



**Politique de Certification
– Autorité de certification CertiNomis
CORPORATE**

© 2007, CertiNomis. Tous droits réservés

Avril 2007

Version : 3.1

Référence : PCCorp_DM-EC-PA_003.1

Ce document est la propriété de CertiNomis SA. Aucune copie même partielle de ce document n'est autorisée sauf accord explicite de son propriétaire.

Historique du document

Référence	Version	Date	Statut	Rédaction	Validation
PCCorp_DM-EC-PA_001	0	9/11/05	Première version	PA	AC-EC
PCCorp_DM-EC-PA_002	1	17/01/06	Version intégrant les certificats de serveur	PA	
PCCorp_DM-EC-PA_003	2	13/11/06	Modifications suite à une réunion	PA	
PCCorp_DM-EC-PA_003.1	3	05/04/07	Modifications après consultation d'un distributeur	PA	DM

Historique des modifications :

Version 0 : Première version de la PC Réseau fermé

Version 1 : Version intégrant les certificats de serveur

Version 2 : Version intégrant les modifications souhaitées par CertiNomis

Version 3.1 : Version intégrant certaines modifications proposées par un distributeur

AVERTISSEMENT

La présente Politique de Certification est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle, 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 autorisée 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.

1 PREAMBULE

Le présent document constitue la politique de certification appliquée par la société CERTINOMIS en tant qu'autorité de certification mutualisée dans le cadre de la fourniture de services de certification pour un réseau fermé. Il a pour objectif de définir les dispositions prévues pour la délivrance de services de certification prévue pour les réseaux fermés aux utilisateurs de certificats ainsi que les droits et obligations des différents intervenants de la procédure.

La PC est opposable et applicable :

- à tous les utilisateurs, émetteurs ou destinataires, de certificats dans le cadre du réseau fermé préalablement défini par le client ;
- aux Clients, ayant contracté avec CERTINOMIS ou avec tout Distributeur en relations contractuelles avec CERTINOMIS ;
- aux composantes de l'ICP.

2 PRESENTATION GENERALE

2.1 Résumé de la PC

La présente PC est destinée à être utilisée par l'ensemble des utilisateurs de services de certification au sein d'un réseau fermé fédéré par un Client.

La présente PC couvre la gestion et l'utilisation de certificats servant aux fonctions d'authentification forte, de signature électronique des données pour en garantir l'authenticité, l'intégrité ainsi que la non-répudiation dans le cadre du Réseau fermé.

Les Certificats délivrés en vertu de la présente PC peuvent notamment servir à vérifier l'identité des correspondants, permettre l'accès à distance d'un système d'information (extranet), ou encore permettre la signature d'actes entre utilisateurs reconnaissant la valeur juridique d'un certificat utilisé dans le cadre du réseau fermé.

La délivrance d'un Certificat ne signifie pas que le Client ou l'Utilisateur soit autorisé de quelque façon que ce soit à effectuer des transactions commerciales, ou autres, au nom de CERTINOMIS.

CERTINOMIS s'engage à délivrer, à gérer et à révoquer les Certificats dans le strict respect des procédures prévues dans la présente Politique ainsi que tout document particulier négocié entre CERTINOMIS et le Client ou tout Distributeur.

CERTINOMIS 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 relatives à l'application, l'élaboration, l'interprétation et la validité des PC.

2.1.1 Champ d'application

La présente politique s'applique aux membres de l'ICP à leur responsable, à leur personnel, aux Clients, aux Distributeurs ainsi qu'aux Utilisateurs et aux Parties qui se fient du Réseau fermé.

2.1.2 Liste des applications appropriées

Les certificats émis en vertu de la présente politique sont appropriés pour établir le lien qui existe entre une identité déclarée et une clé publique.

Dans le cadre d'un Réseau fermé, ils sont appropriés pour :

- vérifier l'identité du demandeur d'accès à des données sensibles, par exemple à caractère personnel ;
- vérifier l'identité de l'expéditeur d'un envoi électronique ;
- vérifier l'identité de l'auteur d'un document électronique ;
- vérifier l'identité de clients et de serveurs informatiques (serveurs WEB...) ;
- vérifier la volonté d'adhésion au contenu d'un document ou d'un envoi électronique ;
- vérifier l'intégrité des documents et des envois électroniques ; et
- vérifier la volonté d'engagement d'achat de biens et/ou de services.

Les fonctions ci-dessus devront être, selon toute vraisemblance, couplées avec la mise en place d'une convention de preuve juridiquement valable entre les membres du réseau fermé.

2.1.3 Liste des applications interdites

Rien n'empêche techniquement la mise en œuvre d'applications considérées comme interdites au sens des critères énoncés ci-après. Toutefois, celui qui réaliserait ces opérations le ferait à ses seuls et entiers risques et périls, et serait tenu pour seul responsable des conséquences.

A titre indicatif, les Certificats émis par CERTINOMIS ne peuvent pas être utilisés :

- hors du cadre du réseau fermé et en dehors des applications autorisées par le Client ou tout Distributeur ;
- à des fins de chiffrement de données.

Tout Client, tout Utilisateur recourant aux Certificats en dehors des applications appropriées ou en dehors du réseau fermé, et en particulier pour effectuer une application interdite, telles que définies aux termes de la présente politique ou de la DPC, il le fait sous sa seule responsabilité et à ses entiers risques et périls.

Si le Certificat est utilisé en dehors du réseau fermé, la partie qui s'y fie en assume seule tous les risques.

La responsabilité de CERTINOMIS ne pourra être mise en jeu dans aucune des hypothèses visées ci-dessus.

Sauf accord préalable, écrit et signé d'un représentant légal de CERTINOMIS personne n'est autorisé à utiliser la clé privée associée à un certificat pour signer un autre certificat ou une LCR.

La liste des applications interdites peut être complétée dans le cadre d'un document particulier établi entre CERTINOMIS et son Client ou un Distributeur.

2.2 Infrastructure à Clé Publique

Une Infrastructure à Clé Publique (ICP) est 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 ICP, nécessaire à la sécurité et à la confiance, ouvre une palette de services à valeur ajoutée pour les transactions électroniques (par exemple : courrier électronique, transactions commerciales, téléprocédures, protection locale des données, etc). Ces services ont pour objectif d'assurer :

- l'intégrité des messages,
- l'identification et l'authentification¹,
- la non répudiation de l'origine,
- et la confidentialité. Ce service n'est pas assuré dans le cadre de la présente PC.

2.2.1 Les composantes de l'ICP

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 qui indique, par l'accréditation, la confiance que l'on peut accorder à une Autorité de Certification.

Autorité de Certification (AC) :

L'Autorité de Certification est responsable vis-à-vis de ses Clients, mais aussi de tout Utilisateur de tout Certificat qu'elle a émis, de l'ensemble du processus de certification, et donc de la validité des certificats qu'elle émet. A ce titre, elle édicte la Politique de Certification et valide les Déclarations de Pratique 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 de la technologie mise en œuvre, mais aussi du cadre réglementaire et contractuel qu'elle définit et s'engage à respecter.

L'Autorité de Certification peut définir plusieurs Politiques de Certification en fonction du mode d'enregistrement et de l'usage du certificat. Elle distingue alors des classes de certificats et elle définit en même temps les conditions et le niveau de sa responsabilité.

Lorsque l'Autorité d'Enregistrement s'est assurée de l'identité et des droits du demandeur, de manière plus ou moins poussée selon la garantie associée, l'Autorité de Certification prend la décision d'émettre un certificat adapté. Elle est responsable non seulement de l'émission des certificats mais encore de leur gestion durant tout leur cycle de vie, et en particulier s'il en est besoin de la révocation. Elle est responsable de la mise à jour des listes de certificats révoqués. Pour les prestations techniques, elle s'appuie sur l'Opérateur de Certification, qu'il soit interne ou externe, dont elle approuve et audite les moyens et procédures. Elle peut par ailleurs fournir des services annexes, selon la demande de chaque utilisateur et selon la gamme de certificats, comme la conservation et le recouvrement des clés, ou la publication des certificats.

Opérateur de certification (OC) :

L'Opérateur de Certification assure les prestations techniques, en particulier cryptographiques, nécessaires au processus de certification. Il est en charge du bon fonctionnement et de la sécurité des moyens informatiques et

¹ Etant 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

techniques, notamment de la publication de la liste de certificats révoqués. Il est en charge de la sécurité des personnels, des locaux et, plus généralement, du bon respect des procédures, toutes choses indispensables pour garantir un niveau de fiabilité.

Il est techniquement dépositaire de la clé privée de l'Autorité de Certification utilisée pour la signature des certificats. Une des principales missions est de la protéger contre toute compromission.

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

Autorité d'enregistrement (AE) :

L'Autorité d'Enregistrement applique des procédures d'identification des personnes physiques ou morales, 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. Ces procédures d'identification sont variables selon le niveau de confiance que l'on entend apporter à cette vérification.

L'Autorité d'Enregistrement est le lien entre l'Autorité de Certification et l'Utilisateur. Qu'elle soit ou non directement en contact physique avec l'Utilisateur, 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.

Administrateur d'Autorité d'Enregistrement (ou Administrateur) :

Personne physique représentant l'Autorité d'Enregistrement et désignée par le Client ou un Distributeur. L'Administrateur est en charge (i) de l'enregistrement et de la validation des demandes de Certificats d'Utilisateurs, (ii) de la validation le cas échéant des Certificats d'Opérateurs d'Enregistrement, (iii) de la gestion dans le temps des droits de ces derniers. et (iv) du respect des obligations du Client dans le cadre des présentes. Il est l'interlocuteur entre CERTINOMIS et les Utilisateurs.

Opérateur d'Enregistrement (ou OE) :

Personne physique à laquelle l'Administrateur a affecté des droits lui permettant de traiter les demandes d'émission de Certificats d'Utilisateur et leur cycle de vie. L'OE appliquera les procédures de la Politique de Certification ainsi que les procédures déterminées par l'AE. L'OE est sous la responsabilité de l'Administrateur.

2.2.1.1 Certificat

Certificat :

Attestation électronique signée par une AC, certifiant le lien entre une identité (entité identifiée) et une clé publique dans le cadre d'un Réseau fermé.

Elle peut être utilisée :

- dans le cadre de la signature des échanges, messages et données électroniques afin d'en garantir l'authenticité et l'intégrité ;
- dans le cadre de la confidentialité des échanges, messages et données électroniques afin d'en permettre le chiffrement. Cette fonction n'est pas assurée dans le cadre de la présente PC ;
- dans le cadre de l'authentification forte de l'Utilisateur ou de l'Entité identifiée.

2.2.1.2 Les Utilisateurs, Clients, personnes qui se fient, Réseau fermé

Utilisateur :

Personne physique titulaire du Certificat délivré par CERTINOMIS qui en est physiquement le détenteur. L'Utilisateur peut permettre l'identification d'un dispositif ou d'une application dont les données sont inscrites dans le Certificat qu'il détient.

L'Utilisateur peut être amené à transmettre son propre Certificat ou à vérifier le Certificat d'un autre Utilisateur au sein du réseau fermé.

L'Utilisateur doit respecter la notice d'utilisation du Certificat et ses obligations vis-à-vis de l'Administrateur et des Opérateurs d'Enregistrement telles que décrites dans la PC.

Client :

Personne morale, qui contracte directement ou par le biais d'un Distributeur avec CERTINOMIS pour bénéficier d'une offre de services de certification

Distributeur :

Personne morale ayant préalablement contracté avec CERTINOMIS pour distribuer les offres de services de certification au sein d'un Réseau fermé auprès de Clients

Entité identifiée:

La personne, le dispositif ou l'application dont les données d'identification sont inscrites dans le certificat.

