POLITIQUE DE CERTIFICATION

CERTIFICAT DE SIGNATURE À USAGE UNIQUE

EMETTEUR	DESTINATAIRES	COPIES
CERTINOMIS	PUBLIC	

Certinomis

Certinomis SA au capital de 40 156 euros.

Siège social : 45-47 Boulevard Paul Vaillant-Couturier

94200 Ivry sur Seine – France. RCS Créteil B 433 998 903

Historique des versions

DATE	VERSION	EVOLUTION	AUTEUR
13/07/2018	1.0	Validation	F. LEROY
19/09/2018	1.1	Ajout OID professionnel	F. LEROY
15/04/2021	2.0	Réécriture des méthodes de génération et d'activation des clés privées des signataires	F. CHASSERY
21/07/2021	2.01	Révision du §1.1 avec ajout de la hiérarchie d'AC	F.CHASSERY

Table des matières

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

AVERTISSEMENT

La présente Politique de Certification est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de Certinomis. La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisées préalablement par écrit par Certinomis ou ses ayants droit, sont strictement interdites.

Le Code de la Propriété Intellectuelle n'autorise, aux termes de l'article L.122-5, d'une part, que « les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinés à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (article L.122-4 du Code de la Propriété Intellectuelle).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

La Déclaration des Pratiques de Certification, propriété de la société Certinomis peut être concédée par des accords de licence à toutes entités privées ou publiques qui souhaiteraient l'utiliser dans le cadre de leurs propres services de certification.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

1 INTRODUCTION

1.1 PRESENTATION GENERALE

1.1.1 IGC Certinomis

Certinomis est un Prestataire de Service de Certification Electronique (PSCE) dont le métier est la garantie de l'identité au sens large dans les échanges électroniques : identité des personnes physiques agissant pour leur compte propre ou au nom d'une personne morale, ou identification d'une personne morale responsable de la mise en œuvre d'une application informatique.

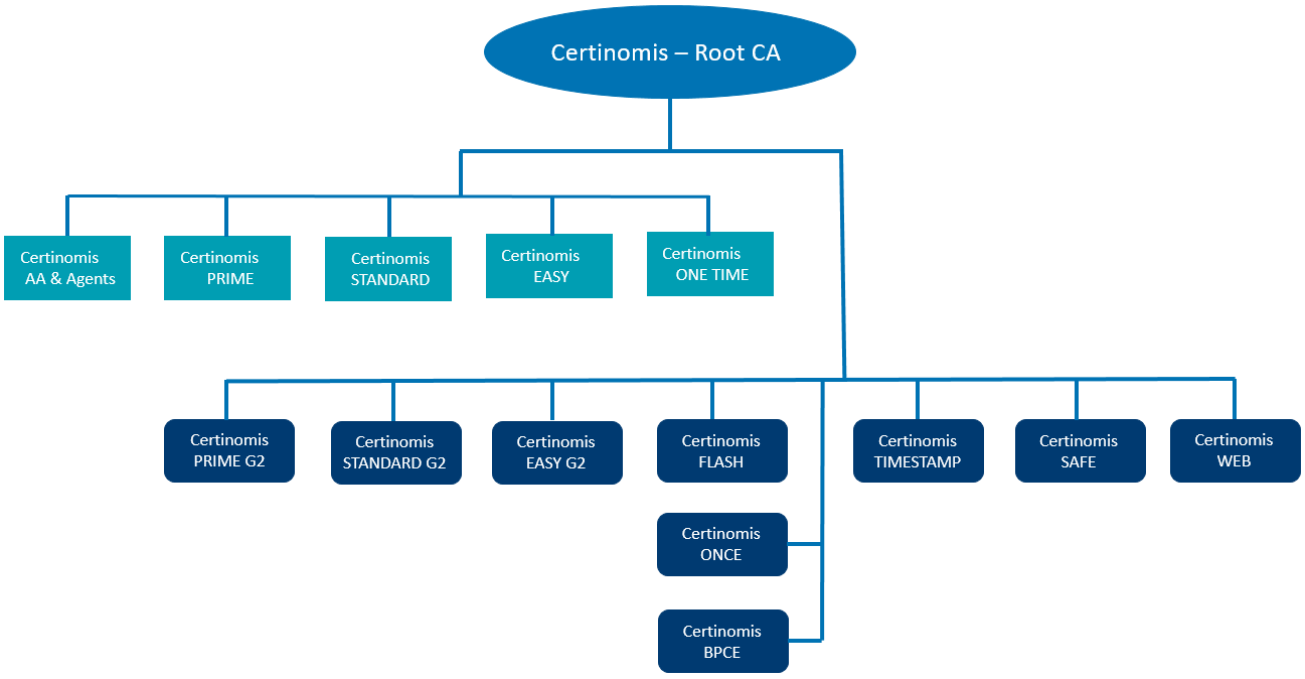
Le PSCE réalise ses missions en émettant des certificats électroniques au travers de différentes Autorités de Certification (AC) qui s'insèrent dans une Infrastructure à Clé Publique (IGC), un ensemble de moyens techniques, humains, documentaires et contractuels mis à la disposition d'utilisateurs pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques.

La mise en place d'une IGC, nécessaire à la sécurité et à la confiance, ouvre une palette de services à valeur ajoutée pour les transactions électroniques (par exemple : transactions commerciales, signature de contrats, téléprocédures, etc.).

Ils ont pour fonction d'assurer :

- l'intégrité des messages ;
- l'identification et l'authentification[1] ;
- l'authenticité de l'origine ;
- et la confidentialité.

L'IGC de Certinomis regroupe plusieurs AC sous une même Autorité de Certification Racine et peut être visualisée ainsi :



1.1.2 Objet du document

La présente Politique de Certification a pour objet de permettre l'émission de certificats à usage unique identifiant des signataires, personnes physiques, valables pour un laps de temps réduit et qui seront utilisés pour la création d'une seule signature électronique.

Elle concerne les AC Certinomis Flash, Certinomis Once et Certinomis BPCE.

[1] Étant précisé que ce n'est pas au sens des actes authentiques, tels qu'ils sont régis par les articles 1317 et suivants du code civil, mais au sens technique d'authentification cryptographique

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

La Politique de Certification définie dans le présent document est destinée à être utilisée par les individus dans le cadre de transactions de signature électronique. Les personnes qui consultent et utilisent ce document peuvent s'informer auprès de l'AC émettrice afin d'obtenir plus de détails sur sa mise en œuvre.
La Politique de Certification couvre la gestion et l'utilisation de certificats contenant les clés publiques servant aux fonctions de vérification, d'intégrité et de concordance des clés.

La délivrance d'un certificat de clé publique en vertu de la présente politique ne signifie pas que le client ou le bénéficiaire soit autorisé de quelque façon que ce soit à faire des transactions commerciales, ou autres, au nom de l'organisation qui exploite l'AC.

L'AC est assujettie aux lois et règlements en vigueur sur le territoire de la République française, ainsi qu'aux normes européennes en vigueur et aux conventions internationales ratifiées par la France, et qui touchent à l'application, l'élaboration, l'interprétation et la validité des politiques de certification mentionnées dans le présent document.

L'AC se réserve le droit de ne pas conclure d'accord de certification croisée avec une autorité de certification externe.

1.2 IDENTIFICATION DU DOCUMENT

Désignation des numéros d'identification d'objet (OID) pour la présente politique :

AC FLASH	
OID	*Niveau de qualification*
Signature : 1.2.250.1.86.2.6.10.2.1	ETSI/EN 319 411 LCP

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

AC ONCE		
OID		*Niveau de qualification*
Signature : **Signature Pro :**	1.2.250.1.86.2.6.11.2.1 1.2.250.1.86.2.6.12.2.1	ETSI/EN 319 411 NCP ETSI/EN 319 411 NCP

AC SIGNATURE BPCE		
OID		*Niveau de qualification*
Signature : **Signature Pro :**	1.2.250.1.86.2.6.11.2.1 1.2.250.1.86.2.6.12.2.1	ETSI/EN 319 411 NCP ETSI/EN 319 411 NCP

1.3 ENTITES INTERVENANT DANS L'IGC

Lorsqu'un prestataire fournit des services de certification, à savoir qu'il délivre des certificats ou qu'il fournit d'autres services liés aux signatures numériques, il convient de distinguer plusieurs métiers ou fonctions, desquels découlent des rôles et des responsabilités distincts.

Le processus de certification et la gestion du cycle de vie du certificat font appel à une grande diversité d'intervenants dans la chaîne de la confiance :

- Autorité de certification,
- Autorité d'enregistrement,
- Bénéficiaire du certificat délivré par l'Autorité de Certification,
- Tiers utilisateurs.

1.3.1 Autorités de certification

L'Autorité de Certification est responsable vis-à-vis de ses clients, mais aussi de toute personne se fiant à un certificat qu'elle a émis, de l'ensemble du processus de certification, et donc de la validité des certificats qu'elle émet. À ce titre, elle édicte la Politique de Certification et valide les Déclarations de Pratiques de Certification respectées par les différentes composantes de l'Infrastructure à Clé Publique.

La garantie apportée par l'Autorité de Certification vient de la qualité des techniques mises en œuvre, mais aussi du cadre réglementaire et contractuel qu'elle définit et s'engage à respecter.

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 infrastructure de gestion de clés (IGC).

Les prestations de l'AC sont le résultat de différentes fonctions qui correspondent aux différentes étapes du cycle de vie des bi-clés et des certificats (cf. ci-dessous).

Autorité d'enregistrement (AE) - Cette fonction vérifie les informations d'identification du futur bénéficiaire d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC (cf. ci-dessous). L'AE a également en charge, lorsque cela est nécessaire, la re-vérification des informations du bénéficiaire du certificat lors du renouvellement du certificat de celui- ci. Dans le cadre de la présente PC la vérification des justificatifs d'identité et la demande de certificat associée peuvent être automatisées.

Fonction de génération des certificats - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du sujet provenant de la fonction de génération des éléments secrets du bénéficiaire.

Fonction de génération des éléments secrets du bénéficiaire - Cette fonction génère les éléments secrets à destination du bénéficiaire, et les prépare en vue de leur remise au bénéficiaire (par exemple code d'activation envoyé par SMS).

Fonction de publication - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux bénéficiaires et/ou aux utilisateurs de certificats, hors informations d'état des certificats. L'AC ne met pas à disposition les certificats valides de ses bénéficiaires.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Fonction de gestion des révocations - Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats.

Fonction d'information sur l'état des certificats - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués, suspendus, etc.). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers : LCR, LAR.

Un certain nombre d'entités / personnes physiques externes à l'IGC interagissent avec cette dernière. Il s'agit notamment :

Porteur (ou Bénéficiaire) - La personne physique identifiée dans le certificat et qui est le responsable des certificats qui lui sont attribués.

Utilisateur de certificat - L'entité ou la personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du bénéficiaire du certificat.

Personne autorisée- Il s'agit d'une personne autre que le Bénéficiaire et qui est autorisée par la Politique de Certification de l'AC ou par contrat avec l'AC à mener certaines actions pour le compte du Bénéficiaire (demande de révocation, de renouvellement, ...). Typiquement, dans une entreprise ou une administration, il peut s'agir d'un responsable hiérarchique du Bénéficiaire ou d'un responsable des ressources humaines.

Dans le cadre de ses fonctions opérationnelles, les exigences qui incombent à l'AC en tant que responsable de l'ensemble des composantes de l'IGC sont les suivantes :

- Être une entité légale au sens de la loi française.
- Être en relation par voie contractuelle / hiérarchique / réglementaire avec le Porteur pour la gestion de ses certificats.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux promoteurs d'application d'échanges dématérialisés de l'administration, aux bénéficiaires, aux utilisateurs de certificats,... qui mettent en œuvre ses certificats.
- S'assurer que les exigences de la PC et les procédures de la DPC sont appliquées par chacune des composantes de l'IGC et sont adéquates et conformes aux normes en vigueur.
- Mener 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. Elle élabore sa DPC en fonction de cette analyse.
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, correspondant au minimum aux fonctions de la présente PC, notamment en matière de génération des certificats, de remise au bénéficiaire, de gestion des révocations et d'information sur l'état des certificats.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans sa PC, notamment en termes de fiabilité, de qualité et de sécurité.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats, de LCR), ou faire renouveler ses certificats si l'AC est rattachée à une AC hiérarchiquement supérieure. Diffuser ses certificats d'AC aux bénéficiaires et utilisateurs de certificats.

1.3.2 Autorité d'enregistrement

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

L'Autorité d'Enregistrement est le lien entre l'Autorité de Certification et le Bénéficiaire. Qu'elle soit ou non directement en contact physique avec le bénéficiaire, elle reste dépositaire de ses informations personnelles.

Sa responsabilité ne peut être engagée que par l'Autorité de Certification. L'Autorité de Certification a un devoir de contrôle et d'audit des Autorités d'Enregistrement.

L'AE a pour rôle de vérifier l'identité du futur sujet du certificat. Pour cela, l'AE assure les tâches suivantes :

- la prise en compte et la vérification des informations du futur porteur. Ce processus de vérification des justificatifs d'identité fournis par le porteur peut être automatisé ;
- l'établissement et la transmission de la demande de certificat à la fonction adéquate de l'IGC suivant l'organisation de cette dernière et les prestations offertes ;
- l'archivage des pièces du dossier d'enregistrement (ou l'envoi vers la composante chargée de l'archivage) ;
- la conservation et la protection en confidentialité et en intégrité des données personnelles d'authentification du bénéficiaire y compris lors des échanges de ces données avec les autres fonctions de l'IGC (notamment,

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

elle respecte la législation relative à la protection des données personnelles).

1.3.2.1 Rôles

Le responsable de l'AC attribue à une partie de son personnel ou délègue à une entité externe dans le cadre d'un contrat d'AE les fonctions suivantes :

- coordonner les demandes d'identification électronique ;
- vérifier les caractéristiques d'identification des bénéficiaires identifiées ;
- distribuer aux Bénéficiaires les Données d'Activation nécessaire à l'utilisation de son certificat ;
- gérer et protéger les données personnelles et de sécurité des bénéficiaires ; et
- maintenir, administrer, exploiter et protéger les machines et logiciels utilisés pour remplir ces fonctions.

