Politique de Certification

02 septembre 2002

Version : 1.2

Référence : MET-JSL/DA 101-02-A

Historique du document

Référence	Version	Date	Statut	Rédaction	Validation
MET-JSL/DA 101-02-A	1.2	02/09/02	Document définitif	EC, PA, JSL	DA
MET-JSL/DA 302-00-A	1.1	10/09/00	Document définitif	JSL	DA
MET-JSL/DA 300-00-A	1.0	10/05/00	Document définitif	EC, CG, JSL	DA, IS

Historique des modifications :

Version 1.2 Modification des procédures de renouvellement

Version 1.1 Prise en compte de la nouvelle plate-forme technique CertiNomis (P1.2)

Version 1.0 Première version de la P.C.

AVERTISSEMENT

1 INTRODUCTION

1.1 Introduction générale

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…). Ils ont pour fonction d'assurer :

- l'intégrité des messages ,
- l'identification et l'authentification[1] ,
- la non répudiation de l'origine ,
- et la confidentialité.

1.1.1 L'Infrastructure à Clé Publique (ICP)

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

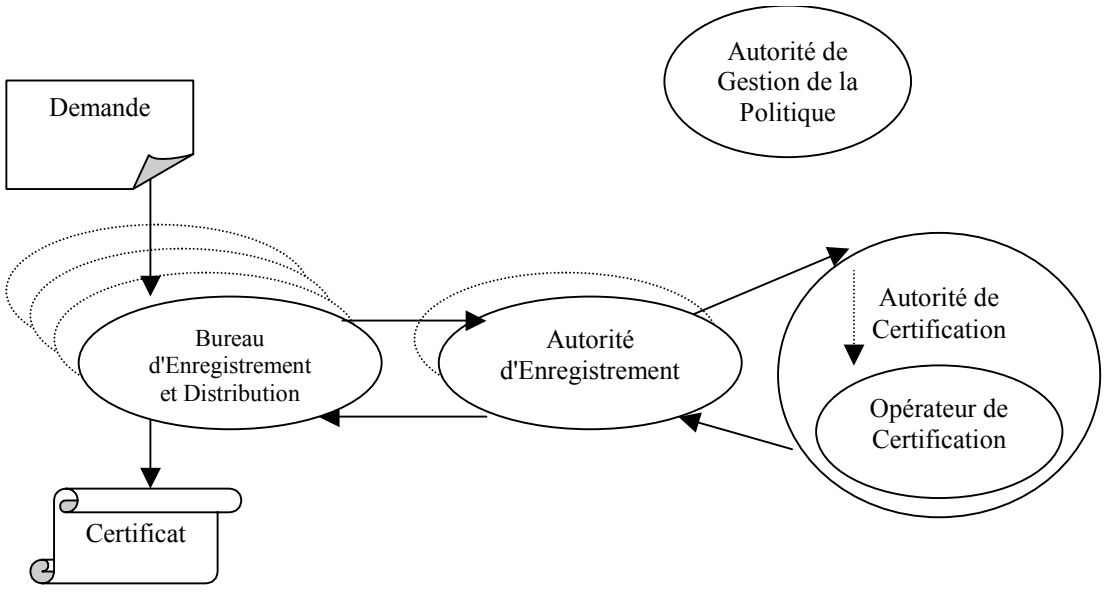

Figure 1: Exemple d'organisation et d'interaction entre les composantes de l'ICP

pour l'obtention d'un certificat

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

1.1.1.1 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 morale 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 toute personne se fiant à un certificat qu'elle a émis, de l'ensemble du processus de certification, et donc de la validité des certificats qu'elle émet. 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 publication des listes de révocations. 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.

Il est possible de définir des hiérarchies d'Autorité de Certification. Une Autorité de Certification, dite maître, peut certifier une autre Autorité de Certification dite déléguée. Une Autorité de Certification qui n'est pas déléguée, et qui se certifie elle-même, est dite Autorité de Certification racine.

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 techniques. 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 de ses premières missions est de la protéger contre toute compromission.
Sa responsabilité ne peut être engagée que par l'Autorité de Certification et se limite au respect des procédures établies dans la Déclaration des Pratiques de Certification approuvée par l'Autorité de Certification. L'Autorité de Certification a un devoir de contrôle et d'audit de l'Opérateur de Certification.
Dans cette politique, son rôle et ses obligations ne sont pas distingués de ceux de l'Autorité 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'abonné. Qu'elle soit ou non directement en contact physique avec l'abonné, 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.

Bureau d'enregistrement (BE) :
Bureau d'Enregistrement et de Distribution (BED) :
L'Autorité d'Enregistrement peut s'appuyer sur un réseau de bureaux de proximité dont le rôle est, selon les besoins, de collecter les pièces justificatives, de valider le face-à-face, et de distribuer les supports de certificats. Leurs procédures sont conformes aux règles définies par l'Autorité de Certification. Un Bureau d'Enregistrement et de Distribution est un point de contact physique avec l'abonné.
Les Bureaux d'Enregistrement et de Distribution sont sous la responsabilité de l'Autorité d'Enregistrement, ainsi que toutes leurs actions. L'Autorité d'Enregistrement a un devoir de contrôle et d'audit des Bureaux d'Enregistrement et de Distribution.
Dans cette politique, son rôle et ses obligations ne sont pas distingués de ceux de l'Autorité d'Enregistrement.

1.1.1.2 Certificat

Certificat :

Attestation électronique liant les données afférentes au chiffrement ou à la vérification de signature, des échanges, messages et documents électroniques à une personne, afin d'en assurer la confidentialité ou d'en assurer l'authentification et l'intégrité.

Il est sous la responsabilité d'un abonné qui en est physiquement le détenteur.

1.1.1.3 Les parties abonnés, clients et utilisateurs

Dispositif ou application:
Matériel ou logiciel pouvant faire usage des certificats pour établir automatiquement un contexte de sécurité qui lui est propre. Par exemple, un serveur web, ou un routeur utilisant un certificat pour s'authentifier lors des échanges.

Client :
La personne, physique ou morale, qui contracte avec l'Autorité de Certification pour bénéficier de ses services.

Entité identifiée:
La personne, le dispositif ou l'application dont les données d'identifications sont inscrites dans le certificat.

Abonné :
La personne physique responsable du certificat et de son utilisation. Il en est physiquement le détenteur et s'engage sur ses conditions d'utilisation et ses obligations vis-à-vis de l'Autorité de Certification.

Les quelques exemples suivants détaillent ce partage des rôles:

- un particulier demande un certificat pour son usage propre:
  - le particulier est "client", car il contracte,
  - le particulier est "entité identifiée", car son identité est dans le certificat,
  - le particulier est "abonné", car il est responsable du certificat.
- une société demande un certificat pour un de ses salariés:
  - la société est "cliente", car elle contracte,
  - le salarié est "entité identifiée", car son identité professionnelle est dans le certificat
  - le salarié est "abonné", car il est responsable du certificat.
- une société demande un certificat pour un serveur WEB
  - la société est "cliente", car elle contracte,
  - le serveur est "entité identifiée", car son URL[1] est dans le certificat,
  - le web-master, ou le responsable technique du site est "abonné", car il est responsable du certificat et de sa mise en œuvre.

Tiers utilisateur ou Partie qui se fie:

[1] Universal Resource Locator

Personne qui utilise le certificat d'une entité identifiée afin de vérifier l'authenticité de sa signature numérique ou de chiffrer des messages à son intention.

Mandataire de certification:
Personne ayant, directement par la loi ou par délégation, le pouvoir d'autoriser une demande de certificat portant le nom de l'organisation. Il peut aussi avoir d'autre pouvoir au nom de l'organisation, comme celui de révocation. Dans le cas d'une entreprise, il s'agit du représentant légal ou de toute personne qu'il aura désignée.

