondants et des procédures de bascule sur l'un et l'autre des deux sites garantit la continuité de service de chacune des composantes de l'IGC. Cette capacité est mise en évidence dans le PCA de la société.

5.7.5 Fin de vie de l'IGC

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

Le transfert d'activité est défini comme :

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

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

5.7.6 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 disponibilités pour ses fonctions définies dans la présente PC ;
– Elle communique aux responsables d'applications listés au chapitre 1.4.1 les principes du plan d'action destinés à faire face à la cessation d'activité ou à organiser le transfert d'activité.

5.7.7 Cessation d'activité affectant l'AC

Dans l'hypothèse d'une cessation d'activité totale, avant que l'AC ne mette un terme à ses services, elle effectue les procédures suivantes :
– Elle informe les autres composantes de l'IGC et les tiers par mail de la cessation d'activité. Cette information sera relayée également directement auprès des entités utilisatrices ;
– Elle révoque tous les certificats d'autorité intermédiaire qu'elle a signés et qui sont encore valides ;
– 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 part de secret.

La cessation d'activité de l'AC Certigna Racine a des répercutions directes sur les AC intermédiaires qu'elle a certifiées. En l'occurrence, ces AC sont également en cessation d'activité et doivent appliquer les procédures correspondantes exigées dans leur PC respective.

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, Dhimyotis 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, Dhimyotis 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 du DGME/SDAE (http ://www.synergies-publiques.fr) est immédiatement informé en cas de cessation d'activité de l'AC Certigna Racine . Le DGME/SDAE se réserve le droit de diffuser par tout moyen l'information auprès des promoteurs d'application au sein des autorités administratives et auprès des usagers.

Chapitre 6

Mesures de sécurité techniques

6.1 Génération et installation de bi-clés

6.1.1 Génération des bi-clés

Clés de l'AC Certigna Racine

Ce chapitre décrit le contexte de génération du bi-clé de l'AC Certigna Racine

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.

La génération de la clé de signature de l'AC Certigna Racine est effectuée dans des circonstances parfaitement contrôlées, par des personnes dans des rôles de confiance (cf. chapitre 5.2.1), dans le cadre de « cérémonies de clés ». Ces personnes sont identifiées dans un document interne à l'IGC Certigna. La cérémonie se déroule suivant un script préalablement défini :

- Elle se déroule sous le contrôle d'au moins deux personnes ayant des rôles de confiance 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 du bi-clé de signature de l'AC Certigna Racine 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 les clés de signatures d'AC. Ces secrets sont des parties de la clé privée de l'AC décomposée suivant un schéma à seuil de Shamir (3 parties parmi 4 sont nécessaires pour reconstituer la clé privée).

Suite à leur génération, les parts de secrets ont été remises à leurs porteurs désignés au préalable et habilités à ce rôle de confiance par l'AC. Un seul porteur ne peut détenir qu'une seule part de secret d'une même AC. Les parts de secret sont placés dans des enveloppes scellées, placées elles même dans des coffres de banque.

Clés générées par les AC intermédiaires

La génération des clés de signature d'AC intermédiaire est effectuée dans des circonstances parfaitement contrôlées (procédure « Cérémonie de clés ») sous le contrôle de l'opérateur système de l'AC intermédiaire et en présence de plusieurs témoins. Cette procédure est décrite dans les PC respectives des AC intermédiaires.

6.1.2 Transmission de la clé privée à son titulaire

Sans objet

6.1.3 Transmission de la clé publique à l'AC de niveau supérieur

L'AC Certigna Racine est l'AC de plus haut niveau. Sa clé publique n'est pas signée par une AC de niveau supérieur.

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

La délivrance de la clé publique de l'AC Certigna Racine , 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 de cette clé publique (l'authentification n'est pas garantie car le certificat est auto-signé).

La clé publique de l'AC Certigna Racine est diffusée dans un certificat auto-signé.

La clé publique de l'AC Certigna Racine , ainsi que sa valeur de contrôle, sont diffusées et récupérées par les systèmes d'information de tous les accepteurs de certificats par l'intermédiaire du site Internet de Certigna à l'adresse http ://www.certigna.fr et http ://www.dhimyotis.com (cf. 2.2.2. Publication des certificats d'AC).

