



KEYNECTIS

K•Websign®

POLITIQUE DE CERTIFICATION

Certificats KWS Service K.Websign® AUTORITE DE CERTIFICATION AC KEYNECTIS KWEBSIGN 1

© 2007 KEYNECTIS, tous droits réservés

Date :	24 Janvier 2007
Version :	1.01
Référence :	PC/KEY/K-Web/AC KEYNECTIS KWEBSIGN 1
OID :	1.3.6.1.4.1.22234.2.3.3.3.1 .

HISTORIQUE DES MODIFICATIONS

Historique du document :

Date	Version	Rédacteur	Objet	Statut
25 août 2005	0	MQ	Rédaction	Projet
01/12/2005	0.1	DM	Adaptation K Websign	Projet
15/12/05	0.2	EM1	Relecture, formalisation et mise au format PRIS v2	Projet
15/12/05	0.3	MQ	Relecture et corrections mineures	Projet
11/01/06	0.6	DM,TR	prise en compte remarques TRB & séparation KWA et KWS	Projet
19/01/06	0.8	MQ	Relecture	Projet
21/01/06	0.9	DM	Relecture	Projet
25/01/06	0.93	EM	Création de la version 0.93	Projet
30/01/06	0.94	DM	Relecture	Projet
22/02/06	1.00	DM	Intégration des relecteurs	finale
24/01/07	1.01	DM	Mise à jour	finale

SOMMAIRE

AVERTISSEMENT	7
1 INTRODUCTION	8
1.1 Présentation générale de la politique de certification	8
1.2 Identification de la politique de certification	8
1.3 Les composantes de l'Infrastructure de Gestion de Clés	9
1.3.1 L'Autorité de Certification (AC)	9
1.3.2 L'Autorité d'Enregistrement (AE)	10
1.3.3 L'Opérateur de Certification (OC)	10
1.3.4 Porteurs de certificats	11
1.3.5 Application utilisatrice ou Utilisateur de certificat	11
1.4 Usages des certificats et applications concernés par la politique de certification	11
1.4.1 Certificat KWS- Intégrité	11
1.4.2 Certificat KWS - Signature	12
1.4.3 Certificat KWS - Chiffrement	12
1.4.4 Usages pour les certificats d'AC et de composantes	12
1.4.5 Usages interdits	12
1.5 Gestion de la politique de certification	13
1.5.1 Entité gérant la PC	13
1.5.2 Point de contact	13
1.5.3 Entité déterminant la conformité d'une DPC avec cette PC	13
1.6 Acronymes et définitions	13
1.6.1 Liste des acronymes	13
1.6.2 Définitions	14
2 OBLIGATIONS CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES	17
2.1 Entités chargées de la mise à disposition des informations	17
2.2 Types d'informations publiées	17
2.3 Délais et fréquences de publication	17
2.3.1 Politique de certification	17
2.3.2 Liste des Certificats Révoqués - certificats de porteur	17
2.3.3 Liste des Certificats Révoqués - certificats de l'AC	17
2.4 Contrôles d'accès aux informations publiées	17
2.4.1 Politique de certification	17
2.4.2 Liste des Certificats Révoqués	18
2.4.3 Liste des Certificats Révoqués - certificats de l'AC	18
3 IDENTIFICATION ET AUTHENTIFICATION POUR LA DELIVRANCE DE CERTIFICAT	19
3.1 Nommage	19
3.1.1 Types de noms	19
3.1.2 Nécessité d'utilisation de noms explicites	19
3.1.3 Anonymisation ou pseudonymisation des porteurs	19
3.1.4 Règles d'interprétation des différentes formes de nom	19
3.1.5 Unicité des noms	19
3.1.6 Procédure de résolution de litige sur déclaration de nom	19
3.1.7 Méthode pour prouver la possession de la clé privée	19
3.2 Enregistrement initial d'un porteur et validation de la demande d'émission d'un certificat	20
3.3 Authentification et validation d'une demande de révocation par le porteur	20
3.4 Authentification d'une demande de renouvellement	20
4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS	21
4.1 Origine d'une demande de certificat	21



4.1.1	Processus de demande initiale d'un certificat.....	21
4.1.2	Traitement d'une demande de certificat	21
4.1.3	Délivrance du certificat.....	21
4.1.4	Acceptation du certificat.....	21
4.2	Révocation d'un certificat.....	22
4.2.1	Causes possibles de révocation	22
4.2.2	Origines d'une demande de révocation	22
4.2.3	Processus de demande de révocation	22
4.2.4	Procédure et délai de traitement d'une demande de révocation	22
4.2.5	Publication des causes de révocation de certificat.....	23
4.2.6	Exigences de vérification de la révocation par les utilisateurs de certificats	23
4.2.7	Fréquence d'établissement des LCR.....	23
4.2.8	Délai maximum de publication d'une LCR.....	23
4.3	Renouvellement d'un certificat Modification d'un certificat de porteur	23
4.4	Suspension d'un certificat de porteur.....	23
4.5	Fonction d'information sur l'état des certificats	23
4.6	Séquestre et recouvrement de clés.....	23
5	LE SEQUESTRE ET LE RECOUVREMENT DE CLES PRIVEES DES PORTEURS NE SONT PAS AUTORISES PAR LA PRESENTE POLITIQUE DE CERTIFICATION.MESURES DE SECURITE NON TECHNIQUES DES OPERATIONS	23
5	MESURES DE SECURITE NON TECHNIQUES DES OPERATIONS	24
5.1	Mesures de sécurité physique	24
5.1.1	Situation géographique	24
5.1.2	Accès physique.....	24
5.1.3	Energie et air conditionné	24
5.1.4	Exposition aux liquides	24
5.1.5	Prévention et protection incendie.....	24
5.1.6	Mise hors service des supports	24
5.1.7	Sauvegardes hors site	24
5.2	Mesures de sécurité procédurales	25
5.2.1	Rôles de confiance	25
5.2.2	Nombre de personnes nécessaires à l'exécution de tâches sensibles	25
5.2.3	Identification et authentification des rôles.....	25
5.3	Mesures de sécurité vis-à-vis du personnel.....	26
5.3.1	Qualifications, compétence et habilitations requises	26
5.3.2	Procédures de vérification des antécédents.....	26
5.3.3	Exigences en matière de formation initiale	26
5.3.4	Exigences et fréquence en matière de formation continue	26
5.3.5	Gestion des métiers	26
5.3.6	Sanctions en cas d'actions non autorisées.....	26
5.3.7	Exigences vis-à-vis du personnel des prestataires externes.....	26
5.3.8	Documentation fournie au personnel.....	26
5.4	Procédures de constitution des données d'audit.....	27
5.4.1	Type d'événements à enregistrer	27
5.4.2	Processus de journalisation	28
5.4.3	Protection des journaux d'événements.....	28
5.4.4	Procédures de sauvegarde des journaux d'événements	28
5.4.5	Système de collecte des journaux d'événements.....	28
5.4.6	Evaluation des vulnérabilités	28
5.5	Archivage des données	28
5.5.1	Type de données archivées.....	29
5.5.2	Période de conservation des archives.....	29
5.5.3	Protection des archives.....	29
5.5.4	Procédures de sauvegardes des archives.....	29
5.5.5	Exigences d'horodatage des données.....	29
5.5.6	Système de collecte des archives.....	29