1.1.2 Politique de Certification et Déclarations des Pratiques de Certification

Politique de Certification (PC) :
Texte contractuel qui établit les devoirs et responsabilités de l'Autorité de Certification, de ses clients et abonnés, des tiers 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, les abonnés ainsi que par tous les tiers 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 des reconnaissances entre Autorités de Certification.
Les certificats d'entité identifiée émis par une Autorité de Certification contiennent un identificateur issu d'une branche enregistrée auprès de l'AFNOR, désigné par le sigle (OID), qui identifie la Politique 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.

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.

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

Classe 2, 2+
OID
1.2.250.1.86.2.1.2.2

1.3 Rôle des composantes de l'ICP et des intervenants

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

- Autorité de certification et ses propres composantes ou services,
- Autorité d'enregistrement,
- Clients et abonnés de l'Autorité de Certification,
- Tiers utilisateurs.

1.3.1 Autorité de certification

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

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

- coordonner les demandes de certificat ;
- générer et conserver les moyens de recouvrir les clés privées de confidentialité de manière à en assurer le recouvrement, selon les gammes de produits et uniquement sur demande expresse du client ;
- générer des certificats liant le nom distinctif des entités identifiées 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 ;
- faire respecter la PC par les différentes composantes de l'ICP, les clients et les abonnés;
- faire respecter la DPC par les différentes composantes de l'ICP;

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.

L'AC qui satisfait aux conditions mentionnées ci-dessus peut alors être autorisée par l'Autorité de Gestion de la Politique à inscrire l'identifiant d'objet (OID) de la présente politique dans les certificats qu'elle émet.

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

1.3.1.1 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 ; et
- négocier les contrats de certification croisées ;

Avant d'établir un accord de certification croisée avec une autre AC, le responsable de l'AC doit :

- consulter toute Autorité de Gestion de la Politique à laquelle l'AC est subordonnée;
- vérifier les politiques et les procédures opérationnelles de l'AC requérante ; et
- négocier toutes les améliorations des procédures opérationnelles, les éventuelles restrictions sur l'utilisation de certificats croisés, la période de validité du certificat croisé, la responsabilité, et tout autre élément nécessaire en fonction des besoins.

Les modalités de toute certification croisée doivent faire l'objet d'un contrat écrit.

1.3.1.2 Intervenants requis pour la gestion de l'AC

Le responsable de l'AC se conformant à la présente politique doit attribuer à son personnel, entre autres, les fonctions suivantes:

- maintenir, administrer, exploiter et protéger les machines et logiciels utilisés par l'AC ;
- gérer les informations et les dossiers des clients et abonnés 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.

1.3.2 Autorité d'Enregistrement

Le responsable de l'AC doit attribuer à une partie de son personnel ou à des entités déléguées les fonctions suivantes:

- coordonner les demandes d'identification électronique ;
- vérifier les caractéristiques d'identification des entités identifiées selon la classe du certificat envisagé ;

Classe 2, 2+
Caractéristiques d'identification
Identité civile ou fonctionnelle

- distribuer à l'abonné, 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 personnelles et de sécurité des abonnés; et
- maintenir, administrer, exploiter et protéger les machines et logiciels utilisés pour emplir ces fonctions.

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

Le personnel d'une AE doit :

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

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

Les données à caractère personnel collectées par, ou pour, l'AC lors de l'enregistrement des clients et des abonnés 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.

1.3.3 Client

1.3.3.1 Personne physique

Elle a les obligations et les responsabilités de l'abonné.

1.3.3.2 Organisation

Elle est responsable :

- de l'authenticité, de l'exactitude, et de la complétude des données d'identification de l'organisation fournies à l'AE lors de l'enregistrement ainsi que des qualités des abonnés relevant des seules prérogatives de l'organisation;
- d'établir et de faire respecter une politique de sécurité sur les postes informatiques utilisés pour mettre en œuvre les certificats.

Elle 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.

1.3.4 Abonné

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 des données d'identification de l'entité identifiée fournies à l'AE lors de l'enregistrement ; et
- de l'utilisation de ses clés et certificats, 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.

1.3.4.1 Individus agissant en leur nom personnel

L'abonné doit dans ce cas être une personne physique agissant pour son propre compte et en son nom.

L'individu agissant en son nom personnel qui satisfait aux conditions définies ci-dessus et dont le certificat porte le numéro d'identification d'objet (OID) de la présente politique est, de ce fait, autorisé par le responsable de l'AC à utiliser son certificat et les clés associées selon les règles prévues à cet effet.

1.3.4.2 Individus agissant pour le compte d'une organisation

Une organisation peut être une entreprise de droit privé ou de droit public, elle peut être individuelle, société anonyme, société de capitaux ou société de personne, une entité administrative ou gouvernementale, une association, ou tout autre groupement doté de la personne morale. Cette organisation doit avoir été enregistrée officiellement par l'AE reconnue par le responsable de l'AC.

L'abonné doit dans ce cas :

- être une personne physique dûment autorisée à agir pour le compte d'une organisation ; et
- faire inscrire le nom de l'organisation qu'il représente dans son certificat.

Les certificats émis au nom d'une organisation sont expressément exclus pour des utilisations au nom personnel de l'abonné.

L'individu agissant pour le compte d'une organisation qui satisfait aux conditions définies ci-dessus et dont le certificat porte le numéro d'identifiant d'objet (OID) de la présente politique est de ce fait, autorisé par le responsable de l'AC à utiliser son certificat et les clés associés selon les règles prévues à cet effet.

1.3.5 Tiers utilisateur

Un tiers utilisateur peut être toute personne qui utilise un certificat d'un abonné, régi par la présente politique, afin de vérifier au moyen de la clé publique qui y est contenue l'authenticité d'une signature numérique, ou afin de chiffrer des données à l'attention de l'abonné en utilisant cette même clé.

Avant d'accorder sa confiance au dit certificat, le tiers utilisateur 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, le tiers utilisateur assume seul tous les risques de ses actions non conformes aux exigences de la présente politique, CertiNomis ne garantissant, dès lors, plus aucune valeur juridique aux certificats qu'elle a émis et qui pourraient avoir été révoqués ou qui ne seraient pas valides.

1.3.6 Résumé de la Politique de Certification

1.3.6.1 Aperçu général

La Politique de Certification définie dans le présent document est destinée à être utilisée par les entreprises, les associations, les ministères, les entités administratives ou gouvernementales et groupements de toute sorte, et les individus. Les personnes qui consultent et utilisent ce document peuvent s'informer auprès de l'AC émettrice afin d'obtenir plus de détails sur sa mise en œuvre.

La Politique de Certification couvre la gestion et l'utilisation de certificats, selon leurs classes, contenant les clés publiques servant aux fonctions de vérification, d'authentification, d'intégrité et de concordance des clés. Par exemple, les certificats délivrés en vertu de la présente politique pourraient servir à vérifier l'identité des correspondants s'échangeant du courrier électronique ou permettre l'accès distant à un système informatique, vérifier l'identité des individus ou d'autres personnes morales (de droit privée et de droit public), ou encore préserver l'intégrité des serveurs, des logiciels et des documents.

La Politique de Certification couvre aussi la gestion et l'utilisation de certificats contenant les clés publiques servant aux fonctions de confidentialité. Les certificats délivrés en vertu de la présente politique permettent d'assurer le secret d'informations, considérées comme privées ou sensibles par leur propriétaire, dans certaines applications comme le courrier électronique ou les communications par le Web. Ils ne servent pas à protéger les renseignements classifiés.

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

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

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

1.3.6.2 Aperçu de la politique

Classe 2, 2 +
Politique de Certification

La désignation de l'identification objet (OID) pour la présente politique est : 1.2.250.1.86.2.1.2.2

Selon cette politique, sont émis des clés privées et des certificats à clés publiques utilisés pour l'identification :

- des individus désirant accéder à des données sensibles, par exemple des données nominatives, à démontrer le consentement et à engager l'achat de biens et/ou de services de faible montant par transaction ;
- ou encore des entités identifiées dans le certificat.