Rappel :
Suivant le système d'exploitation et/ou le navigateur utilisé par l'utilisateur le certificat de l'AC Certigna Racine peut être automatiquement installé dans les magasins de certificats des autorités de confiance grâce aux mécanismes de mise à jour (pour les éditeurs ayant reconnu l'autorité Certigna comme autorité de confiance)

6.1.5 Tailles des clés

Clés de l'AC Certigna Racine

Le bi-clé d'AC est de type RSA 2048 bits
L'algorithme de hachage est de type SHA-1 (160 bits)

Clés d'AC intermédiaires

Le bi-clé d'AC est de type RSA 2048 bits
L'algorithme de hachage est de type SHA-256 (256 bits)

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

Clé de l'AC Certigna Racine

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant au bi-clé (cf. caractéristiques du module TrustWay CryptoBox).

Clés d'AC intermédiaires

L'équipement de génération de bi-clés utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant au bi-clé (cf. caractéristiques du module TrustWay CryptoBox).

6.1.7 Objectifs d'usage de la clé

Clés de l'AC Certigna Racine

L'utilisation de la clé privée de l'AC Certigna Racine et du certificat associé est exclusivement limitée à la signature de certificats d'AC intermédaires et de LAR (cf. chapitre 1.4.1).

Clés d'AC intermédiaires

L'utilisation de la clé privée de l'AC intermédiaire et du certificat associé est exclusivement limitée au service de signature (signature de certificats porteurs/serveurs, de LCR et de réponse OCSP) (cf. chapitre 1.4.1).

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 des AC

Le module cryptographique utilisé par l'AC Certigna Racine et par les autorités intermédiaires pour la génération et la mise en œuvre de leurs clés de signature est la TrustWay CryptoBox de la société BULL évaluée au niveau EAL4+ des critères communs.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'AC Certigna Racine pour l'exportation ou l'importation dans un module cryptographique.
La génération du bi-clé est traitée au chapitre 6.1.1, l'activation de la clé privée au chapitre

6.2.8 et sa destruction au chapitre 6.2.10.

Le contrôle de la clé privée de signature de l'AC Certigna Racine est assuré par du personnel de confiance (porteurs de secrets d'AC) 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).
Dans la pratique, à la génération du secret, ce dernier est partagé en quatre parts et trois porteurs doivent être réunis pour reconstituer le secret (selon la méthode du partage de Shamir). Chaque part de secret est détenue dans un coffre attribué à son porteur.

6.2.3 Séquestre de la clé privée

Clé de l'AC Certigna Racine

La clé privée de l'AC Certigna Racine n'est en aucun cas séquestrée.

Clés des AC intermédiaires

Les clés privées des AC intermédiaires sont exploitées exclusivement à des fins de signature et ne font par conséquent pas l'objet de séquestre.

6.2.4 Copie de secours de la clé privée

Clé de l'AC Certigna Racine

La clé de l'AC Certigna Racine fait l'objet d'une copie de secours hors du module cryptographique. Cette copie est chiffrée par Triple-DES et protégée en intégrité et authenticité avec un calcul de MAC.
La clé de chiffrement de longueur 168 bits est obtenue par diversification d'une clé de base avec un secret d'initialisation partagé entre deux opérateurs. La durée de vie de la copie de secours (sous forme d'un fichier unique) est limitée dans le temps. Cette copie est en effet partagée entre plusieurs opérateurs (partage de Shamir). Une fois ce partage effectué toute trace de la copie de secours est effacée (effacement sécurisé) de la machine hôte sur laquelle la copie a été générée.

Clés des AC intermédiaires

Même procédé que pour la clé de l'AC Certigna Racine .

6.2.5 Archivage de la clé privée

Clé de l'AC Certigna Racine

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

Clés des AC intermédiaires

Les clés privées des AC intermédiaires ne sont en aucun cas archivées.

6.2.6 Transfert de la clé privée avec le module cryptographique

La clé privée de l'AC Certigna Racine est générée dans le module cryptographique. Comme décrit en 6.2.4, cette clé privée n'est exportable/importable dans le module cryptographique que sous forme chiffrée.
Il en est de même pour les clés privées des AC intermédiaires.

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 de l'AC Certigna Racine

L'activation de la clé privée de l'AC Certigna Racine dans le module cryptographique (correspond à la génération ou la restauration des clés) 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 (responsable sécurité, et un opérateur habilité à administrer le module cryptographique).