Partie qui se fie au Certificat :

Personne qui utilise le Certificat d'un Utilisateur afin de vérifier l'authenticité de sa signature numérique. Il est expressément convenu que la Partie qui se fie doit avoir préalablement accepté les Conditions générales de services d'autorité de certification mutualisée de CERTINOMIS. A ce titre, la Partie qui se fie au Certificat est soumise aux mêmes obligations et aux mêmes responsabilités que l'Utilisateur.

La Partie qui se fie au Certificat est un Utilisateur.

Réseau fermé :

Ensemble des Utilisateurs liés juridiquement au Client échangeant des informations, messages, documents par voie électronique telles que par exemple dans le cadre d'un Intranet ou d'un extranet.

2.2.2 Politique de Certification et Déclarations des Pratiques de Certification

La Politique de Certification indique quel niveau de confiance peut être attribué à un Certificat suivant les principes énoncés. La Déclaration des Pratiques de Certification indique de quelle façon pratique on établit ce niveau de confiance.

Politique de Certification (PC) :

Ensemble de règles établissant les devoirs et responsabilités de l'Autorité de Certification, des Clients et Utilisateurs, et de toutes les composantes de l'ICP intervenant dans l'ensemble du cycle de vie d'un Certificat. Elle est librement consultable par les Clients ainsi que par tous les Utilisateurs. Définissant un cadre clair, elle permet d'établir la confiance à l'égard des certificats émis par l'Autorité de Certification, selon l'usage et la finalité recherchés. Elle permet aussi de définir les reconnaissances entre Autorités de Certification.

La Politique de Certification est de la responsabilité de l'Autorité de Certification qui l'énonce et la publie.

La Déclaration des Pratiques de Certification (DPC) :

Texte définissant les « *pratiques utilisées par une Autorité de Certification pour émettre des certificats.* »¹ et, plus largement, les pratiques de toutes les composantes de l'ICP dans l'ensemble du cycle de vie d'un certificat. Elle contient la description détaillée des services offerts et de toutes les procédures associées à la gestion du cycle de vie des certificats. Elle peut comprendre également des services spécifiques.

2.3 Identification de la politique – O.I.D. (identification alphanumérique)

Les Certificats d'Utilisateur émis par CERTINOMIS contiennent un identificateur issu d'une branche enregistrée auprès de l'AFNOR, désigné par le sigle OID qui identifie de façon biunivoque la PC. L'identification de la présente PC est la suivante 1.2.250.1.86.2.1.20

¹ extrait du document "Internet X. 509 Public Key Infrastructure Certificate and Certificate Practice Framework" :

2.4 Coordonnées de l'organisme responsable

2.4.1 Organisme responsable de la présente PC

La présente PC est établie sous la responsabilité de la société CERTINOMIS.

2.4.2 Personne Responsable

Monsieur Daniel Martin
Directeur Général
CertiNomis
20 rue Louis Armand
75015 Paris

Téléphone : (33) (0)1.58.09.80.60
Télécopieur : (33) (0)1.58.09.80.67
Courrier électronique : service.commercial@certinomis.com

2.4.3 Personne déterminant la conformité de la DPC avec la présente Politique

CERTINOMIS détermine la conformité de la DPC avec la présente PC, soit directement soit indirectement en faisant appel à des experts indépendants spécialisés dans le domaine de la sécurité et des ICP.

2.5 Rôle des composantes de l'ICP et des intervenants

2.5.1 Autorité de certification

L'AC se conformant à la présente politique a pour fonction de :

- coordonner les demandes de Certificat ;
- générer des certificats liant le nom distinctif de l'Utilisateur à leur clé publique respective ;
- garantir l'intégrité des Certificats émis ;
- révoquer sur demande les Certificats ;
- diffuser les informations relatives aux Certificats et aux autorités révoqués ;
- surveiller la stricte application la PC par les différentes composantes de l'ICP, les Clients et les Utilisateurs ;
- vérifier la légitimité des opérations effectuées par l'Administrateur ou un Opérateur autorisés par le Client dont le nom est porté dans le nom distinctif des Certificats.

et pour ce faire de mettre en œuvre les moyens techniques, humains et organisationnels nécessaires à la réalisation des prestations auxquelles elle s'engage.

L'AC doit se conformer aux exigences de la présente politique de certification et la publier. Elle se réserve le droit de diffuser un résumé ou des éléments de sa Déclaration des Pratiques de Certification conformément à l'article 8.2.

Les obligations mentionnées ci-dessus doivent être assumées par le responsable de l'AC et par le personnel de l'AC sous sa responsabilité.

2.5.1.1 Responsable de l'AC

Le responsable de l'AC se conformant à la présente politique a pour fonction de :

- gérer l'évolution de l'AC ;
- sélectionner, recruter et suivre le personnel de l'AC, suivant les règles de la Politique de Certification;
- appliquer et faire respecter les règles d'attribution des rôles et pouvoirs associés aux personnels de l'AC et aux opérateurs mandatés ;
- vérifier périodiquement le respect de la PC, et de la DPC reliées au fonctionnement de l'AC.

2.5.1.2 Intervenants requis pour la gestion de l'AC

Le responsable de l'AC se conformant à la présente politique doit attribuer à son personnel et à toute personne légalement ou contractuellement mandatée, entre autres, les fonctions suivantes:

- gérer les informations et les dossiers des Clients et Utilisateurs de l'AC ;
- planifier et pourvoir à l'évolution de l'infrastructure technologique de l'AC ;
- faire respecter les règles, principes et procédures énoncés dans la PC et la DPC, reliés au fonctionnement de l'AC ;
- gérer les autorisations, les droits, les attributs, les clés et les certificats du personnel de l'AC et des opérateurs mandatés ; et
- traiter les journaux de vérification de la sécurité de l'AC.

Le personnel de l'AC remplissant ces fonctions doit :

- connaître et respecter les règles, principes et procédures énoncés dans la PC et la DPC, reliés au fonctionnement de l'AC ;
- être désigné par le responsable de l'AC ; et
- être un employé à temps plein de l'AC, ou être un mandataire dûment et expressément autorisé par le responsable de l'AC.

2.5.2 Autorité d'Enregistrement

Le responsable de l'AC doit attribuer à une entité déterminée par le Client ou au Client directement dans un cadre contractuel les fonctions suivantes:

- coordonner les demandes d'identification électronique ;
- vérifier les caractéristiques d'identification des Utilisateurs selon le certificat envisagé ;
- distribuer à l'Utilisateur, en cas de besoin, un support physique (carte à puce, papier...) nécessaire à l'acquisition, au transport ou à l'utilisation de son Certificat ;
- gérer et protéger les données à caractère personnel et de sécurité des Utilisateurs; et
- maintenir, administrer, exploiter et protéger les machines et/ou logiciels utilisés pour remplir ces fonctions.

L'AE est conjointement placée sous la responsabilité du Client d'une part, et, d'autre part, de l'AC. L'AE applique les règles de contrôle pour l'émission et la révocation des Certificats que l'AC aura préalablement acceptées. En tout état de cause, l'AE doit contrôler la conformité entre les champs du Certificat d'Administrateur traitant de l'identification du Client/du Réseau fermé et le réseau fermé.

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 présente politique.

Les données à caractère personnel collectées par, ou pour, l'AC lors de l'enregistrement des Clients et des Utilisateurs peuvent donner lieu à l'exercice du droit d'accès et de rectification en application des dispositions de la loi n°78-13 du 6 janvier 1978 en s'adressant à l'adresse indiquée sur le site Internet de l'AC.

En tant que dépositaire des données à caractère personnel des Utilisateurs, l'AE doit respecter toutes les dispositions de la loi n°78-13 du 6 janvier 1978 et notamment son article 33.

L'AE désigne des acteurs particuliers dans le cadre de la gestion du cycle de vie des Certificats :

- **l'Administrateur** : personne physique sous la responsabilité du Client, nommé et formellement mandatée par le Client, garante des opérations d'enregistrement effectuées pour le compte du Client et responsable de l'AE. L'identification de l'Administrateur vis-à-vis de l'AC est réalisée par un certificat de classe 3 délivré par CERTINOMIS. L'Administrateur est également un Utilisateur et un Opérateur ;
- **l'Opérateur** : personne physique sous la responsabilité de l'Administrateur qui lui délègue tout ou partie de ses prérogatives pour ce qui concerne les opérations d'enregistrement et de révocation de Certificats. L'Opérateur est identifié vis-à-vis de l'AC grâce à un Certificat délivré par l'AC, à l'initiative de l'Administrateur. L'Opérateur est également un Utilisateur.

2.5.3 Opérateur de certification

L'opérateur de certification est une entité externe à l'AC qui assure pour le compte de l'AC l'ensemble des opérations techniques, y compris cryptographiques, nécessaires à la gestion du cycle de vie des Certificats qui seront remis aux Utilisateurs, selon les demandes qui lui auront été faites par l'AE. Il est techniquement dépositaire des clés privées de signature de l'AC.

L'Opérateur de certification s'engage par contrat auprès de l'AC pour mettre en œuvre et respecter des pratiques qui permettent d'assurer que les exigences de la PC et de la DPC associée et qui s'appliquent à lui sont respectées.

L'Opérateur de certification doit maintenir, administrer, exploiter et protéger les machines et logiciels utilisés par l'AC.

2.5.4 Service de publication

Il s'agit d'une entité externe mettant à la disposition de tous les Utilisateurs, Clients, Parties qui se fient la liste des certificats émis et la liste des certificats mis en opposition. L'OC assure également ce rôle.

2.5.5 Client

Il est responsable :

- de l'authenticité, de l'exactitude, et de la complétude des données d'identification de la personne morale et des personnes physiques fournies à l'AE lors de l'émission des Certificats ainsi que des qualités/attributs des Utilisateurs relevant des seules prérogatives de la personne morale ;
- d'établir et de faire respecter une politique de sécurité sur les postes informatiques utilisés pour mettre en œuvre les Certificats.

Il doit communiquer à l'AC, par les canaux que l'AC aura désignés, toute information ayant pour conséquence la révocation d'un certificat émis pour son compte.

2.5.6 Utilisateur

Il est responsable :

- de la protection, de l'intégrité et de la confidentialité de ses clés privées et des éventuelles données d'activation, liées aux certificats;
- de la sécurité de ses équipements matériels, logiciels et de ses réseaux impliqués dans l'utilisation de ses certificats;
- de l'authenticité, de l'exactitude, et de la complétude de ses données d'identification fournies à l'AE lors de l'enregistrement ; et
- de l'utilisation de ses clés et certificats au sein du Réseau fermé, qui doit être conforme à la présente Politique de Certification.

Il doit communiquer à l'AC, par les canaux qu'elle aura désignés, toute information ayant pour conséquence la révocation de son certificat.

2.5.7 Partie qui se fie

La partie qui se fie est une personne qui utilise un certificat d'un Utilisateur, régi par la présente politique, afin de vérifier au moyen de la clé publique qui y est contenue l'authenticité d'une signature électronique. La partie qui se fie doit être un Utilisateur au sein du Réseau fermé.

Avant d'accorder sa confiance au dit certificat, la Partie qui se fie doit impérativement vérifier sa validité auprès de CERTINOMIS en consultant les Listes des Certificats Révoqués appropriées les plus récentes, ainsi qu'en vérifiant sa validité intrinsèque, en particulier sa signature, et la validité de tout certificat sur l'itinéraire de confiance. A défaut de remplir cette obligation, la Partie qui se fie assume seule 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.

En outre, la responsabilité de CERTINOMIS ne saurait être engagée pour toute utilisation des Certificats en dehors du Réseau fermé.

3 DISPOSITIONS GENERALES

Ce chapitre contient des dispositions relatives aux obligations respectives de l'AC, du personnel de l'AC, des diverses entités composant l'ICP, des Clients, et des Utilisateurs. Elle contient aussi des dispositions juridiques, relatives notamment à la loi applicable et à la résolution des litiges.