Le personnel de l'AC ou l'entité externe remplissant ces fonctions constituera une Autorité d'Enregistrement (AE).Le personnel d'une AE doit :

- connaître et respecter les règles, principes et procédures énoncées dans la PC et la DPC reliées au fonctionnement de l'AE ;
- être désigné par le responsable de l'AE et accepté par l'AC ; et
- être un employé de l'AE.

L'AE qui satisfait aux conditions susmentionnées peut être autorisée par le responsable de l'AC à vérifier l'identité des demandeurs d'identification électronique dont le certificat portera l'identifiant (OID) de la PC associée à la présente déclaration.

1.3.3 Clients

Dans le cadre de la présente PC, un Client est une personne physique en relation contractuelle avec l'AC, ou une personne morale qui autorise le Porteur à la représenter. De manière générale le Client recourt aux processus de l'AE pour fournir ses éléments d'identification et accepte les processus d'utilisation des certificats électroniques conformément à ce qui est décrit dans la présente PC.

1.3.4 Bénéficiaires de certificats

Dans le cadre de la présente PC, un porteur de certificats ne peut être qu'une personne physique.

Les personnes agissant pour le compte d'une organisation, utilisent leur clé privée et le certificat correspondant dans le cadre de leurs activités en relation avec l'entité identifiée dans le certificat et avec laquelle ils ont un lien contractuel / hiérarchique / réglementaire.

1.3.5 Utilisateurs de certificats

L'utilisateur du certificat peut être ;

- Une entité ou une personne physique qui reçoit un certificat et qui s'y fie pour vérifier une signature électronique provenant du bénéficiaire du certificat.
- Un serveur sous la responsabilité d'une personne physique ou morale, qui utilise un certificat et un dispositif de vérification de signature pour vérifier la signature électronique apposée sur des données ou un message par le bénéficiaire du certificat. L'application met en œuvre la politique et les pratiques de sécurité édictées par le responsable d'application.

Avant d'accorder sa confiance au dit certificat, le tiers utilisateur doit impérativement vérifier sa validité auprès de Certinomis en interrogeant le serveur OCSP approprié, ainsi qu'en vérifiant sa validité intrinsèque, en particulier sa date d'expiration et sa signature, et la validité de tout certificat sur l'itinéraire de confiance. À défaut de remplir cette obligation, le tiers utilisateur assume seul tous les risques de ses actions non conformes aux exigences de la présente politique, Certinomis ne garantissant, dès lors, plus aucune valeur juridique aux certificats qu'elle a émis et qui pourraient avoir été révoqués ou qui ne seraient pas valides.

1.3.6 Autres participants

1.3.6.1 Composantes de l'IGC

La décomposition fonctionnelle de L'IGC est décrite dans la DPC

1.4 USAGE DES CERTIFICATS

1.4.1 Domaines d'utilisation applicables

1.4.1.1 Bi-clés et certificats émis

La présente PC traite des bi-clés et des certificats à destination des catégories de bénéficiaires identifiées au chapitre 1.3.3 ci-dessus, afin que ces bénéficiaires puissent signer électroniquement des données (documents ou messages) dans le cadre d'échanges dématérialisés avec les catégories d'utilisateurs de certificats identifiées au chapitre 1.3.4 ci-dessus.

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.

L'utilisation de la clé privée du bénéficiaire et du certificat associé doit rester strictement limitée au service de signature (cf. chapitre 4.5.1 ci-dessous). L'utilisateur du certificat a ainsi l'assurance que le bénéficiaire identifié dans le certificat a manifesté son consentement quant au contenu des données signées électroniquement à l'aide de la clé privée correspondante.

1.4.1.2 Bi-clés et certificats d'AC et de composantes

L'AC génère et signe différents types d'objets : certificats (bénéficiaires et répondeur OCSP) et LCR. Pour signer ces objets, l'AC dispose d'une bi-clé.

L'AC dispose d'une seule bi-clé et le certificat correspondant est rattaché à une AC de niveau supérieur (hiérarchie d'AC).

Les bi-clés et certificats de l'AC sont utilisés pour la signature de certificats et uniquement utilisés qu'à cette fin. Ils ne sont pas utilisés ni à des fins de confidentialité, ni à des fins d'authentification.

1.4.2 Domaines d'utilisation interdits

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

L'AC publie dans ses Conditions Générales d'Utilisation les termes et conditions relatives à l'utilisation des certificats émis.

Le certificat n'étant pas remis au bénéficiaire et n'étant utilisé que par un serveur de signature, aucune utilisation interdite ne pourrait être mise en œuvre.

1.5 GESTION DE LA PC

La présente politique s'applique aux AC et aux partenaires, à leur responsable, à leur personnel, aux certificats émis par les AC, aux Listes de Certificats Révoqués émises par les AC, aux clients et bénéficiaires des AC et aux tiers utilisateurs de certificats émis par les AC.

1.5.1 Entité gérant la PC

La présente politique de certification est sous la responsabilité de la société Certinomis.

1.5.2 Point de contact

Le directeur général de Certinomis

45-47, Boulevard Paul Vaillant-Couturier

94200 Ivry sur Seine

Téléphone : 0810 184 956

Télécopieur : (33) (0)1. 56.29.72.67

Courrier électronique : politiquecertification@certinomis.fr

1.5.3 Entité déterminant la conformité d'une DPC avec cette PC

La Direction de Certinomis détermine la conformité de la DPC avec la présente politique de certification, soit directement soit indirectement en faisant appel à des experts indépendants spécialisés dans le domaine de la sécurité et des IGC.

1.5.4 Procédures d'approbation de la conformité de la DPC

L'AC est garante de l'application de la DPC avec la Politique de Certification.

L'AC est responsable de la gestion (mise à jour, révisions) de la DPC. Toute demande de mise à jour de la DPC suit le processus d'approbation mis en place. Toute nouvelle version de la DPC est publiée, conformément aux exigences du paragraphe 2.2 sans délai.

Une AGP peut demander l'examen de la DPC conformément aux procédures en vigueur.

1.6 DEFINITIONS ET ACRONYMES

1.6.1 Acronymes

Les acronymes utilisés dans la présente PC sont les suivants :

- AC Autorité de Certification
- AE Autorité d'Enregistrement
- AGP Autorité de Gestion des Politiques
- AH Autorité d'Horodatage
- DN Distinguished Name
- DPC Déclaration des Pratiques de Certification
- ETSI European Telecommunications Standards Institute
- IGC Infrastructure de Gestion de Clés.
- LAR Liste des certificats d'AC Révoqués
- LCR Liste des Certificats Révoqués
- OID Object Identifier
- PC Politique de Certification
- PSCE Prestataire de Services de Certification Électronique
- PSCo Prestataire de Services de Confiance
- RSA Rivest Shamir Adelman
- SP Service de Publication
- SSA Serveur de Signature Applicatif
- SSI Sécurité des Systèmes d'Information
- URL Uniform Resource Locator

1.6.2 Définitions

1.6.2.1.1 Autorité de Certification (AC) :

Au sein d'un PSCE, une Autorité de Certification a en charge, au nom et sous la responsabilité de ce PSCE, l'application d'au moins une politique de certification et est identifiée comme telle, en tant qu'émetteur (champ "issuer" du certificat), dans les certificats émis au titre de cette politique de certification. Dans le cadre de la présente PC, le terme de PSCE n'est pas utilisé en dehors du présent chapitre et du chapitre 1.1 et le terme d'AC est le seul utilisé. Il désigne l'AC chargée de l'application de la politique de certification, répondant aux exigences de la présente PC, au sein du PSCE souhaitant faire qualifier la famille de certificats correspondante.

1.6.2.1.2 Autorité d'enregistrement (AE) :

L'Autorité d'Enregistrement applique des procédures d'identification des personnes physiques, conformément aux règles définies par l'Autorité de Certification. Son but est d'établir que le demandeur a bien l'identité et les qualités qui seront indiquées dans le certificat.
L'Autorité d'Enregistrement est le lien entre l'Autorité de Certification et le bénéficiaire. Qu'elle soit ou non directement en contact physique avec le bénéficiaire, elle reste dépositaire de ses informations personnelles.

1.6.2.1.3 Autorité de Gestion de la Politique (AGP) :

L'Autorité de Gestion de la Politique, pour les usages qui la concerne, établit les besoins et les exigences en termes de sécurité dans l'ensemble du processus de certification et d'utilisation des certificats. Elle établit des lignes directrices, qui peuvent prendre la forme d'un canevas de Politique de Certification, que doivent respecter toutes les Autorités de Certification qu'elle accrédite. Elle valide et suit toute évolution des politiques de certification des Autorités de Certification qu'elle accrédite.

Son rôle est celui d'une autorité morale qui indique par l'accréditation la confiance que l'on peut accorder à une Autorité de Certification.

1.6.2.1.4 Bénéficiaire :

Personne physique identifiée par l'AE qui porte la responsabilité des certificats qui lui sont attribués.

1.6.2.1.5 Certificat :

Attestation électronique liant les données afférentes au chiffrement ou à la vérification de signature, des échanges,

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

messages et documents électroniques à un sujet, afin d'en assurer la confidentialité ou d'en assurer l'authentification et l'intégrité.

1.6.2.1.6 Client :

Bénéficiaire de certificat qui est en relation contractuelle avec l'AE (voir 1.3.4) ou personne morale au nom de laquelle agit le Bénéficiaire.

1.6.2.1.7 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.

1.6.2.1.8 Dispositif de création de signature (DCS) :

Logiciel, ou module cryptographique configuré, servant à créer une signature électronique à distance par rapport au contexte du signataire et qui vise à garantir que la clé de signature est utilisé sous le contrôle du signataire.

1.6.2.1.9 Données d'Activation :

Information ou procédé utilisé pour protéger la clé du porteur.

1.6.2.1.10 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 bénéficiaires et les utilisateurs de certificats.

1.6.2.1.11 Prestataire de services de certification électronique (PSCE) :

Personne morale responsable de la gestion de certificats électroniques tout au long de leur cycle de vie, vis-à-vis des Bénéficiaires et utilisateurs de ces certificats. Un PSCE peut fournir différentes familles de certificats correspondant à des finalités différentes et/ou des niveaux de sécurité différents. Un PSCE met en œuvre au moins une AC mais peut en comporter plusieurs en fonction de son organisation. Les différentes AC d'un PSCE peuvent être indépendantes les unes des autres et/ou liées par des liens hiérarchiques ou autres (AC Racines / AC Filles). Un PSCE est identifié dans un certificat dont il a la responsabilité au travers de son AC ayant émis ce certificat et qui est elle-même directement identifiée dans le champ "issuer" du certificat.

1.6.2.1.12 Serveur de Signature Applicatif (SSA) :

Serveur applicatif qui séquence la création d'une signature pour le compte des Porteurs.

Le SSA lie la clé de signature aux Données d'Activation du Signataire, directement ou via le DCS, et vérifie que ces Données d'Activation sont utilisées pour autoriser l'utilisation de la clé de signature par le DCS.

1.6.2.1.13 Sujet :

Identité vérifiée par l'AE et portée dans le certificat généré par l'AC.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

2 RESPONSABILITES CONCERNANT LA MISE À DISPOSITION DES INFORMATIONS DEVANT ÊTRE PUBLIEES

2.1 ENTITES CHARGEES DE LA MISE À DISPOSITION DES INFORMATIONS

La fonction de publication de l'AC met à disposition l'information sur l'état des certificats par le biais de fichier « LCR » et d'un répondeur OCSP.

La LCR de l'AC est accessible par internet suivant le point d'accès :

- HTTP sur le serveur www.certinomis.fr

L'OCSP de l'AC est accessible par internet suivant le point d'accès :

- OCSP sur le serveur pki-ocsp.certinomis.com

Les liens exacts dont définis dans l'extension « Point de distribution de la liste de révocation des certificats» de chaque certificat émis par l'AC.

Les LCR sont aussi accessibles en téléchargement, directement sur le serveur WEB public : www.certinomis.fr dans la rubrique « Documents et liens / Nos listes de révocations ».

2.2 INFORMATIONS DEVANT ETRE PUBLIEES

La Politique de Certification, les certificats d'AC, les contrats et conditions générales en vertu desquels les certificats sont émis, sont soit disponibles sur le site WEB de l'AC à l'adresse suivante http://www.certinomis.fr, soit communiqués dans le cadre de la négociation commerciale.

Une copie peut également être obtenue par courrier électronique.

Les procédures, qui donnent, entre autres, le détail des moyens mis en œuvre pour assurer la protection des installations de l'AC, ne sont pas publiées pour des raisons de sécurité liées au besoin d'en connaître.

Toutefois, l'AC peut fournir, autant que de besoin, la liste complète des procédures, lors d'une demande d'un organisme autorisé (AGP, AC maître, autre AC pour certification croisée…) à des fins de vérification, d'audit ou de contrôle, prévues à cet effet dans la présente déclaration, ainsi que dans le cadre du respect de la loi.

Si la DPC contient des informations touchant la sécurité de l'AC ou des informations qu'elles considèrent confidentielles, la publication n'est pas effectuée. Il est possible d'obtenir sur demande expresse un résumé ou des extraits de la DPC sous forme électronique.

De plus, compte tenu de la complexité de lecture d'une PC pour des porteurs ou des utilisateurs de certificats non spécialistes du domaine, l'AC publie également des conditions générales d'utilisation sur son site web http://www.certinomis.fr dans la rubrique : « Documents et liens / Nos conditions générales d'utilisation ».

La Liste des Certificats Révoqués est fournie par l'AC qui en assure la publication sur son site public, dans la limite des éléments autorisés par ses clients et bénéficiaires.

2.3 DELAIS ET FREQUENCES DE PUBLICATION

Les délais et les fréquences de publication dépendent des informations concernées : Pour les informations liées à l'IGC (nouvelle version de la PC, formulaires, etc.), l'information est publiée dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs de l'AC.

Pour les certificats d'AC, ils sont diffusés préalablement à toute émission de certificats et/ou de LCR correspondants sous délai de 24 heures.

Pour les informations d'état des certificats, les Listes de Certificats Révoqués sont mises à jour dans des délais maximum de 24 heures. Une fois la mise à jour effectuée, la LCR est publiée dans un délai maximum de 30 minutes.