Clés des AC intermédiaires

Idem clé de l'AC Certigna Racine

6.2.9 Méthode de désactivation de la clé privée

Clés de l'AC Certigna Racine

Le module cryptographique (carte PCI intégrée dans le boitier 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 du boîtier.

Clés des AC intermédiaires

Idem clé de l'AC Certigna Racine

6.2.10 Méthode de destruction des clés privées

Clés de l'AC Certigna Racine

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 AC intermédiaires

Idem clé de l'AC Certigna Racine

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques de l'AC Certigna Racine et des AC intermédiaires 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 AC intermédiaires couverts par la présente PC ont une durée de validité de 10 ans maximum.
La durée de validité du certificat de l'AC Certigna Racine est de 20 ans.

La fin de validité d'un certificat de l'AC Certigna Racine 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 Certigna Racine

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).
Les données d'activation correspondent au code PIN des cartes à puce d'administration du module cryptographique.

Génération et installation des données d'activation correspondant à la clé privée des AC intermédiaires

Idem clé de l'AC Certigna Racine

6.4.2 Protection des données d'activation

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

Les données d'activation ne sont en aucune manière conservées sous forme électronique ou manuscrite. Il s'agit pour rappel d'une carte 'administrateur' et du code PIN associé, détenus respectivement par le responsable sécurité et l'administrateur du module cryptographique.

En cas de panne matérielle ou d'oubli des données d'activation, il existe une seconde carte 'administrateur' dont le code PIN est détenu par le second administrateur.

Protection des données d'activation correspondant aux clés privées des AC intermédiaires

Idem clé de l'AC Certigna Racine

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) ;
- Protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés 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 pare-feu ;
- Communication sécurisée inter-site (tunnel VPN IPSec) ;
- Fonctions d'audits (non-répudiation et nature des actions effectuées).

Des dispositifs de surveillance (vidéosurveillance et alarme automatique) 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

Le boitier BULL TrustWay CryptoBox exploité par l'IGC est certifiée EAL4+ par la DCSSI. Le boitier répond aux exigences de sécurité du profil de protection CWA 14167-2 version 0.28 du 27 octobre 2003, certifié par la DCSSI sous la référence [PP/0308].

6.6 Mesures de sécurité des systèmes durant leur cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

Lors de la conception de tout nouveau projet de développement, une analyse sur le plan de la sécurité est réalisée et doit être approuvée par le Comité de Sécurité de l'AC.
La configuration des systèmes de l'AC Certigna Racine 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.
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 Certigna Racine pour validation.

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

Le niveau de sécurité du cycle de vie des systèmes est adapté à l'exploitation de l'IGC.

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. Le réseau est équipé notamment de deux firewall (un par site d'exploitation) intégrant un système de détection des intrusions IPS (avec émission d'alertes).

6.7.1 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. Cette source est obtenue auprès de quatre serveurs de temps : Angers, Reims, IMAG (Grenoble), UNILIM (Limoges).

Chapitre 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 Profil du certificat de l'AC Certigna Racine

Le certificat de l'AC Certigna Racine contient les champs de base et les extensions suivantes :

Champs de base

Champ	**Description**
Version	V3
Serial Number	Numéro de série unique
Signature	Identifiant de l'algorithme de signature de l'AC SHA-1 160 bits RSA 2048 bits
Issuer	DN={ } countryName : C=FR organizationName : O=Dhimyotis commonName : CN=Certigna
Validity	Dates et heures d'activation et d'expiration du Certificat
Subject	DN={ } countryName : C=FR organizationName : O=Dhimyotis commonName : CN= *Nom de l'AC intermédiaire*
Subject Public Key Info	RSA 2048 bits

Extensions

Champ	**C**	**Description**
Authority Key Identifier	N	Identifiant de la clé publique de l'autorité Certigna Racine
Subject Key Identifier	N	Identifiant de la clé publique de l'autorité intermédiaire
Key Usage	O	Signature de certificat Signature de la liste de révocation hors connexion Signature de la liste de révocation
Basic Constraints	N	SujectType = CertAuthority PathLengthConstraint = aucune
netscape-cert-type	N	SSL, S/MIME, signature

7.2 Profil des certificats émis par l'AC Certigna Racine

Les certificats émis par l'AC Certigna Racine contiennent les champs de base et les extensions suivantes :