5.5.7	Procédures de récupération et de vérification des archives	29
5.6	Changement de clé d'AC	30
5.7	Reprise suite à compromission et sinistre	30
5.7.1	Procédures de remontée et de traitement des incidents et des compromissions	30
5.7.2	Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données) et en cas de compromission de la clé privée d'une composante	30
5.7.3	Capacités de continuité d'activité suite à un sinistre	30
5.8	Fin de vie de l'ICP	30
6	MESURES DE SECURITE TECHNIQUES ET LOGIQUES	31
6.1	Génération et installation de biclés	31
6.1.1	Génération des bi-clés	31
6.1.1.1	Clés d'AC	31
6.1.1.2	Clés de porteur de certificat KWS	31
6.1.2	Transmission de la clé privée à son propriétaire	31
6.1.3	Transmission de la clé publique à l'AC	31
6.1.4	Transmission de la clé publique de l'AC aux utilisateurs de certificats	32
6.1.5	Taille des clés	32
6.1.6	Contrôle de la qualité des paramètres des clés	32
6.1.7	Objectifs d'usage de la clé	32
6.2	Mesures de sécurité pour la protection des clés privées	32
6.2.1	Standards et mesures de sécurité pour les modules cryptographiques	32
6.2.1.1	Module AC	32
6.2.1.2	Module porteur	32
6.2.2	Contrôle de la clé privée d'AC par plusieurs personnes	32
6.2.3	Séquestre de la clé privée	32
6.2.4	Copie de secours de la clé privée	32
6.2.5	Archivage de la clé privée	33
6.2.6	Méthode d'activation de la clé privée	33
6.2.6.1	Clé d'AC	33
6.2.6.2	Clé KWS	33
6.2.7	Méthode de destruction des clés privées	33
6.3	Autres aspects de la gestion des bi-clés	33
6.3.1	Archivage des clés publiques	33
6.3.2	Durée de vie des biclés et des certificats	33
6.4	Données d'activation	33
6.4.1	Données d'activation correspondant à la clé privée de l'AC	33
6.4.2	Données d'activation correspondant à la clé privée KWS du porteur	33
6.5	Mesures de sécurité des systèmes informatiques	33
6.6	Mesures de sécurité du système durant son cycle de vie	34
6.6.1	Mesures de sécurité liées au développement des systèmes	34
6.6.2	Gestion de la sécurité	34
6.7	Mesures de sécurité réseau	34
6.8	Mesures de sécurité pour les modules cryptographiques	34
7	PROFILS DES CERTIFICATS ET DES LISTES DE CERTIFICATS REVOQUES	35
7.1	Profil des certificats	35
7.1.1	Numéro de version	35
7.1.2	Extensions du certificat	35
7.1.3	OID des algorithmes	35
7.1.4	Forme des noms	35
7.1.5	Contraintes sur les noms	36
7.1.6	OID des PC	36
7.1.7	Utilisation de l'extension "contraintes de politique"	36
7.1.8	Sémantique et syntaxe des qualifiants de politique	36
7.1.9	Sémantiques de traitement des extensions critiques de la PC	36
7.2	Profil de LCR	36



8	AUDIT DE CONFORMITE ET AUTRES EVALUATIONS	37
8.1	Fréquences et / ou circonstances des évaluations	37
8.2	Identités / qualifications des évaluateurs	37
8.3	Relations entre évaluateurs et entités évaluées	37
8.4	Sujets couverts par les évaluations	37
8.5	Actions prises suite aux conclusions des évaluations	37
8.6	Communication des résultats	37
9	DISPOSITIONS DE PORTEE GENERALE	37
9.1	Barèmes des prix	37
9.1.1	Tarifs pour la fourniture ou le renouvellement de certificats	37
9.1.2	Tarifs pour accéder aux certificats	37
9.1.3	Tarifs pour accéder aux informations d'état et de révocation des certificats	37
9.1.4	Tarifs pour d'autres services	38
9.1.5	Politique de remboursement	38
9.2	Responsabilité financière	38
9.2.1	Couverture par les assurances	38
9.2.2	Autres ressources	38
9.2.3	Couverture et garantie concernant les entités utilisatrices	38
9.3	Loi applicable et juridictions compétentes	38
9.4	Droits de propriété intellectuelle	38
9.5	Politique de confidentialité	38
9.5.1	Types d'informations considérées comme confidentielles	38
9.5.2	Délivrance aux autorités habilitées	38
9.6	Protection des données personnelles	38
9.7	Durée et fin anticipée de validité de la politique de certification	39
9.7.1	Durée de validité	39
9.7.2	Fin anticipée de validité	39
9.7.3	Effets de la fin de validité et clauses restant applicables	39
9.8	Administration de la politique de certification	39
9.8.1	Délai de préavis	39
9.8.2	Forme de diffusion des avis	39
9.8.3	Modifications nécessitant l'adoption d'une nouvelle politique	40
9.9	Procédures d'informations	40
9.10	Rôles et obligations de l'ICP et de ses composantes	40
9.10.1	Autorité de certification	40
9.10.2	Autorités d'enregistrement	40
9.10.3	Porteurs de certificats	41
9.10.4	Utilisateurs de certificats	41
9.11	Limite de responsabilité	41

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

AVERTISSEMENT

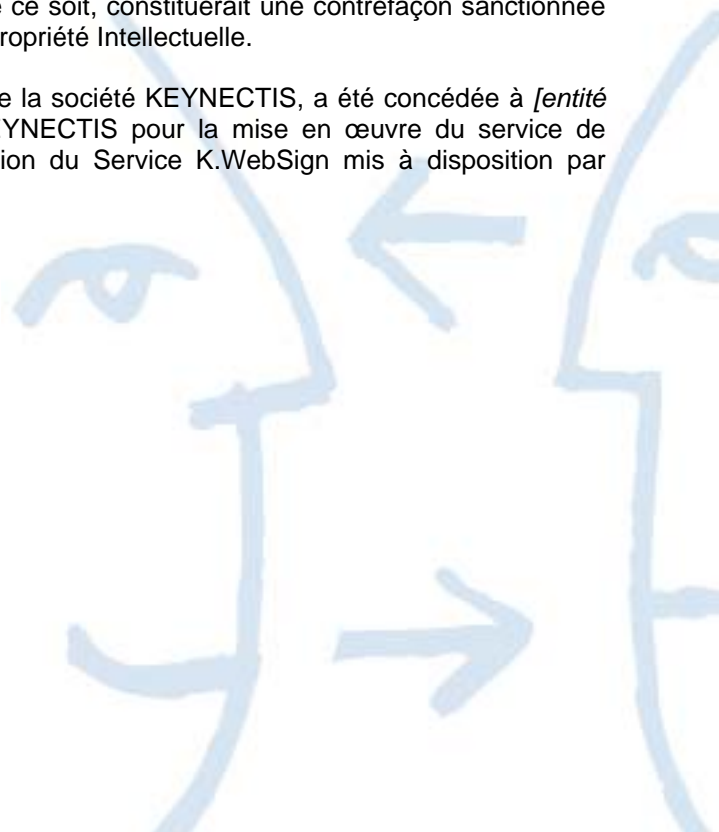
La présente politique de certification est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1er juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de KEYNECTIS.