Le site web de publication et le serveur OCSP sont disponible 24/24 ; 7/7.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

2.4 CONTROLE D'ACCES AUX INFORMATIONS PUBLIEES

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture.
L'accès en modification aux systèmes de publication des informations d'état des certificats (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC, au travers d'un contrôle d'accès fort.
L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées de l'IGC, au moins au travers d'un contrôle d'accès de type mots de passe basé sur une politique de gestion des mots de passe.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

3 IDENTIFICATION ET AUTHENTIFICATION

Le présent chapitre définit les exigences en matière d'enregistrement des demandes de certificats, c'est-à-dire, des Clients, des Bénéficiaires et des entités identifiées. Il définit également les exigences de vérification en matière de pouvoir, représentation et mandat.

3.1 NOMMAGE

3.1.1 Types de noms

Les noms utilisés sont conformes aux spécifications de la norme [X.500].

Dans chaque certificat conforme à la norme [X.509] l'AC émettrice (issuer) et le sujet (subject) sont identifiés par un "Distinguished Name" (DN) de type [X.501].

Le chapitre 7 « Profils des certificats, OCSP et des LCR» fournit des règles à ce sujet.

3.1.2 Nécessité d'utilisation de noms explicites

Le contenu des champs de nom Subject et Issuer doit avoir un lien explicite avec l'entité authentifiée.

Le nom distinctif doit contenir soit une combinaison du prénom, du nom de famille et facultativement d'initiales. Dans le cas d'un autre type d'entité identifiée, le nom distinctif doit refléter son nom légal authentifié.

Particulier
Noms explicites
Un nom distinctif doit contenir de manière obligatoire les champs suivants : • le champ CountryName (C) ; • le champ Common Name (CN) : • le champ SerialNumber.

Professionnel
Noms explicites
Un nom distinctif doit contenir de manière obligatoire les champs suivants : • le champ CountryName (C) ; • le champ Organisation (O) ; • le champ Organisational Unit (OU). • le champ Common Name (CN) ; • le champ SerialNumber.

L'AC définit sa politique de nommage et, à ce titre, elle se réserve le droit de prendre toutes décisions concernant les noms des personnes. Une partie demandant un certificat doit être en mesure de prouver qu'elle a le droit d'utiliser un nom en particulier.

Une partie qui demande un certificat doit avoir le droit d'utiliser le nom qu'elle souhaite y voir figurer.

En cas de différend au sujet d'un nom dans un dépôt de documents dont elle n'a pas le contrôle, l'AC doit s'assurer qu'il existe, dans le contrat associé à ce dépôt, une procédure de règlement des différends au sujet des noms.

3.1.3 Anonymisation ou pseudonymisation des identités

Les certificats objets de la présente PC ne peuvent en aucun cas être anonymes. L'identifiant de l'entité dans son certificat ne peut être un pseudonyme.

3.1.4 Règles d'interprétation des différentes formes de nom

La DPC fournit les règles à ce sujet.

3.1.5 Unicité des noms

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Les noms distinctifs sont uniques pour toutes les entités identifiées d'une AC. Ainsi le DN contient un champ spécifique (serialNumber) composé d'un grand entier afin de garantir le caractère unique du nom distinctif.
La DPC fournit les règles à ce sujet.

3.1.6 Identification, authentification et rôle des marques déposées

Le droit d'utiliser un nom qui est une marque de fabrique, de commerce ou de services ou un autre signe distinctif (nom commercial, enseigne, dénomination sociale) au sens des articles L. 711-1 et suivants du Code de la Propriété intellectuelle (codifié par la loi n°92-957 du 1er juillet 1992 et ses modifications ultérieures) appartient au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires.

L'AC ne pourra voir sa responsabilité engagée en cas d'utilisation illicite par les clients et bénéficiaires des marques déposées, des marques notoires et des signes distinctifs, ainsi que les noms de domaine.

3.2 VALIDATION INITIALE DE L'IDENTITE

3.2.1 Méthode pour prouver la possession de la clé privée

La demande de certificat est transmise par l'AE sous la forme d'une demande de signature de certificat (CSR) au format PKCS#10 signée par la clé de signature pour fournir une preuve de possession de celle-ci.

3.2.2 Validation de l'identité d'un organisme

L'enregistrement du futur porteur (personne physique) représentant une entité nécessite l'identification de cette entité et, l'identification de la personne physique et la preuve du rattachement de la personne physique à l'entité.

La DPC précise les documents à fournir et les procédures d'enregistrement mises en œuvre par l'AE, en concertation avec l'AC.

3.2.3 Validation de l'identité du bénéficiaire

Le certificat doit toujours contenir le nom de la personne identifiée et, éventuellement, toutes les informations complémentaires permettant d'identifier son titulaire sans ambiguïté.

La DPC précise les documents à fournir et les procédures d'enregistrement mises en œuvre par l'AE, en concertation avec l'AC.

3.2.4 Informations non vérifiées

Les certificats émis sous la présente PC ne comportent aucune information non vérifiée.

3.2.5 Validation de l'autorité du demandeur

Toute personne est susceptible de demander un certificat pour sa propre identité. La demande provient donc nécessairement du bénéficiaire.

3.2.6 Critères d'interopérabilité

Il n'est prévu aucune interopérabilité avec d'autres AC.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

3.3 IDENTIFICATION ET VALIDATION D'UNE DEMANDE DE RENOUVELLEMENT DES CLES

Pour les certificats des bénéficiaires, la durée de vie des clés étant éphémère, il n'y a pas de possibilité de faire une demande de renouvellement des clés.

Pour les certificats d'une composante de l'IGC, le traitement de la demande de renouvellement est identique à celle de la demande initiale.

Ainsi chaque demande de certificat est une demande initiale (cf. chapitre 3.2).

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 REVOCATION

La demande de révocation peut être effectuée sur le site web de l'AE par le bénéficiaire. Pour que la demande soit autorisée, l'utilisateur doit être identifié grâce aux éléments identification connus de l'AE.

Une demande de révocation peut également être faite par courrier adressé à l'AE. Elle doit alors être signée par le demandeur et le service de gestion des révocations s'assure de l'identité du demandeur (vérification de la signature manuscrite par rapport à une signature préalablement enregistrée) et de son autorité par rapport au certificat à révoquer.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

Le présent chapitre définit les pratiques opérationnelles relatives à la gestion des clés et des certificats.

4.1 DEMANDE DE CERTIFICAT

4.1.1 Origine d'une demande de certificat

Particulier
Origine d'une demande
Un certificat ne peut être demandé que par le futur bénéficiaire ou par le représentant d'un incapable majeur ou d'un mineur.

Professionnel
Noms explicites
Un certificat peut être demandé par un représentant légal de l'entité ou par une personne dûment mandatée pour cette entité, avec dans tous les cas consentement préalable du futur porteur.

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

La demande d'identification électronique envoyée à l'AE doit au moins contenir le nom, le prénom du demandeur.

Chaque demande doit être associée à des pièces, elles aussi transmises à l'AE, qui permettent de prouver l'identité des futurs bénéficiaires conformément aux procédures applicables (articles 3.2.2, 3.2.3 et 3.3).

La vérification des pièces justificatives peuvent être réalisée par un processus automatisé. Les éléments recevables sont décrits au paragraphe 4.2.1.

4.2 TRAITEMENT D'UNE DEMANDE DE CERTIFICAT

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

Une demande de certificat n'oblige en aucune façon l'AC à émettre un certificat numérique.

L'émission d'un certificat par une AC indique que celle-ci a définitivement et complètement approuvé la demande de certificat selon les procédures décrites dans la DPC.

L'AE conserve ensuite une trace des justificatifs d'identité présentés.

Le processus de vérification de l'identité du futur porteur de certificat se base sur les éléments suivants :

Niveau LCP
Processus de validation
L'AE vérifie que : • De manière automatisée les informations contenues sur la copie de la carte d'identité correspondent bien au contrôle de la piste MRZ

Niveau NCP Particulier
Processus de validation
L'AE vérifie que : • la personne physique est en possession d'un élément d'identification reconnu par l'AE, et • que l'élément d'identification est connue d'une source faisant autorité et il se rapporte à une personne réelle, et • que la personne physique s'est présenté en personne et • que des mesures ont été prises pour minimiser le risque que l'identité de lapersonne physique ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration de l'élément d'identification.

Niveau NCP Professionnel
Processus de validation
L'AE vérifie que : • le porteur personne physique est en possession d'un élément d'identification le concernant reconnu par l'AE, et • que l'élément d'identification est connue d'une source faisant autorité et il se rapporte à une personne réelle, et • que le porteur personne physique s'est présenté en personne et • que des mesures ont été prises pour minimiser le risque que l'identité de lapersonne physique ne soit pas l'identité alléguée, en tenant compte par exemple du risque de perte, de vol, de suspension, de révocation ou d'expiration de l'élément d'identification. ET • le porteur personne physique est en possession d'un élément d'identification de la personne morale au nom de laquelle il agit qui est reconnu par l'AE, et • que l'élément d'identification est connue d'une source faisant autorité et il se rapporte à une personne morale réelle, et • que des mesures ont été prises pour minimiser le risque de falsification de cet élément d'identification ET • qu'un représentant habilité de la personne morale a autorisé la production du certificat

4.2.2 Acceptation ou rejet de la demande

À la réception d'une demande de certificat, l'AC s'assure que :

- s'assure que la demande a bien été prise en compte par une AE qu'elle reconnait comme légitime,
- que ladite AE a traité la demande et fourni une trace imputable de son avis ;

Si les critères sont remplis, l'AC génère et signe le certificat.

En cas de rejet de la demande, l'AE en informe le bénéficiaire, en justifiant le rejet.

4.2.3 Durée d'établissement du certificat

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

4.3 DELIVRANCE DU CERTIFICAT

4.3.1 Actions de l'AC concernant la délivrance du certificat

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, l'AC déclenche les processus de génération et de préparation des différents éléments destinés au bénéficiaire.

Les clés sont maintenues et gérées sous le contrôle du SSA.

- L'AE envoi un ordre de production de clés au SSA en lui indiquant les Données d'Activation,
- Le SSA génère les clés ou les fait générer par le Dispositif de Création de Signature,
- Le SSA produit, ou retire, la CSR puis la transmet à l'AE qui fait suivre à l'AC.
- Le sujet est créé dans le système d'AC, un numéro unique lui est attribué.
- L'AC génère le certificat, le retourne à l'AE qui le transmet au SSA, lequel l'insère dans le Dispositif de Création de Signature le cas échéant.

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

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

Le certificat et les clés sont protégés par le SSA selon les modalités précisées dans la DPC.

Les clés ne sont pas utilisables sans la communication des Données d'Activation selon les modalités précisées dans la DPC

4.4 ACCEPTATION DU CERTIFICAT

4.4.1 Démarche d'acceptation du certificat

Le certificat étant mis à la disposition du bénéficiaire, le fait que ce dernier procède à son utilisation vaut, de sa part, acceptation du certificat dans les conditions commerciales, juridiques et techniques définies par l'AC.

En acceptant un certificat, le bénéficiaire reconnaît expressément consentir aux termes et aux conditions d'utilisation contractuelles et, plus généralement, à tous les éléments publiés dans la présente Politique de certification de l'AC.

4.4.2 Publication du certificat

Les certificats émis ne font pas l'objet d'une publication par l'AC.

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

Sans objet.

4.5 USAGES DE LA BI-CLE ET DU CERTIFICAT

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

L'utilisation de la clé privée du bénéficiaire et du certificat associé est strictement limitée au service défini par l'OID de sa politique (cf. chapitre 1.4.1.1).

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

Cf. chapitre précédent et chapitre 1.4.

4.6 RENOUVELLEMENT D'UN CERTIFICAT

Nota : Conformément au [RFC3647], la notion de "renouvellement de certificat" correspond à la délivrance d'un nouveau certificat pour lequel seul les dates de validité sont modifiées, toutes les autres informations sont identiques au certificat précédent (y compris la clé publique).
La présente PC impose que les certificats et les bi-clés correspondantes aient la même durée de vie, il ne peut donc pas y avoir de renouvellement de certificat sans renouvellement de la bi-clé.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

4.6.1 Causes possibles de renouvellement d'un certificat

Sans objet.

4.6.2 Origine d'une demande de renouvellement

Sans objet.

4.6.3 Procédure de traitement d'une demande de renouvellement

Sans objet.

4.6.4 Notification au bénéficiaire de l'établissement du nouveau certificat

Sans objet.

4.6.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.6.6 Publication du nouveau certificat

Sans objet.

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

Sans objet.

4.7 DELIVRANCE D'UN NOUVEAU CERTIFICAT SUITE A CHANGEMENT DE LA BI- CLE

Nota : Conformément au [RFC3647], ce chapitre traite de la délivrance d'un nouveau certificat au bénéficiaire liée à la génération d'une nouvelle bi-clé.

4.7.1 Causes possibles de changement d'une bi-clé

Sans objet.

4.7.2 Origine d'une demande d'un nouveau certificat

Sans objet.

4.7.3 Procédure de traitement d'une demande d'un nouveau certificat

Sans objet.

4.7.4 Notification au bénéficiaire de l'établissement du nouveau certificat

Sans objet.

4.7.5 Démarche d'acceptation du nouveau certificat

Sans objet.

4.7.6 Publication du nouveau certificat

Sans objet.

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

Sans objet.

4.8 MODIFICATION DU CERTIFICAT

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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

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

4.8.1 Causes possibles de modification d'un certificat

Sans objet.

4.8.2 Origine d'une demande de modification d'un certificat

Sans objet.

4.8.3 Procédure de traitement d'une demande de modification d'un certificat

Sans objet.

4.8.4 Notification au bénéficiaire de l'établissement du certificat modifié

Sans objet.

4.8.5 Démarche d'acceptation du certificat modifié

Sans objet.

4.8.6 Publication du certificat modifié

Sans objet.

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

Sans objet.

4.9 REVOCATION ET SUSPENSION DES CERTIFICATS

4.9.1 Causes possibles d'une révocation

4.9.1.1 Certificats des bénéficiaires

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

- Le bénéficiaire a fait une demande de révocation auprès de l'AC :
- Le bénéficiaire n'a pas respecté les modalités applicables d'utilisation du certificat ;
- Le bénéficiaire et/ou l'entité n'ont pas respecté leurs obligations découlant de la PC de l'AC;
- Une erreur (intentionnelle ou non) a été détectée dans le dossier d'enregistrement du bénéficiaire ;
- La clé privée du bénéficiaire est suspectée de compromission, est compromise, est perdue ou est volée.

