



POLITIQUE DE CERTIFICATION

AC CORPORIS

© 2003 PK7 SAS, TOUS DROITS RESERVES

Date : 24 novembre 2003
Version : 2.1
Référence : MET-JSL/DA0100-03
OID PC : 1.2.250.1.86.2.1.20

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

Historique du document

Référence	Version	Date	Statut Rédaction	Validation
MET-JSL/DA 100-03	2.1	9/12/03	Document public	DA
MET-JSL/DA 100-03	2.0	24/11/03	Document définitif	DA
MET-JSL/DA 100-03	1.1	10/03/03	Document définitif	JSL/DA
MET-JSL/DA 108-02	1.0	10/12/02	Document définitif	JSL/DA

Historique des modifications :

Version 2.1	Révision pagination et corrections mineures
Version 2.0	Mise en conformité exigences ACR, refonte de l'organisation de la PC
Version 1.1	Révision de modification de processus
Version 1.0	Première version de la PC

Table des matières

TABLE DES MATIERES.....	3
1 PREAMBULE.....	8
2 PRESENTATION GENERALE	9
2.1 RESUME DE LA POLITIQUE DE CERTIFICATION CORPORIS.....	9
2.1.1 <i>Champ d'application</i>	9
2.1.2 <i>Applications appropriées</i>	10
2.1.3 <i>Liste des applications interdites</i>	10
2.2 INFRASTRUCTURE A CLE PUBLIQUE (ICP).....	10
2.3 COMPOSANTES DE L'ICP	11
2.3.1 <i>Autorité de Certification (AC)</i>	11
2.3.2 <i>Opérateur de Certification (OC)</i>	12
2.3.3 <i>Autorité d'enregistrement (AE)</i>	13
2.3.4 <i>Certificat</i>	14
2.3.5 <i>Liste de Certificats Révoqués (LCR)</i>	14
2.4 PARTIES UTILISATRICES DES SERVICES DE L'ICP	14
2.4.1 <i>Dispositif et Application</i>	14
2.4.2 <i>Client</i>	14
2.4.3 <i>Entité identifiée</i>	14
2.4.4 <i>Abonné</i>	14
2.4.5 <i>Tiers utilisateur (ou partie qui se fie)</i>	14
2.5 POLITIQUE DE CERTIFICATION ET DECLARATIONS DES PRATIQUES DE CERTIFICATION	15
2.5.1 <i>Identification</i>	15
2.5.2 <i>Politique de Certification (PC)</i>	15
2.5.3 <i>Déclaration des Pratiques de Certification (DPC)</i>	15
2.6 COORDONNEES DE LA PERSONNE RESPONSABLE.....	15
2.6.1 <i>Organisme responsable</i>	15
2.6.2 <i>Personne Responsable</i>	15
2.7 PERSONNE DETERMINANT LA CONFORMITE DE LA DPC AVEC LA PC	16
3 DISPOSITIONS GENERALES	17
3.1 OBLIGATIONS COMMUNES	17
3.2 OBLIGATIONS DE L'AC CORPORIS	17
3.2.1 <i>Obligations spécifique du service de publication</i>	18
3.2.2 <i>Obligations spécifique du service de recouvrement</i>	18
3.3 OBLIGATIONS DE L'AUTORITE D'ENREGISTREMENT	18
3.3.1 <i>Obligations spécifiques de l'Administrateur</i>	18
3.3.2 <i>Obligations spécifiques de l'opérateur</i>	19
3.4 OBLIGATIONS DU CLIENT	19
3.5 OBLIGATIONS DE L'ABONNE.....	19
3.6 OBLIGATIONS DU TIERS UTILISATEUR	20
3.7 RESPONSABILITE DE L'AC CORPORIS ET DE SON PERSONNEL.....	20
3.7.1 <i>Limites de responsabilité</i>	21
3.7.2 <i>Exonération de responsabilité</i>	21
3.7.3 <i>Force majeure</i>	21

3.8	RESPONSABILITE DE L'AE	22
3.9	RESPONSABILITES DU CLIENT	22
3.10	RESPONSABILITE DE L'ABONNE	22
3.11	INDEPENDANCE DES PARTIES ET ABSENCE DE ROLE DE REPRESENTATION	22
3.12	INTERPRETATION ET MISE EN APPLICATION	22
3.12.1	<i>Droit applicable</i>	22
3.12.2	<i>Règlement des différends</i>	23
3.12.3	<i>Règlement des litiges - Tribunal compétent</i>	23
3.12.4	<i>Intégralité, divisibilité, survie, notification</i>	23
3.13	PUBLICATION ET DEPOT DE DOCUMENTS	23
3.13.1	<i>Informations publiées</i>	23
3.13.2	<i>Fréquence de diffusion</i>	24
3.13.3	<i>Contrôle d'accès</i>	24
3.13.4	<i>Bases documentaires</i>	24
3.14	CONTROLE DE CONFORMITE	24
3.15	CONFIDENTIALITE DES DONNEES A CARACTERE PERSONNEL ET DES INFORMATIONS	25
3.15.1	<i>Données à caractère personnel détenues par l'AC Corporis et l'AE</i>	25
3.15.2	<i>Informations confidentielles</i>	25
3.15.3	<i>Données à caractère personnel contenues dans les Certificats et la LCR</i>	25
3.16	SECRET DES CORRESPONDANCES ET INTERCEPTIONS	25
3.17	DROITS RELATIFS A LA PROPRIETE INTELLECTUELLE	26
3.18	DISPOSITIONS PENALES	26
4	IDENTIFICATION ET VERIFICATION D'IDENTITE	27
4.1	ENREGISTREMENT INITIAL	27
4.1.1	<i>Types de nom</i>	27
4.1.2	<i>Règles de nommage</i>	27
4.1.3	<i>Règles d'interprétation des diverses formes de noms</i>	27
4.1.4	<i>Unicité des noms</i>	27
4.1.5	<i>Procédure de règlement des différends au sujet des noms</i>	27
4.1.6	<i>Reconnaissance, vérification et rôles des noms de marques de fabrique, de commerce et de services</i>	28
4.1.7	<i>Méthode de vérification de la possession de la clé privée</i>	28
4.1.8	<i>Vérification de l'identité d'un Abonné</i>	28
4.1.9	<i>Vérification du droit sur un Dispositif ou une Application</i>	28
4.2	VERIFICATION AUX FINS DE RENOUELEMENT DES CERTIFICATS	28
4.3	VERIFICATION AUX FINS DE RENOUELEMENT DES CLES APRES UNE REVOCATION	29
4.4	VERIFICATION AUX FINS DE RECOUVREMENT	29
4.5	VERIFICATION AUX FINS DE REVOCATION	29
5	DISPOSITIONS OPERATIONNELLES	30
5.1	DEMANDE DE CERTIFICAT	30
5.2	EMISSION ET DISTRIBUTION D'UN CERTIFICAT	30
5.3	ACCEPTATION DU CERTIFICAT	30
5.4	RECOUVREMENT DE CLES DE CONFIDENTIALITE	30
5.5	SUSPENSION ET REVOCATION D'UN CERTIFICAT	31
5.5.1	<i>Motifs de révocation</i>	31
5.5.2	<i>Personne habilitées à demander une révocation</i>	31
5.5.3	<i>Procédure de demande de révocation d'un Certificat</i>	31
5.5.4	<i>Prise en compte des révocations et délai de traitement</i>	31
5.5.5	<i>Motifs de suspension</i>	32
5.5.6	<i>Personne habilitées à demander une suspension</i>	32
5.5.7	<i>Procédure de demande de suspension d'un Certificat</i>	32
5.5.8	<i>Limites d'une période de suspension</i>	32
5.5.9	<i>Fréquence de publication de la liste des Certificats révoqués (LCR)</i>	32
5.5.10	<i>Exigences de vérification des LCR</i>	32
5.5.11	<i>Publication des motifs de révocation</i>	32

5.5.12	<i>Exigences spéciales concernant la compromission des clés</i>	32
5.6	JOURNALISATION DES EVENEMENTS.....	33
5.6.1	<i>Types d'événements consignés</i>	33
5.6.2	<i>Fréquence de traitement des journaux d'événements</i>	33
5.6.3	<i>Période de conservation des journaux</i>	34
5.6.4	<i>Protection des journaux</i>	34
5.6.5	<i>Procédures de sauvegarde des journaux</i>	34
5.6.6	<i>Système de collecte des journaux</i>	34
5.6.7	<i>Imputabilité</i>	34
5.6.8	<i>Evaluation de la vulnérabilité</i>	34
5.7	SAUVEGARDE ET ARCHIVAGE.....	34
5.8	RENOUVELLEMENT DES CLES.....	35
5.9	COMPROMISSION ET MESURES ANTI-SINISTRE.....	35
5.9.1	<i>Corruption des ressources informatiques, des logiciels et/ou des données</i>	35
5.9.2	<i>Révocation de la clé publique d'une composante de l'ICP</i>	35
5.9.3	<i>Compromission de la clé privée d'une composante de l'ICP</i>	36
5.9.4	<i>Sécurisation d'une installation après une catastrophe naturelle ou un autre sinistre</i>	36
5.10	FIN DES ACTIVITES.....	36
6	MESURES DE SECURITE PHYSIQUE, CONTROLE DES PROCEDURES ET DU PERSONNEL.....	37
6.1	MECANISMES DE CONTROLE DE LA SECURITE PHYSIQUE DES LOCAUX DE L'AC CORPORIS.....	37
6.2	MESURES DE CONTROLE DE LA SECURITE DES PROCEDURES.....	37
6.2.1	<i>Rôles de confiance de l'AC Corporis</i>	37
6.2.2	<i>Rôles de confiance de l'AE</i>	38
6.2.3	<i>Nombre de personnes requises par tâche</i>	38
6.2.4	<i>Identification et vérification pour chacun des rôles</i>	39
6.3	MESURES DE CONTROLE DU PERSONNEL.....	39
6.3.1	<i>Antécédents professionnel, qualités, expériences</i>	39
6.3.2	<i>Procédures de vérification des antécédents</i>	39
6.3.3	<i>Dispositions en matière de formation</i>	40
6.3.4	<i>Formation professionnelle – fréquence et exigences</i>	41
6.3.5	<i>Rotation des emplois</i>	41
6.3.6	<i>Sanctions en cas d'actions non autorisées</i>	41
6.3.7	<i>Contrôle des personnels des entreprises cocontractantes</i>	41
6.3.8	<i>Documentation fournie au personnel</i>	41
7	MESURES TECHNIQUES DE SECURITE.....	42
7.1	PRODUCTION ET INSTALLATION DES BI-CLES.....	42
7.1.1	<i>Production des bi-clés</i>	42
7.1.2	<i>Remise de la clé publique à l'AC Corporis</i>	42
7.1.3	<i>Remise de la clé publique de l'AC Corporis aux utilisateurs</i>	42
7.1.4	<i>Tailles des clés asymétriques</i>	42
7.1.5	<i>Production des paramètres des clés publiques</i>	43
7.1.6	<i>Vérification de la qualité des paramètres</i>	43
7.1.7	<i>Nature de la ressource de production de clés</i>	43
7.1.8	<i>Utilisation de la clé publique</i>	43
7.2	PROTECTION DES CLES PRIVEES.....	43
7.2.1	<i>Normes relatives au calculateur cryptographique</i>	44
7.2.2	<i>Contrôle des clés privées par plusieurs personnes</i>	44
7.2.3	<i>Recouvrement des clés privées</i>	44
7.2.4	<i>Sauvegarde des clés privées</i>	44
7.2.5	<i>Archivage des clés privées</i>	44
7.2.6	<i>Initialisation et conservation d'une clé privée dans un module cryptographique</i>	44
7.2.7	<i>Méthode d'activation de la clé privée</i>	44
7.2.8	<i>Méthode de désactivation des clés privées</i>	45
7.2.9	<i>Méthode de destruction des clés privées</i>	45