Champs de base

Champ	**Description**
Version	V3
Serial Number	Numéro de série unique
Signature	Identifiant de l'algorithme de signature de l'AC SHA-256 250 bits RSA 2048 bits
Issuer	DN={ } countryName : C=FR organizationName : O=Dhimyotis commonName : CN=Certigna
Validity	Dates et heures d'activation et d'expiration du Certificat
Subject	DN={ } serialNumber : *Numéro de série unique* countryName : C=FR organizationName : O=Dhimyotis organizationUnitName : OU=0002 481463081 commonName : CN= *Nom de l'AC intermédiaire*
Subject Public Key Info	RSA 2048 bits

Extensions

Champ	**C**	**Description**
Authority Key Identifier	N	Identifiant de la clé publique de l'autorité Certigna Racine
Subject Key Identifier	N	Identifiant de la clé publique de l'autorité intermédiaire
Key Usage	O	Signature de certificat Signature de la liste de révocation hors connexion Signature de la liste de révocation
CRL Distribution Points	N	URL=http ://crl.certigna.fr/certigna.crl URL=http ://crl.dhimyotis.com/certigna.crl
Basic Constraints	N	SujectType = CertAuthority PathLengthConstraint = aucune
netscape-cert-type	N	S/MIME, signature
netscape-revocation-url	N	URL=http ://crl.certigna.fr/certigna.crl

7.3 Profil des LAR

Champs de base

Champ	Description
Version	V2
Signature	Identifiant de l'algorithme de signature de l'AC SHA-1 160 bits RSA 2048 bits
Issuer	DN={ } countryName : C=FR organizationName : O=Dhimyotis commonName : CN=Certigna Racine
This Update	Date de génération de la LAR
Next Update	Date de prochaine mise à jour de la LAR
Revoked Certificates	Liste des n° de série des certificats révoqués

Extensions

Champ	C	Description
Authority Key Identifier	N	Identifiant de la clé publique de l'autorité Certigna Racine
CRL Number	N	Contient le n° de série de la LAR

Chapitre 8

Audit de conformité et autres évaluations

Les audits et les évaluations concernent 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 sa PC et aux pratiques identifiées dans sa DPC. En l'occurrence l'IGC Certigna fait appel à un cabinet d'audit externe pour réaliser cette prestation.

8.1 Fréquences et/ou circonstances des évaluations

Un programme d'audit annuel a été mis en place pour auditer l'ensemble de l'IGC Certigna. Ce programme inclut une intervention mensuelle suivant un plan d'audit spécifique.

8.2 Identités/qualifications des évaluateurs

Le contrôle est assigné par l'AC Certigna Racine 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

Les auditeurs et l'AC entretiennent une relation contractuelle relative à l'exécution des audits et les auditeurs sont suffisamment séparés de l'AC auditée d'un point de vue organisationnel pour fournir une évaluation objective et indépendante.

L'équipe d'audit ne doit pas appartenir à l'entité opérant 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 Certigna Racine , un avis parmi les suivants : « réussite », « échec », « à confirmer ».

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

8.6 Communication des résultats

Les résultats des audits de conformité effectués par le cabinet d'audit (audits récurrents) sont tenus à la disposition de l'organisme en charge de la qualification des différentes autorités de certification intermédiaires.

Chapitre 9

Autres problématiques métiers et légales

9.1 Tarifs

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Sans objet

9.1.2 Tarifs pour accéder aux certificats

La présente PC ne prévoit pas de tarifs pour accéder aux certificats.

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

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

9.1.4 Tarifs pour d'autres services

Sans objet

9.1.5 Politique de remboursement

Sans objet

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

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 Certigna Racine ;
- La clé privée de l'AC, des composantes et des AC intermédiaires ;
- Les données d'activation associées aux clés privées de l'AC Certigna Racine et des AC intermédiaires ;
- Tous les secrets de l'IGC ;
- Les journaux d'événements des composantes de l'IGC ;
- Les causes de révocations 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.

9.4 Protection des données personnelles

9.4.1 Politique de protection des données personnelles

Sans objet

9.4.2 Informations à caractère personnel

Sans objet

9.4.3 Informations à caractère non personnel

Sans objet

9.4.4 Responsabilité en termes de protection des données personnelles

Sans objet

9.4.5 Notification et consentement d'utilisation des données personnelles

Sans objet

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

Sans objet

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.