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a connaissance (elle en est informée ou elle obtient l'information au cours d'une de ses vérifications, lors de la délivrance d'un nouveau certificat notamment), le certificat concerné est révoqué.

4.9.1.2 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 (y compris un certificat d'AC pour la génération de certificats ou d'OCSP) :

- 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 DPC (par exemple, suite à un audit de qualification ou de conformité négatif) ;
- cessation d'activité de l'entité opérant la composante.

4.9.2 Origine d'une demande de révocation

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

4.9.2.1 Certificats des bénéficiaires

Seuls peuvent demander la révocation d'un certificat :

- le Bénéficiaire ;
- le Client
- le personnel de l'AC émettrice ;
- le personnel de l'AE.

Le bénéficiaire est informé des personnes / entités susceptibles d'effectuer une demande de révocation pour son certificat dans les conditions générales d'utilisation et sur le site web de Certinomis.

4.9.2.2 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 responsable de l'AC.

4.9.3 Procédure de traitement d'une demande de révocation

Les motifs de la révocation d'un certificat donné ne sont jamais divulgués à des tiers sauf en cas d'accord écrit du bénéficiaire ou du client.

Dans le cadre des audits et contrôles auxquels l'AC est soumise en vertu de la présente politique de certification, des éléments sur les motifs de révocation, non nominatifs et non liés à un certificat, pourront être fournis. D'une manière plus générale, ces éléments pourront être utilisés à des fins statistiques.

4.9.3.1 Révocation d'un certificat de bénéficiaire

Tant que le certificat est dans sa période de validité, le personnel de l'AE ou de l'AC procède à la révocation du certificat directement sur les interfaces de l'IGC.

Une fois la date de fin de validité atteinte, le certificat ne peut plus être révoqué, il est néanmoins expiré et donc n'est plus utilisable dans une transaction.

Quelle que soit la cause ayant entrainé la révocation d'un certificat, le bénéficiaire est toujours informé par une notification de la révocation de son certificat. Cette notification indique la date à laquelle la révocation du certificat a pris effet. Elle peut prendre la forme d'un courrier électronique.

4.9.3.2 Révocation d'un certificat d'une composante de l'IGC

En cas de révocation d'un des certificats de la chaîne de certification, l'AC informe dans les plus brefs délais et par tout moyen (et si possible par anticipation) l'ensemble des bénéficiaires concernés que leurs certificats ne sont plus valides. Pour cela, l'IGC pourra par exemple envoyer des récépissés aux AE. Ces derniers devront informer les bénéficiaires de certificats en leur indiquant explicitement que leurs certificats ne sont plus valides car un des certificats de la chaîne de certification n'est plus valide.

La révocation du certificat de l'AC, est facilitée par la signature d'une LAR par l'autorité de certificat racine.

Le point de contact identifié sur le site : http://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 bénéficiaire pour formuler la demande de révocation

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

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

4.9.5.1 Révocation d'un certificat de bénéficiaire

La demande de révocation d'un certificat de bénéficiaire sera traitée en moins de 24h.

4.9.5.2 Révocation d'un certificat d'une composante de l'IGC

La révocation d'un certificat d'une composante de l'IGC est effectuée dès la détection d'un évènement décrit dans les causes de révocation possibles pour ce type de certificat. La révocation du certificat est effective lorsque le numéro de série du certificat est introduit dans la liste de révocation de l'AC qui a émis le certificat.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

La révocation d'un certificat de signature de l'AC (signature de certificats, de LCR / LAR) doit être effectuée dans les plus brefs délais, particulièrement dans le cas de la compromission de la clé.

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

Avant toute utilisation de certificats, notamment lorsque les dits certificats créent des effets juridiques, le tiers utilisateur doit impérativement vérifier la validité des certificats auxquels il entend se fier auprès de Certinomis, en consultant le service OCSP ou la LCR ainsi qu'en contrôlant la validité intrinsèque du certificat, en particulier sa signature, et la validité du certificat de l'émetteur.

4.9.7 Fréquence d'établissement des LCR

Les LCR sont publiées quotidiennement et après chaque révocation d'un certificat.

4.9.8 Délai maximum de publication d'une LCR

Le moment où la LCR est générée et le délai où elle est accessible sur le site de publication est inférieur à 60 minutes.

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

Une publication suivant le protocole OCSP est disponible.

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

Cf. chapitre 4.9.6 ci-dessus.

4.9.11 Autres moyens disponibles d'information sur les révocations

Aucun autre moyen n'est disponible.

4.9.12 Exigences spécifiques en cas de compromission de la clé privée

En cas de compromission avérée ou soupçonnée de la clé privée de signature d'une AC, l'AC avise sans tarder toutes les AGP qui l'accréditent.

La connaissance de la compromission avérée ou soupçonnée de la clé privée, par le client ou le bénéficiaire emporte obligation de procéder sans délais à la vérification de la révocation du certificat associé et de la demander dans les plus brefs délais si celle-ci n'a pas été faite.

La procédure de révocation d'une AC est réalisée par une opération de cérémonie de clé, détaillée dans la DPC.

4.9.13 Causes possibles d'une suspension

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

4.9.14 Origine d'une demande de suspension

Sans objet.

4.9.15 Procédure de traitement d'une demande de suspension

Sans objet.

4.9.16 Limites de la période de suspension d'un certificat

Sans objet.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

4.10 FONCTION D'INFORMATION SUR L'ETAT 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 LAR et l'état du certificat de l'AC Racine.

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

4.10.2 Disponibilité de la fonction

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

4.10.3 Dispositifs optionnels

Aucun dispositif optionnel n'est disponible.

4.11 FIN DE LA RELATION ENTRE LE BENEFICIAIRE ET L'AC

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

4.12 SEQUESTRE DE CLE ET RECOUVREMENT

Les clés privées d'AC ne sont pas séquestrées.

Les clés privées des certificats émis ne sont pas séquestrées.

4.12.1 Politique et pratiques de recouvrement par séquestre des clés

Sans objet.

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

Sans objet.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

5 MESURES DE SECURITE NON TECHNIQUES

5.1 MESURES DE SECURITE PHYSIQUE

Les locaux techniques, qui accueillent les moyens de certification et notamment sa clé privée de signature, sont fortement protégés. Ils sont dans une zone à accès contrôlé, protégée contre tous les risques courants (incendie, inondation…).

Le niveau de protection des locaux techniques est essentiel dans la garantie de la sécurité des moyens de certification et de l'exploitation de ces moyens.

La DPC précise les conditions de sécurité physique et les règles appliquées aux – ainsi que dans les locaux, en particulier sur les sujets suivants :

- Emplacement, construction et accès physique
- Système électrique et système de conditionnement d'air
- Dégâts causés par l'eau
- Prévention et protection-incendie
- Entreposage des supports
- Mise au rebut du matériel, destruction
- Sauvegarde à l'extérieur des locaux

5.1.1 Situation géographique et construction des sites

La présente PC ne formule pas d'exigence spécifique concernant la localisation géographique.

La construction des sites respecte les règlements et normes en vigueur et le cas échéant, des exigences spécifiques face à des risques de type tremblement de terre ou explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques,…).

5.1.2 Accès physique

Afin d'éviter toute perte, dommage et compromission des ressources de l'IGC et l'interruption des services de l'AC, les accès aux locaux des différentes composantes de l'IGC sont contrôlés.

L'accès est strictement limité aux seules personnes autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logiques.

Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines.

Nota -On entend par machines l'ensemble des serveurs, boîtiers cryptographiques, stations et éléments actifs du réseau utilisés pour la mise en œuvre de ces fonctions.

5.1.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements de l'IGC telles que fixées par leurs fournisseurs.

Elles permettent également de respecter les exigences en matière de disponibilité des fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.4 Vulnérabilité aux dégâts des eaux

Les moyens de protection contre les dégâts des eaux permettent de respecter les exigences de la présente PC en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences de la présente PC en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

5.1.6 Conservation des supports

Dans le cadre de l'analyse de risque, les différentes informations intervenant dans les activités de l'IGC ont été identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité).

Les supports (papier, disque dur, disquette, CD, etc.) correspondant à ces informations sont traités et conservés conformément à ces besoins de sécurité.

La procédure de conservation des supports est détaillée dans la DPC.

5.1.7 Mise hors service des supports

En fin de vie, les supports devront être soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes.

Les procédures et moyens de destruction et de réinitialisation sont conformes aux différents niveaux de confidentialité.

La procédure de mise hors service des supports est détaillée dans la DPC.

5.1.8 Sauvegardes hors site

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

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

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

La procédure de sauvegardes hors site est détaillée dans la DPC.

5.2 MESURES DE SECURITE PROCEDURALES

5.2.1 Rôles de confiance

Chaque composante de l'IGC distingue au moins les cinq rôles fonctionnels de confiance suivants :

Responsable de sécurité - Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et est chargé de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.

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.

Ingénieur système - Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante.

Opérateur - Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation des applications pour les fonctions mises en œuvre par la composante. Il assure notamment les actions liées au traitement des demandes de révocation

Auditeur Système - Personne désignée par une autorité compétente et dont le rôle est de consulter les archives et d'analyser les traces de l'IGC.

En plus de ces rôles de confiance au sein de chaque composante de l'IGC, l'AC distingue également en tant que rôle de confiance, les rôles de porteur de parts de secrets d'IGC : cf. chapitres 6.1 et 6.2.

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

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Les différents rôles de confiance sont détaillés dans la DPC.

5.2.2 Nombre de personnes requises par tâches

Selon le type d'opération effectuée, le nombre et la qualité des personnes devant nécessairement être présentes, en tant qu'acteurs ou témoins, peuvent être différents.

Pour des raisons de sécurité, les fonctions sensibles sont réparties sur plusieurs personnes. La présente PC définit un certain nombre d'exigences concernant cette répartition, notamment pour les opérations liées aux modules cryptographiques de l'IGC (cf. chapitre 6)

La DPC précise les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter.

5.2.3 Identification et authentification pour chaque rôle

Tous les membres du personnel de l'AC doivent faire vérifier leur identité et leurs autorisations avant :

- que leur nom soit ajouté à la liste d'accès aux locaux de l'AC ; ou
- que leur nom soit ajouté à la liste des personnes autorisées à accéder physiquement au système de l'AC.

Tous les intervenants sur le système de l'AC, ou d'une autre composante de l'IGC, doivent faire vérifier leur identité et leur autorisation avant :

- qu'un certificat leur soit délivré pour accomplir le rôle qui leur est dévolu ; ou
- qu'un compte soit ouvert en leur nom dans le système.

Chacun de ces certificats et comptes (à l'exception des certificats de signatures de l'AC) :

- est attribué directement à une personne ;
- ne doit pas être partagé ;
- doit être utilisé seulement pour les tâches autorisées pour le rôle assigné ; un mécanisme de contrôle est mis en place.

Les opérateurs distants intervenant sur le système de l'AC doivent être identifiés au moyen de mécanismes cryptographiques forts.

L'AC et les composantes de l'IGC s'assurent que tout processus de vérification qu'elles utilisent permet de superviser toutes les activités des personnes qui en leur sein détiennent des rôles privilégiés.

Les différents rôles de confiance sont détaillés dans la DPC.

5.2.4 Rôles exigeant une séparation des attributions

Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur
- contrôleur et tout autre rôle
- ingénieur système et opérateur

Les attributions associées à chaque rôle sont décrites dans la DPC.

5.3 MESURES DE SECURITE VIS-A-VIS DU PERSONNEL

5.3.1 Qualifications, compétences et habilitations requises

Le responsable de l'AC s'assure que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation d'une AC, qu'ils dépendent de l'AC directement, de l'AE :

- sont nommés à un poste faisant l'objet d'une description détaillée par écrit ;
- sont liés par contrat ou par la loi aux postes qu'ils occupent ;
- ont reçu toute la formation nécessaire pour accomplir leurs tâches ;

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

- sont tenus par contrat ou par la loi de ne pas divulguer de renseignements ayant trait à la sécurité de l'AC, aux clients ou aux bénéficiaires ; une clause de confidentialité est expressément inscrite dans les contrats de travail des membres du personnel de l'AC ;

Les mesures de sécurité vis-à-vis du personnel sont détaillées dans la DPC.

5.3.2 Procédures de vérification des antécédents

L'AC s'assure de l'honnêteté des personnels amenés à travailler au sein des composantes de l'IGC, les personnels ne doivent pas avoir de condamnation de justice en contradiction avec leurs attributions.

L'AC s'assure que les personnes ayant un rôle de confiance ne souffrent pas de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement.

La procédure de vérification est détaillée dans la DPC.

5.3.3 Exigences en matière de formation initiale

L'AC s'assure que tous les membres du personnel qui accomplissent des tâches touchant à l'exploitation d'une AC ou d'une AE ont reçu une formation complète concernant :

5.3.4 Les principes de fonctionnement et les mécanismes de sécurité de l'AC ou de l'AE.

Le personnel de l'AC suit un programme de formation pour accomplir correctement ses fonctions. Il porte :

- sur les différentes applications et versions d'applications auxquelles il pourrait avoir accès dans le cadre de ses fonctions au sein du système de l'AC ;
- sur toutes les tâches qu'il devra accomplir dans le cadre de l'IGC ;
- sur le matériel et les systèmes d'exploitation formant l'environnement opérationnel de l'AC ;
- sur le plan de secours de l'AC après un sinistre et les procédures de maintien des activités.

Avant l'entrée en fonction, il sera procédé à une familiarisation aux règles de sécurité en vigueur. Les exigences en matière de formation sont détaillées dans la DPC.

5.3.5 Exigences et fréquence en matière de formation continue

Les exigences décrites à la section 5.3.3 sont tenues à jour afin de refléter les changements apportés au système de l'AC.

Des cours de formation professionnelle sont offerts en fonction des besoins, et l'AC revoit ses exigences au moins une fois par an.
Le personnel de l'AC participe régulièrement à des séances de formation sur la sécurité. Les exigences en matière de formation sont détaillées dans la DPC.

5.3.6 Fréquence et séquence de rotation entre différentes attributions

Aucune exigence particulière.

5.3.7 Sanctions en cas d'actions non autorisées

Si une personne a réellement fait ou est soupçonnée d'avoir fait une action non autorisée dans l'accomplissement de ses tâches en rapport avec l'exploitation d'une AC ou d'une AE, l'AC peut lui interdire l'accès au système.
En outre, si les faits sont avérés, elle peut prendre toutes sanctions disciplinaires adéquates. Les sanctions prévues sont détaillées dans la DPC.