7.3	AUTRES ASPECTS DE LA GESTION DES BI-CLES	45
7.3.1	<i>Archivage des clés publiques</i>	45
7.3.2	<i>Périodes d'utilisation des clés publiques et privées</i>	45
7.4	DONNEES D'ACTIVATION.....	45
7.4.1	<i>Génération et installation des données d'activation</i>	45
7.4.2	<i>Protection des données d'activation</i>	46
7.4.3	<i>Autres aspects touchant les données d'activation</i>	46
7.5	MECANISMES DE SECURITE INFORMATIQUE DES POSTES DE TRAVAIL.....	46
7.5.1	<i>Sécurité informatique – Exigences techniques spécifiques</i>	46
7.5.2	<i>Indice de sécurité informatique</i>	46
7.6	CONTROLE TECHNIQUE DU SYSTEME DURANT SON CYCLE DE VIE.....	46
7.6.1	<i>Contrôle des développements des systèmes</i>	46
7.6.2	<i>Contrôle de la gestion de la sécurité</i>	47
7.7	MECANISMES DE CONTROLE DE LA SECURITE RESEAU.....	47
7.8	MECANISMES DE CONTROLE TECHNIQUE DU MODULE CRYPTOGRAPHIQUE	47
8	PROFIL DES CERTIFICATS ET DES LCR.....	48
8.1	FORME ET CONTENU DES CERTIFICATS.....	48
8.1.1	<i>Signature du Certificat</i>	48
8.1.2	<i>Champs d'extensions</i>	48
8.1.3	<i>Interprétation sémantique des champs critiques</i>	48
8.2	FORMES ET CONTENU DES LISTES DE CERTIFICATS REVOQUES	48
9	ADMINISTRATION DE LA POLITIQUE DE CERTIFICATION	50
9.1	PROCEDURES DE MODIFICATIONS	50
9.1.1	<i>Délais de préavis</i>	50
9.1.2	<i>Forme de diffusion des avis</i>	50
9.1.3	<i>Période de commentaires</i>	50
9.1.4	<i>Traitement des commentaires</i>	50
9.1.5	<i>Modifications nécessitant l'adoption d'une nouvelle politique</i>	50
9.2	PROCEDURE DE PUBLICATION.....	51
9.2.1	<i>Éléments non diffusés dans la DPC</i>	51
9.2.2	<i>Publication de la politique de Certification et de la DPC</i>	51
9.3	PROCEDURES D'APPROBATION DE LA DPC.....	51

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

AVERTISSEMENT

La présente Politique de Certification est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1^{er} juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de PK7. La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement par écrit par PK7 ou ses ayants droit, sont strictement interdites.

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

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

La Déclaration des Pratiques de Certification, propriété de la société PK7 peut être concédée par des accords de licence à toutes entités privées ou publiques qui souhaiteraient l'utiliser dans le cadre de leurs propres services de Certification.

*
**

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 7 / 51
---------	---	---------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

1 PREAMBULE

Le présent document constitue la Politique de Certification appliquée par la société PK7 en qualité d'Autorité de Certification Déléguée de CertiNomis SA dans le cadre de la fourniture de services de certification basés sur l'offre Corporis commercialisée par PK7. Il a pour objectif de définir les dispositions prévues pour la délivrance aux Abonnés du Client de Certificats à clé publiques, ainsi que les droits et obligations des parties prenantes aux services de certification assurés par l'Autorité de Certification Déléguée, appelée **AC Corporis** dans la suite du texte.

Les intervenants suivants devraient prendre connaissance de la présente Politique de Certification :

- tout Abonné détenteur de Certificat délivré par l'AC Corporis ;
- toute partie souhaitant se fier valablement à un certificat délivré par l'AC Corporis ;
- tout organisme délivrant un label, un référencement ou une qualification de tout ou partie des services de certification de l'AC Corporis, ainsi que tout tiers mandaté par cet organisme ;
- tout Client lié contractuellement à l'AC Corporis dans le cadre de son implication au service d'Autorité d'Enregistrement.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

2 PRESENTATION GENERALE

2.1 Résumé de la Politique de Certification Corporis

La Politique de Certification définie dans le présent document est destinée à être utilisée par les utilisateurs des services de certification Corporis souscrits par une personne morale, public ou privée, dans le cadre de la mise en œuvre d'applications sécurisées accessibles auxdits utilisateurs constituant de ce fait une communauté d'intérêt fédérée par ladite personne morale.

La Politique de Certification couvre la gestion et l'utilisation de Certificats contenant les clés publiques servant aux fonctions de vérification, d'authentification, d'intégrité et de concordance des clés. Les Certificats délivrés en vertu de la présente politique peuvent notamment servir à vérifier l'identité de correspondants échangeant du courrier électronique et 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 délivrance d'un Certificat de clé publique en vertu de la présente Politique de Certification ne signifie pas que le Client ou l'Abonné soit autorisé de quelque façon que ce soit à effectuer des transactions commerciales, ou autres, au nom de l'organisation qui exploite l'AC Corporis.

Pk7 s'engage à vérifier, grâce aux moyens techniques mis en place, que les demandes d'émission et de révocation des Certificats sont effectivement effectuées par des opérateurs autorisés par le Client Corporis dont le nom est porté dans les Certificats.

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

2.1.1 Champ d'application

Deux éléments déterminent le niveau de confiance d'un Certificat :

- la qualité de l'exploitation et du maintien de la sécurité technique de la plateforme de certification ; Pk7 applique des règles similaires pour les différentes plateformes qu'il gère en sa qualité d'opérateur, garantissant ainsi une qualité de service constante ;
- le mode d'enregistrement ; dans une communauté fermée gérée par une organisation prenant en charge l'enregistrement des membres de la communauté des utilisateurs de Certificats, l'identification de manière sûre des demandeurs est possible sans nuire à la qualité du Certificat ; tous les membres de la communauté faisant confiance à l'organisation peuvent ainsi se fier aux Certificats émis.

Les services de certification Corporis sont dédiés aux communautés fermées et permettent de créer un environnement de confiance en appliquant des règles d'enregistrement propres à ces communautés. L'enregistrement au travers des moyens techniques Corporis est délégué au fédérateur d'une communauté donnée, appelé le Client Corporis. Le nom de la communauté est porté dans le Certificat de manière explicite au sein du nom distinctif. En outre, cette communauté, selon les besoins, peut être régie par une convention de preuve gérée par le Client Corporis.

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 9 / 51
---------	---	---------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

2.1.2 Applications appropriées

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

Les Certificats émis par l'AC Corporis au sein d'une communauté sont appropriés pour vérifier :

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

Selon les besoins, les usages peuvent être couverts par une convention de preuve liant les membre de la communauté vis-à-vis de l'usage des Certificats.

2.1.3 Liste des applications interdites

Les certificats émis par l'AC Corporis ne devraient pas être utilisés :

- hors du cadre de la communauté portée dans les certificats ni hors du cadre de la convention de preuve liant explicitement cette communauté quand elle existe ;
- à des fins de chiffrement de données, telles que notamment les données situées sur le poste de travail d'un Abonné.

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

Tout Client ou Abonné utilisant les certificats en dehors des applications appropriées et, en particulier, dans une application interdite telles que définies aux termes de la présente politique, le fait sous sa seule responsabilité et à ses entiers risques et périls.

Tout Tiers utilisateur se fiant à un Certificat alors que l'application est interdite ou restreinte aux termes de la présente Politique de Certification en assume seul tous les risques.

La responsabilité de PK7 ne pourra être mise en jeu dans aucune des hypothèses visées ci-dessus.

Sauf accord préalable écrit et signé d'un représentant légal de Pk7, nul n'est autorisé à utiliser la clé privée associée à un Certificat pour signer un autre Certificat ou une LCR en tant qu'AC.

2.2 Infrastructure à Clé Publique (ICP)

Une Infrastructure à Clé Publique (ICP) est un ensemble de moyens techniques, tels que notamment des systèmes de cryptographie asymétrique, humains, documentaires et contractuels mis à la disposition d'utilisateurs pour assurer un environnement sécurisé aux échanges électroniques.

La mise en place d'une ICP participant à la sécurité et à la confiance ouvre une palette de services à valeur ajoutée pour les transactions électroniques telles que notamment le courrier électronique, les transactions commerciales, les téléprocédures et la protection locale des données.

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 10 / 51
---------	---	----------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
	MET-JSL/DA0100-03		2.1	

Lesdits services à valeur ajoutée ont pour fonction d'assurer l'intégrité des messages, l'identification et l'authentification¹, la non répudiation de l'origine, ainsi que la confidentialité.

2.3 Composantes de l'ICP

La fourniture de services de certification, à savoir la délivrance de Certificats ou de tout autre service lié aux signatures numériques, met en œuvre plusieurs métiers ou fonctions, desquels découlent des rôles et des responsabilités distincts.

2.3.1 Autorité de Certification (AC)

En sa qualité d'Autorité de Certification racine, **CertiNomis SA** déploie une hiérarchie d'AC engendrant des AC subordonnées, dites AC filles. Toute AC fille revêtant le statut de personne morale juridiquement indépendante et certifiée par CertiNomis est dite AC Déléguée (**ACD**), à l'instar de **PK7 SAS**, expressément autorisé par CertiNomis à fournir des services de certification dans le cadre de son offre commerciale **Corporis™**. Ainsi, une Autorité de Certification qui n'est pas ACD et qui se certifie elle-même est dite Autorité de Certification racine, ou **ACR**.