La reproduction, la représentation (hormis la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement de manière expresse par KEYNECTIS 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.

L'utilisation de la présente politique de certification, propriété de la société KEYNECTIS, a été concédée à [entité cliente] dans la cadre du contrat de service conclu avec KEYNECTIS pour la mise en œuvre du service de certification électronique de [entité cliente] associé à l'utilisation du Service K.WebSign mis à disposition par KEYNECTIS.



	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

1 INTRODUCTION

1.1 Présentation générale de la politique de certification

Ce document constitue la politique de certification de KEYNECTIS agissant en tant qu'Autorité de Certification appelé AC KEYNECTIS KWEBSIGN 1 (ci-après désignée « AC ») pour les besoins de sécurisation de la plate-forme K.Websign® et du service K.Websign® mis à disposition des Clients par la société KEYNECTIS.

La présente politique de certification s'adresse aux utilisateurs et de la plate-forme des services K.Websign® qui utiliseront dans ce cadre des certificats qui leurs sont dédiés dans leurs modes de gestion et d'émission.

Les certificats électroniques gérés et émis conformément à la présente politique de certification, ci-après désignés dans le présent document « certificats KWS K.Websign® », sont délivrés à la plate-forme K.Websign® désignés dans le cadre de la mise en œuvre et de l'usage du service K.Websign®.

Les certificats KWS seront utilisés pour des besoins de chiffrement et de signature électronique de documents sous format XML localement présents chez KEYNECTIS sur la plate-forme K.Websign®. Ces documents ainsi traités sont ensuite transmis à l'application web du Client avec un accusé de réception. Les certificats KWS comporteront par conséquent l'identification de KEYNECTIS, et l'identité du serveur Web traitant les données reçus du Client et de ses utilisateurs et élaborant la preuve de la transaction électronique.

Les caractéristiques des certificats KWS sont par types de certificat les suivantes :

- KWS_Signature : d'identifier KEYNECTIS ou le Client en tant que personne morale habilitée à émettre des preuves électroniques dans le cadre de transaction électroniques mise en œuvre par une autre personne morale dénommé le Client et un utilisateur ;
- KWS_Intégrité : d'identifier KEYNECTIS ou le Client en tant que personne morale en charge de la transmission des données nécessaires à la preuve de la réalisation d'une transaction électronique entre le Client et l'utilisateur du service K.Websign® ;
- KWS_Chiffrement : d'identifier KEYNECTIS ou le Client en tant que personne morale qui échange des clefs de chiffrement pour la protection en confidentialité des échanges entre l'application Client et la plateforme K.Websign®

Cette politique de certification décrit d'une part l'ensemble des engagements de l'AC relatifs à l'émission et à la gestion des certificats KWS, étant précisé que la gestion des certificats couvre toutes les opérations relatives à la vie d'un certificat depuis son émission jusqu'à son expiration ou sa révocation le cas échéant, et d'autre part les conditions d'utilisation des certificats KWS.

Les certificats, et les listes de certificats révoqués (LCR) correspondantes, objets de la présente PC sont conformes à la norme [X.509].

La présente politique de certification a été établie à partir du document « Procédures et Politiques de Certification de Clés (PC²) » émis par la Commission Interministérielle pour la Sécurité des Systèmes d'Information (CISSI), des documents types de « Politique de Référencement Intersectorielle de Sécurité v2.0 » de l'ADAE et du SGN-DCSSI, ainsi que du document RFC 3647 « Certificate Policy and Certification Practices Framework » de l'IETF.

1.2 Identification de la politique de certification

La présente politique de certification est identifiée par l'OID 1.3.6.1.4.1.22234.2.3.3.3.1 Le numéro d'OID de cette PC Type est indiqué à titre de gestion documentaire pour la société KEYNECTIS.

La déclaration des pratiques de certification correspondante est référencée par l'OID 1.3.6.1.4.1.22234.3.1.4.1.1. Le numéro d'OID de cette DPC Type est indiqué à titre de gestion documentaire pour la société KEYNECTIS.

La politique de certification et sa déclaration des pratiques de certification correspondant aux OID ci-dessus indiqués sont ci-après désignées sous le nom de « PC KWS-KEYNECTIS » et de « DPC KWS-KEYNECTIS ».

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

1.3 Les composantes de l'Infrastructure de Gestion de Clés

En préambule, il est rappelé que le service de certification électronique de KEYNECTIS ayant pour objet la délivrance de certificats KWS repose sur la mise en œuvre et l'exploitation d'une Infrastructure de Gestion de Clés (IGC).

A cette fin, KEYNECTIS a déployé une Autorité de Certification qui a en charge la fourniture des prestations de délivrance et de gestion des certificats KWS tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...).

La décomposition en fonctions de l'IGC est présentée dans le cadre de ce chapitre ; les composantes de l'IGC mettant en œuvre ces fonctions sont présentées dans la DPC.

Les différentes fonctions de l'IGC, coordonnées par l'AC, correspondant aux différentes étapes du cycle de vie des bi-clés et des certificats, sont les suivantes :

- Fonction demande de certification - Cette fonction reçoit les informations d'identification du futur porteur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'IGC, en fonction des services rendus et de l'organisation de l'IGC. Dans le cadre de la présente PC et de la DPC associée, cette fonction est mise en œuvre par un administrateur de KEYNECTIS pour les certificats KWS en tant qu'Autorité d'Enregistrement. Le rôle exact de l'AE est détaillé ci-dessous ;
- Fonction de génération des certificats - Cette fonction génère (création du format, signature électronique avec la clé privée de l'AC) les certificats à partir des informations transmises par l'autorité d'enregistrement et de la clé publique du porteur provenant de la fonction de génération de la bi-clé cryptographique du porteur, si c'est cette dernière qui génère la bi-clé du porteur, ou du porteur lui-même si c'est lui qui génère sa bi-clé cryptographique avec ses propres outils. Dans le cadre de la présente PC et de la DPC associée, cette fonction est obligatoirement mise en œuvre au sein de la société KEYNECTIS en tant qu'opérateur de certification ;
- Fonction de génération de la bi-clé cryptographique du porteur - Cette fonction génère la bi-clé cryptographique à destination du porteur. Pour les certificats KWS le support de la clé cryptographique est logiciel ou matériel ;
- Fonction de génération du code d'activation : ce code est lié au dispositif de stockage de la clé privée du porteur ou encore des codes ou clés temporaires permettant au porteur de mener le processus d'utilisation de la clé cryptographique associée à son certificat. La mise en œuvre de cette fonction est laissée au choix pour les certificats KWS elle est initialisé par KEYNECTIS en tant qu'opérateur de certification (noté OC) ;
- Fonction de remise au porteur - Cette fonction remet au porteur au minimum son certificat ainsi que, le cas échéant, les autres éléments fournis par l'AC (dispositif du porteur, clé privée du porteur, codes d'activation,...). Le support de la bi-clé cryptographique associée au certificat KWS sont logiciels (Pkcs#12). Cette fonction est mise en œuvre par la société KEYNECTIS en tant qu'opérateur de certification ;
- Fonction de publication - Cette fonction met à disposition des différentes parties concernées, les conditions générales, politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux porteurs et/ou aux utilisateurs de certificats, hors informations d'état des certificats. Cette fonction est mise en œuvre par KEYNECTIS pour les certificats KWS ;
- Fonction de gestion des révocations - Cette fonction traite les demandes de révocation (notamment identification et authentification du demandeur) et détermine les actions à mener. Les résultats des traitements sont diffusés via la fonction d'information sur l'état des certificats. Cette fonction est par contre utilisée pour la gestion des certificats KWS et est mise en œuvre par la société KEYNECTIS ;
- Fonction d'information sur l'état des certificats - Cette fonction fournit aux utilisateurs de certificats des informations sur l'état des certificats (révoqués ou valides). Cette fonction est mise en œuvre selon un mode de publication d'informations mises à jour à intervalles réguliers (Liste de Certificats Révoqués) de 24 heures.