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

L'AC s'assure que les personnels des entreprises cocontractantes peuvent accéder à ses locaux conformément aux indications de l'article 5.1.1.

Les exigences relatives au personnel des entreprises cocontractantes sont identiques à celles relatives aux employés, en particulier à celles décrites aux articles 5.3, 5.3.2 et 5.3.6.

Les exigences vis-à-vis du personnel des prestataires externes sont détaillées dans la DPC.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

5.3.9 Documentation fournie au personnel

L'AC met à la disposition des membres du personnel de l'AC et de l'AE les Politiques de Certification qu'elle accepte, ainsi que toute loi, toute politique ou tout contrat qui s'appliquent aux postes qu'ils occupent.

Tout le personnel de l'AC à accès à des manuels complémentaires relatifs à leurs responsabilités. Ces manuels portent sur l'ensemble des procédures en vigueur.

La documentation fournie au personnel est détaillée dans la DPC.

5.4 PROCEDURES DE CONSTITUTION DES DONNEES D'AUDIT

La journalisation d'évènements consiste à les enregistrer sous forme manuelle ou sous forme électronique par saisie ou par génération automatique.

Les fichiers résultants, sous forme papier ou électronique, rendent possible la traçabilité et l'imputabilité des opérations effectuées.

5.4.1 Type d'évènements à enregistrer

L'AC consigne dans les registres de vérification tous les événements ayant trait à la sécurité de son système, notamment :

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de 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.

Tous les registres et journaux, qu'ils soient électroniques ou papiers, contiennent la date et l'heure de l'événement, prise auprès d'une source de temps suffisamment fiable, et indiquer l'entité en cause.

L'AC recueille et collige, par des moyens électroniques ou papiers, de l'information sur la sécurité qui n'est pas produite par le système de l'AC, notamment :

- journaux des accès physiques ;
- maintenance et changements de la configuration du système ; changements apportés au personnel ;
- registres sur la destruction des supports contenant des clés, des données d'activation ou des renseignements personnels sur les bénéficiaires.

Le type d'événements à enregistrer est détaillé dans la DPC.

5.4.2 Fréquence de traitement des journaux d'évènements

L'AC s'assure que ses journaux sont revus périodiquement sur la base d'un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé fait apparaître les anomalies et les falsifications constatées.

La fréquence de traitement des journaux d'événements est détaillée dans la DPC.

5.4.3 Période de conservation des journaux d'évènements

L'AC conserve (en les rendant accessibles dès première demande) les journaux pendant au moins un mois et ensuite les archivent conformément aux instructions indiquées à l'article 5.5.

La période de conservation des journaux d'événements est détaillée dans la DPC.

5.4.4 Protection des journaux d'évènements

Le système des journaux électroniques touchant directement les opérations de certification comprennent des mécanismes de protection contre les tentatives non autorisées de modification et de suppression des journaux.

L'information de vérification obtenue par des moyens manuels est également protégée contre les tentatives non autorisées de modification et de destruction.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Le système de datation des évènements respecte les exigences du chapitre 6.8. La protection des journaux d'événements est détaillée dans la DPC.

5.4.5 Procédure de sauvegarde des journaux d'évènements

Les journaux et leur résumé sont sauvegardés, ou copiés (photocopie ou numérisation) s'ils sont sur support papier.

La procédure de sauvegarde des journaux d'événements est détaillée dans la DPC.

5.4.6 Système de collecte des journaux d'évènements

L'AC indique dans la DPC quels systèmes elle utilise pour recueillir les données de vérification.

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

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

5.4.8 Évaluation des vulnérabilités

Les événements qui surviennent dans le processus de vérification sont consignés, en partie, afin de contrôler les points vulnérables du système. L'AC s'assure qu'une évaluation de ces points vulnérables est effectuée, revue et révisée, après examen de ces événements.

L'évaluation des vulnérabilités est détaillée dans la DPC.

5.5 ARCHIVAGE DES DONNEES

5.5.1 Types de données à archiver

Des dispositions en matière d'archivage sont également prises par l'AC. Cet archivage permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'IGC.

Les données archivées sont les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les PC ;
- les DPC ;
- les conditions générales d'utilisation ;
- les accords contractuels avec d'autres AC ;
- les certificats et LCR tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les justificatifs d'identité des bénéficiaires et, le cas échéant, de leur entité de rattachement ;
- les journaux d'évènements des différentes entités de l'IGC. Les types de données à archiver sont précisés dans la DPC.

5.5.2 Période de conservation des archives

Les certificats de signature électronique, ainsi que les LCR produites par l'AC, sont conservés pendant au moins sept (7) ans après l'expiration des clés.

Seront conservées pendant sept (7) ans après l'expiration des clés les renseignements liés à la gestion du cycle de vie des certificats, en particulier tous les renseignements liés à l'enregistrement.
Outre les données papier susmentionnées sont aussi conservées, sous forme papier et/ou électronique, et ce pour une durée de sept (7) ans après leur expiration ou leur fin de validité :

- toutes les versions et révisions des DPC applicables par l'AC ou une composante de l'IGC
- tous les accords signés par Certinomis avec d'autres AC et composantes de l'IGC Les périodes de conservation des archives sont précisés dans la DPC.

5.5.3 Protection des archives

Une copie de tout le matériel informatique archivé ou sauvegardé est protégée soit par des mesures de sécurité physique seulement, soit par une combinaison de mesures physiques et cryptographiques. Le site d'archivage protège adéquatement le matériel contre les dangers naturels, par exemple les excès de température, d'humidité et de magnétisme.

De plus, les informations conservées ou sauvegardées par l'AC peuvent être assujetties aux lois et règlements en vigueur et applicables à l'archivage et la conservation.

La protection des archives est détaillée dans la DPC.

5.5.4 Procédure de sauvegarde des archives

Il n'est pas réalisé de sauvegarde des archives.

5.5.5 Exigences d'horodatage des données

Cf. chapitre 5.4.4 pour la datation des journaux d'évènements.
Le chapitre 6.8 précise les exigences en matière de datation / horodatage. Les exigences d'horodatage des données sont précisées dans la DPC.

5.5.6 Système de collecte des archives

Le système de collecte des archives, qu'il soit interne ou externe, respecte les exigences de protection des archives concernées.

Le système de collecte des archives est détaillé dans la DPC.

5.5.7 Procédures de récupération et de vérification des archives

L'AC vérifiera régulièrement la restauration de ses archives.

Les archives (papier et électroniques) sont récupérables dans un délai inférieur à 5 jours ouvrés, sachant que seule l'AC peut accéder à toutes les archives (par opposition à une entité opérant une composante de l'IGC qui ne peut récupérer et consulter que les archives de la composante considérée).

L'AC vérifiera la restauration de ses archives par échantillonnage au moins tous les douze (12) mois.

5.6 CHANGEMENT DE CLE D'AC

L'AC ne peut pas générer de certificat dont la date de fin serait postérieure à la date d'expiration du certificat correspondant de l'AC.

Pour cela la période de validité de ce certificat de l'AC est supérieure à celle des certificats qu'elle signe.

Le certificat de l'AC sera renouvelé dans la dernière année de sa date d'expiration.

Dès qu'une nouvelle bi-clé d'AC est générée et opérationnelle, seule cette nouvelle clé privée sera 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.
Le certificat ne peut être prorogé au-delà de sa date de validité. Donc, l'émission d'un nouveau certificat nécessitera un renouvellement des clés.

Ce processus est détaillé dans la DPC.

5.7 REPRISE SUITE A COMPROMISSION ET SINISTRE

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

Toutes les procédures à suivre lors de la compromission de la clé privée de l'AC, des composantes de l'IGC et du personnel de l'AC sont documentées.

De même, les mesures en cas de désastre ou autres catastrophes naturelles pour les données, les équipements et les logiciels de l'AC sont documentées.

Dans l'hypothèse d'un déclassement ou d'une réduction du niveau de reconnaissance d'une AC, son certificat sera révoqué. Un nouveau certificat sera émis, qui correspondra à ce déclassement.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Ce processus est détaillé dans la DPC.

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

La seule activité critique que l'AC maintienne en fonctionnement est la prise en compte et la publication des révocations de certificats.

L'AC établit des procédures visant à assurer le maintien des activités et décrit, dans ces procédures, les étapes prévues en cas de corruption ou de perte des ressources informatiques, logicielles ou de données nécessaires. Lorsque le dépôt de documents ne relève pas de l'AC, celle-ci s'assure que tous les contrats conclus avec le dépositaire prévoient la mise en place, par celui-ci, de procédures visant à la préservation des données.
L'AC prévoit un plan de secours et de redémarrage de ses activités (PCA/PRA). Ce processus est détaillé dans la DPC.

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

La connaissance de la compromission avérée ou soupçonnée de la clé privée par un membre d'une composante de l'IGC emporte obligation de procéder sans délais à la vérification de la révocation du certificat associé, et de la demander dans les plus brefs délais si celle-ci n'a pas été faite.

En cas de compromission de la clé de signature électronique d'une AC, et avant de redéfinir un certificat au sein de l'IGC, l'AC révoque sa clé publique.

S'il faut révoquer le certificat de signature électronique d'une AC, celle-ci avise dans les plus brefs délais :

- les AGP qui l'accréditent ;
- tous les bénéficiaires.

En outre, l'AC :

- publie le numéro de série du certificat dans la LCR appropriée ;
- révoque tous les certificats signés au moyen du certificat de signature électronique révoqué.

Après avoir corrigé les problèmes ayant motivé la révocation, l'AC peut :

- produire une nouvelle bi-clé de signature et publier les certificats associés ; et
- émettre de nouveaux certificats à toutes les entités.

S'il est nécessaire de révoquer le certificat de signature électronique de toute autre entité, l'AC suivra les directives de l'article 4.9.

5.7.4 Capacités de continuité d'activité suite à un sinistre

L'AC définit dans un plan anti-sinistre les mesures à prendre pour rétablir une installation sécuritaire en cas de catastrophe naturelle ou de tout autre type de sinistre. L'AC s'assure qu'il est précisé, dans tous contrats qui auraient été conclus avec des partenaires, qu'un plan anti-sinistre doit être mis en place et documenté par le dépositaire.

Ce processus est détaillé dans la DPC.

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 pour des raisons diverses.

L'AC prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où l'AC serait en faillite ou pour d'autres raisons serait incapable de couvrir ces coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite.

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

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

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

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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

- Met en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des bénéficiaires et des informations relatives aux certificats) ;
- Assure la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ses fonctions définies dans la PC.
- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis à vis des bénéficiaires ou des utilisateurs de certificats, l'AC les en avise aussitôt que nécessaire sous un délai d'un mois ;
- L'AC communique au point de contact identifié sur le site http://www.ssi.gouv.fr, les principes du plan d'action mettant en œuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle y présentera notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PC. L'AC communiquera à l'ANSSI, selon les différentes composantes de l'IGC concernées, les modalités des changements survenus. L'AC mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les bénéficiaires et les utilisateurs de certificats ;
- L'AC tient informée l'ANSSI de tout obstacle ou délai supplémentaire rencontrés dans le déroulement du processus.

5.8.2 Cessation d'activité affectant l'AC

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

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

L'AC procède aux actions suivantes :

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

Lors de l'arrêt du service, l'AC :

- S'interdit de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- Prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- Révoque son certificat ;
- Révoque tous les certificats qu'elle a signés et qui seraient encore en cours de validité ;
- Informe (par exemple par récépissé) tous les bénéficiaires des certificats révoqués ou à révoquer, ainsi que leur entité de rattachement le cas échéant.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

6 MESURES DE SECURITE TECHNIQUES

Le présent chapitre a pour objet de définir les dispositions de gestion des bi-clés de l'AC, du personnel de l'AC et des bénéficiaires.

6.1 GENERATION ET INSTALLATION DE BI CLES

6.1.1 Génération des bi-clés

Le principe de séparation des clés est appliqué à toutes les clés utilisées dans le cadre du système technique de l'AC. La séparation des clés indique qu'une bi-clé ne peut être utilisée que pour une fonction cryptographique donnée, à savoir :

- une bi-clé dédiée à la création et à la vérification de signature ;
- une bi-clé dédiée à la confidentialité.

L'AC produit son propre bi-clé de signature électronique au moyen d'un algorithme de cryptographie et selon une procédure impliquant plusieurs rôles.

6.1.1.1 Clés d'AC

La génération des clés de signature d'AC est effectuée dans un environnement sécurisé (cf. chapitre 5).

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique.

La génération des clés de signature d'AC est effectuée dans des circonstances parfaitement contrôlées, par des personnels dans des rôles de confiance (cf. Chapitre 5.2.1), dans le cadre de "cérémonies de clés". Ces cérémonies se déroulent suivant des scripts préalablement définis.

L'initialisation de l'IGC et/ou la génération des clés de signature d'AC s'accompagne de la génération de parts de secrets d'IGC. Ces parts de secrets sont des données permettant de gérer et de manipuler, ultérieurement à la cérémonie de clés, les clés privées de signature d'AC, notamment, de pouvoir initialiser ultérieurement de nouveaux modules cryptographiques avec les clés de signatures d'AC.

Ces parts de secrets sont générées suivant un schéma à seuil de Shamir (n parties parmi m sont nécessaires et suffisantes pour reconstituer le secret), Ce secret permet de déclencher le chargement sécurisé, dans un nouveau module cryptographique, de la (ou des) clé(s) privée(s) d'AC sauvegardée(s) lors de la cérémonie de clés.

Suite à leur génération, les parts de secrets sont remis à des porteurs de parts de secrets désignés au préalable et habilités à ce rôle de confiance par l'AC. Quelle qu'en soit la forme (papier, support magnétique ou confiné dans une carte à puce ou une clé USB), un même porteur ne peut détenir plus d'une part de secrets d'une même AC à un moment donné. Chaque part de secrets est mise en œuvre par son porteur.

Les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes ayant des rôles de confiance et en présence de plusieurs témoins dont au moins un est externe à l'AC et est impartial.

Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini.

Les modalités sont détaillées dans la DPC.