3.1 Obligations

Les différentes composantes de l'ICP 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 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 et de la DPC qu'elle reconnaît ;
- 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'ICP.

3.1.1 Obligations de l'AC

L'AC garantit le lien qui existe entre un Utilisateur donné et un bi-clé au sein du Réseau fermé.

L'AC veille à ce que les AE qui agissent en son nom se conforment à toutes les modalités pertinentes de la présente Politique de Certification ainsi que tout autre document particulier négocié entre l'AE et l'AC.

L'AC veille à ce que l'OC se conforme à toutes les modalités pertinentes de la présente Politique de Certification, concernant le fonctionnement de l'OC ainsi que tout autre document particulier négocié entre l'AC et l'OC.

L'AC et le responsable de l'AC doivent se conformer 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 et Utilisateurs de certificats eu égard aux lois et règlements en vigueur.

L'AC doit informer les Utilisateurs de la révocation du certificat d'un Utilisateur ou d'une composante de l'ICP en transmettant dans les plus brefs délais la révocation du certificat auprès de l'OC qui a en charge de publier les Listes de Certificats Révoqués.

L'AC doit valider la génération des certificats, transmettre les informations concernant la révocation des certificats et procéder le cas échéant au renouvellement de ceux-ci.

Le personnel de l'AC, ainsi que l'ensemble des opérateurs mandatés, 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, et des Utilisateurs de certificats eu égard aux lois et règlements en vigueur.

3.1.2 Obligations de l'Autorité d'Enregistrement

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

L'AE doit :

- traiter les demandes de certificat en s'assurant de leur pertinence;
- vérifier les données personnelles d'identification et les données contenues dans le certificat ;
- transmettre à l'OC les demandes de génération, révocation, renouvellement des certificats qu'elle aurait traité favorablement ;
- transmettre à l'AC une trace imputable de la validité de cette vérification;
- transmettre en toute confidentialité des supports physiques ou des codes d'activation aux Utilisateurs ; et
- conserver et protéger en confidentialité et en intégrité toutes les données à caractère personnel et d'identification collectées lors des procédures d'enregistrement.

L'AE doit se soumettre à tout contrôle technique et audits de qualité des procédures que pourrait demander l'AC.

L'AE doit veiller en outre que son personnel :

- soit qualifié et formé pour exercer les rôles qui lui sont confiés ;
- connaisse et respecte les règles, principes et procédures énoncées dans la PC ou établies par elle-même ;
- soit nommément désigné par le responsable de l'AE ;
- soit salarié de l'AE ou un mandataire dûment et expressément autorisé par le responsable de l'AE.

3.1.3 Obligations spécifiques de l'Administrateur

L'Administrateur :

- Prend connaissance et se conforme aux exigences de la présente PC et des procédures internes formalisées par l'AE ;
- Se soumet aux obligations résultant de sa qualité d'Utilisateur des services de certification fournis par l'AC ;
- Assure la gestion des Opérateurs placés sous sa responsabilité telle que notamment leur désignation auprès de l'AC et la délégation de tout ou partie de ses droits ;
- Signe électroniquement les ordres transmis à l'AC par utilisation des moyens techniques mis à sa disposition ;
- Communique à l'AC, par tous moyens désignés par celle-ci, toute information ayant pour conséquence la révocation de son propre Certificat ou la révocation d'un Opérateur ;
- Demande sans délai la révocation de tout Certificat en cas de compromission avérée ou soupçonnée de la clé privée associée, au travers des moyens techniques mis à sa disposition.

3.1.4 Obligations spécifiques de l'Opérateur

L'Opérateur :

- Prend connaissance et se conforme aux exigences de la présente PC et des procédures internes formalisées par l'AE ;
- Se soumet aux obligations résultant de sa qualité d'Utilisateur des services de certification fournis par l'AC ;
- Signe électroniquement les ordres transmis à l'AC par utilisation des moyens techniques mis à sa disposition ;
- Communique à l'AC, par tous moyens désignés par celle-ci, toute information ayant pour conséquence la révocation de son propre Certificat ou la révocation d'un Opérateur ;
- Demande sans délai la révocation de tout Certificat en cas de compromission avérée ou soupçonnée de la clé privée associée, au travers des moyens techniques mis à sa disposition.

3.1.5 Obligations de l'OC

L'OC doit, en accord avec l'AC, mettre en œuvre des matériels selon les procédures qui permettent de lui rendre un service de certification à l'AC tel que toutes les exigences de la présente politique de certification et de la DPC associée soient respectées.

L'OC doit mettre en œuvre le système qui permet de générer les certificats et d'assurer la gestion de leur cycle de vie, incluant la génération des LCR et le renouvellement des certificats selon les demandes qui lui auront été transmises par l'AE.

L'OC doit se soumettre à tout contrôle technique et audits de qualité des procédures que pourrait demander l'AC.

L'OC doit :

- utiliser des ressources cryptographiques d'un niveau de sécurité compatible avec la classe de certificats émis ; et
- contrôler les accès physiques et les limiter strictement et exclusivement aux personnes dûment autorisées.

L'OC s'engage à maintenir une disponibilité de l'ensemble de ses services, en conformité avec le § 4 ci-après.

3.1.6 Obligations du service de publication

Le responsable du service de publication doit mettre à jour et préserver l'intégrité des listes (LCR) et documents qu'il publie. Il doit en outre, en prenant toutes les mesures raisonnables, maintenir la disponibilité des listes (LCR).

3.1.7 Obligations du service de recouvrement de clés de confidentialité

Aucune obligation dans le cadre de la présente politique de certification.

3.1.8 Obligations du Client

Lorsqu'il est AE, le Client doit respecter les obligations figurant aux § 3.1.2 à 3.1.4.

Le Client doit se conformer à toutes les exigences de la présente Politique de Certification et des éléments de la DPC diffusés par l'AC.

Il doit clairement spécifier au moment de la signature du contrat l'étendue exacte du Réseau fermé pour lequel il contracte.

Il garantit que les informations qu'il fournit à l'AC ou, le cas échéant, à une AE, notamment pour l'identification de l'Utilisateur, sont exactes, complètes et que les documents transmis ou présentés sont valides.

Lorsqu'il est AE, le Client doit désigner nominativement et formellement un Administrateur et (i) porte à sa connaissance les obligations et responsabilités y afférents, et (ii) lui fait souscrire un Certificat de Classe 3 auprès de CERTINOMIS.

Il fait respecter une politique de sécurité sur les postes informatiques utilisés pour mettre en œuvre les Certificats et notamment les postes informatiques des Utilisateurs.

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 client 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.

Le Client doit établir ou faire établir une convention de preuve associée à l'utilisation des Certificats et rendant opposables juridiquement à tous les Utilisateurs, membres du Réseau fermé, les documents, transactions signés à l'aide du Certificat ou les opérations d'authentification au sein du Réseau fermé.

3.1.9 Obligations de l'Utilisateur

L'Utilisateur ne doit pas utiliser le Certificat en dehors du Réseau fermé.

Il doit se conformer à toutes les exigences de la présente Politique de Certification et des éléments de la DPC diffusés par l'AC. Il doit exclusivement utiliser ses clé privée et certificat à des fins autorisées par la présente Politique de Certification, ainsi que dans le respect des lois et règlements en vigueur.

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

Il doit protéger en confidentialité et en intégrité ses clés privées, ses codes d'activation ou d'accès.

Il doit prendre toutes les mesures raisonnables pour en éviter la perte, la divulgation, la compromission, la modification ou l'utilisation non autorisée.

Il s'engage à suivre toute prescription du client en matière de politique de sécurité dans le cadre de l'usage du certificat.

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.

3.1.10 Obligations de la Partie qui se fie

La Partie qui se fie est un Utilisateur au sein du Réseau fermé.

La Partie qui se fie à un Certificat doit se conformer à toutes les exigences mentionnées dans le cadre de la présente Politique de Certification et des éléments de la DPC diffusés par l'AC émettrice du dit certificat, documents contractuels qu'il reconnaît expressément avoir lu et approuvé.

Avant toute utilisation de certificats, notamment lorsque lesdits certificats créent des effets juridiques, la Partie qui se fie doit impérativement vérifier la validité des Certificats auxquels elle entend se fier auprès de CERTINOMIS, en consultant les Listes des Certificats Révoqués appropriées les plus récentes, ainsi qu'en vérifiant sa validité intrinsèque, en particulier sa signature, et la validité de tout certificat sur l'itinéraire de confiance. A défaut de remplir cette obligation, la Partie qui se fie assume seule 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, la Partie qui se fie doit aussi vérifier que la clé publique du certificat correspond à la clé privée de signature utilisée.

La Partie qui se fie doit toujours vérifier que le certificat est utilisé à des fins pertinentes et conformément aux applications autorisées.

3.2 Responsabilités

L'AC, le personnel de l'AC, les composantes de l'ICP, les Clients et les 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.

3.2.1 **Responsabilité de l'AC et de son personnel**

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 et par la DPC associée, ainsi que par toutes autres clauses contractuelles applicables.

L'AC est responsable de tout manquement aux obligations figurant en 3.1.1.

Le personnel de l'AC et les opérateurs mandatés à qui ont été assignés des rôles spécifiques de l'ICP (responsable de l'AC, responsable de la sécurité...) sont personnellement responsables de leurs actes dont l'imputabilité est garantie par l'AC à des fins probatoires.

3.2.1.1 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, dans la DPC associée, 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 délictueux, 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, au delà des limites fixées ci-dessous, par un 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 politique, Déclaration des pratiques 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 de services conclu entre l'AC et son Client ou du contrat conclu entre le Client et un Distributeur

3.2.1.2 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 remis pour bénéficier d'un Certificat.

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 l'Utilisateur non conforme à la réglementation en vigueur relative à la protection des logiciels, quant au non-respect par l'Utilisateur des procédures de contrôle de validité des certificats et bi-clés connexe qu'elle émet lors d'une transaction, quant à l'usure normale des média informatiques de l'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 Déclaration des pratiques associées, ou dans le cadre du contrat de services conclu entre l'AC et son Client ou du contrat conclu entre le Client et une personne morale ayant préalablement contracté avec CERTINOMIS dans le cadre d'une offre de services de certification au sein d'un Réseau fermé.

3.2.1.3 Force majeure

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 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 :

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.

3.2.2 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 l'Utilisateur ou le Client..

3.2.3 Responsabilité de l'OC

La responsabilité de l'OC pourra être engagée uniquement par l'AC. Ainsi, la responsabilité de l'OC ne peut jamais être directement mise en cause par l'Utilisateur ou le Client. .

3.2.4 Responsabilité du Client

Le Client accepte toutes les responsabilités associées aux obligations telles qu'énoncées dans le cadre de la présente PC et du contrat de services conclu entre l'AC et son Client ou du contrat conclu entre le Client et un Distributeur.

3.2.5 Responsabilité de l'Utilisateur

L'Utilisateur est responsable de tout manquement aux obligations figurant en § 3.1.9 et 3.1.10.

3.3 Indépendance des parties et absence de rôle de représentation

L'émission de Certificats, conformément à la présente Politique de Certification, ne fait pas de l'AC, de l'une des composantes de l'ICP, du responsable de l'AC et du personnel de l'AC et des composantes de l'ICP 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.

En conséquence de quoi, les Clients et les 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'ICP, 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'ICP. 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.

Le fait que le nom d'un Client soit dans un certificat de signature ne constitue pas en soi un mandat spécial ou général de ce Client en faveur de l'Utilisateur.

3.4 Interprétation et mise en application

3.4.1 Droit applicable

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 être appliquées en partie en-dehors du territoire de la République française

3.4.2 Règlement des différends

En cas de contestation ou de litige, les parties décident de soumettre cette difficulté à une procédure amiable, préalablement à toute procédure devant un tribunal. A ce titre, toute partie qui souhaite mettre en jeu ladite procédure

doit notifier par lettre recommandée avec avis de réception, une telle volonté, en laissant un délai de quinze (15) jours à l'autre partie.