1.3.1 L'Autorité de Certification (AC)

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

L'AC a pour fonction principale de définir la politique de certification et de la faire appliquer, garantissant ainsi un certain niveau de confiance aux Utilisateurs.

KEYNECTIS est l'autorité de certification émettrice des certificats et assure la gestion de leur cycle de vie, l'enregistrement et le traitement des demandes d'émission de certificats électroniques. Pour l'opération technique de l'IGC, KEYNECTIS en qualité d'AC, a confié cette fonction à l'opérateur de certification KEYNECTIS.

L'autorité de certification de KEYNECTIS est une autorité de certification auto signée. Elle n'est donc pas rattachée en termes de hiérarchie technique à une autre autorité de certification.

Dans le cadre de ses fonctions opérationnelles, qu'elle assume directement où qu'elle sous-traite à des entités externes, les exigences qui incombent à l'AC en tant que responsable de l'ensemble de l'IGC sont les suivantes :

- Etre en relation par voie contractuelle / hiérarchique / réglementaire avec l'entité pour laquelle elle a en charge la gestion des certificats des porteurs de cette entité.
- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux porteurs de certificats et aux utilisateurs de certificats qui gèrent et mettent œuvre les certificats KWS ;
- S'assurer que les exigences de la PC et les procédures de la DPC associées sont appliquées par chacune des composantes de l'IGC ;
- Mener une analyse de risque permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'IGC et les mesures de sécurité techniques et non techniques correspondantes à mettre en œuvre. Elle élabore sa DPC en fonction de cette analyse de risques qui prend en compte et distingue notamment la partie identification et authentification des porteurs de certificats KWS ;
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, notamment en matière de génération des certificats, de remise au porteur, de gestion des révocations et d'information sur l'état des certificats.
- Mettre en œuvre tout ce qui est nécessaire pour respecter les engagements définis dans cette PC, notamment en termes de fiabilité, de qualité et de sécurité.
- Générer, et renouveler lorsque nécessaire, ses bi-clés et les certificats correspondants (signature de certificats et de LCR), ou faire renouveler ses certificats si le cas échéant l'AC est rattachée à une AC hiérarchiquement supérieure.
- Diffuser son ou ses certificat(s) d'AC aux porteurs et utilisateurs de certificats.

1.3.2 L'Autorité d'Enregistrement (AE)

L'AE a pour rôle de vérifier l'identité du demandeur de certificat KWS. L'AE est désignée et habilitée par l'AC et par conséquent applique les procédures établies par l'AC pour la vérification de l'identité du demandeur.

L'AE assure les tâches suivantes :

- la prise en compte et la vérification des informations du demandeur de certificat et la constitution du dossier de demande de certificat KWS conformément aux procédures définies par KEYNECTIS ;
- l'établissement et la transmission de la demande de certificat à l'AC après vérification de l'identité selon les procédures applicables ;
- la conservation des pièces du dossier de demande de certificat KWS ou le cas échéant l'envoi vers la composante chargée de l'archivage ;
- la conservation et la protection en confidentialité et en intégrité des données personnelles d'identification du porteur, y compris lors des échanges de ces données avec les autres fonctions de l'IGC.

1.3.3 L'Opérateur de Certification (OC)

L'opérateur de certification assure des prestations techniques, en particulier cryptographiques, nécessaires au processus de certification, conformément à la présente politique de certification et aux pratiques de certification définies par l'AC. L'OC est techniquement dépositaire de la clé privée de l'AC utilisée pour la signature des certificats KWS. Sa responsabilité ne peut être engagée que par l'AC et se limite au respect des procédures qu'il définit afin de répondre aux exigences de la présente politique de certification. La société KEYNECTIS est l'opérateur de certification de l'AC visée par la présente politique de certification.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

1.3.4 Porteurs de certificats

Le porteur de certificat KWS est l'application web identifiée comme s'exécutant sur une machine dont le nom est dans le certificat et appartenant à KEYNECTIS ou au Client par son N° de SIREN. Le porteur du certificat KWS est une personne morale agissant pour le compte de KEYNECTIS ou du Client dans le cadre de la signature de contrats électroniques par l'organisme au travers de son site Web et dans le cadre d'échange de messages chiffré et signés avec la plateforme K.Websign® de KEYNECTIS.

KEYNECTIS est la personne morale qui met en œuvre une plate-forme de signature électronique et d'élaboration de preuve de transaction électronique au profit de Client et d'utilisateur. Elle est représentée par un numéro de SIREN présent dans les certificats KWS mis en œuvre par le serveur web.

1.3.5 Application utilisatrice ou Utilisateur de certificat

Le Client édicte la politique et les pratiques de sécurité dédiées à la contractualisation électronique en ligne utilisées par les utilisateurs de certificat KWS. Dans le cadre de la présente PC et de l'application utilisatrice, les types d'utilisateur de certificat sont :

- Le Client K.Websign® utilise :
 - un certificat KWS-signature et un dispositif de signature afin de réaliser la signature électronique des données métiers transmises à la plate-forme K.Websign® de KEYNECTIS dans les données (BLOB) envoyées par le Client suite à une transaction électronique ;
 - un certificat KWS-Intégrité et un dispositif de vérification de signature afin de vérifier la signature électronique apposée par la plate-forme K.Websign® de KEYNECTIS sur les données (BLOB) envoyées par KEYNECTIS suite à une transaction électronique ;
 - un certificat KWS-Chiffrement et un dispositif de chiffrement afin de protéger des données en confidentialité à destination de la plate-forme K.Websign® de KEYNECTIS ;
- Le Plate-forme K.Websign® utilise :
 - un certificat KWS-Intégrité pour transférer, et protéger en intégrité, l'ensemble des données BLOB générées par la plate-forme K.Websign® et transmise au Client initiateur de la Transaction ;
 - un certificat KWS-Chiffrement hébergé sur la plate-forme K.Websign® pour chiffrer la totalité du BLOB fourni par le serveur du Client ;
 - un certificat KWS-Signature hébergé sur la plate-forme K.Websign® et permettant de créer la preuve K.Websign® signée électroniquement et relative à une transaction électronique entre le Client et l'utilisateur.

Un utilisateur de certificat (noté UC) utilise une chaîne de confiance unique pour chacun des certificats KWS. Cette chaîne de confiance, composée du certificat KWS et du certificat d'AC (certificat auto-signé) qui est pris comme référence pour l'opération de validation mis en œuvre dans le cadre des services K.Websign®.

1.4 Usages des certificats et applications concernés par la politique de certification

1.4.1 Certificat KWS- Intégrité

Les certificats KWS décrits dans cette politique de certification comportent l'identification de KEYNECTIS et de la machine sur laquelle s'exécute l'application K.Websign®.