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.) ;
- 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 Certigna Racine s'engage à :
– Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour une autorité intermédiaire ;
– Garantir et maintenir la cohérence de sa DPC avec sa PC ;
L'AC assume toute conséquence dommageable résultant du non-respect de sa PC, par elle-même ou l'une de ses composantes.

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.

9.6.2 Service d'enregistrement

Sans objet

9.6.3 Détenteurs de certificats (AC intermédiaires)

L'AC intermédiaire a le devoir de :
– Protéger sa clé privée par des moyens appropriés à son environnement ;
– Protéger ses données d'activation et les mettre en œuvre ;
– Protéger l'accès à sa base de certificats ;
– Respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;
– Informer l'AC Certigna Racine de toute modification concernant les informations contenues dans son certificat ;
– Faire, sans délai, une demande de révocation de son certificat auprès de l'AC Certigna Racine en cas de compromission ou de suspicion de compromission de sa clé privée.

9.6.4 Utilisateurs des certificats émis par les AC intermédiaires

Les tiers utilisateurs doivent :
– Dans le cadre d'utilisation de certificats émis par une AC intermédiaire Certigna, vérifier la signature numérique et la validité (date de validité, statut de révocation) du certificat de cette AC dans le contexte générale de vérification de la chaîne de certification.

9.6.5 Autres participants

Sans objet

9.7 Limite de garantie

San sobjet

9.8 Limite de responsabilité

Il est expressément entendu que Dhimyotis ne saurait être tenue pour responsable ni d'un dommage résultant d'une faute ou négligence d'un accepteur de certificat ni d'un dommage causé par un fait extérieur, notamment en cas de :
- 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 ;
- Force majeure comme définie par les tribunaux français.

9.9 Indemnités

Dhimyotis a notamment souscrit un contrat « Responsabilité civile après livraison ». L'étendue des garanties y est de cinq cent mille (500 000) euros par sinistre.

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 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.

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.

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.

Toute modification majeure de la PC, et par conséquent de la DPC, donne lieu à une vérification de conformité par l'AAP de cette PC par rapport à la PC type. La DPC n'est applicable qu'après approbation de l'AAP.

9.12.2 Mécanisme et période d'information sur les amendements

L'AC communique via son site Internet http ://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

Lorsque la modification de la PC est de nature typographique ou lorsque la modification de la PC porte sur le niveau de qualité et de sécurité des fonctions de l'AC et de l'AE sans perte de conformité d'un certificat émis avec la PC qu'il supporte, les OID de la PC et de la DPC correspondante ne sont pas modifiés.
Lorsque la modification de la PC entraîne la perte de conformité d'un certificat avec la PC qu'il supporte, les OID de la PC et de la DPC sont modifiés et notifiés.

9.13 Dispositions concernant la résolution de conflits

Sans objet

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.

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

Chapitre 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 Certigna Racine pour générer et mettre en œuvre sa clé de signature (pour la génération des certificats électroniques, des LAR), répond aux exigences de sécurité suivantes :

- assurer la confidentialité et l'intégrité de la clé privée de signature de l'AC Certigna Racine durant tout son cycle de vie, et assurer leur destruction sûre en fin de vie ;
- être capable d'identifier et d'authentifier ses utilisateurs ;
- limiter l'accès à ses services en fonction de l'utilisateur et du rôle qui lui a été assigné ;
- être capable de mener une série de tests pour vérifier qu'il fonctionne correctement et entrer dans un état sûr s'il détecte une erreur ;
- permettre de créer une signature électronique sécurisée, pour signer les certificats générés par l'AC, qui ne révèle pas la clé privée de l'AC et qui ne peut pas être falsifiée sans la connaissance de cette clé privée ;
- créer des enregistrements d'audit pour chaque modification concernant la sécurité ;
- si une fonction de sauvegarde et de restauration de la clé privée de l'AC est offerte, garantir la confidentialité et l'intégrité des données sauvegardées et réclamer au minimum un double contrôle des opérations de sauvegarde et de restauration ;
- Le module cryptographique de l'AC doit détecter les tentatives d'altérations physiques et entrer dans un état sûr quand une tentative d'altération est détectée.

10.2 Exigences sur la certification

Le module cryptographique utilisé par l'AC est, dans les conditions prévues par le décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, certifié conforme aux exigences du chapitre 10.1 ci-dessus par le Premier ministre.
Le module cryptographique certifié, suivant les critères communs, conforme au profil de protection PP/0308 est considéré comme répondant aux exigences de la présente annexe.