Les parties désignent alors un expert amiable d'un commun accord dans ledit délai de quinze (15) jours.

A défaut d'accord, compétence expresse est attribuée à M. le Président du Tribunal de Grande Instance de Paris pour effectuer une telle désignation.

L'expert amiable doit tenter de concilier les parties dans un délai de deux (2) mois à compter de sa saisine. Il propose un rapport en vue de concilier chacune des parties. Ce rapport a un caractère confidentiel et ne peut servir que dans le cadre de la procédure d'expertise amiable.

En cas de conciliation, les parties s'engagent à signer un accord transactionnel et confidentiel. Cet accord transactionnel doit expressément préciser si les présentes continuent à s'appliquer.

A défaut d'accord écrit des parties, le conciliateur établit un Procès Verbal de non-Conciliation daté et signé en trois exemplaires, dont un destiné à chaque partie au présent contrat et qu'il conserve à titre probatoire.

Les parties conviennent qu'aucune action contentieuse ne peut être valablement introduite avant que ne se soit écoulé un jour franc à compter de la date figurant sur ce PV de non-Conciliation.

L'AC doit s'assurer que tous les accords qu'elle conclut prévoient des procédures adéquates pour le règlement des différends.

3.4.3 Règlement des litiges - Tribunal compétent

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

3.4.4 Intégralité, divisibilité, survie, notification

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.

3.5 Tarifs

Les questions relatives à la tarification se retrouvent dans le contrat de services conclu entre l'AC et son Client ou dans le contrat conclu entre le Client et le Distributeur.

3.6 Publication et dépôt de documents

3.6.1 Informations publiées

La Politique de Certification, d'éventuels éléments de la DPC, les formulaires de demande de certificat, 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.com>, soit communiqués dans le cadre de la négociation commerciale avec le Client.

La DPC, qui donne, entre autres, le détail des procédures et des moyens mis en œuvre pour assurer la protection des installations de l'AC, n'est pas publiée pour des raisons de sécurité liées au besoin d'en connaître.

Toutefois, l'AC ou l'OC doit fournir, autant que de besoin, la version complète de sa DPC, lors d'une demande d'un organisme autorisé à des fins de vérification, d'audit ou de contrôle, prévues à cet effet dans la présente politique, ainsi que dans le cadre du respect de la loi.

La Liste des Certificats Révoqués est publiée par l'AC. Il en va de même si le Client demande que soient publiés les Certificats valides.

3.6.2 Fréquence de diffusion

Les Listes de Certificats Révoqués seront mises à jour au moins une fois par jour.

La publication de la Politique de Certification et des éventuels éléments de la DPC respectera les dispositions de l'article 9.2 "Procédure de publication" de la présente politique.

3.6.3 Contrôle de l'accès

La Politique de Certification et les éléments de la DPC de l'AC ne seront accessibles, pour création ou modification, qu'au seul personnel autorisé de l'AC, et ce à travers des contrôles d'accès appropriés.

Le service de publication des informations est responsable des conditions de mises en œuvre de mesures de sécurité aux fins de contrôler l'accès aux informations publiées.

3.6.4 Bases documentaires

L'AC est tenue de diffuser les informations identifiées à l'article 3.6.1. "Informations publiées". S'agissant des annuaires, l'AC peut choisir de publier elle-même ou d'utiliser les services d'une de ses composantes pour assurer le service de publication.

3.7 Contrôle de conformité

Un contrôle de conformité permet de déterminer si le comportement réel de toutes les composantes de l'ICP répond aux exigences et normes fixées dans la Déclaration des Pratiques de Certification et satisfait aux exigences de sa Politique de Certification.

Cette vérification comprend :

- l'examen de la validité du processus de vérification que l'AC a mis en place pour valider la qualité de ses services ;
- une comparaison entre les pratiques de l'AC et des composantes de l'ICP, décrites dans la DPC et la conformité à ces déclarations ; et
- une comparaison entre les pratiques de l'AC et des composantes de l'ICP et les exigences des différentes Politiques de Certification a priori supportées.

Ce contrôle de conformité est fait sur demande de l'AC elle-même, selon les conditions précisées dans la DPC.

3.8 Confidentialité des données à caractère personnel et des informations

3.8.1 Données à caractère personnel détenues par une AC

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'ICP (site de la CNIL <http://www.cnil.fr>).

En vertu de la loi, les Utilisateurs 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 agent¹, en particulier l'AE, ayant recueilli ces informations, à l'adresse électronique figurant sur le site WEB de l'AC.

L'AC doit respecter rigoureusement toutes les prescriptions légales applicables et expliquer sur son site, les modalités concrètes d'application de la loi.

La Politique de Certification doit être mise en place dans le respect des principes fondamentaux en matière de protection des données à caractère personnel consacrés dans la loi, la directive européenne 2002/58/CE et toute autre convention internationale entrée en vigueur ainsi que la doctrine de la CNIL.

Toutes les données collectées et détenues par l'AC ou une AE sur une personne physique ou morale (par exemple : procédure d'enregistrement, révocation, autres événements consignés, correspondances échangées entre l'Utilisateur

¹

et l'AC ou l'AE, etc.) sont considérées comme confidentielles et ne doivent pas être divulguées sans avoir obtenu le consentement préalable de l'Utilisateur.

3.8.2 Informations confidentielles

La clé privée de signature électronique de chaque Utilisateur doit demeurer confidentielle. En cas de divulgation par l'Utilisateur de ces informations secrètes ou de toute autre information afférente à ses clés permettant notamment leur délivrance, leur utilisation ou leur révocation, cela s'effectuera à ses propres risques et périls.

Les informations confidentielles transmises par le Client, concernant notamment les membres du Réseau fermé, demeurent confidentielles et ne peuvent être communiquées à un tiers sans l'accord express du Client ou à l'occasion d'une injonction judiciaire.

3.8.3 Données à caractère personnel contenues dans les certificats et la LCR

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

Les Listes des Certificats Révoqués ne contiennent que les numéros d'enregistrement des certificats, et leur date de révocation. Les causes de révocation des certificats sont réputées demeurer strictement confidentielles

3.9 Secret des correspondance et interceptions

Le secret des correspondances émises par voie des communications électroniques 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 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 (JO du 13 juillet 1991, rectification JO du 10 août 1991).

3.10 Droits relatifs à la propriété intellectuelle

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 1^{er} 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>

3.11 Dispositions pénales

En vertu des articles 323-1 à 323-7 du Code pénal, applicable lorsque 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

4 IDENTIFICATION ET VERIFICATION D'IDENTITE

Le présent chapitre définit les exigences en matière d'enregistrement des demandes de certificats, c'est-à-dire, des Utilisateurs et des Clients. Il définit également les exigences de vérification en matière de pouvoir, représentation et mandat pour ce qui concerne l'établissement des certificats.

4.1 Enregistrement initial

4.1.1 Types de nom

Chaque entité doit avoir un nom distinctif (DN) X.501, porté dans le champ Subject du certificat, non seulement facile à distinguer des autres noms, mais aussi unique pour une AC donnée. Ce nom doit être conforme à la partie 1 de la norme PKIX. Il doit être codé sous la forme d'une chaîne imprimable (printableString) X. 501 et ne doit pas être vide.

Chaque entité peut employer, en plus de son nom distinctif, un nom de remplacement, en utilisant pour ce faire le champ SubjectAlternateName, lequel doit être conforme à la partie 1 de la norme PKIX.

4.1.2 Règles de nommage

Les composantes de l'ICP, et en particulier l'AC, doivent toutes avoir dans leurs certificats un nom significatif qui permet de retrouver leur attache physique ainsi que la dénomination sociale de l'entité.

De même, les Certificats de l'Administrateur et les Opérateurs de l'AE doivent porter un nom significatif qui permette d'identifier de manière biunivoque les titulaires dudit Certificat.

Un demandeur de Certificats doit (i) être en mesure de prouver qu'il a le droit d'utiliser un nom en particulier et (ii) avoir le droit d'utiliser le nom qu'il souhaite y voir figurer.

L'AC s'assure que le contenu des champs de nom Subject et Issuer a un lien explicite avec l'Utilisateur.

4.1.3 Règles d'interprétation des diverses formes de noms

Aucune exigence n'est stipulée.

4.1.4 Unicité des noms

Les noms distinctifs doivent être uniques pour toutes les entités identifiées d'une AC. Il est possible d'ajouter un champ spécifique (SerialNumber) composé de nombres ou de lettres afin de garantir le caractère unique du nom distinctif.

4.1.5 Procédure de règlement des différends au sujet des noms

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, des organisations, qu'elles soient de droit public ou de droit privé, et de toutes autres entités identifiées dans le cadre des certificats signés.

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.

4.1.6 Reconnaissance, vérification et rôles des noms de marques de fabrique, de commerce et de services

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 1^{er} 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 Utilisateurs et les Clients des marques déposées, des marques notoires et des signes distinctifs, ainsi que les noms de domaine.

4.1.7 Méthode de vérification de la possession de la clé privée

L'AC doit vérifier que le demandeur est véritablement en possession de la clé privée associée à la clé publique de vérification de signature qui a été inscrite dans son certificat. Cette vérification peut être réalisée à partir d'un paquet de demande de certificat au standard PKCS #10 ou par tout autre moyen à la discrétion de l'AC.

4.1.8 Vérification de l'identité du Client

L'AE vérifie l'identification du Client, de son représentant légal et de toutes personnes désignées par ce dernier, directement ou indirectement, pour le représenter vis-à-vis de l'AC ou de l'AE.

L'AC ou l'AE doit archiver toutes les informations pertinentes relatives à cet enregistrement.

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

4.1.9 Vérification de l'identité de l'Utilisateur

Les règles de vérification d'identité de l'Utilisateur élaborées par le Client dans le cadre d'un Réseau fermé doivent avoir été soumises et acceptées expressément par CERTINOMIS.

4.2 Vérification aux fins de renouvellement des certificats

Les règles de vérification d'identité aux fins de renouvellement des Certificats élaborées par le Client dans le cadre d'un Réseau fermé doivent avoir été soumises et acceptées expressément par CERTINOMIS.

4.3 Vérification aux fins de renouvellement des clés après une révocation

Si un certificat a été révoqué, il ne peut jamais y avoir de renouvellement. Il faut procéder à la certification de nouvelles clés de la même façon que pour un enregistrement initial.

4.4 Vérification aux fins de recouvrement

Sans objet dans le cadre de la présente PC.

4.5 Vérification aux fins de révocation

Seuls le Client, l'Utilisateur et l'AC peuvent demander la révocation d'un certificat.

Les règles de vérification d'identité aux fins de révocation des Certificats élaborées par le Client ou par le Distributeur dans le cadre d'un Réseau fermé doivent avoir été soumises et acceptées expressément par CERTINOMIS.

L'AC doit s'assurer du bon droit de la personne qui fait une demande de révocation. Elle établit la validité de la demande soit au moyen d'une signature électronique valide reconnue par l'AC, soit de toute autre façon non équivoque.

5 EXIGENCES OPERATIONNELLES EN MATIERE DE GESTION DES CERTIFICATS

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

5.1 Demande de certificat

L'AC doit s'assurer que toutes les procédures et les exigences concernant une demande de certificat sont dûment consignées et publiées par l'AE. Les demandeurs d'identification électronique doivent suivre et respecter les procédures publiées.

Les informations suivantes doivent au moins figurer dans la demande de certificat :

- les informations qui seront inscrites dans le nom distinctif (DN) du Certificat ;
- la clé publique à certifier (lorsqu'elle est générée par le demandeur) ; et
- la preuve de possession de la clé privée correspondante.