L'Autorité de Certification (**AC Corporis**), en la personne de PK7 SAS, est responsable de la validité des Certificats qu'elle émet et de l'ensemble du processus de certification, tel que notamment la révocation des Certificats et la publication des Listes de Certificats Révoqués. Cette responsabilité s'applique tant vis-à-vis des Clients et Abonnés que de toute personne se fiant à un Certificat qu'elle a émis. A ce titre, elle édicte une Politique de Certification et valide les Déclarations de Pratique de Certification respectées par les différentes composantes de l'ICP, internes ou tierces.

L'Autorité de Certification peut par ailleurs fournir des services annexes, selon la demande et le type de Certificat, comme par exemple la conservation et le recouvrement des clés, ou la publication des Certificats.

La garantie apportée par l'AC Corporis résulte pour partie du cadre réglementaire et contractuel qu'elle définit et s'engage à respecter, et pour partie de la qualité de la technologie mise en œuvre. Elle s'appuie en particulier sur un Opérateur de Certification dont elle approuve et audite les moyens et procédures.

Les principales fonctions assurées par l'AC Corporis sont les suivantes :

- génération des Certificats liant le nom distinctif des Entités identifiées à leur clé publique respective ;
- coordination les demandes de Certificat ;
- révocation des Certificats ;
- diffusion les informations relatives aux Certificats et aux autorités révoqués ;
- surveillance de la stricte application de la PC et des procédures par les différentes composantes de l'ICP, les Clients et les Abonnés ;
- vérification de la légitimité des opérations effectuées par l'Administrateur ou un Opérateur autorisés par le Client dont le nom est porté dans le nom distinctif des Certificats et ;
- mise en œuvre des moyens techniques, humains et organisationnels nécessaires à la réalisation des prestations auxquelles l'AC Corporis s'engage.

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

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

2.3.1.1 Responsable de l'AC Corporis

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

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

2.3.1.2 Intervenants requis pour la gestion de l'AC Corporis

Le responsable de l'AC Corporis se conformant à la présente politique attribue notamment au personnel et aux opérateurs mandatés dont il est responsable les missions suivantes :

- maintien, administration, exploitation et protection des machines et logiciels utilisés par l'AC Corporis ;
- gestion des informations et des dossiers des Clients de l'AC Corporis ;
- planification et gestion de l'évolution de l'infrastructure technologique de l'AC Corporis ;
- respect des règles, principes et procédures énoncés dans la PC et la DPC ;
- gestion des autorisations, des droits, des attributs, des clés et les Certificats du personnel de l'AC Corporis ainsi que des opérateurs mandatés ;
- traitement des journaux de vérification de la sécurité de l'AC Corporis.

L'AC Corporis veille à ce que le personnel remplissant ces missions :

- connaisse et respecte les règles, principes et procédures énoncés dans la PC et la DPC ;
- soit nommément désigné pour assurer ces missions ;
- s'il ne s'agit pas d'un salarié employé à plein temps par l'AC Corporis, soit dûment mandaté et expressément autorisé par le responsable de l'AC Corporis pour effectuer ces missions.

2.3.2 **Opérateur de Certification (OC)**

L'Opérateur de Certification (**OC**) 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, de la sécurité du personnel et des locaux et, plus généralement, du respect des procédures et de toutes dispositions permettant de garantir un niveau de fiabilité élevé.

Il est techniquement dépositaire de la clé privée utilisée par l'AC Corporis pour la signature des Certificats. Sa mission essentielle est donc de protéger cette clé privée contre toute compromission.

La responsabilité de l'OC ne peut être engagée que par l'AC Corporis et se limite au respect des procédures établies dans la Déclaration des Pratiques de Certification approuvée par elle. L'AC Corporis assure régulièrement le contrôle et l'audit de l'Opérateur de Certification.

Dans la présente Politique de Certification, son rôle et ses obligations ne sont pas distingués de ceux de l'AC Corporis qui est son propre OC.

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 12 / 51
---------	---	----------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

2.3.3 Autorité d'enregistrement (AE)

L'Autorité d'Enregistrement (**AE**) applique des procédures d'identification des personnes physiques ou morales, conformément aux règles définies par elle-même en fonction de ses besoins. Son rôle est d'établir que le demandeur justifie de l'identité et des 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 assure le lien entre l'AC Corporis et l'Abonné. Elle est dépositaire des informations personnelles de l'Abonné, qu'elle ait ou non eu un contact physique avec celui-ci au cours de la procédure d'identification.

L'AC Corporis assure un devoir de contrôle et d'audit de l'AE.

Dans le cadre de la mise en place de la fonction d'AE, le responsable de l'AC Corporis attribue au Client, personne morale juridiquement indépendante, les missions suivantes :

- coordination des demandes d'identification électronique ;
- vérification des caractéristiques d'identification des Entités identifiées, selon le type du Certificat ;
- distribution à l'Abonné, en cas de besoin, d'un support physique (carte à puce, papier...) nécessaire à l'acquisition, au transport ou à l'utilisation de son Certificat ;
- gestion et protection des données personnelles des Abonnés, telles que notamment les coordonnées privées de l'Abonné, si elles sont exigées par l'AE dans le cadre du processus d'enregistrement, et ;
- administration, exploitation et protection des moyens techniques mis à la disposition de l'AE par l'AC Corporis et utilisés par ladite AE pour remplir ces missions.

Dans la présente Politique de Certification, l'AE est conjointement placée sous la responsabilité du Client souscrivant aux services de certification et de l'AC Corporis elle-même. L'AE applique ses propres règles de contrôle pour l'émission et la révocation des Certificats, l'AC Corporis lui imposant seulement des mesures visant à s'assurer que les demandes d'émission et de révocation sont sous la seule responsabilité du Client.

L'AE désigne des acteurs particuliers interagissant avec l'AC Corporis dans le cadre de la gestion du cycle de vie des Certificats :

- **l'Administrateur** : personne physique sous la responsabilité du Client, nomé et formellement mandatée par le Client, garante des opérations d'enregistrement effectuées pour le compte du Client et responsable de l'AE ; l'identification de l'Administrateur vis-à-vis de l'AC Corporis est réalisée grâce à un certificat dit de classe « 3+ » (enregistrement en face-à-face) délivré par une AC tierce du marché, CertiNomis SA en l'occurrence ; l'Administrateur est également un Opérateur et un Abonné, aux sens définis ci-dessous ;
- **l'Opérateur** : personne physique sous la responsabilité de l'Administrateur qui lui délègue tout ou partie de ses prérogatives pour ce qui concerne les opérations d'enregistrement et de révocation des Certificats ; l'Opérateur est identifié vis-à-vis de l'AC Corporis grâce à un Certificat délivré par l'AC Corporis, à l'initiative de l'Administrateur ; l'Opérateur est également un Abonné au sens défini ci-dessous.

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

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

2.3.4 Certificat

Attestation électronique délivrée par l'AC Corporis, liant une Entité identifiée et les données afférentes à la vérification de signature (respectivement au chiffrement) des échanges, messages et documents électroniques, afin d'en assurer l'authentification et l'intégrité (respectivement la confidentialité).

Le Certificat est sous la responsabilité de l'Abonné.

2.3.5 Liste de Certificats Révoqués (LCR)

Fichier informatique comportant les numéros de série des Certificats révoqués, horodaté, signé et publié périodiquement par l'AC Corporis selon des conditions telles que stipulées dans la présente Politique de Certification.

2.4 Parties utilisatrices des services de l'ICP

Les parties utilisatrices des services de l'ICP se définissent comme l'ensemble des intervenants acquérant, utilisant et se fiant aux Certificats émis par l'AC Corporis.

2.4.1 Dispositif et Application

Matériel et/ou logiciel mettant en oeuvre un ou des Certificats pour établir automatiquement un contexte de sécurité qui lui est propre, tel que notamment un serveur Web ou un routeur, utilisant un Certificat pour s'authentifier lors d'un échange.

2.4.2 Client

La personne morale qui contracte avec l'AC Corporis pour bénéficier de ses services et accepte de ce fait toutes les responsabilités associées telles que stipulées par contrat entre PK7 et le Client.

2.4.3 Entité identifiée

La personne, le Dispositif ou l'Application dont les données d'identification sont inscrites dans le Certificat.

2.4.4 Abonné

La personne physique responsable du Certificat et de son utilisation. L'Abonné est le détenteur physique du Certificat et s'engage à respecter les conditions d'utilisation et à remplir les obligations stipulées par l'AC Corporis émettrice du Certificat. Le terme Abonné désigne également la personne demanderesse d'un certificat dans la présente PC, permettant ainsi d'en faciliter la lecture.

2.4.5 Tiers utilisateur (ou partie qui se fie)

Toute personne ayant connaissance des dispositions de la présente Politique de Certification et se fiant au Certificat d'un Abonné afin de vérifier, au moyen de la clé publique qui y est contenue, l'authenticité d'une signature numérique apposée par l'Abonné (respectivement de chiffrer des données à l'attention de l'Abonné en utilisant cette même clé).

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
	MET-JSL/DA0100-03		2.1	

2.5 Politique de Certification et Déclarations des Pratiques de Certification

La Politique de Certification indique quel niveau de confiance peut être attribué à un Certificat, suivant les principes énoncés, tandis que la Déclaration des Pratiques de Certification stipule au plan pratique comment est établi ce niveau de confiance.

2.5.1 Identification

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 de façon biunivoque la Politique de Certification.

L'identification de la présente Politique de Certification est la suivante :

OID Corporis : 1.2.250.1.86.2.1.20

2.5.2 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. La Politique de Certification 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.

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

2.5.3 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. La Déclaration des Pratiques de Certification fournit une description détaillée des services offerts et de toutes les procédures associées à la gestion du cycle de vie des Certificats. Elle peut comprendre également des services spécifiques.

2.6 Coordonnées de la personne responsable

2.6.1 Organisme responsable

La présente Politique de Certification est sous la responsabilité de la société **PK7 SAS** agissant en qualité d'Autorité de Certification Déléguée de **CertiNomis SA**. Dans la suite du présent document, « PK7 » et « AC Corporis » désignent donc indifféremment l'Autorité de Certification émettrice de la PC.

2.6.2 Personne Responsable

Monsieur Didier ARPIN
Président-Directeur Général
PK7 SAS
20-22, rue Louis Armand
75015 Paris

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

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

Téléphone : (33) (0)1 58.09.80.50
 Télécopieur : (33) (0)1.58.09.80.51
 Courrier électronique : didier.arpin@pk7.fr

2.7 Personne déterminant la conformité de la DPC avec la PC

La société PK7 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.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

3 DISPOSITIONS GENERALES

Le présent Article stipule les dispositions appliquées respectivement par l'AC Corporis, son personnel et les diverses entités composant l'ICP, dont notamment l'AE, ainsi que les obligations auxquelles doivent se conformer les parties utilisatrices des services de certification. Il précise également un certain nombre de dispositions juridiques relatives, notamment, à la loi applicable et à la résolution des litiges.