L'application identifiée dans la présente politique de certification pour les certificats KWS-Intégrité est la signature électronique des BLOB issus du service K.Websign® à destination de l'application web du Client. L'utilisateur d'un certificat KWS-Intégrité a donc l'assurance que le BLOB émis par KEYNECTIS est intègre et qu'il a été émis par KEYNECTIS. A ce titre, l'utilisation par le porteur de son certificat KWS ne doit être réalisée que dans le cadre de l'exercice de sa qualité d'identité de KEYNECTIS. Le niveau d'assurance dépend, notamment, des moyens mis en œuvre par l'AE pour identifier le porteur KWS et des moyens mis en œuvre par l'AC tout au long du cycle de vie du certificat. De même, le niveau d'assurance dans l'intégrité dépendra des moyens mis en œuvre par KEYNECTIS pour protéger et utiliser la clé privée cryptographique associée aux certificats KWS-Intégrité.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

L'AC décline toute responsabilité dans le cas où le porteur utiliserait son certificat à d'autres fins que celles autorisées au §1.4.1et §1.4.2. Pour le cas où les certificats KWS seraient amenés à être utilisés dans le cadre de nouvelles applications cette politique de certification sera revue pour que le présent paragraphe les mentionne de façon explicite.

1.4.2 Certificat KWS - Signature

Les certificats KWS décrits dans cette politique de certification comportent l'identification de la machine sur laquelle s'exécute l'application K.Websign® de création de preuve électronique d'une transaction électronique entre un Client et un utilisateur.

L'application identifiée dans la présente politique de certification pour les certificats KWS-Signature est la signature électronique de la preuve de la réalisation d'une transaction électronique portant sur une donnée métier signée électroniquement par un Client et un utilisateur à une date et une heure sûre (contenue dans le fichier de preuve). C'est donc au Client de limiter, ou pas, le type de contrat qu'il est possible de signer ainsi à l'aide d'un certificat KWS. L'utilisateur d'un certificat KWS-signature a donc l'assurance que la preuve est émise par KEYNECTIS à l'aide du service K.Websign® et est bien relative à une transaction électronique dûment identifiée. A ce titre, l'utilisation par le porteur de son certificat KWS ne doit être réalisée que dans le cadre de l'exercice de sa qualité d'identité KEYNECTIS. Le niveau d'assurance dépend, notamment, des moyens mis en œuvre par l'AE pour identifier le porteur KWS et des moyens mis en œuvre par l'AC tout au long du cycle de vie du certificat. De même, le niveau d'assurance dans l'intégrité dépendra des moyens mis en œuvre par la société pour protéger et utiliser la clé privée cryptographique associée aux certificats KWS-Signature.

L'autorité de certification décline toute responsabilité dans le cas où le porteur utiliserait son certificat à d'autres fins que celles autorisées au §1.4.1et 1.4.2. Pour le cas où les certificats KWS seraient amenés à être utilisés dans le cadre de nouvelles applications cette politique de certification sera revue pour que le présent paragraphe les mentionne de façon explicite. C'est donc au Client de limiter, ou pas, le type de document qu'il est possible de signer ainsi à l'aide d'un certificat KWS.

1.4.3 Certificat KWS - Chiffrement

Les certificats KWS décrits dans cette politique de certification comportent l'identification de KEYNECTIS.

L'application identifiée dans la présente politique de certification pour les certificats KWS-chiffrement est le chiffrement électronique du BLOB, émis par le Client à l'aide de l'application web du Client.

Cette catégorie d'application permet d'être indépendant du mécanisme de génération et d'utilisation des données échangées. C'est donc au Client de limiter, ou pas, le type de mécanisme qu'il est possible d'employer pour générer et mettre en œuvre les échanges de données. L'utilisateur d'un certificat KWS-chiffrement a donc l'assurance que les données ne seront connues que des deux entités échangeant des données.

L'AC décline toute responsabilité dans le cas où le porteur utiliserait son certificat à d'autres fins que celles autorisées au §1.4.1et 1.4.2. Pour le cas où les certificats KWS seraient amenés à être utilisés dans le cadre de nouvelles applications cette politique de certification sera revue pour que le présent paragraphe les mentionne de façon explicite.

1.4.4 Usages pour les certificats d'AC et de composantes

L'AC est une autorité de certification auto-signée dénommée AC KEYNECTIS KWEBSIGN 1. Elle n'est pas rattachée en terme de hiérarchie technique à une autre autorité de certification.

1.4.5 Usages interdits

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

Il s'agit de tout usage qui ne figure pas dans la liste des usages autorisés (Cf. chapitre 1.4.1 et 1.4.2) ou de tout usage non licite.

1.5 Gestion de la politique de certification

1.5.1 Entité gérant la PC

L'entité en charge de l'administration et de la gestion de la politique de certification est l'Autorité administrative de l'AC. KEYNECTIS est en charge de la gestion de la politique de certification de référence de l'application K.Websign®. Toute évolution de la politique de certification de référence effectuée par la société KEYNECTIS le sera dans le cas d'évolution de l'application K.Websign®. En ce sens l'AA de K.Websign® sera tenue informée des évolutions de la politique de certification de référence K.Websign®. L'AA est responsable de l'élaboration, du suivi et de la modification, dès que nécessaire, de la présente politique de certification.

A cette fin, elle met en œuvre et coordonne une organisation dédiée, qui statue à échéances régulières, sur la nécessité d'apporter des modifications à la PC.

1.5.2 Point de contact

L'AA de l'AC est l'entité à contacter pour toutes questions concernant la présente PC. KEYNECTIS est la société à contacter pour la politique de référence de l'application K.Websign®.

Société	Nom, prénom	Adresse email	Téléphone
KEYNECTIS	FAUROIS Jean Yves	Jean-Yves.fauois@keynectis.com	33153942230

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

Les personnes habilitées à déterminer la conformité de la déclaration des pratiques de certification avec la présente politique de certification sont désignées par l'AA sur la base, en particulier, de leur capacité à faire de l'évaluation de la sécurité.

1.6 Acronymes et définitions

1.6.1 Liste des acronymes

AA	Autorité administrative
AAE	Administrateur d'Autorité d'Enregistrement
AC	Autorité de certification
ADAE	Agence pour le Développement de l'Administration Electronique
AE	Autorité d'enregistrement
CISSI	Commission Interministérielle de la Sécurité des Systèmes d'Information
CRL ou LCR	Certificate Revocation List (Liste des Certificats Révoqués)
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information du SGDN
DPC	Déclaration des Pratiques de Certification
ICD	International Code Designator
ICP	Infrastructure à Clés Publiques
IETF	Internet Engineering Task Force
ISO	International Organization for Standardization
LCR ou CRL	Liste des Certificats Révoqués ou (Certificate Revocation List)
OC	Opérateur de Certification

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

OE	Opérateur d'Enregistrement
PC	Politique de certification
URL	Uniform Resource Locator

1.6.2 Définitions

Le symbole (*) signifie que le terme est défini dans ce paragraphe. Il est utilisé dans le reste du document lorsqu'il est important de renvoyer à la définition du terme employé.

Application utilisatrice : désigne un service applicatif exploitant les certificats* émis par l'autorité de certification* pour des besoins d'authentification ou de signature du porteur* du certificat.