6.1.1.2 Clés des bénéficiaires générées sous le contrôle de l'AC

La génération des clés des bénéficiaires est effectuée dans un environnement sécurisé (cf. chapitre 5) suivant les prescriptions de l'AC

Niveau LCP
Génération des clés
Les clés de signature des Bénéficiaires sont générées par le SSA, préférentiellement au sein d'un module cryptographique

Niveau NCP
Génération des clés
Les clés de signature des Bénéficiaires sont générées au sein du module cryptographique du DCS.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

6.1.1.3 Clés des bénéficiaires générées par le bénéficiaire

Les bénéficiaires ne peuvent pas générer leur clé.

6.1.2 Transmission de la clé privée au bénéficiaire

Sans objet. La clé privée est conservée par le SSA ou le DCS le temps de la transaction de signature.

6.1.3 Transmission de la clé publique à l'AC

Sans objet.

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

La clé publique de vérification de l'AC est diffusée sous la forme d'un certificat numérique qui est téléchargeable sur le site web de l'AC.

6.1.5 Tailles des clés

Les bi-clés d'une AC dont la durée de validité est supérieure ou égale à 10 ans sont d'une complexité au moins équivalente à 4096 bits pour l'algorithme RSA.

Les bi-clés AC d'une complexité inférieure à 4096 bits pour l'algorithme RSA, ne sont pas supportées par cette PC.

Les bi-clés des certificats émis sont d'une complexité au moins équivalente à 2048 bits pour l'algorithme RSA et P-256 pour l'algorithme ECDSA-GF(P).

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

Le moyen de génération des bi-clés (AC ou certificats émis) doit utiliser des paramètres respectant les normes internationales de sécurité propres à l'algorithme considéré.

Les choix suivants seront retenus par Certinomis :

- l'exposant public sera 65537 ;
- le choix des premiers p et q peut être aléatoire ou fort, sous réserve d'appliquer les recommandations applicables du document cité en référence.

6.1.7 Objectifs d'usage de la clé

Les différents usages possibles des clés publiques sont définis et ainsi contraints par l'utilisation d'une extension de certificat X.509 v.3 (champ KeyUsage).

La clé publique de vérification de l'AC est la seule clé utilisable pour vérifier la signature des certificats.

L'utilisation d'une clé privée d'AC et du certificat émis associé est strictement limitée à la signature de certificats (cf. chapitre 1.4.1.2).

L'utilisation de la clé privée des bénéficiaires et du certificat émis associé est strictement limitée au service définis dans les chapitres 1.4.1.1, 4.5.

6.2 MESURES DE SECURITE POUR LA PROTECTION DES CLES PRIVEES ET POUR LES MODULES CRYPTOGRAPHIQUES

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Modules cryptographiques de l'AC

Les modules cryptographiques, utilisés par l'AC, pour la génération et la mise en œuvre de ses clés de signature, ainsi que le cas échéant pour la génération des clés des futurs certificats, sont des modules cryptographiques.

Le module cryptographique matériel utilisé pour la génération et la mise en œuvre des clés des Autorités est évalué selon les Critères Communs au niveau EAL 4+.

Le type de module cryptographique de l'AC est détaillé dans la DPC.

6.2.1.2 Dispositifs cryptographique des bénéficiaires

Niveau NCP
Module Cryptographique
Les modules cryptographiques, utilisés pour la génération et la mise en œuvre des clés de signature des bénéficiaires, sont des modules cryptographiques : • Bull Crypt2protect, FIPS 140-2 level 3, CSPN. • Bull Proteccio, CC EAL 4+, Qr • Thales nShield, FIPS 140-2 level 3 ou CC EAL 4+.

6.2.2 Contrôle de la clé privée par plusieurs personnes

Ce chapitre porte sur le contrôle de la clé privée de l'AC pour l'exportation / l'importation hors / dans un module cryptographique. La génération de la bi-clé est traitée au chapitre 6.1.1.1, l'activation de la clé privée au chapitre 6.2.8 et sa destruction au chapitre 6.2.10.

Plusieurs personnes contrôlent les opérations de production des clés de l'AC. Les données utilisées pour leur création sont partagées par plusieurs personnes. Le partage du secret permettant la génération ou la régénération de la clé de l'AC est fait entre trois (3) personnes.

Les modalités sont détaillées dans la DPC.

6.2.3 Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des certificats émis ne sont en aucun cas séquestrées.

6.2.4 Copie de secours de la clé privée

Une entité identifiée peut sauvegarder ses propres clés de signature électronique ou de confidentialité sous sa seule, exclusive et entière responsabilité. Le cas échéant, les clés sauvegardées doivent être enregistrées sous forme chiffrée et être protégées logiquement ou physiquement contre tout accès illicite. Les mesures de protection prises sur la clé sauvegardée doivent être au moins du même niveau que celles prises pour la clé d'origine.

Les modalités sont détaillées dans la DPC.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC ne sont en aucun cas archivées.

Les clés privées des certificats émis ne sont en aucun cas archivées ni par l'AC ni par aucune des composantes de l'IGC.

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

6.2.6.1 Clés privées des Autorités

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

6.2.6.2 Clés privées des bénéficiaires

Les clés privées des bénéficiaires ne peuvent en aucun cas être transférées.

6.2.7 Stockage de la clé privée dans un module cryptographique

Les clés privées sont stockées dans un module cryptographique.

Cependant, dans le cas des copies de secours, le stockage peut être effectué en dehors du module cryptographique moyennant le respect des exigences du chapitre 6.2.4.

Quel que soit le moyen utilisé, l'AC/AE garantit que les clés privées ne sont pas compromises pendant leur stockage ou leur transport.

6.2.8 Méthode d'activation de la clé privée

6.2.8.1 Clés privées d'AC

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

L'activation des clés privées d'AC dans le module cryptographique est contrôlée via des données d'activation (cf. chapitre 6.4) et fait intervenir au moins deux personnes dans des rôles de confiance (par exemple, responsable sécurité et opérateur).

L'activation est précisée au niveau de la DPC.

6.2.8.2 Clés privées des bénéficiaires

L'activation de la clé privée du bénéficiaire est liée à l'utilisation des Données d'Activation reçu par le bénéficiaire pour permettre la génération de son bi-clé.

6.2.9 Méthode de désactivation de la clé privée

6.2.9.1 Clés privées d'AC

La désactivation des clés privées d'AC dans un module cryptographique est automatique dès que l'environnement du module évolue : arrêt ou déconnexion du module, déconnexion de l'opérateur, etc.

Une clé privée d'AC peut également être désactivée après une certaine période d'inactivité. Ces conditions de désactivation permettent de répondre aux exigences définies dans le chapitre 11 pour le niveau de sécurité considéré.

La désactivation est précisée au niveau de la DPC.

6.2.9.2 Clés privées des bénéficiaires

Les clés privées des bénéficiaires sont désactivées après leur première utilisation.

6.2.10 Méthode de destruction des clés privées

6.2.10.1 Clés privées d'AC

Lorsque l'AC procède à la destruction de sa clé privée, elle réinitialise le module cryptographique, ce qui implique la réécriture complète de toute forme de mémoire dans le module cryptographique. Elle détruit aussi tous les secrets de génération qui ont été partagés.

Pour détruire une clé privée, il faut écraser toutes les copies des clés privées quel qu'en soit le support. Les procédures de destruction des clés privées sont décrites dans la DPC.

En cas ou la réinitialisation n'est pas possible suite à une panne du matériel, celui-ci est détruit. Cette destruction est tracée par un PV de destruction.

Les modalités sont détaillées dans la DPC.

6.2.10.2 Clés privées des bénéficiaires

Les clés privées des bénéficiaires sont effacées après expiration du certificat associé.

6.2.11 Niveau d'évaluation sécurité du module cryptographique

La ressource cryptographique matérielle de l'AC est évaluée au niveau EAL 4+, selon les Critères Communs.

Les dispositifs cryptographiques des bénéficiaires sont évalués au niveau correspondant à l'usage visé, tel que précisé au chapitre 12 ci-dessous. Se reporter au chapitre 6.2.1.2.

6.3 AUTRES ASPECTS DE LA GESTION DES BI-CLES

6.3.1 Archivage des clés publiques

L'AC émettrice archive ou fait archiver toutes les clés publiques de vérification conformément à l'article 5.5.

6.3.2 Durées de vie des bi-clés et des certificats

L'utilisation d'une longueur particulière de clé est déterminée conformément à l'évaluation de la menace et des risques prenant en compte l'évolution des technologies d'attaque.

Général
Durée de vie des certificats

L'utilisation des clés AC (4096 bits) pour l'émission de certificat est limitée à dix (10) ans. La durée de vie maximale d'un certificat de signature émis par l'AC pour un Bénéficiaire est de vingt (20) minutes.

La durée de vie des clés est définie dans la DPC.

6.4 DONNEES D'ACTIVATION

6.4.1 Génération et installation des données d'activation

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

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

Les modalités sont détaillées dans la DPC.

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

Les Données d'Activation sont générées par le SSA et transmis au bénéficiaire pour qu'il active son bi-clé lors d'une signature.

6.4.2 Protection des données d'activation

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

Les données d'activation qui sont générées par l'AC pour les modules cryptographiques de l'IGC sont protégées en intégrité et en confidentialité jusqu'à la remise à leur destinataire. Ce destinataire a ensuite la responsabilité d'en assurer la confidentialité, l'intégrité et la disponibilité.

Les modalités sont détaillées dans la DPC.

6.4.2.2 Protection des données d'activation correspondant aux clés privées des bénéficiaires

Les Données d'Activation sont transmises selon une méthode fixée dans la DPC et en utilisant un canal de communication déterminé au moment de la phase d'identification.

6.4.3 Autres aspects liés aux données d'activation

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

6.5 MESURES DE SECURITE DES SYSTEMES INFORMATIQUES

6.5.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

Les systèmes de l'IGC mis à disposition de l'AC offrent les fonctions suivantes, selon le rôle imparti à l'opérateur :

- contrôle de l'accès aux services de l'IGC ;
- distinction rigoureuse des tâches ;
- utilisation de la cryptographie pour assurer la sécurité des communications ;
- protection contre les virus informatiques, y compris les vers et chevaux de Troie ;
- fonctions d'audits, assurant l'imputabilité et la connaissance de la nature des actions réalisées ;
- archivage des historiques et des journaux de vérification de l'IGC ;
- vérification des événements relatifs à la sécurité ;
- gestion de reprise sur erreur.

Ces fonctions peuvent être fournies par le système d'exploitation, ou par une combinaison de fonctions offertes par le système d'exploitation, le système de l'IGC et des mécanismes de protection physique.

L'interface entre l'IGC et l'AC est également être sécurisée pour éviter toute altération ou intrusion pendant la transmission des données entre les deux.

Les dispositions sont détaillées dans la DPC.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

6.5.2 Niveau d'évaluation sécurité des systèmes informatiques

Le niveau minimal d'assurance dans la sécurité offerte est défini dans la DPC.

6.6 MESURES DE SECURITE DES SYSTEMES DURANT LEUR CYCLE DE VIE

6.6.1 Mesures de sécurité liées au développement des systèmes

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

Les mesures sont détaillées dans la DPC.

6.6.2 Mesures liées à la gestion de la sécurité

L'AC applique une méthode de gestion de la configuration pour installer le cœur cryptographique de l'AC et en assurer la maintenance. La première fois qu'il est chargé, le logiciel de l'AC fournit une méthode permettant à l'AC ou à toute personne habilitée expressément de vérifier si le logiciel installé sur le système :

- vient de la société qui l'a mis au point ;
- n'a pas été modifié avant d'être installé ;
- correspond bien à la version voulue.

L'AC ou toute personne habilitée expressément prévoit un mécanisme permettant de vérifier périodiquement l'intégrité des logiciels.

L'AC ou toute personne habilitée expressément met également en place des mécanismes et (ou) des politiques lui permettant de contrôler et de surveiller la configuration du système de l'IGC.

Toute évolution est documentée et apparaît dans les procédures de fonctionnement interne et est conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

Les mesures sont détaillées dans la DPC.

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

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

6.7 MESURES DE SECURITE RESEAU

Les systèmes de l'IGC sont protégés contre les attaques provenant de tout réseau, en particulier les réseaux ouverts. Une telle protection est assurée par l'installation de passerelles de sécurité configurées de façon à permettre la seule utilisation des protocoles et des commandes nécessaires à la bonne marche de l'IGC.

L'AC définit les protocoles et commandes dans la DPC.

6.8 HORODATAGE / SYSTEME DE DATATION

L'AC précise les modalités techniques permettant l'horodatage des événements liés à l'activité des composantes de l'IGC dans la DPC.

7 PROFILS DES CERTIFICATS, OCSP ET DES LCR

Ce chapitre contient les règles et directives relatives à l'utilisation de certains types de certificats X.509, des champs, des extensions des LCR conformes aux normes PKIX.

Le contenu des certificats et des LCR, sont conformes aux exigences de la RFC 5280 : « Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile », dont les profils sont définis dans la norme ETSI EN 319 412-2.

7.1 PROFIL DES CERTIFICATS D'AC

AC FLASH
DN de l'AC
C=FR, O=Certinomis, OrgId=NTRFR-433998903, CN= Certinomis - Flash CA

AC ONCE
DN de l'AC
C=FR, O=Certinomis, OrgId=NTRFR-433998903, CN= Certinomis - Once CA

AC SIGNATURE BPCE
DN de l'AC
C=FR, O=Certinomis, OrgId=NTRFR-433998903, CN= AC SIGNATURE BPCE

Les chaines de certificats sont disponibles sur le site de l'AC :
https://www.certinomis.fr/documents-et-liens/nos-certificats-racines

Les champs suivants sont renseignés par le logiciel de l'AC :

- version : version du certificat X.509
- serialNumber : numéro de série unique du certificat
- signature : identifiant de l'algorithme de signature de l'AC
- issuer : nom de l'AC émettrice
- validity : dates d'activation et d'expiration du certificat
- subject : nom distinctif de l'entité identifiée
- subjectPublicKeyInfo : identifiant de l'algorithme d'usage de la clé publique contenue dans le certificat, et valeur de la clé publique
- extensions : les extensions du certificat définies en 7.1.2.

Le format précis des certificats d'AC est donné dans la DPC.

7.2 PROFIL DES CERTIFICATS EMIS

Le format précis des certificats émis est donné dans la DPC.