Les certificats de classe 2+ comporte un niveau d'assurance garantie, précisé par contrat et accessible à la partie utilisatrice.
Lors de l'enregistrement initial, l'identité des détenteurs potentiels de certificats doit être vérifiée par une AE reconnue par l'AC, quoique les individus ne sont pas tenus de se présenter en personne (envoi de copies de documents d'identité par courrier). L'AC garantit le lien qui existe entre le détenteur du certificat et une paire de clés.

Les certificats et les clés privées associées sont portés par un support physique dédié et approuvé par CertiNomis (classe 2+) ou sont conservés sous une autre forme notamment logicielle (classe 2).

1.4 Personne responsable, coordonnées

1.4.1 Organisme responsable de la présente politique

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

1.4.2 Personne Responsable

Monsieur, Didier Arpin
Directeur Général
CertiNomis
20 rue Louis Armand
75015 Paris

Téléphone : (33) (0)1.58.09.80.52
Télécopieur : (33) (0)1.58.09.80.51Courrier électronique : didier.arpin@certinomis.com

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

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

1.6 Champs d'application de la politique

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

1.6.1 Liste des applications appropriées

Classe 2, 2+

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

Ils sont appropriés pour :

- vérifier l'identité du demandeur d'accès à des données sensibles, par exemple nominatives ;
- 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 ;
- vérifier la volonté d'engagement d'achat de biens et/ou de services ; et
- assurer la confidentialité des documents et des envois électroniques.

La classe 2 est plus appropriée pour les transactions du commerce électronique courant.

1.6.2 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.

Si un abonné utilise ses certificats en dehors des applications appropriées, et en particulier dans 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 tiers utilisateur d'un certificat se fie à celui-ci alors que l'application est interdite ou restreinte aux termes de la présente politique ou de la DPC, il en assume seul tous les risques.

Dans aucune des hypothèses visées ci-dessus, la responsabilité de l'AC ne pourra être mise en jeu.

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 en tant qu'AC.

Classe 2, 2+
Les certificats appartenant à cette classe n'autorisent aucune transaction commerciale, ou échange électronique, dont les conséquences financières directes ou indirectes sont d'un montant supérieur à un montant précisé dans le contrat et accessible à la partie qui se fie.

2 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, des abonnés et des tiers utilisateurs. Elle contient aussi des dispositions juridiques, relatives notamment à la loi applicable et à la résolution des litiges.

2.1 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 ses 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.

2.1.1 Obligations de l'AC

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

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, concernant le fonctionnement des AE.

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, abonnés et tiers utilisateurs de certificats eu égard aux lois et règlements en vigueur.

L'AC doit :

- informer les tiers utilisateurs de la révocation du certificat d'un abonné ou d'une composante de l'ICP en publiant des Listes de Certificats Révoqués ;
- documenter les schémas de certification qu'elle entretient avec d'autres AC ;
- 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'AC est responsable de l'information de ses clients et de ses abonnés des procédures à suivre au cours du cycle de vie des certificats ; cela concerne, notamment, l'émission, la révocation, le retrait.

L'AC doit générer les certificats, publier les informations concernant la révocation des certificats (article 2.1.2) et procéder au renouvellement des certificats.

L'AC doit maintenir une disponibilité maximale de l'ensemble de ses services. Toutefois la maintenance et la réparation du système, ou encore d'autres facteurs qui échappent au contrôle de l'AC, peuvent influer sur cette disponibilité.

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, des abonnés et des tiers utilisateurs de certificats eu égard aux lois et règlements en vigueur.

Les membres du personnel de l'AC, et les opérateurs mandatés, à qui sont assignés des rôles relatifs à l'ICP (responsable de l'AC, responsable de la sécurité de l'AC…) doivent être personnellement responsables de leurs actes. L'expression « personnellement responsable » signifie que l'on puisse prouver qu'une telle personne a bel et bien fait une telle action.

2.1.2 Obligations du service de publication

Le responsable du service de publication doit mettre à jour et préserver l'intégrité des listes qu'il publie. Il doit aussi, en prenant toutes les mesures raisonnables, maintenir la disponibilité des listes sur son serveur.

2.1.3 Obligations du service de recouvrement de clés de confidentialité

Ce service peut-être offert sur une base volontaire dans le cadre des prestations de services de certification sous la responsabilité de l'AC.

Ce service est totalement exclu pour les bi-clés de signature numérique.

Pour les bi-clés de confidentialité, si l'AC le propose, le client peut, lors de l'enregistrement, et s'il le souhaite, demander le service de recouvrement. Selon le cas, l'AC génèrera alors la clé privée de confidentialité et sera en mesure de la reconstituer en cas de perte ou elle fournira au client les moyens de reconstituer ladite clé de confidentialité.
Si le client ne souhaite pas bénéficier du service de recouvrement de clés de chiffrement, l'abonné génèrera lui-même sa clé privée de confidentialité, lors de l'enregistrement, et par conséquent, l'AC ne pourra jamais reconstituer cette clé.

2.1.4 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. En outre, une AE doit:

- traiter les demandes de certificat ;
- vérifier les données personnelles d'identification et les données contenues dans le certificat ;
- 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 abonnés ; 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 ou les AGP qui l'accréditent.

2.1.5 Obligations du client

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 s'engage à respecter le contrat qui le lie à l'AC.

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

Si le client est une organisation, il doit établir et faire respecter une politique de sécurité sur les postes informatiques utilisés pour mettre en œuvre les certificats.

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.

2.1.6 Obligations de l'abonné

L'abonné doit se conformer à toutes les exigences de la présente Politique de Certification et des éléments de la DPC diffusés par l'AC. L'abonné doit exclusivement utiliser ses clé privées et certificats 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 l'identification de l'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 conformément à l'article 6.2. 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.

2.1.7 Obligation du tiers utilisateur

Le tiers utilisateur d'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, le tiers utilisateur 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, le tiers utilisateur assume seul tous les risques de ses actions non conformes aux exigences de la présente politique, CertiNomis ne garantissant aucune valeur juridique aux certificats qu'elle a émis et qui pourraient avoir été révoqués ou qui ne seraient pas valides.
En outre, lors de la vérification d'une signature électronique, le tiers utilisateur doit aussi vérifier que la clé publique du certificat correspond à la clé privée de signature utilisée.

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

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

2.2 Responsabilités

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

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

Pour la mise en œuvre des services de certification qu'elle fournit, une obligation de moyen pèse sur l'AC. Dans l'hypothèse où la responsabilité de l'AC serait mise en cause, celle-ci pourra être engagée selon les règles du droit commun.
Aucune responsabilité ne sera assumée par l'AC et par le personnel de l'AC pour l'utilisation d'un certificat dans des conditions qui ne seraient pas conformes ou non autorisées par la présente Politique de Certification et par la DPC associée, ainsi que par toutes autres clauses contractuelles applicables.

2.2.1.1 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 délictuel, d'un contrat ou d'une autre cause à l'égard d'un service en relation avec l'émission, l'utilisation ou la fiabilité d'un certificat électronique, offrant un niveau d'assurance selon la classe du certificat ou du bi-clé connexe, au delà des limites fixées ci-dessous, par l'utilisation, par un abonné ou un tiers utilisateur. Cette limite de responsabilité s'entend, et de façon non limitative, de tout préjudice financier ou commercial, perte de bénéfices, perte d'exploitation, trouble commercial, manque à gagner, pertes ou actions intentées par un tiers contre le client, trouvant leur origine ou étant la conséquence de la présente 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 la notice d'assurance.

2.2.1.2 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 lors de l'abonnement aux prestations de services de certification.

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 télécommunication.

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'abonné ou le tiers utilisateur non conforme à la réglementation en vigueur relative à la protection des logiciels, quant au non-respect par l'abonné ou le tiers 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'abonné ou du tiers utilisateur, la détérioration des informations portées sur les dits médias informatiques due à l'influence des champs 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 pratique associée, dans la notice d'assurance, ou dans le contrat d'abonnement.

2.2.1.3 Force majeure

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

L'AC ne saurait être tenue responsable et n'assume aucun engagement, pour tout retard dans l'exécution d'obligations ou pour toute inexécution d'obligations résultant de la présente politique lorsque les circonstances y donnant lieu et qui pourraient résulter de l'interruption totale ou partielle de son activité, ou de sa désorganisation, relèvent de la force majeure au sens de l'article 1148 du Code civil.