L'AC Corporis, l'AE, leur personnel respectif, les composantes de l'ICP et les parties utilisatrices des services de certification 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.

3.1 Obligations communes

Les différentes composantes de l'ICP doivent :

- assurer l'intégrité et la confidentialité des clés privées dont elles sont dépositaires, ainsi que des données d'activation desdites clés privées, le cas échéant ;
- n'utiliser les clés publiques et privées dont elles sont dépositaires (i) qu'aux seules fins pour lesquelles elles ont été émises et (ii) avec les moyens appropriés ;
- mettre en œuvre les moyens techniques adéquats et employer les ressources humaines nécessaires à la réalisation des prestations auxquelles elles s'engagent ;
- documenter leurs procédures internes de fonctionnement à l'attention de leur personnel respectif ayant à en connaître dans le cadre des fonctions qui lui sont dévolues en qualité de composante de l'ICP ;
- respecter et appliquer les termes de la présente PC qu'elles reconnaissent ;
- accepter le résultat et les conséquences d'un contrôle de conformité et, en particulier, remédier aux non-conformités qui pourraient être révélées et ;
- respecter les conventions qui les lient aux autres entités composantes de l'ICP.

3.2 Obligations de l'AC Corporis

Le personnel de l'AC Corporis et opérateurs dûment mandatés se conforment à toutes les exigences pertinentes de la présente Politique de Certification et de la DPC associée, ainsi qu'à la PC et à la DPC édictées par l'ACR. Ils sont également tenus de respecter les droits des Clients, Abonnés et Tiers utilisateurs, eu égard aux lois et règlements en vigueur.

L'AC Corporis :

- génère les Certificats, publie les informations concernant la révocation desdits Certificats (Article 3.2.1) et procède à leur renouvellement ;
- établit et applique la DPC, sous le contrôle de l'ACR CertiNomis ;
- documente les schémas de certification qu'elle entretient avec des AC tierces ;
- utilise des ressources cryptographiques d'un niveau de sécurité compatible avec la classe de Certificats émis ;
- contrôle les accès physiques en les limitant strictement et exclusivement aux personnes dûment autorisées ;
- maintient la disponibilité de l'ensemble de ses services, en veillant à minimiser les effets des opérations de maintenance et de réparation du système, ou encore d'autres facteurs qui échappent à son contrôle ;
- met à la disposition de l'AE l'ensemble des moyens techniques nécessaires à la réalisation de ses obligations, à l'exception des postes informatiques utilisés pour l'accès aux services de certification.

 POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
	Référence	Version
	MET-JSL/DA0100-03	2.1

3.2.1 Obligations spécifique du service de publication

Le responsable du service de publication met à jour et préserve l'intégrité des Listes de Certificats Révoqués qu'il publie. Il informe 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. Il maintient également la disponibilité de ces LCR en prenant toutes les mesures qu'il juge pertinentes.

3.2.2 Obligations spécifique du service de recouvrement

Aucune obligation dans le cadre de la présente édition de la Politique de Certification.

3.3 Obligations de l'Autorité d'Enregistrement

Toute AE agréée par l'AC Corporis se conforme à l'ensemble des exigences de la présente Politique de Certification, ainsi qu'à des procédures internes qu'elle formalise dans le cadre de la gestion du cycle de vie des Certificats destinés aux membres de la communauté qu'elle fédère. En outre, l'AE :

- traite les demandes de Certificat en s'assurant de leur pertinence ;
- vérifie les données personnelles d'identification et les données portées dans le Certificat ;
- transmet à l'AC Corporis une trace imputable de la validité de cette vérification ;
- transmet en toute confidentialité les codes d'activation et, le cas échéant, les supports physiques de confinement aux Abonnés et ;
- conserve et protège en confidentialité et en intégrité toutes les données à caractère personnel et d'identification collectées lors des opérations d'enregistrement ;
- se soumet à tout audit que pourrait demander l'AC Corporis quant à l'utilisation des moyens techniques mis à sa disposition, à l'existence avérée et à la communication des procédures d'utilisation desdits moyens techniques aux Opérateurs et aux Administrateurs, sans préjudice des dispositions de protection du secret professionnel auxquelles pourrait être soumise l'AE.

L'AE veille en outre à ce que son personnel :

- connaisse et respecte les règles, principes et procédures énoncées dans la PC ou établies par elle-même ;
- soit nommément désigné par le responsable de l'AE et ;
- soit salarié de l'AE ou, dans le cas contraire, soit un mandataire dûment et expressément autorisé par le responsable de l'AE.

3.3.1 Obligations spécifiques de l'Administrateur

L'Administrateur :

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

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

3.3.2 Obligations spécifiques de l'opérateur

L'Opérateur :

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

3.4 Obligations du Client

Outre les obligations lui incombant en sa qualité d'AE, telles que stipulées à l'Article 3.3, le Client :

- se conforme à toutes les exigences de la présente Politique de Certification et fait respecter ces exigences aux parties utilisatrices ;
- déclare auprès de l'AC Corporis le nom de la communauté qu'il souhaite voir porter dans le Certificat et garantit à l'AC Corporis qu'il en dispose le droit d'usage ;
- désigne nominativement et formellement un Administrateur et (i) porte à sa connaissance les obligations y afférents, et (ii) lui fait signer une convention d'utilisation du Certificat d'Administrateur ;
- fait respecter une politique de sécurité sur les postes informatiques utilisés pour mettre en œuvre les Certificats ;
- garantit que les informations qu'il fournit à l'AC Corporis, notamment pour l'identification de l'Entité identifiée, sont exactes et complètes, et que les demandes transmises sont valides ;
- s'il soupçonne la compromission d'une clé privée en avise l'AC Corporis dans les plus brefs délais, selon les instructions données par celle-ci et ;
- le cas échéant, établit une convention de preuve associée à l'utilisation des Certificats et liant les membres de la communauté d'intérêt dont il est fédérateur.

3.5 Obligations de l'Abonné

Les Certificats Corporis émis au nom du Client sont expressément exclus pour des utilisations au nom personnel de l'Abonné.

L'Abonné doit se conformer à toutes les exigences de la présente Politique de Certification et des procédures internes formalisées par l'AE dont il dépend. L'Abonné doit exclusivement utiliser ses clés privées et Certificats à des fins autorisées par la présente Politique de Certification, dans le respect des lois et règlements en vigueur.

En particulier, l'Abonné :

- garantit que les informations qu'il fournit à l'AC Corporis ou à l'AE, notamment pour l'identification de l'Entité identifiée, sont exactes, complètes et que les documents transmis ou présentés sont valides ;
- est tenu de protéger en confidentialité et en intégrité ses clés privées, ses codes d'activation ou d'accès, conformément à l'Article 7.2 et doit prendre toutes les mesures raisonnables pour en éviter la perte, la divulgation, la compromission, la modification ou l'utilisation non autorisée ;

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

- s'engage à suivre toute prescription du Client en matière de politique de sécurité dans le cadre de l'usage du Certificat et ;
- doit communiquer à l'AE, par les canaux qu'elle aura désignés, toute information ayant pour conséquence la révocation de son Certificat et, notamment, s'il soupçonne la compromission d'une clé privée, en avise l'AE dont il dépend dans les plus brefs délais, selon les instructions données par celle-ci.

L'individu 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 Corporis à utiliser son Certificat et les clés associés selon les règles prévues à cet effet.

3.6 Obligations du Tiers utilisateur

Le Tiers utilisateur doit se conformer à toutes les exigences stipulées dans le cadre de la présente Politique de Certification, document contractuel qu'il reconnaît expressément avoir lu et approuvé.

Avant toute utilisation d'un Certificat émis par l'AC Corporis, notamment lorsque ledit Certificat crée des effets juridiques, le Tiers utilisateur doit impérativement vérifier auprès de l'AC Corporis la validité du Certificat auquel il entend se fier en consultant les Listes des Certificats Révoqués appropriées les plus récentes, ainsi qu'en vérifiant sa validité intrinsèque, en particulier la signature électronique apposée par l'AC Corporis ainsi que la validité de tout Certificat figurant 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, PK7 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 (i) la clé publique du Certificat correspond à la clé privée de signature utilisée et (ii) que le Certificat est utilisé à des fins pertinentes et conformément aux applications autorisées

Enfin, le Tiers utilisateur ne doit utiliser les Certificats que conformément à la procédure de validation de l'itinéraire de Certification telle que spécifiée dans les normes X509 et PKIX. et déterminée par la recommandation ISO/IEC 9594-8.

3.7 Responsabilité de l'AC Corporis et de son personnel

L'AC Corporis n'est tenue qu'à une obligation de moyen pour la mise en œuvre des services de certification qu'elle fournit. Dans l'hypothèse où sa responsabilité serait mise en cause, celle-ci pourra être engagée selon les règles du droit commun.

L'AC Corporis est responsable vis-à-vis des Clients, Abonnés et Tiers utilisateurs, des opérations relatives aux services de certification réalisés 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 Corporis est responsable de l'information des Clients et des Abonnés, relativement aux procédures appliquées durant le cycle de vie des Certificats, dont notamment l'émission, la révocation et le retrait des Certificats.

Les membres du personnel de l'AC Corporis et les opérateurs mandatés à qui sont assignés des rôles relatifs à l'ICP (responsable de l'AC Corporis, responsable de la sécurité de l'AC Corporis, ...), sont personnellement responsables de leurs actes dont l'imputabilité est garantie par l'AC Corporis à des fins probatoires.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
	MET-JSL/DA0100-03		2.1	

3.7.1 Limites de responsabilité

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

L'AC Corporis 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.

3.7.2 Exonération de responsabilité

L'AC Corporis 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 Corporis n'assume aucun engagement quant à la signification ou l'authenticité des renseignements portés dans le Certificat à la demande de l'AE.

L'AC Corporis 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 Corporis n'assume aucun engagement ni responsabilité quant à l'utilisation par l'Abonné ou le Tiers utilisateur des Certificats et bi-clés qu'elle émet, 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 DPC associée, dans la notice d'assurance ou dans le contrat d'abonnement.

3.7.3 Force majeure

L'AC Corporis 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.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

3.8 Responsabilité de l'AE

La responsabilité de l'AE vis-à-vis des Tiers utilisateurs personnes physiques ou morales juridiquement indépendants du Client ne pourra être engagée que par l'AC Corporis. En particulier, la responsabilité de l'AE ne pourra être engagée de quelque façon que ce soit quant à l'application par l'AC Corporis des dispositions contractuelles entre l'AC Corporis et l'ACR CertiNomis, telle que notamment la DPC.

3.9 Responsabilités du Client

Le Client accepte toutes les responsabilités associées à son rôle d'AE par la signature du contrat d'ouverture des services de certification Corporis, qu'il s'engage à respecter.