5.2 Emission et distribution d'un certificat

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

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

A la réception d'une demande de certificat émise par l'AE, l'AC, ou l'OC pour la partie technique de ces obligations, doit :

- s'assurer que la demande a bien été prise en compte par une AE qu'elle a reconnue et que ladite AE a traité la demande et fourni une trace imputable de sa demande de certificat ;
- générer et signer le Certificat ;
- notifier à l'Utilisateur ou au Client, suivant le schéma retenu, la mise à disposition de son certificat et lui fournir l'ensemble des procédures à suivre pour être en mesure de l'obtenir et de l'utiliser en cas d'acceptation ; et
- mettre le Certificat à disposition de l'Utilisateur, c'est-à-dire rendre accessible par des moyens physiques ou logiques les informations permettant l'obtention du Certificat.

5.3 Acceptation du certificat

Les informations nécessaires à l'obtention du certificat étant mises à la disposition de l'Utilisateur, le fait que ce dernier procède à son retrait vaut, de sa part, acceptation du Certificat dans les conditions commerciales, juridiques et techniques définies par l'AC.

En acceptant un Certificat, l'Utilisateur 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.

Un certificat n'est réputé valide que lorsqu'il a été accepté.

5.4 Recouvrement de clés de confidentialité

Sans objet dans le cadre de la présente PC.

5.5 Suspension et révocation d'un certificat

5.5.1 Motifs de révocation

La connaissance de la compromission avérée ou soupçonnée de la clé privée par le client ou l'Utilisateur emporte obligation pour ces derniers 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 effectuée.

La connaissance de la modification d'une information contenue dans le certificat par le Client ou l'Utilisateur emporte obligation pour ces derniers de procéder sans délais à la vérification de sa révocation et de la demander dans les plus brefs délais si celle-ci n'a pas été faite.

Outre les cas de révocation de certificats mentionnés plus haut, l'AC peut révoquer le certificat de l'Utilisateur dès lors qu'elle est en possession d'informations de nature à indiquer que la situation de l'Utilisateur a subi des modifications qui ne lui ont pas été transmises par celui-ci, ou qu'elle a des soupçons graves quant à la compromission de la clé privée de l'Utilisateur. Plus généralement, l'AC peut, à sa discrétion, révoquer le certificat d'un Utilisateur lorsque le client ne respecte pas les obligations énoncées dans la présente politique de certification et dans tous documents contractuels ainsi que dans toute loi et règlement applicable.

5.5.2 Personne pouvant demander une révocation

Seuls peuvent demander la révocation d'un certificat :

- l'Utilisateur, responsable du certificat, en s'adressant à l'AE dont il dépend ;
- l'Administrateur et les Opérateurs de l'AE ;
- le personnel de l'AC émettrice ; ou
- toute personne dûment habilitée de l'AE qui a enregistré la demande du Utilisateur.

5.5.3 Procédure de demande de révocation d'un certificat

L'AC doit s'assurer que le Client consigne et publie toutes les procédures et exigences relatives aux demandes de révocation d'un Certificat.

L'AC met à disposition un moyen d'accès rapide, électronique ou téléphonique, au service de révocation qui authentifiera la demande dans des conditions fixées au Chapitre 4. Ce service de révocation pourra être assuré directement par l'AC ou par une AE reconnue par l'AC.

La demande de révocation doit contenir les informations d'identification du certificat à révoquer. La demande peut également contenir la description détaillée des causes de la révocation, et, éventuellement, les justificatifs de cette cause.

Si la procédure de demande de révocation d'un certificat se déroule correctement, la révocation est déclenchée. L'ensemble des opérations et des mesures prises par l'AC doit être consigné et sauvegardé.

Quelle que soit la cause ayant entraîné la révocation d'un certificat de l'Utilisateur, l'Utilisateur et le Client doivent toujours être informés par une notification de la révocation du certificat de l'Utilisateur. Cette notification doit indiquer la date à laquelle la révocation du certificat a pris effet.

Elle peut prendre la forme d'un courrier électronique.

5.5.4 Temps de traitement d'une révocation

La prise en compte des demandes de révocation par le service de révocation de l'AC doit être effective au moins pendant les heures ouvrées et si possible 24h/24 et 7j/7.

La procédure relative à la prise en compte des demandes de révocation par l'AE élaborées par le Client doit avoir été soumise et acceptée expressément par CERTINOMIS.

Si la demande comporte toutes les informations nécessaires à l'authentification du demandeur et si les motifs correspondent à l'un des motifs décrits au 5.5.1, alors la révocation doit être effectuée dans les plus brefs délais.

5.5.5 Motifs de suspension

Le service de suspension de certificats n'est pas assuré dans le cadre de la présente PC.

5.5.6 Personne pouvant demander une suspension

Sans objet.

5.5.7 Procédure de demande de suspension d'un certificat

Sans objet.

5.5.8 Limites d'une période de suspension

Sans objet.

5.5.9 Fréquence de publication de la liste des certificats révoqués (LCR)

L'AC émettrice doit publier la révocation d'un certificat dans le cadre d'une LCR au plus tard 24 heures après validation de la demande de révocation de certificat.

5.5.10 Exigences de vérification des LCR

Avant toute utilisation de Certificats, notamment lorsque les dits Certificats créent des effets juridiques, la Partie qui se fie à un Certificat donné doit impérativement vérifier la validité des certificats auxquels elle entend se fier auprès de CertiNomis, en consultant les Listes des Certificats Révoqués valides les plus récentes ainsi qu'en contrôlant la validité intrinsèque du Certificat, en particulier sa signature, et la validité du Certificat de l'émetteur.

La validité d'une LCR est contrôlée par vérification de sa signature et vérification de la validité du Certificat de l'émetteur.

5.5.11 Publication des motifs de révocation

La procédure de divulgation des motifs de la révocation d'un certificat donné, élaborée par le Client dans le cadre d'un Réseau fermé doit avoir été soumise et acceptée expressément par CERTINOMIS.

Dans le cadre des audits et contrôles auxquels l'AC ou l'AE 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, sans préjudice des dispositions relevant du secret professionnel auquel l'AE pourrait être soumise.

5.5.12 Exigences spéciales concernant la compromission des clés

En cas de compromission avérée ou soupçonnée de la clé privée de signature d'une AC, l'OC doit s'en tarder en aviser l'AC qui lui a confiée sa clé privée de signature.

En cas de compromission avérée ou soupçonnée de la clé privée de signature d'une AC, l'AC doit sans tarder en aviser ses Clients ainsi que les Distributeurs dans le cadre d'un Réseau fermé.

La connaissance de la compromission avérée ou soupçonnée de la clé privée, par le client ou l'Utilisateur 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.

5.6 Journalisation des événements

5.6.1 Types d'événements consignés

L'OC et l'AE doivent consigner dans les registres de vérification et pour le compte de l'AC tous les événements ayant trait à la sécurité de son système, notamment :

- démarrage et arrêt du système ;
- démarrage et arrêt de l'application de l'AC ;
- tentatives de créer, d'extraire, d'établir, ou de modifier les privilèges ;
- changements des caractéristiques et (ou) des clés de l'AC ;
- changements aux politiques de création des certificats, p. ex., période de validité ;
- tentatives d'ouverture et de fermeture de session ;
- tentatives autorisées ou non d'accès par réseau au système de l'AC ou de l'OC ;
- tentatives autorisées ou non d'accès aux fichiers système ;
- génération des clés de l'AC et des clés des entités subalternes ;
- création et révocation de certificats ;
- tentatives d'initialiser, d'extraire, de valider et d'invalider des Utilisateurs, et de récupérer leurs clés

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

L'OC doit aussi recueillir et colliger, par des moyens électroniques ou papier, de l'information sur la sécurité qui n'est pas produite par le système de l'OC, notamment :

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

La DPC détaille le type d'information qu'il faut consigner.

Afin de faciliter le processus décisionnel, toutes les ententes et toute la correspondance touchant les services de l'AC doivent être recueillies et colligées par des moyens électroniques ou manuels, et regroupées en un seul et même endroit.

5.6.2 Fréquence de traitement des journaux d'événements

L'OC et l'AE doivent s'assurer pour le compte de l'AC que ses journaux sont revus par son personnel de manière périodique, comme indiqué dans la DPC, et que tous les éléments importants font l'objet d'un compte-rendu. A cette fin, on doit notamment vérifier si la liste a été falsifiée, et on doit vérifier brièvement toutes les entrées et, plus en détail, les mises en garde et les irrégularités. On doit comparer les listes papiers et électroniques connexes de l'OC et de l'AE si une mesure est considérée suspecte.

Les mesures prises à la suite de ces examens doivent être dûment documentées par l'AE et l'OC.

5.6.3 Période de conservation des journaux

L'OC et l'AE conservent (en les rendant accessibles dès première demande) les journaux pendant au moins un mois et ensuite les archiver conformément aux instructions indiquées à l'article 5.7.

5.6.4 Protection des journaux

Le système des journaux électroniques touchant directement les opérations de certification doit comprendre 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 doit également être protégée contre les tentatives non autorisées de modification et de destruction.

5.6.5 Procédures de sauvegarde des journaux

Les journaux doivent être sauvegardés, ou copiés s'ils sont sur support papier.

5.6.6 Système de collecte des journaux

L'OC doit indiquer quels systèmes il utilise pour recueillir les données de vérification.

5.6.7 Imputabilité

Tous les types d'événements, et leur contenu, consignés par le système de collecte des données de vérification sont communiqués à la personne et/ou l'organisation qui en est la cause.

Cette personne ou cette organisation reconnaît de facto être responsable des événements dont ils sont la cause.

5.6.8 Evaluations de la vulnérabilité

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

5.7 Sauvegarde et archivage

Les Certificats ainsi que les LCR publiées par l'AC, sont conservés pendant au moins dix (10) ans après l'expiration des clés associées.

Toutes les informations liées à la gestion du cycle de vie des Certificats, telles que notamment les données d'enregistrement collectées par l'AE ainsi que les configurations et applications pour cette gestion, sont conservées par les composantes de l'ICP (AC, OC, AE) pour les informations dont elles sont dépositaires pendant au moins dix (10) ans, sauf obligation légale particulière.

Une copie de toutes les données informatiques archivées ou sauvegardées doit être protégée soit par des mesures de sécurité physique seulement, soit par une combinaison de mesures physiques et cryptographiques. Tout site d'archivage doit protéger adéquatement le matériel contre les dangers naturels, par exemple les excès de température, d'humidité et de magnétisme.

Outre les données papier sus-mentionnées, présentes par exemple dans les dossiers d'enregistrement, sont aussi conservées, sous forme papier et électronique, et ce pour une durée de dix (10) 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'ICP.

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.

5.8 Renouvellement des clés

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 associées.

5.9 Compromission et mesures anti-sinistre

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

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

5.9.1 Corruption des ressources informatiques, des logiciels et (ou) des données

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

L'OC, en accord avec l'AC, doit établir des procédures visant à assurer le maintien des activités et décrire, 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 doit s'assurer 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'OC, en accord avec l'AC, doit également envisager un plan de secours et de redémarrage de ses activités.

5.9.2 Révocation de la clé publique d'une composante de l'ICP

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

- Les Clients;
- Les AE ; et
- Tous les Utilisateurs.

En outre, l'OC, après transmission de l'information par l'AC, doit :

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

Après avoir corrigé les problèmes ayant motivé la révocation, l'OC peut, après transmission de l'information par l'AC :

- produire un nouveau bi-clé de signature et publier les certificats y 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'article 5.5. trouve à s'appliquer.

5.9.3 Compromission de la clé privée d'une composante de l'ICP

En cas de compromission de la clé de signature électronique d'une AC, celle-ci doit, avant de redéfinir un certificat au sein de l'ICP, révoquer sa clé publique et, dans ce cas, l'article 5.9.2 s'applique.

La connaissance de la compromission avérée ou soupçonnée de la clé privée par un membre d'une composante de l'ICP 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 effectuée.