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

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 télécommunications, y compris des réseaux de télécommunications, 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.

2.2.2 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'abonné, le client ou le tiers utilisateur.

2.3 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 de l'abonné, 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 abonnés, les clients et les tiers utilisateurs de certificat sont des personnes juridiquement et financièrement indépendantes et, à ce titre, ne disposent d'aucun pouvoir ni de représentation, ni d'engager l'AC ou l'une des composantes de l'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 d'abonnement 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'une organisation soit dans un certificat de signature numérique ne constitue pas en soi un mandat spécial ou général de cette organisation en faveur de l'abonné.

2.4 Interprétation et mise en application

2.4.1 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.

2.4.2 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.

2.4.3 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

2.4.4 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.

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

2.5 Tarifs

2.5.1 Frais d'émission de certificats et de renouvellement

Des frais d'émission de certificat seront facturés selon une échelle de tarifs diffusés par l'AC sur son site WEB, ou négociés dans le cadre d'un contrat commercial.

2.5.2 Frais d'accès au certificat

Des frais d'accès au certificat peuvent être facturés par l'AC selon une échelle de tarifs diffusés ou négociés avec l'AC.

2.5.3 Frais de vérification de validité des certificats

Des frais de vérification de validité des certificats peuvent être facturés par l'AC selon une échelle des tarifs diffusés ou négociés avec l'AC. Un moyen gratuit de contrôle du statut du certificat est toujours laissé à la disposition du tiers utilisateur.

2.5.4 Frais pour d'autres services

Aucun frais ne sera facturé pour l'accès en direct à cette Politique de Certification ou aux éléments publiés de la DPC. Cependant, des frais peuvent être facturés pour des copies sur support papier ou par voie électronique.

2.5.5 Politique de remboursement

Aucune exigence particulière.

2.6 Publication et dépôt de documents

2.6.1 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.
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 dans son intégralité pour des raisons de sécurité liées au besoin d'en connaître.
Toutefois, l'AC doit fournir, autant que de besoin, la version complète de sa DPC, lors d'une demande d'un organisme autorisé (AGP, AC maître, autre AC pour certification croisée…) à des fins de vérification, d'audit ou de contrôle, prévues à cet effet dans la présente politique, ainsi que dans le cadre du respect de la loi.

La Liste des Certificats Révoqués est fournie par le service de publication. La liste des certificats, dont la publication est autorisée par le client, peut aussi être fournie par le service de publication.

2.6.2 Fréquence de diffusion

Les Listes de Certificats Révoqués seront mises à jour dans des délais tels que prévus à l'article 4.5.

La publication de la Politique de Certification et des éventuels éléments de la DPC respectera les dispositions de l'article 8.2 "Procédure de publication" de la présente politique.

2.6.3 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.

2.6.4 Bases documentaires

L'AC est tenue de diffuser les informations identifiées à l'article 2.6.1 "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.

2.7 Contrôle de conformité

Un contrôle de conformité permet de déterminer si le comportement réel de l'AC et de toutes les composantes de l'ICP répond aux exigences et normes fixées dans sa 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 d'une AGP ou sur demande de l'AC elle-même, selon les conditions précisées dans la DPC.

2.8 Confidentialité des données à caractère personnel et des informations

2.8.1 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 s'applique au contenu de tous les documents détenus ou transmis par l'AC ou par un de ses représentants (site de la CNIL http://www.cnil.fr).

En vertu de la loi, les clients et les abonnés disposent d'un droit d'accès, de rectification et d'opposition à la cession de toute information qui les concerne. Ce droit peut s'exercer par l'intermédiaire du service agent, en particulier l'AE, ayant recueilli ces informations, à l'adresse électronique figurant sur le site WEB de l'AC.
L'AC doit respecter rigoureusement toutes les prescriptions légales applicables et expliquer sur son site WEB, les modalités concrètes d'application de la loi.

La Politique de Certification doit être interprétée de manière à respecter les principes fondamentaux en matière de protection des données à caractère personnel consacrés dans la loi, la directive européenne du 24 octobre 1995 et toute autre convention internationale entrée en vigueur.
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'abonné 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'abonné ou du client.

2.8.2 Informations confidentielles

La clé privée de signature numérique et la clé privée de confidentialité de chaque abonné doivent demeurer confidentielles. En cas de divulgation par l'abonné 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.

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

Les renseignements concernant l'identification ou d'autres données à caractère personnel, du client ou de l'abonné, apparaissant sur les certificats sont considérés comme étant confidentiels, sauf si le client ou l'abonné 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

2.9 Secret des correspondance et interceptions

Le secret des correspondances émises par voie des télécommunications est garanti par la loi française. En cas d'atteinte, toute violation est punie par l'article 226-15 du code pénal pour celles commises par un particulier et par les articles 432-9 et 432-17 du code pénal pour celles commises par une personne dépositaire de l'autorité publique.
D'une façon générale, aucun salarié de l'AC et aucun collaborateur ou sous-traitant, dans le cadre de leur participation 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).

2.10 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 1er juillet 1998 (Journal officiel du 2 juillet , 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

2.11 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 1 à 3 ans d'emprisonnement et d'une amende allant de 15.000 à 225.000 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

3 IDENTIFICATION ET VERIFICATION D'IDENTITE

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

3.1 Enregistrement initial

3.1.1 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.

3.1.2 Nécessité d'utiliser des noms explicites

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

Classe 2, 2+,
Dans le cas de personnes physiques, le nom distinctif doit contenir soit une combinaison du prénom, du nom de famille et facultativement d'initiales, soit un pseudonyme identifié comme tel. Il peut aussi contenir une fonction ou un rôle organisationnel. Dans le cas d'un autre type d'entité identifiée, le nom distinctif doit refléter son nom légal authentifié. Un nom distinctif doit contenir de manière obligatoire les champs suivants : • dans tous les cas le Common Name(CN) ; et • lorsqu'on souhaite mentionner le lien à une organisation, le champ Organisation (O). Un certificat émis pour un dispositif ou une application doit inclure le nom du propriétaire du dispositif ou de l'application, qu'il s'agisse d'une personne physique ou d'une organisation.

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

3.1.3 Règles d'interprétation des diverses formes de noms

Aucune exigence n'est stipulée

3.1.4 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.

3.1.5 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. Une partie demandant un certificat doit être en mesure de prouver qu'elle a le droit d'utiliser un nom en particulier.

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

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

Toute AC déléguée est tenue de suivre et d'appliquer la politique de nommage de son AC maître, si elle le demande.

3.1.6 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 1er juillet 1992 et ses modifications ultérieures) appartient au titulaire légitime de cette marque de fabrique, de commerce ou de services, ou de ce signe distinctif ou encore à ses licenciés ou cessionnaires.

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

3.1.7 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.

3.1.8 Vérification de l'identité de l'organisation

L'AE vérifie l'identification de l'organisation, 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. Le représentant légal et ces personnes, qu'il aura désignées en donnant l'étendue de leur mandat, sont les mandataires de certification. A défaut de désignation, le représentant légal est l'unique mandataire de certification.

Lors de l'enregistrement, l'organisation doit apporter la preuve de son existence, la preuve de l'identité de son représentant légal ainsi que la chaîne des mandats conférant leur pouvoir aux mandataires de certification.

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.

3.1.9 Vérification de l'identité des abonnés

3.1.9.1 Vérification de l'identité des individus agissant en leur nom personnel

Classe 2, 2+

L'AE doit vérifier la photocopie d'au moins une pièce d'identité officielle du demandeur en cours de validité comportant sa photo et sa signature, ainsi que la photocopie d'une quittance attestant de son domicile, datée de moins de trois (3) mois à compter du jour du dépôt des pièces réputée être la date figurant au cachet de la poste. L'AE doit conserver les pièces reçues pour l'enregistrement de l'abonné, examiner les pièces et documents remis avec un soin raisonnable et vérifier s'ils présentent ou non l'apparence de conformité et de validité.