3.10 Responsabilité de l'Abonné

L'Abonné 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 ;
- la sécurité de ses équipements matériels, logiciels et réseaux télématiques impliqués dans l'utilisation de ses Certificats ;
- 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 ;
- l'utilisation de ses clés et Certificats, qui doit être conforme à la présente Politique de Certification.

3.11 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 Corporis, de l'une des composantes de l'ICP, du responsable de l'AC Corporis et du personnel de l'AC Corporis 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 Corporis 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 Corporis 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.

3.12 Interprétation et mise en application

3.12.1 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.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

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

3.12.3 Règlement des litiges - Tribunal compétent

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

3.12.4 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 de ladite Politique de Certification.

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

3.13 Publication et dépôt de documents

3.13.1 Informations publiées

La Politique de Certification, les éléments de la DPC rendus publics, 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 Corporis à l'adresse suivante : <http://www.pk7.fr>, soit communiqués dans le cadre de la relation commerciale avec le Client.

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 23 / 51
---------	---	----------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
	MET-JSL/DA0100-03		2.1	

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

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

La Liste des Certificats Révoqués est publiée par l'AC Corporis, ainsi que les Certificats dont la publication est dûment autorisée par le Client.

3.13.2 Fréquence de diffusion

Les Listes de Certificats Révoqués sont mises à jour dans des délais tels que prévus à l'Article 5.5.4.

La publication de la Politique de Certification et des éléments de la DPC rendus publics respecte les dispositions de l'Article 9.2 (Procédure de publication) de la présente Politique de Certification.

3.13.3 Contrôle d'accès

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

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

3.13.4 Bases documentaires

L'AC Corporis diffuse les informations stipulées à l'Article 3.13.1 (Informations publiées). S'agissant des annuaires, l'AC Corporis peut choisir de publier elle-même ou d'utiliser les services d'une de ses composantes pour assurer le service de publication.

3.14 Contrôle de conformité

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

Cette vérification comprend :

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

Ce contrôle de conformité est réalisé sur demande d'une AGP ou sur demande de l'AC Corporis elle-même, selon les conditions précisées dans la DPC.

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 24 / 51
---------	---	----------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
	MET-JSL/DA0100-03		2.1	

3.15 Confidentialité des données à caractère personnel et des informations

3.15.1 Données à caractère personnel détenues par l'AC Corporis et l'AE

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 Corporis ou par un de ses représentants (CNIL, <http://www.cnil.fr>).

En vertu de la loi, 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 »¹, mis à leur disposition par l'AE, selon des modalités qu'elle communique aux Abonnés lors de leur enregistrement aux services de certification Corporis.

L'AC Corporis et l'AE respectent rigoureusement toutes les prescriptions légales applicables et explique les modalités concrètes d'application de la loi sur son site Web.

Les dispositions de la présente Politique de Certification respectent 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 Corporis ou l'AE relativement à une personne physique ou morale (par exemple : procédure d'enregistrement, révocation, autres événements consignés, correspondances échangées entre l'Abonné et l'AC Corporis ou l'AE, etc.) sont considérées comme confidentielles et ne sont divulguées qu'avec le consentement préalable de l'Abonné.

3.15.2 Informations confidentielles

La clé privée de signature numérique de chaque Abonné doit demeurer strictement confidentielles. La divulgation par l'Abonné de ces informations secrètes ou de toute autre information afférente permettant notamment leur délivrance, leur utilisation ou leur révocation, est à ses propres risques et périls.

3.15.3 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 confidentielles, sauf si ledit Client ou 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 leurs dates de révocation. Les causes de révocation des Certificats sont tenues strictement confidentielles par l'AC Corporis.

3.16 Secret des correspondances et interceptions

Le secret des correspondances émises par voie de télécommunication 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 Corporis, ni 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 Corporis, sauf

¹ Terme utilisé par la CNIL pour désigner le point de contact entre la CNIL et l'

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

dans les cas prévus dans la présente politique, ou dans le cadre du régime des interceptions ordonnées par l'autorité judiciaire ou des interceptions de sécurité en vertu de la loi n°91-646 du 10 juillet 1991 (JO du 13 juillet 1991, rectification JO du 10 août 1991).

3.17 Droits relatifs à la propriété intellectuelle

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

Tous les droits de propriété intellectuelle détenus par PK7 sont protégés par la loi, règlement et autres conventions internationales applicables. Ils sont susceptibles d'entraîner la responsabilité civile et pénale en cas de leur non respect. Par exemple, conformément à la loi n°98-536 du 1^{er} juillet 1998 (Journal officiel du 2 juillet, p.10075) et à la directive européenne 96/6/CE du 11 mars 1996, les bases de données constituées par PK7 sont protégées. Le texte de la loi peut être consulté sur le site suivant : <http://www.legifrance.gouv.fr>

3.18 Dispositions pénales

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

Les peines encourues varient de 1 à 3 ans d'emprisonnement assorties 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, ...etc.) est sanctionnée par les Articles L 716-1 et suivants du Code de la propriété intellectuelle.

 POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
	Référence	Version
	MET-JSL/DA0100-03	2.1

4 IDENTIFICATION ET VERIFICATION D'IDENTITE

Le présent Article stipule les dispositions prises par l'AC Corporis en matière d'enregistrement des demandes de Certificat. Il définit également les exigences en matière de pouvoir, représentation et mandat.

4.1 Enregistrement initial

4.1.1 Types de nom

Chaque entité est dotée d'un nom distinctif X501 (DN) porté dans le champ `subject` du Certificat. Ce nom est facilement discernable des autres noms et est unique dans le contexte de l'AC Corporis. Le nom est conforme à la partie 1 de la norme PKIX. Il est codé sous la forme d'une chaîne imprimable (`printableString`) X501 non vide.

Une entité peut employer, en plus de son nom distinctif, un nom de remplacement en utilisant pour ce faire le champ `subjectAlternateName` conforme à la partie 1 de la norme PKIX.

4.1.2 Règles de nommage

L'AC Corporis déléguée de CertiNomis est tenue de suivre et d'appliquer la politique de nommage de l'ACR, si celle-ci le demande.

Les Certificats associés aux composantes de l'ICP, et en particulier à l'AC Corporis, comportent un nom significatif permettant de retrouver leur attache physique ainsi que la dénomination sociale de l'entité.

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

Une partie demandant un Certificat doit (i) être en mesure de prouver qu'elle a le droit d'utiliser un nom en particulier et (ii) avoir le droit d'utiliser le nom qu'elle souhaite y voir figurer.

L'AC Corporis s'assure que le contenu des champs de nom `subject` et `Issuer` a un lien explicite avec l'Entité identifiée.

4.1.3 Règles d'interprétation des diverses formes de noms

Pas de disposition particulière.

4.1.4 Unicité des noms

Les noms distinctifs doivent être uniques pour toutes les Entités identifiées de l'AC Corporis. Un champ spécifique (`serialNumber`) composé de nombres ou de lettres peut être ajouté afin de garantir le caractère unique du nom distinctif.

4.1.5 Procédure de règlement des différends au sujet des noms

L'AC Corporis définit sa propre politique de nommage et, à ce titre, se réserve le droit de prendre toutes dispositions utiles visant à régler tout différend portant sur un nom de personnes, d'organisation de droit public ou privé, ou de toute autre Entité identifiée.

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 27 / 51
---------	---	----------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

L'AC Corporis veille à ce que les procédures de règlement des différends soient expressément stipulées dans les contrats de souscription aux services de certification qu'elle propose.

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

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

L'AC Corporis 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.

4.1.7 Méthode de vérification de la possession de la clé privée

L'AC Corporis vérifie que le demandeur d'un Certificat est véritablement en possession de la clé privée associée à la clé publique de vérification de signature qui sera inscrite dans ledit Certificat. Cette vérification peut être réalisée à partir de la demande de Certificat au standard PKCS#10 ou par tout autre moyen à la discrétion de l'AC Corporis.

4.1.8 Vérification de l'identité d'un Abonné

Les règles de vérification d'identité sont laissées à la discrétion de l'AE, à la condition expresse que ces règles soient formalisées et que leur existence avérée puisse être constatée par l'AC Corporis.

Le Certificat comporte le nom de l'Entité identifiée et, éventuellement, toutes les informations complémentaires permettant d'identifier son titulaire sans ambiguïté.

4.1.9 Vérification du droit sur un Dispositif ou une Application

Toute personne ou organisation jouissant d'un droit d'usage sur un Dispositif ou une Application ayant la capacité de signer numériquement ou de recevoir des messages chiffrés peut demander que ledit Dispositif ou ladite Application soit reconnu comme Entité identifiée par l'AC Corporis.

L'AE vérifie également que le demandeur est autorisé à recevoir des Certificats pour le Dispositif ou l'Application. Le demandeur doit donc 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 informatique, le demandeur doit établir la preuve que le nom de domaine lui appartient.

L'AE consigne le type d'identification utilisée, ainsi que toutes les informations pertinentes relatives à cet enregistrement.

4.2 Vérification aux fins de renouvellement des Certificats

Les règles de vérification sont laissées à la discrétion de l'AE, à la condition expresse que ces règles soient formalisées et que leur existence avérée puisse être constatée par l'AC Corporis.

 <small>OPÉRATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

4.3 Vérification aux fins de renouvellement des clés après une révocation

Un Certificat révoqué ne peut être renouvelé par l'AC Corporis. Il est alors nécessaire de procéder à la certification de nouvelles clés, de la même façon que pour un enregistrement initial.

4.4 Vérification aux fins de recouvrement

Sans objet dans le cadre de la présente édition de la Politique de Certification.

4.5 Vérification aux fins de révocation

Seuls l'Abonné, l'AE et l'AC Corporis peuvent demander la révocation d'un Certificat.

Les règles de révocation d'un Certificat sont laissées à la discrétion de l'AE, à la condition expresse que ces règles soient formalisées et que leur existence avérée puisse être constatée par l'AC Corporis.

L'AC Corporis s'assure du bon droit de la personne qui fait une demande de révocation. Elle établit la validité de la demande au moyen d'une signature numérique valide reconnue par l'AC Corporis.

 <small>OPÉRATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

5 DISPOSITIONS OPERATIONNELLES

Le présent Article stipule les pratiques opérationnelles appliquées par l'AC Corporis pour la gestion des clés et des Certificats.

5.1 Demande de Certificat

L'AC Corporis veille à ce toutes les procédures et exigences relatives aux demandes de Certificat soient dûment consignées et publiées par l'AE. Les demandeurs d'identification électronique doivent suivre et respecter les procédures publiées.