5.9.4 Sécurisation d'une installation après une catastrophe naturelle ou un autre sinistre

L'OC, l'AE et l'AC doivent définir 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 veille qu'il soit précisé, dans tous contrats qui auraient été conclus avec l'OC et l'AE, qu'un plan anti-sinistre doit être mis en place et documenté par le dépositaire.

5.10 Fin des activités d'une AC

Si l'AC interrompt ses activités, elle doit dans les plus brefs délais en aviser ses Utilisateurs et ses Clients, et prendre toutes les dispositions nécessaires pour que les clés et l'information de l'AC continuent d'être archivées.

Dans le cas où une composante de l'ICP autre que l'AC interrompt ses activités, l'AC doit reprendre à sa charge ou faire porter sur une autre entité les obligations de cette composante.

Les archives de l'AC doivent être conservées selon les indications et la période stipulées à l'article 5.7.

6 MESURES DE SECURITE PHYSIQUE, DES PROCEDURES ET DU PERSONNEL

Le présent chapitre définit l'ensemble des mesures de sécurité physique, des procédures et des mesures relatives au personnel applicables en vertu de la présente politique.

6.1 Mécanismes de contrôle de la sécurité physique des locaux de l'OC

Les locaux techniques de l'OC, qui accueillent les moyens de certification et notamment sa clé privée de signature, doivent être fortement protégés. Ils doivent être dans une zone à accès contrôlé, protégée contre tous les risques courants (tels que l'incendie et l'inondation).

Le niveau de protection des locaux techniques de l'OC 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

6.2 Mesures de contrôle de la sécurité des procédures

6.2.1 Rôles de confiance

Les accès physiques et logiques aux logiciels et aux moyens seront répartis aux membres du personnel selon les rôles qui leur auront été attribués par le responsable de l'AC.

6.2.1.1 Rôles de confiance de l'AC

Le responsable de l'AC autrement appelé responsable d'application, s'assure de la mise en œuvre de la présente PC et de la DPC qui la supporte. Entre autres, il a la responsabilité de prévoir que les tâches liées aux fonctions essentielles sont réparties entre plusieurs personnes afin d'éviter qu'une personne seule soit en mesure d'utiliser avec malveillance le système de l'AC sans se faire repérer. Chaque Opérateur a accès au système seulement pour les tâches qui lui incombent.

6.2.1.2 Rôles de confiance de l'AE

L'AC doit s'assurer que les membres du personnel des AE, notamment l'Administrateur et les Opérateurs, comprennent les responsabilités qui leur incombent en ce qui touche l'identification et l'authentification des Utilisateurs éventuels et qu'ils remplissent les fonctions suivantes :

- accepter ou refuser les demandes d'enregistrement, de changement et de révocation des certificats ;
- vérifier l'identité et les autorisations des requérants ;
- transmettre l'information sur le requérant à l'AC ; et
- transmettre en les protégeant en confidentialité des supports physiques ou des codes d'activation aux Utilisateurs ;

6.2.1.3 Rôles de confiance de l'OC

Les accès physiques et logiques aux logiciels et aux moyens sont répartis entre les membres du personnel de l'OC en fonction des rôles qui leurs sont attribués par le responsable de l'OC.

L'opérateur d'administration a pour tâches :

- de configurer et maintenir les équipements et les logiciels du système de l'AC, à l'exclusion de ceux placés sous la responsabilité de l'opérateur de cryptographie ;

- de gérer les droits sur le système (à l'exclusion de ceux placés sous la responsabilité de l'opérateur de cryptographie) ;
- de mettre en marche et arrêter les services de l'AC (à l'exclusion de ceux placés sous la responsabilité de l'opérateur de cryptographie) ;
- de vérifier les journaux (à l'exclusion de ceux placés sous la responsabilité de l'opérateur de cryptographie) ;
- d'assurer le fonctionnement courant du système de l'AC ;
- d'effectuer les sauvegardes du système de l'AC ;

L'opérateur de cryptographie a pour tâches :

- de procéder à l'initialisation du (des) coffret(s) cryptographique(s) de l'AC ;
- de mettre en marche et d'arrêter le(s) coffret(s) cryptographique(s) de l'AC ;
- de configurer et maintenir le(s) moyen(s) cryptographique(s) supportant l'activité de certification de l'AC ;
- de vérifier des journaux sécurisés.

L'opérateur d'exploitation a pour tâches :

- de contrôler le déroulement des processus de gestion du cycle de vie des Certificats ;
- de vérifier l'identification des demandeurs ;
- après réception de la demande validée par l'émission et la révocation d'un Certificat ;
- d'accéder aux données du système pour répondre aux demandes.

Certaines opérations très sensibles nécessitent plusieurs intervenants ayant des rôles distincts.

6.2.2 Nombre de personnes requises par tâche

Le contrôle multi-opérateurs (c'est-à-dire par au moins deux opérateurs) est requis pour la production des clés de l'AC.

Toutes les autres tâches associées aux rôles de l'AC peuvent être effectuées par une même personne.

6.2.3 Identification et vérification pour chacun des rôles

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

- que leur nom soit ajouté à la liste d'accès aux locaux de l'AC, de l'OC et de l'AE ; 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'ICP, 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) :

- doit être 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.

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

6.3 Mesures de contrôle du personnel

6.3.1 Antécédents professionnel, qualités, expériences

Les responsables de l'AC, de l'AE et de l'OC doivent s'assurer 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 ou de l'OC :

- 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 ;

- 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 Utilisateurs ; une clause de confidentialité doit être expressément inscrite dans les contrats de travail des membres du personnel de l'AC ;
- n'ont pas d'engagements ou de liens qui risquent de causer un conflit d'intérêt avec les tâches qui leur incombent à l'égard de l'AC ou de l'AE.

6.3.2 Procédures de vérification des antécédents

Toutes les vérifications des antécédents doivent être faites conformément à la politique de l'AC, de l'OC et de l'AE en matière de sécurité.

Chaque entité opérant une composante de l'ICP met en œuvre les moyens légaux dont elle dispose pour s'assurer de l'honnêteté des personnels amenés à travailler au sein de la composante. Cette vérification est basée sur un contrôle des antécédents de la personne, il est notamment vérifié que chaque personne n'a pas fait l'objet de condamnation de justice en contradiction avec leurs attributions.

Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.

Ces vérifications sont menées préalablement à l'affectation d'un rôle de confiance et revues régulièrement (au minimum tous les 3 ans)..

L'AC, l'OC et l'AE peuvent aussi, de manière discrétionnaire, vérifier que les postulants bénéficient d'un niveau de solvabilité garanti par un établissement bancaire.

6.3.2.1 Vérification des qualifications professionnelles

Les responsables de l'AC, de l'AE et de l'OC doivent procéder à l'égard des postulants à un emploi auprès de l'AC de l'AE ou de l'OC, à la vérification des niveaux d'études exigés, des programmes de formation professionnelle requis et de toutes autres qualifications pertinentes.

6.3.2.2 Vérification de l'expérience

Aucune exigence autre que la vérification des antécédents professionnels.

6.3.2.3 Obligations du personnel de l'AC, de l'AE et de l'OC

Le personnel de l'AC doit attester ne plus avoir aucune attache, notamment juridique ou financière, avec des sociétés ayant des activités concurrentes à celles de l'AC.

Une obligation identique est portée à la charge du personnel de l'OC et de l'AE.

6.3.3 Exigences en matière de formation

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

- les principes de fonctionnement et les mécanismes de sécurité de l'AC.

Le personnel de l'AC doit suivre 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'ICP ;
- 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.

Des obligations identiques sont portées à la charge de l'OC.

L'AC assure la formation initiale du personnel de l'AE. Le programme de formation dispensée porte sur :

- l'application informatique de gestion du cycle de vie des Certificats mise à la disposition du Client par l'AC ;
- toutes les tâches qu'il devra accomplir dans le cadre de la gestion du cycle de vie des Certificats ;

- le matériel et les systèmes d'exploitation du Client formant l'environnement opérationnel du Client.

6.3.4 Formation professionnelle – fréquence et exigences

Les exigences décrites à l'article 6.3.3 doivent être tenues à jour afin de refléter les changements apportés au système de l'AC. Des cours de formation professionnelle doivent être offerts en fonction des besoins, et l'AC doit revoir ses exigences au moins une fois par an.

Des obligations identiques sont portées à la charge de l'OC, de l'AE et de leur personnel.

6.3.5 Rotation des emplois

Aucune exigence particulière.

6.3.6 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, l'AC peut lui interdire l'accès au système et prendre toutes sanctions disciplinaires adéquates.

Des obligations identiques sont portées à la charge de l'OC et de l'AE.

6.3.7 Contrôle des personnels des entreprises cocontractantes

L'AC doit s'assurer que les personnels des entreprises cocontractantes peuvent accéder à ses locaux conformément aux indications de l'article 6.1.1.

Les exigences relatives au personnel des entreprises cocontractantes sont identiques à celles relatives aux employés, en particulier à celles décrites aux articles 6.3, 6.3.2 et 6.3.6.

Des obligations identiques sont portées à la charge de l'OC et de l'AE.

6.3.8 Documentation fournie au personnel

L'AC doit mettre à la disposition des membres du personnel de l'AC, de l'OC 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 doit avoir accès à des manuels complémentaires relatifs à leurs responsabilités. Ces manuels doivent porter sur l'ensemble des procédures en vigueur.

Des obligations identiques sont portées à la charge de l'OC, de l'AE et de son personnel.

7 MESURES TECHNIQUES DE SECURITE

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

7.1 Production et installation des bi-clés

7.1.1 Production des bi-clés

Les clés privées associées aux certificats des Utilisateurs doivent être produites, conservées et utilisées exclusivement sur des moyens cryptographiques approuvés par l'AC.

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. Les fonctions de confidentialité ne sont pas retenues dans la présente PC.

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

Un bi-clé de signature électronique doit être produit par l'Utilisateur, sauf exception contractuellement prévue entre l'AC et le Client ou tout Distributeur dans le cadre d'un Réseau fermé. La procédure devra dans ce dernier cas être parfaitement détaillée.

7.1.2 Remise de la clé publique à l'AC

La clé publique d'un Utilisateur doit être remise à l'AC sous la forme d'une requête attestant de la possession de la clé privée correspondante. La transmission doit assurer l'intégrité de bout en bout.

7.1.3 Remise de la clé publique de l'AC aux utilisateurs

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

7.1.4 Tailles des clés asymétriques

Les bi-clés d'une AC dont la durée de validité est supérieure à 4 ans sont d'une longueur au moins égale à 2048 bits pour l'algorithme RSA.

Les bi-clés d'une AC dont la durée de validité est inférieure ou égale à 4 ans sont d'une longueur au moins égale à 1024 bits pour l'algorithme RSA.

Les bi-clés des entités identifiées sont d'une longueur au moins égale à 1024 bits pour l'algorithme RSA et, si possible, de 2048 bits. En particulier, tous les opérateurs de l'AC ont des certificats avec un bi-clé d'au moins 1024 bits.

7.1.5 Production des paramètres des clés publiques

Le moyen de génération de bi-clé doit utiliser des paramètres respectant les normes internationales de sécurité propres à l'algorithme considéré.

7.1.6 Vérification de la qualité des paramètres

Le contrôle qualité des paramètres des clés doit être effectué en conformité avec l'article 7.1.5.

7.1.7 Nature de la ressource de production de clés

Les bi-clés de l'AC doivent être produits par un module cryptographique matériel.

7.1.8 Utilisation de la clé publique

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).

7.1.8.1 Clé publique de vérification de signature

Une clé publique de vérification peut être utilisée à des fins d'identification, d'authentification, de non-répudiation et/ou d'intégrité. La clé publique de vérification de l'AC est la seule clé utilisable pour vérifier la signature des Certificats.