7.3 PROFIL DES LCR

Le format précis des LCR émis est donné dans la DPC. Les fichiers LCR sont disponibles sur le site web de l'AC :
https://www.certinomis.fr/documents-et-liens/nos-crl

7.4 PROFIL OCSP

Il n'y a pas d'exigence spécifique. Le service est conforme au [RFC 6960]. L'adresse du répondeur OCSP est :
http://ocsp-pki.certinomis.com

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Le présent chapitre ne concerne que les audits et évaluation de la responsabilité de l'AC afin de s'assurer du bon fonctionnement de son IGC.

8.1 FREQUENCES ET / OU CIRCONSTANCES DES EVALUATIONS

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

L'AC procède également régulièrement à un contrôle de conformité de l'ensemble de son IGC, suivant la fréquence de 1 fois tous les 2 ans.

Des contrôles internes sont effectués pour s'assurer du bon fonctionnement de l'IGC entre 2 audits de conformité.

8.2 IDENTITES / QUALIFICATIONS DES EVALUATEURS

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

8.3 RELATIONS ENTRE EVALUATEURS ET ENTITES EVALUEES

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

8.4 SUJETS COUVERTS PAR LES EVALUATIONS

Les contrôles de conformité portent sur une composante de l'IGC (contrôles ponctuels) ou sur l'ensemble de l'architecture de l'IGC (contrôles périodiques) et visent à vérifier le respect des engagements et pratiques définis dans la présente PC et dans la DPC qui y répond ainsi que des éléments qui en découlent (procédures opérationnelles, ressources mises en œuvre, etc.).

8.5 ACTIONS PRISES SUITE AUX CONCLUSIONS DES EVALUATIONS

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

- "réussite",
- "échec",
- "à confirmer".

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

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

8.6 COMMUNICATION DES RESULTATS

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

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

9 AUTRES PROBLEMATIQUES METIERS ET LEGALES

9.1 TARIFS

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Des frais d'émission de certificat sont négociés dans le cadre d'un contrat commercial.

9.1.2 Tarifs pour accéder aux certificats

Il n'y a pas de frais d'accès pour les certificats publiés par l'AC.

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

Un moyen gratuit de contrôle du statut du certificat est toujours laissé à la disposition du tiers utilisateur (répondeur OCSP ou LCR).

9.1.4 Tarifs pour d'autres services

Sans objet.

9.1.5 Politique de remboursement

Aucune exigence particulière.

9.2 RESPONSABILITE FINANCIERE

9.2.1 Couverture par les assurances

La garantie associée au certificat est limitée au montant prévu au contrat. Pour toute transaction commerciale, ou échange électronique, dont les conséquences financières directes ou indirectes sont d'un montant supérieur au montant prévu, la responsabilité des acteurs de l'IGC ne peut être engagée vis-à-vis des clients, bénéficiaires et tiers utilisateurs.

9.2.2 Autres ressources

Aucune exigence particulière.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Les certificats garantis par la présente PC comportent un niveau d'assurance garanti, précisé par contrat et accessible à la partie utilisatrice.

9.3 CONFIDENTIALITE DES DONNEES PROFESSIONNELLES

9.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont les suivantes :

- la DPC de l'AC,
- les clés privées de l'AC, des composantes et des certificats émis,
- les données d'activation associées aux clés privées de l'AC,
- les Données d'Activation des Bénéficiaires
- tous les secrets de l'IGC,
- les journaux d'évènements des composantes de l'IGC,
- le dossier d'enregistrement du client,
- les causes de révocation, sauf accord explicite de publication.

9.3.2 Informations hors du périmètre des informations confidentielles

Aucune exigence particulière.

9.3.3 Responsabilités en terme de protection des informations confidentielles

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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. Lors d'échange de ces données, l'intégrité est garantie par un moyen adapté au type d'information (chiffrement, signature, enveloppe sécurisée…).

L'AC peut mettre à disposition les dossiers d'enregistrement des bénéficiaires à des tiers dans le cadre de procédures légales. Ces dossiers sont aussi accessibles au bénéficiaire conformément au §9.4.1.

9.4 PROTECTION DES DONNEES PERSONNELLES

9.4.1 Politique de protection des données personnelles

Le Règlement Européen UE 2016/679 du 27 avril 2016 relatif à la protection des données personnelles ainsi que la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel s'applique à tous les documents détenus ou transmis par l'AC ou par une des composantes de l'IGC (site de la CNIL http://www.cnil.fr).

En vertu des textes, les clients et les bénéficiaires disposent d'un droit d'accès, de rectification et d'opposition à la cession de toute information qui les concerne. Ce droit peut s'exercer par l'intermédiaire du service agent, en particulier l'AE, ayant recueilli ces informations, à l'adresse figurant sur le site WEB de l'AC. L'AC respecte rigoureusement toutes les prescriptions légales applicables et expliquer sur son site WEB, les modalités concrètes d'application de la loi, notamment dans les rubriques « mentions légales & gestion des données personnelles ». La Politique de Certification respecte les principes fondamentaux en matière de protection des données à caractère personnel consacrés dans la loi, le RGPD et toute autre convention internationale entrée en vigueur.

9.4.2 Informations à caractère personnel

Toutes les données collectées et détenues par l'AC sur une personne physique ou morale (par exemple : procédure d'enregistrement, révocation, autres événements consignés, correspondances échangées entre le bénéficiaire et l'AC ou l'AE, etc.) sont considérées comme confidentielles et ne peuvent pas être divulguées sans avoir obtenu le consentement préalable du bénéficiaire.

Les renseignements concernant l'identification ou d'autres données à caractère personnel, du bénéficiaire, apparaissant sur les certificats sont considérés comme étant confidentiels, sauf si le bénéficiaire a donné son consentement exprès et préalable à toute diffusion.

Les causes de révocation des certificats sont réputées demeurer strictement confidentielles

9.4.3 Informations à caractère non personnel

Aucune exigence particulière.

9.4.4 Responsabilité en termes de protection des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci- dessous)

9.4.5 Notification et consentement d'utilisation des données personnelles

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci- dessous)

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

Cf. législation et réglementation en vigueur sur le territoire français (notamment cf. chapitre 10 ci- dessous)

9.4.7 Autres circonstances de divulgation d'informations personnelles

Le secret des correspondances émises par voie des télécommunications est garanti par la loi française. En cas d'atteinte, toute violation est punie par l'article 226-15 du code pénal pour celles commises par un particulier et par les articles 432-9 et 432-17 du code pénal pour celles commises par une personne dépositaire de l'autorité publique.

D'une façon générale, aucun salarié de l'AC et aucun collaborateur ou sous-traitant, dans le cadre de leur participation

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

aux services de certification, n'a le droit d'intercepter, d'ouvrir, de détourner, de divulguer, de rechercher ou d'utiliser les documents soumis à l'AC, sauf dans les cas prévus dans la présente politique, ou dans le cadre du régime des interceptions ordonnées par l'autorité judiciaire ou des interceptions de sécurité en vertu de la loi n°91-646 du 10 juillet 1991.

9.5 DROITS SUR LA PROPRIETE INTELLECTUELLE ET INDUSTRIELLE

Tous les droits de propriété intellectuelle détenus par Certinomis sont protégés par la loi, règlement et autres conventions internationales applicables. Ils sont susceptibles d'entraîner la responsabilité civile et pénale en cas de leur non-respect. Par exemple, conformément à la loi n°98-536 du 1er juillet 1998 (Journal officiel du 2 juillet 1998, p.10075) et à la directive européenne 96/6/CE du 11 mars 1996, les bases de données réalisées par Certinomis sont protégées. Le texte de la loi peut être consulté sur le site suivant : http://www.legifrance.gouv.fr

9.6 INTERPRETATIONS CONTRACTUELLES ET GARANTIES

Ce chapitre contient des dispositions relatives aux obligations respectives de l'AC, du personnel de l'AC, des diverses entités composant l'IGC, des clients, des bénéficiaires et des tiers utilisateurs. Elle contient aussi des dispositions juridiques, relatives notamment à la loi applicable et à la résolution des litiges.

- Les différentes composantes de l'IGC doivent :
- protéger leurs clés privées et leur éventuelle donnée d'activation en intégrité et en confidentialité ;
- n'utiliser leurs clés publiques et privées qu'aux seules fins pour lesquelles elles ont été émises et avec les moyens appropriés ;
- mettre en œuvre des mécanismes d'authentification multi-facteurs pour les comptes ayant la capacité d'émettre directement des certificats.
- mettre en œuvre les moyens techniques et employer les ressources humaines nécessaires à la réalisation des prestations auxquelles elle s'engage ;
- documenter leurs procédures internes de fonctionnement ;
- respecter et appliquer les termes de la présente PC ;
- accepter le résultat et les conséquences d'un contrôle de conformité, et en particulier remédier aux non-conformités qui pourraient être révélées ; et
- respecter les conventions qui les lient aux autres entités composantes de l'IGC.

9.6.1 Autorités de Certification

L'AC est responsable vis-à-vis de ses clients, bénéficiaires et tiers utilisateurs des opérations relatives aux services de certification réalisées par l'une quelconque des composantes de l'IGC. Elle garantit le lien qui existe entre une entité identifiée et une bi-clé.

L'AC et le responsable de l'AC se conforment à toutes les exigences de la présente Politique de Certification et de la DPC associée. L'AC et le personnel de l'AC doivent respecter les droits des clients, bénéficiaires et tiers utilisateurs de certificats eu égard aux lois et règlements en vigueur.

L'AC informe les tiers utilisateurs de la révocation du certificat d'un bénéficiaire ou d'une composante de l'IGC en transmettant dans les plus brefs délais la révocation du certificat auprès de l'IGC qui a en charge de publier les statuts des certificats ;

L'AC est responsable de la transmission de l'information à l'IGC pour ses clients et ses bénéficiaires des procédures à suivre au cours du cycle de vie des certificats ; cela concerne, notamment, l'émission et la révocation.

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

Le personnel de l'AC doit se conformer à toutes les exigences pertinentes de la présente Politique de Certification et de la DPC associée. Il doit respecter les droits des clients, des bénéficiaires et des tiers utilisateurs de certificats eu égard aux lois et règlements en vigueur et doit informer l'AC de tout problème constaté quant à la disponibilité du site www.certinomis.fr.

Les membres du personnel de l'AC à qui sont assignés des rôles relatifs à l'IGC (responsable de l'AC, responsable de la sécurité de l'AC…) doivent être personnellement responsables de leurs actes. L'expression « *personnellement*

responsable » signifie que l'on puisse prouver qu'une telle personne a bel et bien fait une telle action.

9.6.2 Service d'enregistrement

Une AE se conforme à toutes les exigences de la présente politique de certification et de la DPC associée.

En outre, une AE:

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

L'AE se soumet à tout contrôle technique et audits de qualité des procédures que pourrait demander l'AC ou les AGP qui l'accréditent.

9.6.3 Bénéficiaire de certificats

Le bénéficiaire doit se conformer à toutes les exigences de la présente Politique de Certification. Il s'engage à respecter le contrat qui le lie à l'AC.

Il garantit que les informations qu'il fournit à l'AC pour son identification sont exactes, complètes et que les documents transmis ou présentés sont valides.

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

En aucun cas le bénéficiaire n'acquiert la propriété du certificat émis par l'AC. Il n'en acquiert que le droit d'usage. Par conséquent, tous les certificats demeurent la propriété de l'AC qui les a émis.

9.6.4 Autres participants

9.6.4.1 Obligation du tiers utilisateur

Avant toute utilisation de certificats, notamment lorsque lesdits certificats créent des effets juridiques, le tiers utilisateur doit impérativement avoir un comportement raisonnable : vérifier la validité des certificats auxquels il entend se fier auprès de Certinomis , en consultant les Listes des Certificats Révoqués appropriées les plus récentes, ainsi qu'en vérifiant leur date d'expiration et leur validité intrinsèque, en particulier sa signature, et la validité de tout certificat sur l'itinéraire de confiance. A défaut de remplir cette obligation, le tiers utilisateur assume seul tous les risques de ses actions non conformes aux exigences de la présente politique, Certinomis ne garantissant aucune valeur juridique aux certificats qu'elle a émis et qui pourraient avoir été révoqués ou qui ne seraient pas valides.

En outre, lors de la vérification d'une signature électronique, le tiers utilisateur doit aussi vérifier que la clé publique du certificat correspond à la clé privée de signature utilisée.

Le tiers utilisateur doit toujours vérifier que le certificat est utilisé à des fins pertinentes et conformément aux applications autorisées.

Un tiers utilisateur ne doit utiliser les certificats que conformément à la procédure de validation de l'itinéraire de confiance, procédure qui est spécifiée dans les normes X. 509 et PKIX et déterminée par la recommandation ISO/IEC 9594-8.

9.7 LIMITE DE GARANTIE

L'émission de certificats, conformément à la présente Politique de Certification, ne fait pas de l'AC, de l'une des composantes de l'IGC, du responsable de l'AC et du personnel de l'AC et des composantes de l'IGC un fiduciaire, un mandataire, un garant ou un autre représentant de quelque façon que ce soit du client ou de toutes autres parties concernées. Chaque partie s'interdit de prendre un engagement au nom et pour le compte de l'autre partie à laquelle elle ne saurait en aucun cas se substituer.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

En conséquence de quoi les Clients et les tiers utilisateurs de certificat sont des personnes juridiquement et financièrement indépendantes et, à ce titre, ne disposent d'aucun pouvoir ni de représentation, ni d'engager l'AC ou l'une des composantes de l'IGC, susceptible de créer des obligations juridiques, tant de façon expresse que tacite au nom de l'AC ou de l'une des composantes de l'IGC. Les services de certification ne constituent pas un partenariat ni ne créent une quelconque forme juridique d'association juridique qui imposerait une responsabilité basée sur les actions ou les carences de l'autre. Le contrat ne constitue ni une association, ni une société ou autre groupement, ni un mandat donné par l'une des parties à l'autre.

La garantie associée au certificat est limitée au montant prévu au contrat. Pour toute transaction commerciale, ou échange électronique, dont les conséquences financières directes ou indirectes sont d'un montant supérieur au montant prévu, la responsabilité des acteurs de l'IGC ne peut être engagée vis-à-vis des clients et tiers utilisateurs.