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

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

5.2 Emission et distribution d'un Certificat

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

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

A la réception d'une demande de Certificat, l'AC Corporis :

- s'assure que la demande a bien été prise en compte par une AE reconnue et que ladite AE a traité la demande et fourni une trace imputable de celle-ci ;
- génère et signe le Certificat ;
- notifie l'Abonné ou le Client de la mise à disposition du Certificat et lui fournit l'ensemble des procédures à suivre pour retirer et l'utiliser le Certificat et ;
- met le Certificat à disposition de l'Abonné ou du Client, c'est-à-dire rend accessible par des moyens physiques ou logiques les informations permettant le retrait du Certificat.

5.3 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 Corporis.

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 présente Politique de Certification.

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

5.4 Recouvrement de clés de confidentialité

Sans objet dans le cadre de la Présente Politique de Certification.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

5.5 Suspension et révocation d'un Certificat

5.5.1 Motifs de révocation

La connaissance de la compromission avérée ou soupçonnée de la clé privée d'un Certificat 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 effectuée.

Les obligations faisant suite à la modification d'une information contenue dans le Certificat par le Client ou l'Abonné sont laissées à la discrétion de l'AE, à la condition expresse que ces obligations soient formalisées et que leur existence avérée puisse être constatée par l'AC Corporis.

Outre les cas de révocation mentionnés plus haut, l'AC Corporis peut révoquer le Certificat d'un Abonné dès lors qu'elle a des soupçons graves quant à la compromission de la clé privée de l'Abonné. Plus généralement, l'AC Corporis 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.

5.5.2 Personne habilitées à demander une révocation

Seuls peuvent demander la révocation d'un Certificat :

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

5.5.3 Procédure de demande de révocation d'un Certificat

L'AC Corporis veille à ce que le Client consigne et publie toutes les procédures et exigences relatives aux demandes de révocation d'un Certificat.

L'AC Corporis met à la disposition du Client un moyen d'accès rapide, électronique ou téléphonique, au service de révocation qui authentifie la demande dans des conditions fixées à l'Article 4.

La demande de révocation doit contenir les informations d'identification du Certificat à révoquer. Elle peut également contenir la description détaillée des causes de la révocation.

Si la demande de révocation d'un Certificat se déroule correctement, la révocation est déclenchée. L'ensemble des opérations et des mesures prises par l'AC Corporis sont dûment consignées et sauvegardées par ses soins.

Quelle que soit la cause ayant entraîné la révocation d'un Certificat, l'Abonné et le Client sont systématiquement informés de la révocation du Certificat par une notification pouvant prendre la forme d'un courrier électronique. La notification de révocation précise la date à laquelle la révocation du Certificat a pris effet.

5.5.4 Prise en compte des révocations et délai de traitement

La prise en compte des demandes de révocation par le service de révocation de l'AC Corporis est assurée 24 heures sur 24, 7 jours sur 7.

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 31 / 51
---------	---	----------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

La prise en compte des demandes de révocation par l'AE est laissée à la discrétion du Client, à la condition expresse que les dispositions correspondantes soient formalisées et que leur existence avérée puisse être constatée par l'AC Corporis.

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

5.5.5 Motifs de suspension

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

5.5.6 Personne habilitées à demander une suspension

Sans objet.

5.5.7 Procédure de demande de suspension d'un Certificat

Sans objet.

5.5.8 Limites d'une période de suspension

Sans objet.

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

Dès que la révocation du Certificat d'une Entité identifiée est effective, l'AC Corporis génère sans délais une nouvelle LCR qui est publiée dans les meilleurs délais.

5.5.10 Exigences de vérification des LCR

Avant toute utilisation d'un Certificat, notamment lorsque ledit Certificat crée des effets juridiques, le Tiers utilisateur doit impérativement (i) vérifier auprès de l'AC Corporis la validité du Certificat auquel il entend se fier en consultant les Listes des Certificats Révoqués valides les plus récentes et (ii) contrôler la validité intrinsèque du Certificat, en particulier sa signature, et la validité du Certificat de l'émetteur.

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

5.5.11 Publication des motifs de révocation

La divulgation des motifs de révocation des Certificats est laissée à la discrétion de l'AE, à la condition expresse que les dispositions correspondantes soient formalisées et que leur existence avérée puisse être constatée par l'AC Corporis.

Dans le cadre des audits auxquels l'AE se soumet en vertu de la présente Politique de Certification, des éléments sur les motifs de révocation, non nominatifs et non liés à un Certificat particulier, pourront être fournis à l'AC Corporis, sans préjudice des dispositions relevant de la protection du secret professionnel auxquelles l'AE pourrait être soumise.

5.5.12 Exigences spéciales concernant la compromission des clés

En cas de compromission avérée ou soupçonnée de sa clé privée de signature, l'AC Corporis en avise sans tarder le Client et l'ACR CertiNomis.

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 32 / 51
---------	---	----------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

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.

5.6 Journalisation des événements

5.6.1 Types d'événements consignés

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

- le démarrage et l'arrêt du système ;
- le démarrage et l'arrêt de l'application de l'AC Corporis ;
- toutes les tentatives de création, extraction, établissement des mots de passe ou de modification de privilèges ;
- tout changement des caractéristiques et (ou) des clés de l'AC Corporis ;
- toutes modifications aux politiques de création des Certificats, telles que par exemple la période de validité ;
- toutes tentatives d'ouverture et de fermeture de session ;
- toutes tentatives non autorisées d'accès au système de l'AC Corporis via le réseau ;
- toutes tentatives non autorisées d'accès aux fichiers du système ;
- toute génération de clés associées à l'AC Corporis et aux entités subalternes ;
- toute création et révocation de Certificats ;
- toutes tentatives d'initialiser, d'extraire, de valider et d'invalider des Abonnés et de récupérer leurs clés.

Tous les registres et journaux, qu'ils soient sous forme électronique ou sur support papier, (i) comportent la date et l'heure de l'événement issues d'une source de temps réputée fiable et (ii) indiquent l'entité en cause.

L'AC Corporis recueille et collige, par des moyens électroniques ou physiques, toute information relative à la sécurité non produite par le système de l'AC Corporis, telle que notamment :

- les journaux associés aux contrôle d'accès physiques ;
- les événements de maintenance et de changement de la configuration du système ;
- les changements survenus au sein du personnel ;
- les rapports sur les écarts et les compromissions ;
- les registres consignant 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 consignée par l'AC Corporis.

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

5.6.2 Fréquence de traitement des journaux d'événements

L'AC Corporis s'assure que les journaux produits sont examinés au moins une fois par semaine et que tous les éléments importants constatés sont consignés et analysés dans un document récapitulatif. A cette fin, l'AC Corporis s'assure notamment que ledit document récapitulatif n'a pas été falsifiée et vérifie succinctement toutes les entrées et, plus particulièrement, les mises en garde et les irrégularités constatées. Si un élément est considéré suspect, les journaux connexes produits par l'AC Corporis et l'AE sont rapprochés.

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 33 / 51
---------	---	----------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

Toutes les mesures prises à la suite de ces examens sont dûment documentées par l'AC Corporis.

5.6.3 Période de conservation des journaux

L'AC Corporis conserve sur place les journaux pendant au moins un (1) mois et les archive ensuite, conformément aux dispositions stipulées à l'Article 5.7.

5.6.4 Protection des journaux

Tous les systèmes de journalisation électronique touchant directement les opérations de certification comprennent des mécanismes de protection contre les tentatives non autorisées de modification et de suppression des journaux.

Toute information de vérification obtenue à partir de moyens manuels est également protégée contre toute tentative non autorisée de modification et de destruction.

5.6.5 Procédures de sauvegarde des journaux

Les journaux et leur résumé sont sauvegardés ou photocopiés s'ils sont sur support papier.

5.6.6 Système de collecte des journaux

La DPC précise les systèmes utilisés pour recueillir les données de vérification.

5.6.7 Imputabilité

Les événements consignés par le système de collecte des données de vérification ne donnent pas lieu à une quelconque notification de la personne, de l'organisation, du Dispositif ou de l'Application qui en sont à l'origine.

5.6.8 Evaluation de la vulnérabilité

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

5.7 Sauvegarde et archivage

Les Certificats et les LCR produites par l'AC Corporis sont conservés pendant au moins dix (10) ans après l'expiration des clés associées.

Toutes les informations liées à la gestion du cycle de vie des Certificats, telles que notamment les données d'enregistrement collectées par l'AE, ainsi que les configurations et applications utilisées pour cette gestion, sont conservées par l'AC Corporis et l'AE pendant au moins dix (10) ans.

Chaque copie de données informatiques archivées ou sauvegardées est protégée soit par des mesures de sécurité physique, soit par une combinaison de mesures physiques et cryptographiques. Chaque site d'archivage protège de manière adéquate lesdites données contre les dangers naturels, tels que par exemple les excès de température, d'humidité et de magnétisme.

L'AC Corporis et l'AE vérifient l'intégrité de leurs archives au moins tous les six (6) mois.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

Outre les données sous forme papier susmentionnées, telles que notamment celles figurant dans les dossiers d'enregistrement, sont également 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 Corporis ou une composante de l'ICP ;
- tous les accords signés par PK7 avec d'autres AC tierces et composantes de l'ICP.

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

5.8 Renouvellement des clés

Le Certificat ne peut être prorogé au-delà de sa date de validité. L'émission de tout nouveau Certificat entraîne donc le renouvellement des clés associées.

5.9 Compromission et mesures anti-sinistre

L'AC Corporis documente toutes les procédures à suivre lors de la compromission de la clé privée de l'AC Corporis, des composantes de l'ICP et de son personnel, de même que toutes les mesures à appliquer en cas de désastre ou autres catastrophes naturelles portant sur les données, les équipements et les logiciels de l'AC Corporis.

5.9.1 Corruption des ressources informatiques, des logiciels et/ou des données

L'AC Corporis maintient en fonctionnement optimal l'activité critique de prise en compte et de publication des révocations de Certificats.

L'AC Corporis met en oeuvre des procédures visant à assurer le maintien des activités, dans lesquelles sont décrites 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 Corporis, celle-ci s'assure que tous les contrats conclus avec le dépositaire prévoient la mise en place, par celui-ci, de procédures visant à la préservation des données.

L'AC Corporis dispose également d'un plan de secours et de redémarrage de ses activités.

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

Lorsqu'il est nécessaire de révoquer le Certificat de signature numérique de l'AC Corporis, celle-ci en avise dans les plus brefs délais :

- les Clients ;
- l'ACR CertiNomis ;
- toutes les AE et ;
- les Abonnés.

En outre, l'AC Corporis :

- publie le numéro de série du Certificat révoqué dans la LCR appropriée ;
- demande à l'ACR CertiNomis de révoquer le Certificats qui certifie sa clé publique et ;
- révoque tous les Certificats signés au moyen du Certificat de signature numérique révoqué.