Le champ KeyUsage du certificat doit être utilisé conformément au profil des certificats. Ce champ doit comporter l'une des valeurs suivantes :

- pour les certificats des Utilisateurs : digitalSignature et/ou nonRepudiation
- pour les certificats de l'AC : keyCertSign et/ou cRLSign

7.2 Protection des clés privées

L'Utilisateur doit protéger ses clés privées afin qu'elles ne soient pas divulguées. Il lui appartiendra de s'assurer qu'une maintenance particulière est réalisée sur le poste utilisé ; en particulier de la stabilité du système, de l'absence de virus, vers et chevaux de Troie. Il lui appartient également de choisir le matériel et les logiciels offrant une sécurité suffisante pour la protection et l'utilisation de ses clés privées conformément aux dispositions du présent chapitre 7.

7.2.1 Normes relatives au calculateur cryptographique

La ressource cryptographique matérielle de l'AC doit être évaluable au niveau EAL 4+ selon les Critères Communs.

7.2.2 Contrôle des clés privées par plusieurs personnes

Plusieurs personnes doivent contrôler les opérations de production des clés de l'AC. Les données utilisées pour leur création doivent être partagées par plusieurs personnes. Le partage du secret permettant la génération ou la re-génération de la clé de l'AC doit être fait entre trois (3) personnes au minimum.

7.2.3 Recouvrement des clés privées

Ce service n'est pas proposé par l'AC dans le cadre de la présente PC.

7.2.4 Sauvegarde des clés privées

L'AC tolère qu'un Utilisateur puisse sauvegarder ses propres clés de signature électronique sous certaines conditions. Les clés sauvegardées doivent alors 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.

7.2.5 Archivage des clés privées

Les mesures et les contraintes relatives à l'archivage des clés privées sont identiques à celles qui sont prises en matière de sauvegarde (article 7.2.4.).

7.2.6 Initialisation et conservation d'une clé privée dans un module cryptographique

La procédure de mise à la clé et la procédure de mise sous contrôle des secrets sont spécifiées comme suit :

- Les clés privées de l'AC sont générées dans le module cryptographique en utilisant des données fixes ou aléatoires introduites depuis l'extérieur ; elles sont conservées chiffrées, n'étant en clair qu'au moment requis pour leur utilisation.
- Les clés privées des Utilisateur sont tant que possible générées par un moyen local.

7.2.7 Méthode d'activation de la clé privée

L'Utilisateur doit être identifié avant que la clé privée ne soit activée. Cette authentification peut se faire sous forme de données d'activation (d'un mot de passe ou NIP). Une fois désactivées, les clés privées doivent être conservées tant que possible sous une forme chiffrée.

7.2.8 Méthode de désactivation des clés privées

Lorsque les clés sont désactivées, on doit les effacer de la mémoire. Après un délai d'inactivité prolongé, la clé privée doit être désactivée.

L'Utilisateur ne doit jamais quitter son poste de travail en le laissant dans un état qui permet d'utiliser sa clé privée sans utiliser un secret approprié.

7.2.9 Méthode de destruction des clés privées

Lorsque le certificat de signature électronique arrive à expiration ou s'il est révoqué, la clé privée ne peut plus servir à aucune opération et doit être détruite.

Lorsque l'AC doit détruire sa clé privée, elle doit réinitialiser le module cryptographique, ce qui implique la réécriture complète de toute forme de mémoire dans le module cryptographique. Elle doit aussi détruire 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.

7.3 Autres aspects de la gestion des bi-clés

7.3.1 Archivage des clés publiques

L'AC émettrice doit archiver ou faire archiver toutes les clés publiques de vérification conformément à l'article 5.7.

7.3.2 Périodes d'utilisation des clés publiques et privées

La période de validité de toutes les clés de 1024 bits est d'au plus quatre (4) ans.

La période de validité des clés 2048 bits est d'au plus douze (12) ans.

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

7.4 Données d'activation

7.4.1 Génération et installation des données d'activation

Les données d'activation doivent être aléatoires ou choisies par l'Utilisateur qui prendra soin de les rendre imprévisibles. Les mécanismes cryptographiques et de contrôle de l'accès utilisant ces données doivent être suffisamment robustes pour protéger les clés et les données elles-mêmes.

Si un mot de passe ou un Numéro d'Identification Personnel (NIP) est utilisé, l'Utilisateur doit avoir la possibilité de le modifier. Le mot de passe ou le NIP doit être changé régulièrement et au minimum après une centaine d'utilisation.

7.4.2 Protection des données d'activation

Les données d'activation doivent être protégées en intégrité et en confidentialité.

Si on utilise un système de mots de passe réutilisables, il faut prévoir un mécanisme permettant de bloquer temporairement le compte après un nombre limité et fixé au préalable de tentatives. Cette mesure de protection est obligatoire pour les systèmes de l'AC.

7.4.3 Autres aspects touchant les données d'activation

L'utilisation de mot de passe ou de NIP requiert une longueur d'au moins huit (8) caractères et, dans le cas d'un mot de passe, la présence de chiffres et de lettres.

7.5 Mécanismes de sécurité informatique des postes de travail

7.5.1 Sécurité informatique – Exigences techniques spécifiques

Les systèmes de l'AC doivent offrir les fonctions suivantes, selon le rôle imparti à l'opérateur :

- contrôle de l'accès aux services de l'AC ;
- 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 pour le fonctionnement du système d'AC ;
- 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'AC et des mécanismes de protection physique.

L'interface entre l'OC et l'AC doit également être sécurisé pour éviter toute altération ou intrusion pendant la transmission des données entre les deux.

7.5.2 Indice de sécurité informatique

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

7.6 Contrôle technique du système durant son cycle de vie

7.6.1 Contrôle des développements des systèmes

L'implémentation d'un système permettant de mettre en œuvre les composantes de l'ICP doit être documentée et respecter 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, doivent être documentées et contrôlées.

7.6.2 Contrôle de la gestion de la sécurité

Une méthode de gestion de la configuration doit être appliquée 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 doit fournir 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 doit prévoir un mécanisme permettant de vérifier périodiquement l'intégrité des logiciels.

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

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

7.7 Mécanismes de contrôle de la sécurité réseau

Les systèmes de l'AC doivent être protégés contre les attaques provenant de tout réseau, en particulier les réseaux ouverts. Une telle protection doit être 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'AC.

Les protocoles et commandes sont définis dans la DPC.

7.8 Mécanismes de contrôle technique du module cryptographique

Les modules de cryptographie utilisés par l'AC doivent suivre les recommandations de la Direction Centrale de la Sécurité des Systèmes d'Information (DCSSI) du SGDN.

8 FORME ET CONTENU DES CERTIFICATS ET DES LISTES DE REVOCATION

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 format précis des certificats et LCR est donné dans la DPC.

8.1 Forme et contenu des certificats

Selon la version 3 de la norme X.509 des certificats, les champs suivants doivent être 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 8.1.2.

8.1.1 Signature du certificat

L'AC doit apposer un sceau sur le certificat avec sa clé privée. Ce sceau est le résultat d'une fonction mathématique appliquée sur l'ensemble des champs décrits à l'article 8.1.

Le Certificat dans sa forme identifiée est l'ensemble des éléments suivants :

- *tbsCertificate* : l'ensemble des champs décrits à l'article 8.1 ;
- *signatureAlgorithm* : l'identifiant de l'algorithme utilisé pour produire le sceau d'intégrité du Certificat ; et
- *signatureValue* : le résultat de cet algorithme sur l'ensemble des champs de *tbsCertificate*.

8.1.2 Champs d'extensions

L'AC doit supporter des sous-ensembles d'extensions normalisées et identifiés dans la sous section 5.2 du document de l'IETF : PKIX X.509 Certificate and CRL.

Les extensions permettent d'ajouter des informations sur l'utilisateur, l'AC émettrice, l'usage du certificat et sur les Listes de Certificats Révoqués.

8.1.3 Interprétation sémantique des champs critiques

Les champs critiques seront interprétés selon le document de l'IETF : PKIX X.509 Certificate and CRL.

8.2 Formes et contenu des Listes de Certificats Révoqués

Les LCR doivent contenir les champs de base tels que spécifiés dans la recommandation X 509 CRL V2.

Ces champs sont les suivants :

- version : version de la liste de certificats révoqués X.509.
- signature : identifiant de l'algorithme de signature de l'AC
- issuer : nom de l'AC émettrice
- thisUpdate : date d'émission de cette LCR
- nextUpdate : date limite d'émission de la prochaine LCR
- revokedCertificates : liste d'enregistrement de révocation
 - userCertificate : numéro de série unique du certificat révoqué
 - revocationDate : date de la révocation
 - crlEntryExtensions : extensions propres à cette révocation (motif de révocation, comportement souhaitable face à cette révocation...)
- crlExtensions : extensions générales de la LCR

La LCR dans sa forme finale est l'ensemble des éléments suivants :

- *tbsCertList* : l'ensemble des champs décrits ci-dessus à l'article 7.2 ;

- *signatureAlgorithm* : l'identifiant de l'algorithme utilisé pour produire le sceau d'intégrité de la liste; et
- *signatureValue* : le résultat de cet algorithme sur l'ensemble des champs de *tbsCertList*.

Le détail des champs est précisé dans la DPC.

9 ADMINISTRATION DE LA POLITIQUE DE CERTIFICATION

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

9.1 Procédures de modifications

9.1.1 Délais de préavis

Le responsable de l'AC doit donner un préavis de trente (30) jours aux Clients et Utilisateurs avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, ont un impact majeur sur eux.

Le responsable de l'AC doit donner un préavis de quinze (15) jours aux Clients et Utilisateurs avant de procéder à tout changement de la présente politique qui, selon l'évaluation du responsable de la politique, ont un impact mineur sur eux.

Le responsable de l'AC doit donner un préavis aux Clients et 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.

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

9.1.2 Forme de diffusion des avis

Dans les cas nécessitant un préavis, le responsable de l'AC doit aviser les Clients, les Utilisateurs, des modifications apportées à la politique, en diffusant les changements sur le site de l'AC et par message électronique.

Lorsque l'avis est à destination des Utilisateurs et des Clients, le préavis est communiqué par message électronique si les changements ont un impact majeur, et diffusé sur le site de l'AC et du responsable de la présente politique dans tous les autres cas.

9.1.3 Période de commentaires

Les personnes désirant se prononcer sur les modifications doivent faire parvenir leurs commentaires au responsable de la politique dans des délais inférieurs à la moitié des délais de préavis fixés à l'article 9.1.1.

9.1.4 Traitement des commentaires

Aucune exigence particulière.

9.1.5 Modifications nécessitant l'adoption d'une nouvelle politique

Si un changement de politique a, selon l'évaluation du responsable de la politique, un impact majeur sur un nombre important de clients, des Utilisateurs, le responsable de la politique peut, à sa discrétion, instituer une nouvelle politique avec un nouvel identificateur d'objet (OID).

9.2 Procédure de publication

9.2.1 Éléments non diffusés dans la DPC

Si une DPC contient des informations touchant la sécurité d'une AC ou des informations qu'elles considèrent confidentielles, la publication n'est pas requise. Il est possible de diffuser un résumé ou des extraits de la DPC sous forme électronique.

9.2.2 Publication de la politique de certification et de la DPC

La présente Politique de Certification et d'éventuels éléments de la DPC doivent être publiés et accessibles aux Utilisateurs à l'adresse URL suivante : <http://www.certinomis.com>. Une copie peut également être obtenue par courrier électronique, sur demande auprès de l'AC

Les AC émettrices de certificats qui utilisent l'identifiant (OID) de la présente Politique de Certification rendront accessible à leurs Utilisateurs des copies de cette politique.

9.3 Procédures d'approbation de la DPC

L'OC et l'AC sont garantes de l'adéquation de la DPC avec la Politique de Certification.