Applications web: désigne un ensemble d'application informatique du Client susceptible de faire appel à la plateforme K.Websign® proposée et hébergée par KEYNECTIS

Autorité administrative (AA) : désigne l'entité représentant l'AC* en charge de la politique de certification* et de la déclaration des pratiques de certification* qu'elle s'engage à respecter et à faire appliquer. La garantie de l'autorité administrative vis-à-vis des utilisateurs de certificat par rapport à l'application concernée vient de la qualité de la technologie mise en œuvre et du cadre réglementaire et contractuel régissant les usages et applications qu'elle a définis.

Autorité de certification (AC) : désigne l'entité responsable des certificats* émis et signés en son nom conformément aux règles définies dans la politique de certification et la déclaration des pratiques de certification associée.

Autorité d'enregistrement (AE) : désigne l'entité qui vérifie, conformément à la politique de certification, les données propres au demandeur de certificat ou au porteur de certificat. L'AE est une composante optionnelle de l'ICP qui dépend d'au moins une autorité de certification. L'AE a pour fonction de réceptionner et de traiter les demandes d'émission et de révocation de certificat.

Biclé : désigne un couple composé d'une clé privée (devant être conservée secrète) et d'une clé publique, nécessaire à la mise en œuvre d'une prestation de cryptologie basée sur des algorithmes asymétriques. Deux types de biclés interviennent dans cette infrastructure de clés publiques :

- Les biclés de **signature** dont la clé privée est utilisée à des fins de signature et/ou d'authentification et la clé publique à des fins de vérification,
- Les biclés de **confidentialité**, dont la clé privée est utilisée par une à des fins de déchiffrement de donnée d'activation et la clé publique à des fins de chiffrement de ces mêmes informations.

Binary Large Object (BLOB) : désigne un ensemble formaté de données dont l'intégralité et la confidentialité sont assurées par la mise en œuvre d'une Signature et d'un chiffrement au moyen des certificats KWS.

Certificat électronique : désigne un fichier électronique attestant que la clé publique appartient à l'entité qu'il identifie. Il est délivré par une autorité de confiance : l'autorité de certification qui en signant le certificat valide le lien entre l'entité et le bi-clé. Un certificat contient des informations telles que :

- l'identité du porteur de certificat,
- la clé publique du porteur de certificat,
- la durée de vie du certificat,
- l'identité de l'autorité de certification qui l'a émis,
- la signature de l'AC qui l'a émis.

Un format standard de certificat est normalisé dans la recommandation X509 v3.

Certificat KWS : désigne des certificats de chiffrement et d'intégrité émis par une autorité de Certification autorisé par la présente AC et utilisé pour le transport des BLOB entre la plateforme Web de [entité cliente] et le site de KEYNECTIS hébergeur de l'application K.WEBSIGN.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

Common Name (CN) : désigne l'identité du titulaire du certificat, par exemple CN=Jean Dupont.

Composante de l'IGC : désigne une entité constituée d'au moins un poste informatique, une application, un moyen de cryptologie et jouant un rôle déterminé au sein de l'IGC. Une composante peut être une AC, une AE, un OC etc.

Déclaration des Pratiques de Certification (DPC) : désigne l'énoncé des pratiques de certification effectivement mises en œuvre par une autorité de certification pour émettre et gérer des certificats.

Document électronique: Ensemble de données structurées pouvant faire l'objet de traitement informatique par les applications informatiques du Client.

Données d'activation : désigne les données privées associées à un porteur permettant de mettre en œuvre sa clé privée. Dans le cas d'un certificat KWA c'est le code CUF.

Données métier: C'est un document électronique sous un format PDF ou XML

Données métier signées: désigne les données métiers auxquelles a été apposée une signature électronique avec un certificat KWA émis dans le cadre de cette présente AC.

Emission (d'un certificat) : fait d'exporter un certificat à l'extérieur d'une AC pour être remis à son porteur.

Enregistrement (d'un porteur*) : désigne l'opération qui consiste pour une autorité d'enregistrement à constituer et à traiter le dossier de demande et/ou de révocation de certificat d'un porteur*.

Infrastructure de Gestion de Clés (IGC): désigne un ensemble organisé de composantes fournissant divers types de prestations dédiées à la gestion de clés et de certificats utilisés par des services de sécurité basés sur la cryptographie à clé publique.

Génération (d'un certificat) : action réalisée par une AC et qui consiste à signer les données du certificat à produire

Liste de Certificats Révoqués (LCR) : désigne la liste de certificats ayant fait l'objet d'une révocation avant la fin de sa période de validité.

Opérateur d'Autorité d'Enregistrement : désigne une personne habilitée par l'Administrateur d'AE à traiter les demandes d'émission et de révocation le cas échéant de certificats.

Opérateur de Certification (OC) : désigne une composante de l'ICP disposant d'une plate-forme informatique sécurisée logiquement et physiquement lui permettant de gérer et émettre les certificats pour le compte de l'autorité de certification, lorsque cette dernière ne possède pas de moyens techniques adéquats.

Organisme Client : désigne l'entité ayant contracté avec KEYNECTIS pour l'utilisation du service K.WebSign.

Original: désigne les données métier signées auxquelles a été apposée une signature électronique avec un certificat KWA émis par cette AC dans le cadre d'une autre PC.

Politique de Certification (PC) : désigne l'ensemble de règles, identifié par un nom (OID), qui définit le type d'applications auxquelles un certificat est adapté ou dédié et les conditions d'émission et de gestion du cycle de vie d'un certificat.

Porteur de certificats KWS : désigne une personne physique, abonné d'une société XXX, identifiée dans le certificat, qui fait l'objet de la transaction de signature proposée par le serveur web de l'organisme et à qui est associé un numéro unique de transaction indiqué dans le certificat Il est appelé **porteur de certificat** dès l'instant où il dispose d'un certificat émis par l'AC.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

Protocole de saisie ou d'agrément : désigne un ensemble d'informations (informations contrôlables et ou partagée) et d'actions (Clicks de souris) du porteurs pour signifier son agrément à l'émission du certificat KWA.

Renouvellement (d'un certificat) : opération effectuée en fin de période de validité d'un certificat qui consiste à générer un nouveau certificat pour un porteur. L'émission d'un nouveau certificat après révocation* n'est pas un renouvellement mais un remplacement.