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

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
	MET-JSL/DA0100-03		2.1	

- produire un nouveau bi-clé de signature et publier les Certificats y associés et ;
- émettre de nouveaux Certificats auprès de toutes les entités.

La procédure de révocation d'un Certificat de signature numérique de toute autre entité est telle que stipulée à l'Article 5.5.

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

Toute compromission de la clé de signature numérique de l'AC Corporis, pour quelle que raison que ce soit, entraîne la révocation de la clé publique correspondante, en application de l'Article 5.9.2.

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.

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

L'AC Corporis définit dans un plan anti-sinistre toutes 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 Corporis, celle-ci s'assure 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.

5.10 Fin des activités

En cas de cessation d'activité de l'AC Corporis, celle-ci en avise ses Abonnés et Clients dans les plus brefs délais et prend toutes les dispositions nécessaires pour que les clés et l'information de l'AC Corporis continuent d'être archivées. L'AC Corporis en avise également par écrit l'ACR CertiNomis.

En cas tout changement significatif dans la gestion des activités de l'AC Corporis, celle-ci en avise toutes les entités pour lesquelles elle a émis des Certificats ainsi que l'ACR CertiNomis.

Dans le cas où une composante de l'ICP autre que l'AC Corporis interrompt ses activités, à l'exclusion du Client, l'AC Corporis reprend à sa charge, ou fait porter sur une autre entité, les obligations de cette composante.

Les archives de l'AC Corporis sont conservées selon les indications et la période stipulées à l'Article 5.7.

 POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
	Référence	Version
	MET-JSL/DA0100-03	2.1

6 MESURES DE SECURITE PHYSIQUE, CONTROLE DES PROCEDURES ET DU PERSONNEL

Le présent Article stipule l'ensemble des mesures de sécurité physique, des procédures et des mesures relatives au personnel applicables en vertu de la présente Politique de Certification.

6.1 Mécanismes de contrôle de la sécurité physique des locaux de l'AC Corporis

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

Les locaux techniques de l'AC Corporis qui accueillent les moyens de certification sont fortement sécurisés et sont situés dans une zone à accès contrôlé, protégée contre tous les risques courants tels que notamment incendie et inondation.

La DPC précise les conditions de sécurité physique et les règles appliquées aux (respectivement dans les) locaux, en particulier pour ce qui concerne les aspects 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 et destruction ;
- sauvegarde à l'extérieur des locaux.

6.2 Mesures de contrôle de la sécurité des procédures

6.2.1 Rôles de confiance de l'AC Corporis

Le responsable de l'AC Corporis s'assure 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 Corporis sans se faire repérer. Chaque membre du personnel de l'AC Corporis n'a ainsi accès au système que pour les seules tâches qui lui incombent.

Certaines opérations très sensibles nécessitent plusieurs intervenants ayant des rôles distincts. En particulier, le recouvrement de clés privée de confidentialité exige au moins deux (2) rôles distincts.

Tout autre répartition des responsabilités est acceptable par l'AC Corporis, pourvu que le modèle utilisé partage les pouvoirs de manière à garantir le même degré de robustesse contre les attaques de l'intérieur.

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

Trois types de rôles sont définis pour le personnel de l'AC Corporis.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

6.2.1.1 Administration de la sécurité des ressources cryptographiques

Les tâches et prérogatives associées à ce rôle sont les suivantes :

- initialisation des ressources cryptographiques au titre de détenteur d'une partie des secrets fondateurs ;
- mise en marche et arrêt d'une ressource cryptographique ;
- configuration et maintien des ressources cryptographiques ;
- gestion des droits de signature de jetons des opérateurs ;
- vérification des journaux de sécurité.

6.2.1.2 Exploitation de l'ICP

Les tâches et prérogatives associées à ce profil sont les suivantes :

- contrôle du déroulement des processus de gestion du cycle de vie des Certificats ;
- vérification de l'identification des demandeurs ;
- transmission des jetons signés indiquant l'accord après vérification, pour émission ou révocation d'un Certificat ;
- accès aux données du système pour répondre aux demandes.

6.2.1.3 Administration de l'ICP

Les tâches et prérogatives associées à ce profil sont les suivantes :

- configuration et maintien des équipements informatiques et les logiciels du système de l'AC Corporis, à l'exclusion des moyens cryptographiques ;
- gestion des droits du système, à l'exclusion des moyens cryptographiques ;
- mise en marche et arrêt des services de l'AC Corporis, à l'exclusion des moyens cryptographiques ;
- vérification des journaux, à l'exclusion de ceux relatifs aux moyens cryptographiques ;
- vérification du fonctionnement courant du système de l'AC Corporis ;
- réalisation des sauvegardes du système de l'AC Corporis.

6.2.2 Rôles de confiance de l'AE

L'AC Corporis s'assure que le personnel de l'AE, dont notamment l'Administrateur, assume les responsabilités qui lui incombent et qu'il remplit les fonctions suivantes :

- acceptation des demandes d'enregistrement, de changement et de révocation des Certificats ;
- vérification de l'identité et des autorisations des requérants ;
- transmission des informations concernant le requérant à l'AC Corporis et ;
- transmission en toute confidentialité des supports physiques ou des codes d'activations aux Abonnés.

6.2.3 Nombre de personnes requises par tâche

L'AC Corporis s'assure 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 Corporis. Au moins deux personnes faisant partie du personnel de l'AC Corporis et possédant les qualités nécessaires sont requises pour effectuer les opérations de recouvrement des clés, sur demande du Client.

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 38 / 51
---------	---	----------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

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

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

6.2.4 Identification et vérification pour chacun des rôles

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

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

Tous intervenant sur le système de l'AC Corporis ou autre composante de l'ICP, doit faire vérifier son identité et son autorisation avant :

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

Chacun de ces Certificats et comptes (à l'exception des Certificats de signatures de l'AC Corporis) est soumis à un mécanisme de contrôle garantissant qu'il est attribué directement à une personne, sans partage possible, et qu'il est utilisé uniquement pour les tâches autorisées pour le rôle assigné.

Les opérateurs distants intervenant sur le système de l'AC Corporis, tels que notamment les opérateurs de l'AE, sont identifiés au moyen de mécanismes cryptographiques forts.

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

6.3 Mesures de contrôle du personnel

6.3.1 Antécédents professionnel, qualités, expériences

Le responsable de l'AC Corporis s'assure que tous les membres du personnel qui accomplissent des tâches relatives à l'exploitation de AC Corporis :

- sont affectés 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 Corporis, 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 Corporis ;
- 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 Corporis ou de l'AE.

6.3.2 Procédures de vérification des antécédents

Toute vérification des antécédents est effectués conformément à la politique de l'AC Corporis en matière de sécurité.

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 39 / 51
---------	---	----------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

Le curriculum vitae et les antécédents professionnels des postulants à un emploi auprès de l'AC Corporis sont vérifiés conformément aux procédures de recrutement en vigueur. Le responsable de l'AC Corporis s'assure en outre que ces postulants :

- possèdent un profil de carrière dépourvu de licenciement consécutif à des fautes professionnelles telles que notamment la négligence, l'incompétence ou la perte de confiance dans les fonctions exercées ;
- possèdent un casier judiciaire vierge.

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

6.3.2.1 Vérification des qualifications professionnelles

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

6.3.2.2 Vérification de l'expérience

Aucune disposition autre que la vérification des antécédents professionnels.

6.3.2.3 Obligations du personnel de l'AC Corporis

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

6.3.3 Dispositions en matière de formation

L'AC Corporis s'assure que tous les membres du personnel qui accomplissent des tâches touchant à l'exploitation de l'AC Corporis et de l'AE ont reçu une formation minimum leur permettant de maîtriser les principes de fonctionnement et les mécanismes de sécurité de l'AC Corporis.

Le personnel de l'AC Corporis suit un programme de formation pour accomplir correctement ses fonctions. Ce programme 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 Corporis ;
- toutes les tâches qu'il devra accomplir dans le cadre de l'ICP ;
- le matériel et les systèmes d'exploitation formant l'environnement opérationnel de l'AC Corporis ;
- le plan de secours de l'AC Corporis après un sinistre et les procédures de maintien des activités.

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

- l'application informatique de gestion du cycle de vie des Certificats mise à la disposition du Client par l'AC Corporis ;
- toutes les tâches qu'il devra accomplir dans le cadre de la gestion du cycle de vie des Certificats ;
- le matériel et les systèmes d'exploitation du Client formant l'environnement opérationnel de l'AE.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

6.3.4 Formation professionnelle – fréquence et exigences

Tout changement significatif apporté au système de l'AC Corporis donne lieu à une formation complémentaire du personnel de l'AC Corporis et de l'AE, le cas échéant, à la discrétion du responsable de l'AC Corporis.

Des cours de formation professionnelle sont dispensés au personnel de l'AC Corporis en fonction des besoins et les exigences sont revues par l'AC Corporis au moins une fois par an.

Le personnel de l'AC Corporis reçoit une formation sur la sécurité au moins une (1) fois par an.

6.3.5 Rotation des emplois

Aucune disposition particulière.

6.3.6 Sanctions en cas d'actions non autorisées

Si une personne a réellement fait ou est soupçonnée d'avoir fait une action non autorisée dans l'accomplissement de ses tâches en rapport avec l'exploitation de l'AC Corporis ou de l'AE, l'AC Corporis peut lui interdire l'accès au système et prendre ou demander toutes sanctions disciplinaires adéquates.

6.3.7 Contrôle des personnels des entreprises cocontractantes

L'AC Corporis s'assure que le personnel des entreprises cocontractantes peut accéder à ses locaux conformément aux dispositions de l'Article 6.1.

Les exigences relatives au personnel des entreprises cocontractantes sont identiques à celles relatives aux employés, en particulier à celles décrites aux Article 6.3.1, 6.3.2. et 6.3.6.

6.3.8 Documentation fournie au personnel

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

L'ensemble du personnel de l'AC Corporis a accès à des manuels complémentaires portant sur l'ensemble des procédures en vigueur et relatifs aux responsabilités du personnel.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

7 MESURES TECHNIQUES DE SECURITE

Le présent Article a pour objet de stipuler les dispositions de gestion des bi-clés de l'AC Corporis, du personnel de l'AC Corporis, des AE et des Abonnés.

7.1 Production et installation des bi-clés

7.1.1 Production des bi-clés

Les clés privées associées au Certificat de l'Administrateur doivent être produites, conservées et utilisées exclusivement sur des moyens cryptographiques agréés par l'AC tierce qui a émis le Certificat, CertiNomis SA en l'occurrence.

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

- la création et à la vérification de signature ;
- la confidentialité.

L'AC Corporis produit 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 de préférence être produit au plus près de l'Abonné.

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

7.1.2 Remise de la clé publique à l'AC Corporis

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

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

La clé publique de vérification de l'AC Corporis, ainsi que celle de l'ACR, sont diffusées sous la forme de Certificats numériques téléchargeables depuis le site de l'AC Corporis ou de l'AE.