3.1.9.2 Vérification de l'identité des individus agissant pour le compte d'une organisation

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

Pour toute demande de certificat faite au titre de l'appartenance à une organisation, il faut que la dite demande soit confirmée par écrit par un mandataire de certification.

Classe 2, 2+
L'AE doit vérifier la photocopie d'au moins une pièce d'identité officielle du demandeur en cours de validité comportant sa photo et sa signature, ainsi qu'une autorisation signée par le mandataire de certification au titre de son appartenance à l'organisation, conformément aux dispositions prévues à l'article 3.1.8. L'AE doit conserver les pièces reçues pour l'enregistrement de l'abonné, examiner les pièces et documents remis avec un soin raisonnable et vérifier s'ils présentent ou non l'apparence de conformité et de validité.

3.1.10 Vérification du droit sur les dispositifs et applications

Une personne ou une organisation qui a le droit d'usage d'un dispositif (serveur, …) ou d'une application (signature automatique de messages, …) ayant la capacité de signer numériquement ou de recevoir des messages chiffrés peut demander à CertiNomis qu'il soit reconnu comme étant une entité identifiée.

Si le demandeur est une personne physique, la vérification d'identité doit se faire selon les exigences prévues à l'article 3.1.9.1.
Si le demandeur est une organisation, celle-ci devra désigner la personne physique abonnée qui sera responsable du certificat, du dispositif ou de l'application. La vérification de l'identité de l'organisation doit se faire selon les exigences prévues à l'article 3.1.8. La vérification de l'identité de la personne physique désignée doit se faire selon les exigences prévues à l'article 3.1.9.2.

L'AE doit également vérifier que le demandeur est autorisé à recevoir des certificats pour ce dispositif ou cette application. La personne ou l'organisation qui présente une demande doit établir la preuve de son droit d'usage sur le dispositif ou l'application dont mention sera faite dans le certificat. En particulier dans le cas d'un serveur, elle devra établir la preuve que le nom de domaine lui appartient bien.

L'AE doit consigner le type d'identification utilisée, ainsi que toutes les informations pertinentes relatives à cet enregistrement.
La DPC précise les documents à fournir et les procédures d'enregistrement mises en œuvre par l'AE.

3.2 Vérification aux fins de renouvellement des certificats

3.2.1 Vérification aux fins de renouvellement des certificats de personne agissant en leur nom personnel

Le renouvellement sera effectué selon la procédure d'enregistrement initial prévue à l'article 3.1.9.1.

3.2.2 Vérification aux fins de renouvellement des certificats de personne agissant pour le compte d'une organisation

Si le nom ou l'adresse de courrier électronique de l'abonné ou les informations d'identification de l'organisation qui figurent dans le certificat ne sont plus à jour ou doivent être modifiés, le certificat doit être révoqué, et ne

pourra être renouvelé. Il faudra procéder à un nouvel enregistrement selon la procédure d'enregistrement initial prévue à l'article 3.1.9.2.

Dans le cadre d'une organisation, il est possible de s'appuyer sur la vérification de son identité ainsi que de ses représentants, que cela soit les représentants légaux ou les mandataires de certification. Le premier renouvellement du certificat d'un individu agissant pour le compte d'une organisation peut donc être effectué sans une nouvelle présentation de l'ensemble des pièces justificatives. Par contre, le renouvellement suivant sera effectué selon la procédure d'enregistrement initial prévue à l'article 3.1.9.2.

Pour toute demande de renouvellement de certificat faite au titre de l'appartenance à une organisation, il faut que la dite demande soit confirmée par écrit par un mandataire de certification, qui atteste sur l'honneur que le nom, l'adresse de courrier électronique de l'abonné ainsi que les informations d'identification de l'organisation sont toujours à jour et ne doivent pas être modifiés.

La demande de renouvellement de certificat doit être effectuée au plus tard dans un délai de trois (3) mois à compter de l'expiration du certificat.

Classe 2, 2+
L'AE doit vérifier l'autorisation signée par le mandataire de certification au titre de son appartenance à l'organisation, conformément aux dispositions prévues à l'article 3.1.8. L'AE doit conserver les pièces reçues pour l'enregistrement de l'abonné, examiner les pièces et documents remis avec un soin raisonnable et vérifier s'ils présentent ou non l'apparence de conformité et de validité. La distribution par l'AE peut se faire directement au demandeur par courrier simple à l'adresse portée par le mandataire dans l'autorisation signée.

3.2.3 Vérification aux fins de renouvellement de certificat de dispositif ou d'application

Le renouvellement sera effectué selon la procédure d'enregistrement initial prévue à l'article 3.1.10.

3.3 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.

3.4 Vérification aux fins de recouvrement

Pour les certificats de signature numérique, le recouvrement est impossible quels que soient la classe et le type d'utilisation du certificat.

Pour les certificats de confidentialité, les moyens de recouvrement ne seront donnés qu'à une personne physique habilitée, c'est-à-dire soit à l'abonné, soit au mandataire de certification, après vérification de son identité en face-à-face au moyen d'une pièce d'identité officielle comportant sa photographie et sa signature.

3.5 Vérification aux fins de révocation

Seul le mandataire de certification, l'abonné et l'AC peuvent demander la révocation d'un certificat.

L'AC doit établir et rendre public le mécanisme qu'elle utilise pour traiter les demandes de révocation et en établir la validité.

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 en vérifiant un ensemble d'informations déposées lors de l'enregistrement initial, soit au moyen d'une signature numérique valide reconnue par l'AC, soit de toute autre façon non équivoque.

4 EXIGENCES OPERATIONNELLES EN MATIERE DE GESTION DES CERTIFICATS

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

4.1 Demande de certificat

L'AC doit s'assurer que toutes les procédures et les exigences concernant une demande de certificat sont énoncées dans la DPC ou un document public. 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.

Selon la classe du certificat, la qualité du demandeur (professionnel ou particulier) et le type d'entité identifiée à certifier (personne physique ou dispositif), les informations suivantes doivent figurer dans la demande de certificat :

Classe 2, 2+
La demande d'identification électronique envoyée à l'AE doit au moins contenir le nom, le prénom et l'adresse de courrier électronique du demandeur. Dans le cas d'une organisation, la demande doit également contenir les informations permettant de retrouver le domicile physique ainsi que la dénomination sociale de l'organisation. Dans le cas d'un dispositif ou d'une application, la demande doit également contenir le nom du dispositif ou de l'application. Chaque demande doit être associée à des pièces, elles aussi transmises à l'AE, qui permettent de prouver l'identité et les pouvoirs des futurs abonnés conformément aux procédures applicables en fonction du type de certificat demandé (articles 3.1.8, 3.1.9, 3.1.10 et 3.2), notamment : • la preuve de l'identité du demandeur ; • la preuve des pouvoirs pour les attributs demandés, par exemple d'appartenance à un organisme ou une société, de possession d'un nom de domaine ; • le contrat client ou la référence à un contrat client préexistant Dans le cas d'une organisation, pour chaque demande, il faut qu'il existe une autorisation et un contrat client signés d'un mandataire de certification identifié. Ce contrat doit faire mention des obligations d'information de l'abonné sur ses obligations.

4.2 Emission et distribution d'un certificat

Une demande de certificat n'oblige en aucune façon l'AC à émettre un certificat numérique.
L'émission d'un certificat par une AC indique que celle-ci a définitivement et complètement approuvé la demande de certificat selon les procédures décrites dans la DPC.
A la réception d'une demande de certificat, l'AC 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 son avis ;
- générer et signer le certificat ;
- notifier à l'abonné 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'abonné, c'est-à-dire rendre accessible par des moyens physiques ou logiques les informations permettant l'obtention du certificat .

4.3 Acceptation du certificat

Les informations nécessaires à l'obtention du certificat étant mises à la disposition de l'abonné, 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'abonné reconnaît expressément consentir aux termes et aux conditions d'utilisation contractuelles et, plus généralement, à tous les éléments publiés dans la Déclaration de Pratiques de Certification et dans la présente Politique de certification de l'AC.