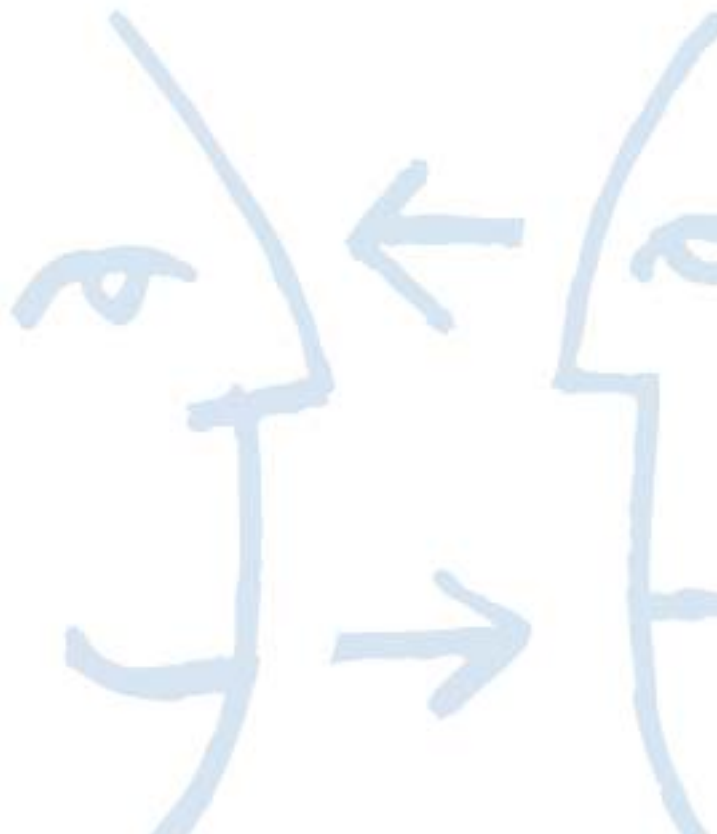
Révocation (d'un certificat) : désigne l'opération demandée par le porteur, l'AC ou une AE conformément à la politique de certification dont le résultat est la suppression de la garantie de l'AC sur un certificat donné, avant la fin de sa période de validité.

Service de publication : désigne l'opération consistant à rendre disponible les certificats de clés publiques émis par une AC à l'ensemble des utilisateurs de ces certificats pour leur permettre de vérifier une signature ou de chiffrer des informations.

TransNUM: désigne un numéro de référence généré par l'application organisme permettant de lier un document électronique sur lequel est apposée une signature électronique par le porteur préalablement identifié par l'application web.

Uniform Resource Locator (URL) : désigne l'adresse d'un site ou d'un dossier disponible sur Internet.

Utilisateur de certificat : désigne les applications qui ont pour fonction d'authentifier le porteur de certificat, de vérifier la signature électronique du porteur de certificat.



2 OBLIGATIONS CONCERNANT LA MISE A DISPOSITION DES INFORMATIONS DEVANT ETRE PUBLIEES

2.1 Entités chargées de la mise à disposition des informations

L'AC a mis en place au sein de son IGC une fonction de publication et une fonction d'information sur l'état des certificats.

2.2 Types d'informations publiées

L'AC publie les informations suivantes :

- la politique de certification
- la Liste de Certificats Révoqués (ou LCR)
- la liste des certificats
- si l'AC est rattachée à une hiérarchie d'AC, les certificats en cours de validité des AC de cette hiérarchie, les différentes politiques de certification correspondantes et les éventuels documents complémentaires, ceci jusqu'à l'AC Racine ;
- pour les certificats d'AC auto signés (AC Racine), les informations permettant aux utilisateurs de certificats de s'assurer de l'origine de ces certificats (cf. chapitre VI.1.4) et de leur état.

L'AC a également pour obligation de publier, à destination des porteurs de certificats et le cas échéant, les différents formulaires nécessaires pour la gestion des certificats (demande d'enregistrement, demande de révocation, demande de renouvellement, etc.).

2.3 Délais et fréquences de publication

2.3.1 Politique de certification

La politique de certification est accessible 24 heures sur 24 et 7 jours sur 7.
Les modifications de la politique de certification sont publiées conformément aux dispositions de l'article 9.8.

2.3.2 Liste des Certificats Révoqués - certificats de porteur

Les listes des Certificats Révoqués qui sont publiées sont accessibles 24 heures sur 24 et 7 jours sur 7.
Elles sont mises à jour toutes les 24 heures.

2.3.3 Liste des Certificats Révoqués - certificats de l'AC

Les AC utilisables pour la validation des certificats sont publiées par le Service de Publication de l'AC au profit de du Client et de l'application K.Websign®.

2.4 Contrôles d'accès aux informations publiées

L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées de l'IGC.

2.4.1 Politique de certification

La PC de l'AC est identifiée par un OID et consultable à l'adresse précisée dans le champ policy Qualifier de chaque certificat sous forme d'une URL.

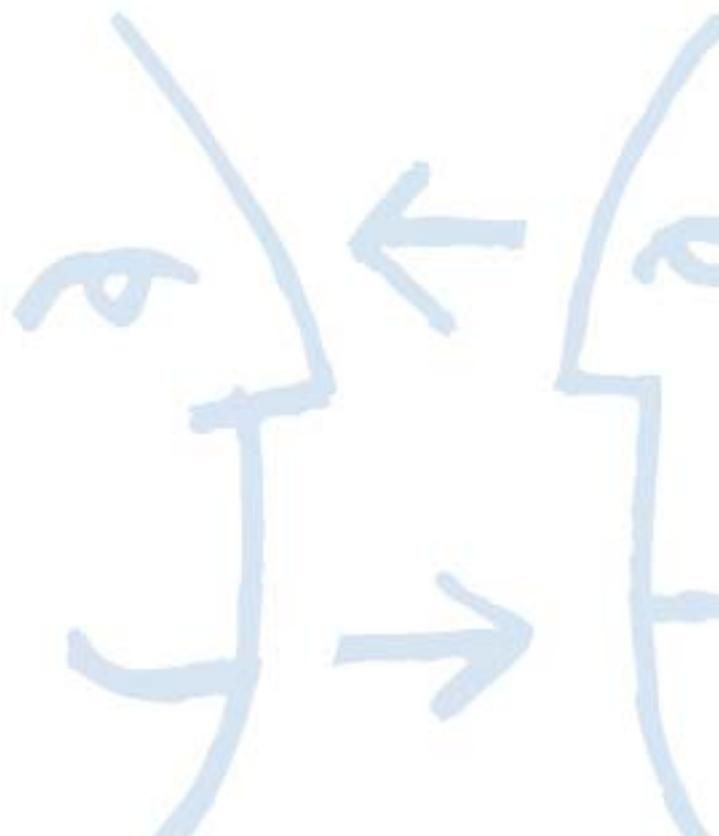
	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

2.4.2 Liste des Certificats Révoqués

Les listes des Certificats Révoqués qui sont publiées sont accessibles 24 heures sur 24 et 7 jours sur 7 au travers d'une URL précisée dans le certificat (valeur du champ CrlDP). Elles sont protégées en intégrité.

2.4.3 Liste des Certificats Révoqués - certificats de l'AC

Les AC utilisables pour la validation des certificats sont publiés par le Service de Publication de l'AC au profit du Client et de l'application K.Websign® au travers de Service de Publication interne à chacun des organismes.



	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

3 IDENTIFICATION ET AUTHENTIFICATION POUR LA DELIVRANCE DE CERTIFICAT

3.1 Nommage

3.1.1 Types de noms

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

Dans chaque certificat, l'AC (issuer) et le porteur (subject) sont identifiés par un « Distinguished Name » (DN) de type X501 dont le format exact est précisé dans le § 7 – Profils des certificats.

3.1.2 Nécessité d'utilisation de noms explicites

Les noms choisis pour désigner les porteurs de certificats doivent être explicites.