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

Table des matières

1	PREAMBULE	4
2	PRESENTATION GENERALE	5
2.1	RESUME DE LA PC	5
2.1.1	Champ d'application	5
2.1.2	Liste des applications appropriées	5
2.1.3	Liste des applications interdites	5
2.2	INFRASTRUCTURE A CLE PUBLIQUE	6
2.2.1	Les composantes de l'ICP	6
2.2.2	Politique de Certification et Déclarations des Pratiques de Certification	8
2.3	IDENTIFICATION DE LA POLITIQUE – O.I.D. (IDENTIFICATION ALPHANUMERIQUE)	8
2.4	COORDONNEES DE L'ORGANISME RESPONSABLE	9
2.4.1	Organisme responsable de la présente PC	9
2.4.2	Personne Responsable	9
2.4.3	Personne déterminant la conformité de la DPC avec la présente Politique	9
2.5	ROLE DES COMPOSANTES DE L'ICP ET DES INTERVENANTS	9
2.5.1	Autorité de certification	9
2.5.2	Autorité d'Enregistrement	10
2.5.3	Opérateur de certification	10
2.5.4	Client	11
2.5.5	Utilisateur	11
2.5.6	Partie qui se fie	11
3	DISPOSITIONS GENERALES	12
3.1	OBLIGATIONS	12
3.1.1	Obligations de l'AC	12
3.1.2	Obligations de l'Autorité d'Enregistrement	12
3.1.3	Obligations spécifiques de l'Administrateur	13
3.1.4	Obligations spécifiques de l'Opérateur	13
3.1.5	Obligations de l'OC	13
3.1.6	Obligations du service de publication	13
3.1.7	Obligations du service de recouvrement de clés de confidentialité	13
3.1.8	Obligations du Client	13
3.1.9	Obligations de l'Utilisateur	14
3.1.10	Obligations de la Partie qui se fie	14
3.2	RESPONSABILITES	15
3.2.1	Responsabilité de l'AC et de son personnel	15
3.2.2	Responsabilité de l'AE	16
3.2.3	Responsabilité de l'OC	16
3.2.4	Responsabilité du Client	16
3.2.5	Responsabilité de l'Utilisateur	16
3.3	INDEPENDANCE DES PARTIES ET ABSENCE DE ROLE DE REPRESENTATION	16
3.4	INTERPRETATION ET MISE EN APPLICATION	16
3.4.1	Droit applicable	16
3.4.2	Règlement des différends	16
3.4.3	Règlement des litiges - Tribunal compétent	17
3.4.4	Intégralité, divisibilité, survie, notification	17
3.5	TARIFS	17
3.6	PUBLICATION ET DEPOT DE DOCUMENTS	17
3.6.1	Informations publiées	17
3.6.2	Fréquence de diffusion	17
3.6.3	Contrôle de l'accès	18
3.6.4	Bases documentaires	18

3.7	CONTROLE DE CONFORMITE	18
3.8	CONFIDENTIALITE DES DONNEES A CARACTERE PERSONNEL ET DES INFORMATIONS	18
3.8.1	<i>Données à caractère personnel détenues par une AC</i>	18
3.8.2	<i>Informations confidentielles</i>	19
3.8.3	<i>Données à caractère personnel contenues dans les certificats et la LCR</i>	19
3.9	SECRET DES CORRESPONDANCE ET INTERCEPTIONS	19
3.10	DROITS RELATIFS A LA PROPRIETE INTELLECTUELLE	19
3.11	DISPOSITIONS PENALES	19
4	IDENTIFICATION ET VERIFICATION D'IDENTITE	20
4.1	ENREGISTREMENT INITIAL	20
4.1.1	<i>Types de nom</i>	20
4.1.2	<i>Règles de nommage</i>	20
4.1.3	<i>Règles d'interprétation des diverses formes de noms</i>	20
4.1.4	<i>Unicité des noms</i>	20
4.1.5	<i>Procédure de règlement des différends au sujet des noms</i>	20
4.1.6	<i>Reconnaissance, vérification et rôles des noms de marques de fabrique, de commerce et de services</i>	20
4.1.7	<i>Méthode de vérification de la possession de la clé privée</i>	20
4.1.8	<i>Vérification de l'identité du Client</i>	21
4.1.9	<i>Vérification de l'identité de l'Utilisateur</i>	21
4.2	VERIFICATION AUX FINS DE RENOUELEMENT DES CERTIFICATS	21
4.3	VERIFICATION AUX FINS DE RENOUELEMENT DES CLES APRES UNE REVOCATION	21
4.4	VERIFICATION AUX FINS DE RECOUVREMENT	21
4.5	VERIFICATION AUX FINS DE REVOCATION	21
5	EXIGENCES OPERATIONNELLES EN MATIERE DE GESTION DES CERTIFICATS	22
5.1	DEMANDE DE CERTIFICAT	22
5.2	EMISSION ET DISTRIBUTION D'UN CERTIFICAT	22
5.3	ACCEPTATION DU CERTIFICAT	22
5.4	RECOUVREMENT DE CLES DE CONFIDENTIALITE	22
5.5	SUSPENSION ET REVOCATION D'UN CERTIFICAT	22
5.5.1	<i>Motifs de révocation</i>	22
5.5.2	<i>Personne pouvant demander une révocation</i>	23
5.5.3	<i>Procédure de demande de révocation d'un certificat</i>	23
5.5.4	<i>Temps de traitement d'une révocation</i>	23
5.5.5	<i>Motifs de suspension</i>	23
5.5.6	<i>Personne pouvant demander une suspension</i>	23
5.5.7	<i>Procédure de demande de suspension d'un certificat</i>	23
5.5.8	<i>Limites d'une période de suspension</i>	23
5.5.9	<i>Fréquence de publication de la liste des certificats révoqués (LCR)</i>	23
5.5.10	<i>Exigences de vérification des LCR</i>	23
5.5.11	<i>Publication des motifs de révocation</i>	24
5.5.12	<i>Exigences spéciales concernant la compromission des clés</i>	24
5.6	JOURNALISATION DES EVENEMENTS	24
5.6.1	<i>Types d'événements consignés</i>	24
5.6.2	<i>Fréquence de traitement des journaux d'événements</i>	24
5.6.3	<i>Période de conservation des journaux</i>	25
5.6.4	<i>Protection des journaux</i>	25
5.6.5	<i>Procédures de sauvegarde des journaux</i>	25
5.6.6	<i>Système de collecte des journaux</i>	25
5.6.7	<i>Imputabilité</i>	25
5.6.8	<i>Evaluations de la vulnérabilité</i>	25
5.7	SAUVEGARDE ET ARCHIVAGE	25
5.8	RENOUELEMENT DES CLES	25
5.9	COMPROMISSION ET MESURES ANTI-SINISTRE	25
5.9.1	<i>Corruption des ressources informatiques, des logiciels et (ou) des données</i>	26
5.9.2	<i>Révocation de la clé publique d'une composante de l'ICP</i>	26
5.9.3	<i>Compromission de la clé privée d'une composante de l'ICP</i>	26

5.9.4	Sécurisation d'une installation après une catastrophe naturelle ou un autre sinistre.....	26
5.10	FIN DES ACTIVITES D'UNE AC.....	26
6	MESURES DE SECURITE PHYSIQUE, DES PROCEDURES ET DU PERSONNEL.....	27
6.1	MECANISMES DE CONTROLE DE LA SECURITE PHYSIQUE DES LOCAUX DE L'OC.....	27
6.2	MESURES DE CONTROLE DE LA SECURITE DES PROCEDURES.....	27
6.2.1	Rôles de confiance.....	27
6.2.2	Nombre de personnes requises par tâche.....	28
6.2.3	Identification et vérification pour chacun des rôles.....	28
6.3	MESURES DE CONTROLE DU PERSONNEL.....	28
6.3.1	Antécédents professionnel, qualités, expériences.....	28
6.3.2	Procédures de vérification des antécédents.....	29
6.3.3	Exigences en matière de formation.....	29
6.3.4	Formation professionnelle – fréquence et exigences.....	30
6.3.5	Rotation des emplois.....	30
6.3.6	Sanctions en cas d'actions non autorisées.....	30
6.3.7	Contrôle des personnels des entreprises cocontractantes.....	30
6.3.8	Documentation fournie au personnel.....	30
7	MESURES TECHNIQUES DE SECURITE.....	31
7.1	PRODUCTION ET INSTALLATION DES BI-CLES.....	31
7.1.1	Production des bi-clés.....	31
7.1.2	Remise de la clé publique à l'AC.....	31
7.1.3	Remise de la clé publique de l'AC aux utilisateurs.....	31
7.1.4	Tailles des clés asymétriques.....	31
7.1.5	Production des paramètres des clés publiques.....	31
7.1.6	Vérification de la qualité des paramètres.....	31
7.1.7	Nature de la ressource de production de clés.....	31
7.1.8	Utilisation de la clé publique.....	32
7.2	PROTECTION DES CLES PRIVEES.....	32
7.2.1	Normes relatives au calculateur cryptographique.....	32
7.2.2	Contrôle des clés privées par plusieurs personnes.....	32
7.2.3	Recouvrement des clés privées.....	32
7.2.4	Sauvegarde des clés privées.....	32
7.2.5	Archivage des clés privées.....	32
7.2.6	Initialisation et conservation d'une clé privée dans un module cryptographique.....	32
7.2.7	Méthode d'activation de la clé privée.....	32
7.2.8	Méthode de désactivation des clés privées.....	32
7.2.9	Méthode de destruction des clés privées.....	33
7.3	AUTRES ASPECTS DE LA GESTION DES BI-CLES.....	33
7.3.1	Archivage des clés publiques.....	33
7.3.2	Périodes d'utilisation des clés publiques et privées.....	33
7.4	DONNEES D'ACTIVATION.....	33
7.4.1	Génération et installation des données d'activation.....	33
7.4.2	Protection des données d'activation.....	33
7.4.3	Autres aspects touchant les données d'activation.....	33
7.5	MECANISMES DE SECURITE INFORMATIQUE DES POSTES DE TRAVAIL.....	33
7.5.1	Sécurité informatique – Exigences techniques spécifiques.....	33
7.5.2	Indice de sécurité informatique.....	34
7.6	CONTROLE TECHNIQUE DU SYSTEME DURANT SON CYCLE DE VIE.....	34
7.6.1	Contrôle des développements des systèmes.....	34
7.6.2	Contrôle de la gestion de la sécurité.....	34
7.7	MECANISMES DE CONTROLE DE LA SECURITE RESEAU.....	34
7.8	MECANISMES DE CONTROLE TECHNIQUE DU MODULE CRYPTOGRAPHIQUE.....	34
8	FORME ET CONTENU DES CERTIFICATS ET DES LISTES DE REVOCATION.....	35
8.1	FORME ET CONTENU DES CERTIFICATS.....	35
8.1.1	Signature du certificat.....	35
8.1.2	Champs d'extensions.....	35

8.1.3	<i>Interprétation sémantique des champs critiques</i>	35
8.2	FORMES ET CONTENU DES LISTES DE CERTIFICATS REVOQUES.....	35
9	ADMINISTRATION DE LA POLITIQUE DE CERTIFICATION	37
9.1	PROCEDURES DE MODIFICATIONS.....	37
9.1.1	<i>Délais de préavis</i>	37
9.1.2	<i>Forme de diffusion des avis</i>	37
9.1.3	<i>Période de commentaires</i>	37
9.1.4	<i>Traitement des commentaires</i>	37
9.1.5	<i>Modifications nécessitant l'adoption d'une nouvelle politique</i>	37
9.2	PROCEDURE DE PUBLICATION.....	37
9.2.1	<i>Éléments non diffusés dans la DPC</i>	37
9.2.2	<i>Publication de la politique de certification et de la DPC</i>	37
9.3	PROCEDURES D'APPROBATION DE LA DPC.....	37
	TABLE DES MATIERES	39