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

4.4 Recouvrement de clés de confidentialité

La clé privée de signature ne peut en aucun cas être recouvrée par l'AC. L'AC ne conserve, ni ne copie, ni n'a accès aux informations qui ont été utiles à la création de la clé privée de signature, conformément à la directive européenne, notamment à l'annexe II, § j et à sa transposition en droit français.
Le recouvrement de la clé privée de confidentialité n'est possible qu'à la condition que le client ait choisi expressément cette option au moment de la demande de certificat.
L'AC doit impérativement respecter les lois et règlements en vigueur qui la régissent.

4.4.1 Individu pouvant demander une recouvrement

Les individus suivants peuvent demander le recouvrement des clés et du certificat d'un abonné :

- l'abonné lui-même ; ou
- le mandataire de certification de l'organisation qui emploie ou employait l'abonné au moment de la délivrance des clés et du certificat à ce dernier.`

4.4.2 Traitement d'une demande de recouvrement

Une demande de recouvrement de clés est toujours considérée comme étant de nature exceptionnelle.
La procédure de la demande de recouvrement de clés de confidentialité est précisée dans la DPC.
Pour pouvoir demander un recouvrement, le certificat en cause doit avoir été préalablement révoqué. La vérification de l'identité du demandeur s'effectuera conformément aux dispositions du chapitre 3.
Toutes les demandes de recouvrement ainsi que les actions subséquentes prises par l'AC doivent être signées par au moins deux représentants de l'AC. De plus, ces actions doivent toujours être documentées et conservées par l'AC.

4.5 Suspension et révocation d'un certificat

4.5.1 Motifs de révocation

La connaissance de la compromission avérée ou soupçonnée de la clé privée par le client ou l'abonné 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 faite.
La connaissance de la modification d'une information contenue dans le certificat par le client ou l'abonné 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'abonné dès lors qu'elle est en possession d'informations de nature à indiquer que la situation de l'abonné 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'abonné. Plus généralement, l'AC peut, à sa discrétion, révoquer le certificat d'une entité identifiée 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.

4.5.2 Personne pouvant demander une révocation

Seuls peuvent demander la révocation d'un certificat :

- l'abonné, responsable du certificat ;
- le mandataire de certification ;
- le personnel de l'AC émettrice ; ou
- le personnel de l'AE qui a enregistré la demande de l'abonné.

4.5.3 Procédure de demande de révocation d'un certificat

L'AC doit s'assurer que toutes les procédures et exigences concernant la révocation d'un certificat figurent dans la DPC ou dans un autre document public.

L'AC offre un moyen d'accès rapide, électronique ou téléphonique, au service de révocation qui authentifiera la demande dans des conditions fixées au Chapitre 3. 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 est justifiée et 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, l'abonné doit toujours être informé par une notification de la révocation de son certificat. Dans le cas d'une organisation, le mandataire de certification peut également être notifié. Cette notification doit indiquer la date à laquelle la révocation du certificat a pris effet. Elle peut prendre la forme d'un courrier électronique.

4.5.4 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.
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 4.5.1, alors la révocation doit être effectuée au plus vite.

4.5.5 Motifs de suspension

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

4.5.6 Personne pouvant demander une suspension

Sans objet.

4.5.7 Procédure de demande de suspension d'un certificat

Sans objet.

4.5.8 Limites d'une période de suspension

Sans objet.

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

Dès que la révocation du certificat d'une entité identifiée est effective, l'AC émettrice doit générer sans délais une nouvelle LCR (Liste des Certificats Révoqués) qui sera publiée au plus vite.

4.5.10 Exigences de vérification des LCR

Avant toute utilisation de certificats, notamment lorsque les dits certificats créent des effets juridiques, le tiers utilisateur doit impérativement vérifier la validité des certificats auxquels 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.

4.5.11 Publication des motifs de révocation

Les motifs de la révocation d'un certificat donné ne sont jamais divulgués à des tiers sauf en cas d'accord écrit de l'abonné ou du client.
Dans le cadre des audits et contrôles auxquels l'AC est soumise en vertu de la présente politique de certification, des éléments sur les motifs de révocation, non nominatifs et non liés à un certificat, pourront être fournis. D'une manière plus générale, ces éléments pourront être utilisés à des fins statistiques.

4.5.12 Exigences spéciales concernant la compromission des clés

En cas de compromission avérée ou soupçonnée de la clé privée de signature d'une AC, l'AC doit sans tarder en aviser toutes les AC avec lesquelles elle a un accord de certification croisée ou de reconnaissance mutuelle, ainsi que toutes les AGP qui l'accréditent.

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

4.6 Journalisation des évènements

4.6.1 Types d'événements consignés

L'AC doit consigner dans les registres de vérification 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 des mots de passe 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 non autorisées d'accès par réseau au système de l'AC ;
- tentatives non autorisées 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 abonnés, et de récupérer leurs clés ; et

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

- journaux des accès physiques ;
- maintenance et changements de la configuration du système ;
- changements apportés au personnel ;
- 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 abonnés.

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.

4.6.2 Fréquence de traitement des journaux d'événements

L'AC doit s'assurer que ses journaux sont revus par son personnel au moins chaque semaine, et que tous les éléments importants sont expliqués dans un résumé. 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'AC et de l'AE si une mesure est considérée suspecte.
Il faut documenter les mesures prises à la suite de ces examens.

4.6.3 Période de conservation des journaux

L'AC doit conserver sur place ses journaux pendant au moins un mois et ensuite les archiver conformément aux instructions indiquées à l'article 4.7.

4.6.4 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.

4.6.5 Procédures de sauvegarde des journaux

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

4.6.6 Système de collecte des journaux

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

4.6.7 Imputabilité

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

4.6.8 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'AC doit s'assurer qu'une évaluation de ces points vulnérables est effectuée, revue et révisée, après examen de ces événements.

4.7 Sauvegarde et archivage

Classe 2, 2+
Les certificats de signature numérique, les données nécessaires au recouvrement des clés de confidentialité, ainsi que les LCR produites par l'AC, sont conservés pendant au moins dix (10) ans après l'expiration des clés. Il faut conserver pendant au moins dix (10) ans après l'expiration des clés les renseignements liés à la gestion du cycle de vie des certificats, en particulier tous les renseignements liés à l'enregistrement, ainsi que les configurations et applications ayant servi à cette gestion.

Une copie de tout le matériel informatique archivé ou sauvegardé 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.
L'AC doit vérifier l'intégrité de ses archives au moins tous les six (6) mois.

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 au moins 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
- tous les accords de certification croisée, de reconnaissance mutuelle ou d'autre nature signés par CertiNomis avec d'autres AC et composantes 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.

4.8 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.

4.9 Compromission et mesures antisinistre

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'AC doivent être documentées.

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

La seule activité critique que l'AC doit maintenir en fonctionnement est la prise en compte et la publication des révocations de certificats.
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'AC doit également envisager un plan de secours et de redémarrage de ses activités.

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

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

- les AGP qui l'accréditent ;
- toutes les AC avec lesquelles elle a conclu des accords de certification croisée ou de reconnaissance mutuelle ;
- toutes les AE ; et
- tous les abonnés, tous les clients ;

En outre, l'AC doit :

- publier le numéro de série du certificat dans la LCR appropriée ;
- demander à toutes les AC avec qui elle a conclu des accords de certification croisée de révoquer tous les certificats qui certifient sa clé publique ; et
- révoquer tous les certificats signés au moyen du certificat de signature numérique révoqué.

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

- 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 numérique de toute autre entité, on suivra les directives de l'article 4.5.

4.9.2.1 Réduction du niveau du certificat d'une AC

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

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

En cas de compromission de la clé de signature numérique 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 4.9.2 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 faite.