7.1.4 Tailles des clés asymétriques

Les bi-clés de l'AC Corporis 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 de l'AC Corporis dont la durée de validité est inférieure 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 Corporis et de l'AE ont des Certificats avec un clé d'au moins 1024 bits.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

7.1.5 Production des paramètres des clés publiques

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

Les choix suivants ont été retenus par PK7 :

- exposant public : 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.

7.1.6 Vérification de la qualité des paramètres

Le contrôle qualité des paramètres des clés est effectué en conformité avec l'Article 7.1.5.

7.1.7 Nature de la ressource de production de clés

Les bi-clés de l'AC Corporis sont produits par un module cryptographique matériel. Les bi-clés de chiffrement, lorsqu'ils sont générés par l'AC Corporis, sont également produits au moyen d'un module cryptographique matériel.

7.1.8 Utilisation de la clé publique

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

7.1.8.1 Clé publique de vérification de signature

Une clé publique de vérification peut être utilisée à des fins d'identification, d'authentification, de non-répudiation et/ou d'intégrité. La clé publique de vérification de l'AC Corporis 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 comporte l'une des valeurs suivantes :

- pour les Certificats d'Abonnés : **digitalSignature** et/ou **nonRepudiation**
- pour les Certificats de l'AC Corporis : **keyCertSign** et/ou **cRLSign**

7.1.8.2 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 comporte l'une des valeurs suivantes : **keyEncipherment** et/ou **dataEncipherment**.

7.2 Protection des clés privées

L'Abonné doit protéger ses clés privées afin qu'elles ne soient pas divulguées. Il lui appartient 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 Article.

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 43 / 51
---------	---	----------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

7.2.1 Normes relatives au calculateur cryptographique

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

7.2.2 Contrôle des clés privées par plusieurs personnes

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

7.2.3 Recouvrement des clés privées

Ce service n'est pas proposé par l'AC Corporis dans la présente édition de la Politique de Certification.

7.2.4 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.

7.2.5 Archivage des clés privées

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

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

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

Les clés privées de l'AC Corporis 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, autant 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, autant que possible, conservées chiffrées, n'étant en clair qu'au moment requis pour leur utilisation.

7.2.7 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.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
	MET-JSL/DA0100-03		2.1	

7.2.8 Méthode de désactivation des clés privées

Les clés désactivées doivent être effacées 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.

7.2.9 Méthode de destruction des clés privées

Lorsque le Certificat de signature numérique arrive à expiration ou qu'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 trans-chiffrés, alors la clé de confidentialité ne sert plus et peut être détruite.

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

La destruction d'une clé privée implique la destruction de 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 confinée sur le même support que la clé de signature, elle devra être détruite en même temps que la clé de signature.

7.3 Autres aspects de la gestion des bi-clés

7.3.1 Archivage des clés publiques

L'AC Corporis archive toutes les clés publiques de vérification de signature conformément à l'Article 5.7.

7.3.2 Périodes d'utilisation des clés publiques et privées

La période de validité des clés est fixée comme suit :

- 512 bits : au plus un (1) ans ;
- 1024 bits : au plus quatre (4) ans ;
- 2048 bits : au plus douze (12) ans.

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

7.4 Données d'activation

7.4.1 Génération et installation des données d'activation

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

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

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'utilisations.

7.4.2 Protection des données d'activation

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

Si un système de mots de passe réutilisables est utilisé, il est nécessaire de prévoir un mécanisme permettant de bloquer temporairement le compte après un nombre limité et fixé au préalable de tentatives. Cette mesure de protection est systématiquement appliquée pour les systèmes de l'AC Corporis.

7.4.3 Autres aspects touchant les données d'activation

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

7.5 Mécanismes de sécurité informatique des postes de travail

7.5.1 Sécurité informatique – Exigences techniques spécifiques

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

- contrôle de l'accès aux services de l'AC Corporis ;
- 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 Corporis ;
- 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 Corporis et des mécanismes de protection physique.

7.5.2 Indice de sécurité informatique

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

7.6 Contrôle technique du système durant son cycle de vie

7.6.1 Contrôle des développements des systèmes

L'AC Corporis veille à ce que l'implémentation du système permettant de mettre en œuvre les composantes de l'ICP soit documentée et respectée, dans la mesure du possible, les normes de modélisation et d'implémentation. La configuration du système, des composantes, ainsi que toute modification et mise à niveau sont également documentées et contrôlées.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
	MET-JSL/DA0100-03		2.1	

7.6.2 Contrôle de la gestion de la sécurité

Une méthode de gestion de la configuration est appliquée pour installer le cœur cryptographique de l'AC Corporis et en assurer la maintenance. La première fois qu'il est chargé, le logiciel de l'AC Corporis fournit une méthode permettant à celle-ci de vérifier si le logiciel installé sur le système :

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

L'AC Corporis dispose d'un mécanisme permettant de vérifier périodiquement l'intégrité des logiciels. Elle dispose également de mécanismes et (ou) de politiques lui permettant de contrôler et de surveiller la configuration du système de l'AC Corporis.

Toute évolution est documentée et dûment consignée dans les procédures de fonctionnement interne. Dans le cas de produits évalués, l'AC Corporis veille à ce que chaque évolution soit conforme au schéma de maintenance de l'assurance de conformité.

7.7 Mécanismes de contrôle de la sécurité réseau

Les systèmes de l'AC Corporis sont protégés contre les attaques provenant de tout réseau, en particulier les réseaux ouverts. Une telle protection est notamment 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 Corporis.

Ces protocoles et commandes sont définis dans sa DPC.

7.8 Mécanismes de contrôle technique du module cryptographique

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

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
	MET-JSL/DA0100-03		2.1	

8 PROFIL DES CERTIFICATS ET DES LCR

Le présent Article stipule les règles et directives relatives à l'utilisation de certains types de Certificats X509, des champs, des extensions des LCR conformes aux normes PKIX.

Le format précis des Certificats et LCR est précisé dans la DPC.

8.1 Forme et contenu des Certificats

Selon la version 3 de la norme X.509 des Certificats, les champs suivants sont renseignés par le logiciel de l'AC Corporis :

- **version** : version du Certificat X.509
- **serialNumber** : numéro de série unique du Certificat
- **signature** : identifiant de l'algorithme de signature de l'AC Corporis
- **issuer** : nom de l'AC Corporis
- **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 stipulées à l'Article 8.1.2.

8.1.1 Signature du Certificat

L'AC Corporis appose un sceau sur le Certificat avec sa clé privée. Ce sceau est le résultat d'une fonction mathématique appliquée sur l'ensemble des champs décrits à l'Article 8.1.

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

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

8.1.2 Champs d'extensions

L'AC Corporis supporte 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 Corporis émettrice, l'usage du Certificat et sur les Listes de Certificats Révoqués.

8.1.3 Interprétation sémantique des champs critiques

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

8.2 Formes et contenu des Listes de Certificats Révoqués

Les LCR comportent les champs de base tels que spécifiés dans la recommandation X509 CRL V2. Ces champs sont les suivants :

PK7 SAS	Ce document est la propriété exclusive de la société PK7 SAS. Il ne peut être reproduit ni communiqué sans son autorisation écrite.	Page : 48 / 51
---------	---	----------------

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

- **version** : version de la liste de Certificats révoqués X.509.
- **signature** : identifiant de l'algorithme de signature de l'AC Corporis
- **issuer** : nom de l'AC Corporis
- **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 8.2 ;
- **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.

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS	Date : 24 novembre 2003	
		Référence	Version
		MET-JSL/DA0100-03	2.1

9 ADMINISTRATION DE LA POLITIQUE DE CERTIFICATION

Le présent Article stipule les dispositions prises par l'AC Corporis en matière d'administration et de gestion de la présente politique de Certification.

9.1 Procédures de modifications

9.1.1 Délais de préavis

L'AC Corporis garantit aux Abonnés et aux Tiers utilisateurs un préavis de trente (30) jours avant de procéder à tout changement de la présente Politique de Certification susceptible de produire un effet majeur sur lesdits Abonnés et Tiers utilisateurs.

L'AC Corporis garantit un préavis de quinze (15) jours aux Abonnés et aux Tiers utilisateurs avant de procéder à tout changement de la présente Politique de Certification susceptible de produire un effet mineur sur lesdits Abonnés et Tiers Utilisateurs.

L'AC Corporis garantit un préavis de sept (7) jours aux Abonnés et aux Tiers utilisateurs avant de procéder à tout changement de la présente Politique de Certification résultant d'une situation hors du contrôle du responsable de la politique, à condition que ce changement ait un impact sur lesdits Abonnés et Tiers Utilisateurs.

L'AC Corporis peut modifier la présente politique sans préavis aux Abonnés et aux Tiers utilisateurs lorsque, selon l'évaluation du responsable de la Politique de Certification, ces modifications n'ont aucun impact sur eux.

9.1.2 Forme de diffusion des avis

Dans les cas nécessitant un préavis, l'AC Corporis avise les Clients et les Abonnés des modifications apportées à la présente Politique de Certification, par tous moyens à sa convenance dont notamment le site Web de l'AC Corporis et la messagerie électronique, en fonction de la portée des modifications. Les avis de modification impactant les AC tierces leur sont expressément communiqués.

9.1.3 Période de commentaires

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

9.1.4 Traitement des commentaires

Aucune disposition particulière.

9.1.5 Modifications nécessitant l'adoption d'une nouvelle politique

Si un changement apporté à la présente Politique de Certification 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).

 <small>OPERATEUR DE SERVICES DE CONFIANCE</small>	POLITIQUE DE CERTIFICATION CORPORIS		Date : 24 novembre 2003	
			Référence	Version
			MET-JSL/DA0100-03	2.1

9.2 Procédure de publication

9.2.1 Eléments non diffusés dans la DPC

Certaines informations confidentielles de la DPC touchant à la sécurité de l'AC Corporis ne sont pas publiées, à la discrétion de l'AC Corporis. Un résumé ou des extraits de la DPC peuvent cependant être fournis sous forme électronique, sous certaines conditions et selon l'origine des demandes d'information.

9.2.2 Publication de la politique de Certification et de la DPC

La présente Politique de Certification et certains éléments de la DPC sont publiés et rendus accessibles aux Abonnés et Tiers utilisateurs à l'adresse URL suivante : <http://www.pk7.fr/corporis>. Une copie peut également être obtenue par courrier électronique, sur demande auprès de l'AC Corporis.

9.3 Procédures d'approbation de la DPC

L'AC Corporis garantit l'adéquation de la DPC avec la présente Politique de Certification. L'ACR CertiNomis peut demander l'examen de cette DPC, conformément aux procédures en vigueur.