9.8 LIMITE DE RESPONSABILITE

L'AC, le personnel de l'AC, les composantes de l'IGC, les clients, les tiers utilisateurs sont responsables pour tous dommages et intérêts découlant du non-respect de leurs obligations respectives telles que définies aux termes de la présente Politique de Certification et de la DPC associée.

9.8.1 Responsabilité de l'AC et du personnel de l'AC

Pour la mise en œuvre des services de certification qu'elle fournit, une obligation de moyen pèse sur l'AC. Dans l'hypothèse où la responsabilité de l'AC serait mise en cause, celle-ci pourra être engagée selon les règles du droit commun.

Aucune responsabilité ne sera assumée par l'AC et par le personnel de l'AC pour l'utilisation d'un certificat dans des conditions qui ne seraient pas conformes ou non autorisées par la présente Politique de Certification, ainsi que par toutes autres clauses contractuelles applicables.

9.8.1.1 Limites de responsabilité

L'AC décline absolument toute responsabilité à l'égard de l'usage qui est fait des certificats électroniques qu'elle émet dans des conditions et à des fins autres que celles prévues dans la présente PC, ainsi que dans tout autre document contractuel applicable.

L'AC ne sera en aucun cas tenue responsable des éventuels dommages tant directs qu'indirects, consécutifs ou connexes, ou d'autres réclamations ou obligations quelconques résultant d'un acte délictuel, d'un contrat ou d'une autre cause à l'égard d'un service en relation avec l'émission, l'utilisation ou la fiabilité d'un certificat électronique, offrant un niveau d'assurance selon la classe du certificat ou du bi-clé connexe, au-delà des limites fixées ci-dessous, par l'utilisation, par un bénéficiaire ou un tiers utilisateur. Cette limite de responsabilité s'entend, et de façon non limitative, de tout préjudice financier ou commercial, perte de bénéfices, perte d'exploitation, trouble commercial, manque à gagner, pertes ou actions intentées par un tiers contre le client, trouvant leur origine ou étant la conséquence de la présente déclaration, politiques associées ou autres contrat ou inhérents à l'utilisation ou la fiabilité d'un certificat qu'elle émet.

Les parties conviennent qu'en cas de prononcé d'une quelconque responsabilité de l'une des parties envers l'autre, les dommages et intérêts et indemnités à sa charge, toutes causes confondues, ne sauraient en aucun cas dépasser les limites de responsabilité mentionnées dans le cadre du contrat conclu entre l'AC et son client.

9.8.1.2 Exonération de responsabilité

L'AC n'assume aucun engagement ni responsabilité quant à la forme, la suffisance, l'exactitude, l'authenticité, la falsification ou l'effet juridique des documents et des informations remis lors de la signature du contrat de prestations de services de certification (ou conditions générales d'utilisation).

L'AC n'assume aucun engagement ni responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, ni quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute communication électronique.

En outre, l'AC n'assume aucun engagement ni responsabilité quant à l'utilisation des certificats et bi- clés connexes qu'elle émet par le bénéficiaire ou le tiers utilisateur non conforme à la réglementation en vigueur relative à la protection des logiciels, quant au non-respect par le bénéficiaire ou le tiers utilisateur des procédures de contrôle de validité des certificats et bi-clés connexes qu'elle émet lors d'une transaction, quant à l'usure normale des média informatiques du bénéficiaire ou du tiers utilisateur, la détérioration des informations portées sur les dits médias informatiques due à l'influence des champs magnétiques et, de manière générale, sans que cela soit entendu de façon limitative, tout fait de nature à entrer dans les exclusions de garantie prévues dans la PC associée, ou dans le contrat de

prestations de services de certification.

9.8.2 Responsabilité de l'AE

La responsabilité de l'AE pourra être engagée uniquement par l'AC. Ainsi, la responsabilité de l'AE ne pourra jamais être directement mise en cause par le client ou le tiers utilisateur.

9.8.3 Responsabilité de l'hébergeur

La responsabilité de l'hébergeur pourra être engagée uniquement par l'AC. Ainsi, la responsabilité de l'hébergeur ne peut jamais être directement mise en cause par le client ou le tiers utilisateur. Celle-ci est strictement limitée aux engagements pris par l'hébergeur dans le contrat de services qui le lie à l'AC et au respect des dispositions de la présente PC

9.9 INDEMNITES

Aucune exigence particulière.

9.10 DUREE ET FIN ANTICIPEE DE VALIDITE DE LA PC

9.10.1 Durée de validité

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

9.10.2 Fin anticipée de validité

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

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

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

9.10.3 Effets de la fin de validité et clauses restant applicables

Aucune exigence particulière.

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 devra :

- au plus tard un mois avant le début de l'opération, faire valider 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.
- au plus tard un mois après la fin de l'opération, en informer l'organisme de qualification.

9.12 AMENDEMENTS À LA PC

Le présent chapitre définit les exigences en matière d'administration et de gestion de la présente politique de certification.

9.12.1 Procédures d'amendements

L'AC assure que toute modification de sa PC reste conforme aux exigences de l'ETSI. En cas de changement important, l'AC fera appel à une expertise technique pour en contrôler l'impact.

9.12.2 Mécanisme et période d'information sur les amendements

Le responsable de l'AC donne un préavis aux bénéficiaires et aux tiers utilisateurs dans les sept (7) jours d'un changement de la présente politique qui résulte d'une situation hors du contrôle du responsable de la politique, à condition que ce changement ait un impact sur eux.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

Le responsable de l'AC peut modifier la présente politique sans préavis aux bénéficiaires et aux tiers utilisateurs lorsque, selon l'évaluation du responsable de la politique, ces modifications n'ont aucun impact sur eux.

9.12.3 Circonstances selon lesquelles l'OID doit être changé

Si un changement de politique a, selon l'évaluation du responsable de la politique, un impact majeur sur un nombre important de clients, des bénéficiaires et/ou de tiers utilisateurs, le responsable de la politique institue une nouvelle politique avec un nouvel identificateur d'objet (OID).

9.13 DISPOSITIONS CONCERNANT LA RESOLUTION DE CONFLITS

En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente politique et faute d'être parvenues à un accord amiable ou à une transaction, les parties donnent compétence expresse et exclusive aux tribunaux compétents de Paris, nonobstant pluralité de défendeurs ou d'action en référé ou d'appel en garantie ou de mesure conservatoire

9.14 JURIDICTIONS COMPETENTES

La présente politique de certification est expressément élaborée, régie, appliquée et interprétée selon les lois et règlements français, bien que les activités qui découlent de la présente Politique de Certification puissent avoir des effets juridiques en-dehors du territoire de la République française.

9.15 CONFORMITE AUX LEGISLATIONS ET REGLEMENTATIONS

Les textes législatifs et réglementaires applicables à la présente PC sont, notamment, ceux indiqués au chapitre 10 ci-dessous.

9.16 DISPOSITIONS DIVERSES

9.16.1 Accord global

Aucune exigence particulière.

9.16.2 Transfert d'activités

Cf. chapitre 5.8.

9.16.3 Conséquences d'une clause non valide

Le caractère inapplicable dans un contexte donné d'une disposition de la Politique de Certification n'affecte en rien la validité des autres dispositions, ni de cette disposition hors du dit contexte. La Politique de Certification continue à s'appliquer en l'absence de la disposition inapplicable et ce tout en respectant l'intention des parties.

Les intitulés portés en tête de chaque article ne servent qu'à la commodité de la lecture et ne peuvent en aucun cas être le prétexte d'une quelconque interprétation ou dénaturation des clauses sur lesquelles ils portent.

9.16.4 Application et renonciation

Toute notification devant être donnée au titre de la présente politique sera censée avoir été donnée si elle est envoyée par lettre recommandée avec avis de réception ou par télécopie adressée au domicile élu tel qu'indiqué en entête du contrat de services et sera censée avoir été reçue sept (7) jours après la date de cachet de la Poste dans le cadre de la lettre recommandée avec avis de réception et un (1) jour après la date d'envoi dans le cadre de la télécopie.

9.16.5 Force majeure

Dans un premier temps, les cas de force majeure suspendront l'exécution du contrat. Si les cas de force majeure ont une durée supérieure à celle indiquée dans le contrat, le contrat est résilié automatiquement, sauf accord contraire entre les parties. L'exécution des obligations reprendra son cours normal dès que l'évènement constitutif de la force majeure aura cessé.

L'AC ne saurait être tenue responsable et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'article 1148 du Code civil.

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, outre ceux habituellement retenus par la jurisprudence des cours et tribunaux français, des clauses contractuelles contenues dans la Déclaration des Pratiques associée et toutes autres conventions liant les parties (par exemple le contrat) :

Grève totale ou partielle, lock-out, émeute, trouble civil, insurrection, guerre civile ou étrangère, risque nucléaire, embargo, confiscation, capture ou destruction par toute autorité publique, intempérie, épidémie, blocage des moyens de transport ou d'approvisionnement pour quelque raison que ce soit, tremblement de terre, incendie, tempête, inondation, dégâts des eaux, restrictions gouvernementales ou légales, modifications légales ou réglementaires des formes de commercialisation, panne d'ordinateur, blocage des communications électroniques, y compris des réseaux de télécommunications, toute découverte scientifique majeure remettant en cause en totalité ou en partie les principes de la cryptographie asymétrique, toute conséquence d'une évolution technologique, non prévisible par l'AC, remettant en cause les normes et standards de sa profession et tout autre cas indépendant de la volonté des parties empêchant l'exécution normale du présent contrat.

9.17 AUTRES DISPOSITIONS

9.17.1 Dispositions pénales

En vertu des articles 323-1 à 323-7 du Code pénal, applicable lorsqu'une infraction est commise sur le territoire français, les atteintes et les tentatives d'atteintes aux systèmes de traitement automatisé de données sont sanctionnées, notamment l'accès et le maintien frauduleux, les modifications, les altérations et le piratage de données, etc.

Les peines encourues varient de 2 à 5 ans d'emprisonnement et d'une amende allant de 30.000 à 375.000 euros pour les personnes morales.

La contrefaçon de marques de fabrique, de commerce et de services, dessins et modèles, signes distinctif, droits d'auteur (par exemple : logiciels, pages WEB, bases de données, textes originaux, …) est sanctionnée par les articles L. 716-1 et suivants du Code de la propriété intellectuelle.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

10 ANNEXE 1 : DOCUMENTS CITES EN REFERENCE

10.1 REGLEMENTATION

Renvoi	Document
[DIRSIG]	*Directive 1999/93/CE du Parlement européen et du Conseil, du 13 décembre 1999, sur un cadre communautaire pour les signatures électroniques.*
[LCEN]	*Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique, notamment son article 31 concernant la déclaration de fourniture de cryptologie et son article 33 qui précise le régime de responsabilité des prestataires de services de certification électronique délivrant des certificats électroniques qualifiés.*
[QPSCe]	*Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation*
[SIG]	*Décret n°2001-272 du 30 mars 2001 pris pour application de l'article 1316-4 du code civil et relatif à la signature électronique.*
[EIDAS]	*RÈGLEMENT (UE) No 910/2014 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE*

10.2 DOCUMENTS TECHNIQUES

Renvoi	Document
[EN 419211-1]	*Profils de protection pour dispositif sécurisé de création de signature électronique — Partie 1 : Présentation générale*
[EN 419211-2]	*Profils de protection des dispositifs sécurisés de création de signature — Partie 2 : Dispositif avec génération de clé*
[EN 419211-3]	*Profils de protection des dispositifs sécurisés de création de signature — Partie 3 : Dispositif avec import de clé*
[EN 419211-4]	*Profils de protection des dispositifs sécurisés de création de signature — Partie 4 : Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de génération de certificats*
[ETSI_PKC]	*ETSI EN 319 411 - 1 Policy Requirements for Certification Authorities issuing public key certificates*
[PROF_PKC]	*ETSI EN 319 412-2 Certificate profile for certificates issued to natural persons*
[PROG_ACCRED]	*COFRAC - Programme d'accréditation pour la qualification des prestataires de services de confiance – CEPE REF 21 – version publiée cf www.cofrac.fr*
[RFC 6960]	*IETF - Internet X.509 Public Key Infrastructure - Online Certificate Status Protocol, RFC 6960 - juin 2013*
[RFC 3647]	*IETF - Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practice Framework - novembre 2003*
[X.509]	*Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, Recommendation X.509, version mars 2000 (complete par les correctifs techniques n° 1 d'octobre 2001, n° 2 d'avril 2002 et n° 3 d'avril 2004)*

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

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

11.1 EXIGENCES SUR LES OBJECTIFS DE SECURITE

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

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

11.2 EXIGENCES SUR LA QUALIFICATION

Le module cryptographique utilisé par l'AC fait l'objet d'une qualification, au niveau renforcé selon le processus décrit dans le [RGS], et est conforme aux exigences du chapitre 11.1 ci-dessus.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903

12 ANNEXE 3 : EXIGENCES DE SECURITE DU DISPOSITIF CRYPTOGRAPHIQUE

12.1 EXIGENCES SUR LES OBJECTIFS DE SECURITE

Le dispositif cryptographique, utilisé pour les bénéficiaires pour stocker et mettre en œuvre leur clé privée et, le cas échéant, générer la bi-clé, doit répondre aux exigences de sécurité suivantes :

- si la bi-clé du certificat émis est générée par le dispositif, garantir que cette génération est réalisée exclusivement par des utilisateurs autorisés et garantir la robustesse cryptographique de la bi-clé générée;
- assurer la correspondance entre la clé privée et la clé publique ;
- générer un cachet ou une authentification qui ne peut être falsifiée sans la connaissance de la clé privée.

Par ailleurs, des mesures de sécurité organisationnelles, procédurales ou techniques doivent être mises en place afin de :

- 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 re-génération de la clé privée ;
- garantir la confidentialité et l'intégrité de la clé privée ;
- permettre de garantir l'authenticité et l'intégrité de la clé publique lors de son export hors du dispositif.

12.2 EXIGENCES SUR LA QUALIFICATION

Le dispositif cryptographique, utilisé pour les bénéficiaires pour stocker et mettre en œuvre leur clé privée doit être qualifié au minimum au niveau FIPS 140-2 Level 2 ou CWA 14169 (SSCD), et être conforme aux exigences du chapitre 12.1 ci-dessus.

Certinomis SA au capital de 40 156 euros.
Siège social : 45-47 Boulevard Paul Vaillant-Couturier
94200 Ivry sur Seine. RCS Créteil B 433 998 903