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

L'AC doit définir dans un plan antisinistre les mesures à prendre pour rétablir une installation sécuritaire en cas de catastrophe naturelle ou de tout autre type de sinistre. Lorsque le dépôt de documents ne relève pas de l'AC, celle-ci doit s'assurer qu'il est précisé, dans tous contrats qui auraient été conclus avec le dépositaire, qu'un plan antisinistre doit être mis en place et documenté par le dépositaire.

4.10 Fin des activités d'une AC

Si l'AC interrompt ses activités, elle doit dans les plus brefs délais en aviser ses abonnés et ses clients, et prendre toutes les dispositions nécessaires pour que les clés et l'information de l'AC continuent d'être archivées. L'AC doit également aviser par écrit toutes les AC avec lesquelles elle a conclu des accords de certification croisée et de reconnaissance mutuelle.

En cas de changements dans la gestion des activités de l'AC, celle-ci doit en aviser toutes les entités pour lesquelles elle a émis des certificats et toutes les AC avec lesquelles elle a conclu des accords de certification croisée et de reconnaissance mutuelle.

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 4.7.

4.11 Fin d'abonnement

L'abonnement court tant que le certificat est en cours de validité ou qu'il a été renouvelé.
La personne qui entend mettre fin prématurément à son abonnement doit demander la révocation de son certificat.
La révocation constitue une fin d'abonnement, elle n'ouvre droit à aucun remboursement.
Les personnes qui peuvent demander la fin de l'abonnement sont les mêmes que celles pouvant demander la révocation du certificat conformément aux dispositions de l'article 4.5.2.
Les procédures de fin d'abonnement sont identiques à celles prévues pour la révocation du certificat, conformément aux dispositions de l'article 4.5.3

5 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

5.1 Mécanismes de contrôle de la sécurité physique des locaux de l'AC

Les locaux techniques de l'AC, qui accueillent les moyens de certification, doivent être fortement protégés. Il doivent être dans une zone à accès contrôlé, protégée contre tous les risques courants (incendie, inondation…).

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

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

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

5.2 Mesures de contrôle de la sécurité des procédures

5.2.1 Rôles de confiance

5.2.1.1 Rôles de confiance de l'AC

Le responsable de l'AC doit s'assurer 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 utilisateur a accès au système seulement pour les tâches qui lui incombent.

Le responsable de l'AC doit prévoir au moins trois types de rôles distincts pour le personnel de l'AC, en faisant la distinction entre les tâches suivantes :

Rôles de sécurité coffret
Qui ont pour tâche :

- de procéder à l'initialisation du coffret cryptographique au titre de détenteur d'un partie des secrets fondateurs ;
- de mettre en marche et d'arrêter le coffret cryptographique ;
- de configurer et maintenir des moyens cryptographiques de CertiNomis ;
- de gérer les droits de signature de jetons des opérateurs ;
- de vérifier des journaux sécurisés ;

Rôles fonctionnels-Opérateurs ICP
Qui ont pour tâche :

- de contrôler le déroulement des processus de gestion du cycle de vie des certificats
- de vérifier l'identification des demandeurs
- de transmettre des jetons signés indiquant leur accord après vérification pour émission ou révocation d'un certificat

- d'accéder aux données du système CertiNomis pour répondre aux demandes ;

Rôles d'exploitation
Qui ont pour tâche :

- de configurer et maintenir l'équipement et les logiciels du système de l'AC, à l'exclusion des moyens cryptographiques ;
- de gérer les droits sur le système à l'exclusion des moyens cryptographiques ;
- de mettre en marche et arrêter des services de l'AC, hors des moyens cryptographiques ;
- de vérifier les journaux , hors des moyens cryptographiques ;
- d'assurer le fonctionnement courant du système de l'AC ;
- d'effectuer les sauvegardes du système de l'AC ;

Pour certaines opérations très sensibles, plusieurs intervenants ayant des rôles distincts peuvent être nécessaires. En particulier pour le recouvrement de clés privée de confidentialité, au moins deux (2) rôles distincts sont nécessaires.
On peut répartir autrement les responsabilités, pourvu que le modèle utilisé partage les pouvoirs en offrant le même degré de robustesse contre les attaques de l'intérieur.
Les accès physiques et logiques aux logiciels et aux moyens seront répartis aux membres du personnel en fonction des rôles qui leur auront été attribués par le responsable de l'AC.

5.2.1.2 Rôles de confiance de l'AE

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

- accepter 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 toute confidentialité des supports physiques ou des codes d'activations aux abonnés.

L'AC devra veiller à ce que les tâches liées aux foncions d'une AE soient autant que possible réparties sur plusieurs personnes.

5.2.2 Nombre de personnes requises par tâche

L'AC doit s'assurer qu'une personne seule ne peut avoir accès aux clés privées de confidentialité d'un abonné qui, sous certaines conditions, peuvent être conservées par l'AC. Au moins deux personnes faisant partie du personnel de l'AC et possédant les qualités nécessaires doivent effectuer les opérations de recouvrement des clés sur demande du client.

Le contrôle multi-utilisateurs (c'est-à-dire par au moins deux utilisateurs) est également 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.

5.2.3 Identification et vérification pour chacun des rôles

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

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

Tous les intervenants sur le système de l'AC, ou d'une autre composante de l'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 forts.

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.

5.3 Mesures de contrôle du personnel

5.3.1 Antécédents professionnel, qualités, expériences

Le responsable de l'AC doit s'assurer que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation d'une AC ou d'une AE :

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

5.3.2 Procédures de vérification des antécédents

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

Les antécédents professionnels des postulants à un emploi auprès de l'AC, et l'ensemble de leur curriculum vitae, doivent être vérifiés conformément aux procédures de recrutement en vigueur. Le responsable de l'AC doit aussi vérifier que ces postulants :

- possèdent un profil de carrière dépourvu de licenciement consécutif à des fautes professionnelles, par exemple : la négligence, l'incompétence, la perte de confiance dans les fonctions exercées ;
- possèdent un casier judiciaire vierge ;

L'AC peut aussi, de manière discrétionnaire, vérifier que les postulants bénéficient d'un niveau de solvabilité garanti par un établissement bancaire.

5.3.2.1 Vérification des qualifications professionnelles

Le responsable de l'AC doit procéder à l'égard des postulants à un emploi auprès de l'AC, à la vérification des niveaux d'études exigés, des programmes de formation professionnelle requis et de toutes autres qualifications pertinentes.

5.3.2.2 Vérification de l'expérience

Aucune exigence autre que la vérification des antécédents professionnels.

5.3.2.3 Obligations du personnel de l'AC

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.

5.3.3 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 ou d'une AE ont reçu une formation complète concernant :

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

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.

5.3.4 Formation professionnelle – fréquence et exigences

Les exigences décrites à la section **5.3.3** 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.

Le personnel de l'AC doit participer à des séances de formation sur la sécurité au moins une (1) fois par année.

5.3.5 Rotation des emplois

Aucune exigence particulière.

5.3.6 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 ou d'une AE, l'AC peut lui interdire l'accès au système et prendre toutes sanctions disciplinaires adéquates.

5.3.7 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 5.1.1.

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

5.3.8 Documentation fournie au personnel

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

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

6 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, des AE déléguées, et des abonnés.

6.1 Production et installation des bi-clés

6.1.1 Production des bi-clés

Classe 2+
Les clés privées associées aux certificats de classe 2+ doivent être produites, conservées et utilisées exclusivement sur des moyens cryptographiques agréés par CertiNomis.

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'un bi-clé ne peut être utilisé que pour une fonction cryptographique donnée, à savoir :

- un bi-clé dédié à la création et à la vérification de signature ;
- un bi-clé dédié à la confidentialité.

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

Un bi-clé de signature numérique doit toujours être produit par l'abonné.

Un bi-clé de confidentialité, qui n'est pas utilisé à des fins de signature numérique, peut être généré par l'AC ou par l'abonné.

6.1.2 Remise des clés privées à l'abonné

Si le client a demandé la possibilité de recouvrement des clés de confidentialité alors que l'AC le propose, l'AC peut générer le bi-clé de confidentialité. Alors l'ensemble de la procédure de remise de clé privée doit être protégé en confidentialité tout au long du processus. Cette confidentialité peut être assurée par la remise d'un support physique ou par des mécanismes cryptographiques.

6.1.3 Remise de la clé publique à l'AC

La clé publique d'un abonné 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.

6.1.4 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.

6.1.5 Tailles des clés asymétriques

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

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

Les bi-clés des entités identifiées sont d'une complexité au moins équivalente à 512 bits pour l'algorithme RSA et, si possible, de 1024 bits. En particulier, tous les opérateurs de l'AC ont des certificats avec un clé d'au moins 1024 bits.

6.1.6 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.

Les choix suivants seront retenus par CertNomis :

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

6.1.7 Vérification de la qualité des paramètres

Le contrôle qualité des paramètres des clés doit être effectué en conformité avec l'article 6.1.6.

6.1.8 Nature de la ressource de production de clés

Les bi-clés de l'AC doivent être produits par un module cryptographique matériel. Les bi-clés de chiffrement lorsqu'ils sont générés par l'AC doivent être réalisés au moyen d'un module cryptographique matériel.

6.1.9 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).

6.1.9.1 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 d'abonnés : digitalSignature et/ou nonRepudiation
- pour les certificats de l'AC : keyCertSign et/ou cRLSign

6.1.9.2 Clé publique de confidentialité

Une clé publique de confidentialité peut être utilisée pour échanger ou établir une clé de session de confidentialité des données, ou pour chiffrer directement des données.
Le champ KeyUsage du certificat doit être utilisé conformément au profil des certificats. Ce champ doit comporter l'une des valeurs suivantes :

- keyEncipherment et/ou dataEncipherment.

6.2 Protection des clés privées

L'abonné 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 6

6.2.1 Normes relatives au calculateur cryptographique

La ressource cryptographique matérielle de l'AC doit être évaluable au niveau EAL 5 selon les Critères Communs.

6.2.2 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 regénération de la clé de l'AC doit être fait entre trois (3) personnes au minimum.

6.2.3 Recouvrement des clés privées

Les clés privées de signature numérique ne doivent jamais se trouver en main tierce et leur recouvrement est impossible.
En revanche, pour les clés de confidentialité, le client peut, lors de l'enregistrement, et s'il le souhaite et si l'AC le propose, demander le service de recouvrement. Selon le cas, l'AC générera alors la clé privée de confidentialité et sera en mesure de la reconstituer en cas de perte ou elle fournira au client les moyens de reconstituer ladite clé de confidentialité.

Si le client ne souhaite pas bénéficier du service de recouvrement de clés de chiffrement, l'abonné générera lui-même sa clé privée de confidentialité lors de l'enregistrement. Par conséquent, l'AC ne pourra jamais reconstituer cette clé.

6.2.4 Sauvegarde des clés privées

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

6.2.5 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 6.2.4.).

6.2.6 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 entités identifiées sont tant que possible générées par un moyen local. S'il s'avère nécessaire pour le service de recouvrement d'introduire un bi-clé depuis l'extérieur, celui-ci sera introduit chiffré et sera déchiffré en local, et au sein même de la ressource cryptographique, si elle existe. Les clés privées des entités identifiées sont tant que possible conservées chiffrées, n'étant en clair qu'au moment requis pour leur utilisation.

6.2.7 Méthode d'activation de la clé privée

L'abonné 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.

6.2.8 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'abonné 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.

6.2.9 Méthode de destruction des clés privées

Lorsque le certificat de signature numérique arrive à expiration ou s'il est révoqué, la clé privée ne peut plus servir à aucune opération et doit être détruite.
Lorsque le certificat de confidentialité arrive à expiration ou qu'il est révoqué et que tous les fichiers sauvegardés et archivés ont été déchiffrés ou transchiffrés, alors la clé de confidentialité ne sert plus et peut 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.
Si la clé de confidentialité est sur le même support que la clé de signature, elle devra être détruite en même temps que la clé de signature.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

L'AC émettrice doit archiver toutes les clés publiques de vérification conformément à l'article 4.7.

6.3.2 Périodes d'utilisation des clés publiques et privées

La période de validité de toutes les clés de 512 bits est d'au plus un (1) ans.

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.

6.4 Données d'activation

6.4.1 Génération et installation des données d'activation

Les données d'activation doivent être aléatoires ou choisies par l'abonné 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'abonné 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.

6.4.2 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.

6.4.3 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.

6.5 Mécanismes de sécurité informatique des postes de travail

6.5.1 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 de l'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.

6.5.2 Indice de sécurité informatique

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

6.6 Contrôle technique du système durant son cycle de vie

6.6.1 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.

6.6.2 Contrôle de la gestion de la sécurité

On doit appliquer une méthode de gestion de la configuration pour installer le cœur cryptographique de l'AC et en assurer la maintenance . La première fois qu'il est chargé, le logiciel de l'AC doit fournir une méthode permettant à l'AC 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 doit prévoir un mécanisme permettant de vérifier périodiquement l'intégrité des logiciels.

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

6.7 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.

L'AC doit s'assurer que ses protocoles et commandes sont définis dans sa DPC.

6.8 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.

7 FORME ET CONTENU DES CERTIFICATS ET DES LISTES DE REVOCATIONS

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.

7.1 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 7.1.2.

7.1.1 Signature du certificat

L'AC doit apposer avec sa clé privée un sceau sur le certificat. Ce sceau est le résultat d'une fonction mathématique appliquée sur l'ensemble des champs décrits à l'article 7.1.

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

- *tbsCertificate :* l'ensemble des champs décrits à l'article 7.1 ;
- *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.*

7.1.2 Champs d'extensions

L'AC doit supporter des sous-ensembles d'extensions normalisées et identifiés dans la sous section 4.2 du document de l'IETF : PKIX X.509 Certificate and CRL.
Les extensions permettent d'ajouter des informations sur l'abonné, l'AC émettrice, l'usage du certificat et sur les Listes de Certificats Révoqués.

7.1.3 Interprétation sémantique des champs critiques

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

7.2 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.

8 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.

8.1 Procédures de modifications

8.1.1 Délais de préavis

- Le responsable de l'AC doit donner un préavis de trente (30) jours aux abonnés et aux tiers 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 abonnés et aux tiers 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 abonnés et aux tiers utilisateurs dans les sept (7) jours d'un changement de la présente politique qui résulte d'une situation hors du contrôle du responsable de la politique, à condition que ce changement ait un impact sur eux.
- Le responsable de l'AC peut modifier la présente politique sans préavis aux abonnés et aux tiers utilisateurs lorsque, selon l'évaluation du responsable de la politique, ces modifications n'ont aucun impact sur eux.

8.1.2 Forme de diffusion des avis

Dans les cas nécessitant un préavis, le responsable de l'AC doit aviser les clients, les abonnés et les autres AC, avec lesquelles elle a des accords de certification croisée ou de reconnaissance mutuelle, des modifications apportées à la politique, en diffusant les changements sur le site WEB du responsable de la politique et par message électronique. Lorsque l'avis est à destination des autres AC, le préavis est expressément communiqué. Lorsque l'avis est à destination des abonnés et des clients, le préavis est communiqué par message électronique si les changements ont un impact majeur, et diffusé sur le site web de l'AC et du responsable de la présente politique dans tous les autres cas.

8.1.3 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 8 .1.1.

8.1.4 Traitement des commentaires

Aucune exigence particulière.

8.1.5 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, d'abonnés et/ou de tiers utilisateurs, le responsable de la politique peut, à sa discrétion, instituer une nouvelle politique avec un nouvel identificateur d'objet (OID).

8.2 Procédure de publication

8.2.1 Eléments 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.

8.2.2 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 abonnés et tiers utilisateurs à l'adresse URL suivante : http://www.certinomis.com. Une copie peut également être obtenue par courrier électronique.
Les AC émettrices de certificats qui utilisent l'identifiant (OID) de la présente Politique de Certification rendront accessible à leurs abonnés des copies de cette politique.

8.3 Procédures d'approbation de la DPC

L'AC est garante 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