Le DN du porteur (Champ objet) contient les informations suivantes :

Nom de l'organisme client <i>OU N° d'organisme émetteur-</i>	Nom commercial SIREN-xxx <i>N° d'organisme émetteur-chiffrement</i> <i>N° d'organisme émetteur-intégrité</i> <i>N° d'organisme émetteur-signature</i>	(Obligatoire) (Obligatoire)
Nom du serveur métier CN=<Nom machine> E=<adresse email>	Nom logique du serveur applicatif ou département Nom de machine ou département ou signataire Adresse email associé au CN	(facultatif) (Obligatoire) (Obligatoire)

L'utilisation d'un pseudonyme n'est pas autorisée. Le certificat KWS ne peut en aucun cas être anonyme.

3.1.3 Anonymisation ou pseudonymisation des porteurs

L'utilisation d'un pseudonyme n'est pas autorisée pour les certificats.

3.1.4 Règles d'interprétation des différentes formes de nom

Sans objet.

3.1.5 Unicité des noms

L'unicité d'un certificat est basée sur l'unicité de son numéro de série à l'intérieur du domaine de l'AC. Chaque DN permet d'identifier de façon unique un porteur au sein de l'ICP pour les certificats KWS renforcé par le type de certificat (Signature, intégrité et Chiffrement).

3.1.6 Procédure de résolution de litige sur déclaration de nom

L'AC est responsable de l'unicité des noms de ses porteurs et de la résolution des litiges portant sur la revendication d'utilisation d'un nom. Tout différent portant sur ce point devra être soumis à l'AA de KEYNECTIS.

3.1.7 Méthode pour prouver la possession de la clé privée

Pour les certificats KWS, la preuve de la possession que la clé privée correspondant au certificat KWS utilisé pour la signature est apportée par les moyens techniques et organisationnels utilisés par la plateforme K.Websign® lors de la demande de certificat

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

3.2 Enregistrement initial d'un porteur et validation de la demande d'émission d'un certificat

L'enregistrement d'un porteur se fait directement auprès de l'AE. La procédure d'identification, d'authentification et de validation de la demande d'émission d'un certificat varie selon le demandeur.

Le contenu du formulaire de demande de certificat contient au minimum les informations suivantes :

- informations permettant de remplir le DN du certificat conformément au 3.1.2 ;
- l'identifiant de l'AE qui fait la demande ;
- le type de certificat (KWS) ;
- une attestation d'accord de la part de KEYNECTIS ;
- numéro de téléphone de son responsable hiérarchique ;
- Adresse Internet de KEYNECTIS..

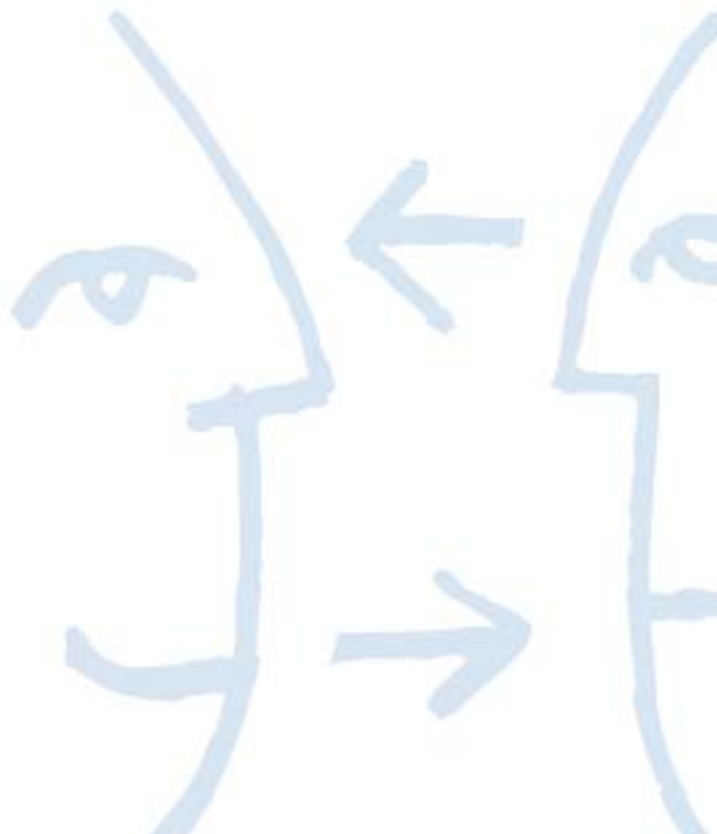
L'authentification du porteur de certificat s'effectue à l'aide de pièce légale (carte d'identité, permis de conduire, passeport, ...) et d'une carte professionnelle dont l'identité est identique à celle porté sur la pièce d'identité légale.

3.3 Authentification et validation d'une demande de révocation par le porteur

Le porteur de certificat envoie un formulaire de révocation de certificat dûment complété et signé à la composante saisie de la demande de révocation au sein de l'AC.

3.4 Authentification d'une demande de renouvellement

La même procédure que pour l'enregistrement initial devra être mise en oeuvre pour remplacer les certificats.



	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

4.1 Origine d'une demande de certificat

Un certificat ne peut être demandé que par le futur porteur KWS avec dans tous les cas consentement préalable de l'AE de KEYNECTIS. Le consentement de l'AE est matérialisé par l'envoi de la demande de certificat conformément au paragraphe 3.2.2.

4.1.1 Processus de demande initiale d'un certificat

Le demandeur de certificat KWS doit remplir et signer le formulaire de demande de certificat et le remettre à l'AE. Le demandeur de certificat doit transmettre à l'AE en face à face le formulaire de demande dûment complété et signé par ses soins.

4.1.2 Traitement d'une demande de certificat

Dans tous les cas, la demande doit être effectuée au travers d'un échange de document. Il est possible de confondre les opérations de Cérémonie des clés et de génération de certificat KWS lors de la même journée afin de minimiser les déplacements et d'optimiser les efforts.

L'AE de KEYNECTIS effectuera alors les opérations suivantes :

- valider l'identité du futur porteur en face à face à l'aide de la carte d'identité légale et professionnelle ;
- contrôler que le formulaire de demande de certificat est correctement complété ;
- vérifier la cohérence des justificatifs présentés et en conserver une trace sous la forme d'une photocopie ;
- s'assurer que le demandeur a pris connaissance des modalités applicables pour l'utilisation du certificat.

En cas de rejet de la demande, l'AE en informe le demandeur de certificat. Suite à l'acceptation de la demande de certificat, le demandeur utilise les informations remises par l'AE et son poste de travail pour obtenir son certificat.

4.1.3 Délivrance du certificat

Après vérification de la complétude des données, l'AE de KEYNECTIS transmet la demande à l'AC pour validation et vérification de l'identité du demandeur avant enregistrement de la demande pour émission des certificats KWS.

Suite à l'authentification de l'origine et à la vérification de l'intégrité de la demande provenant de l'AE, KEYNECTIS déclenche les processus de génération et de préparation des différents éléments destinés au porteur pour que ce dernier puisse recevoir le certificat.

La bi-clé est générée sur un poste sécurisé au sein de KEYNECTIS et la récupération du Certificat sous forme d'un PKCS#12 (noté P12) est faite sur le même poste sécurisé. Une sauvegarde avec le Password choisi par l'AE est réalisée par KEYNECTIS. Ces deux certificats P12, ainsi générés, sont remis à l'AE demandeuse. Cette opération est effectuée pour les certificats KWS.

L'AE a un délai de 5 jours pour confirmer son acceptation à KEYNECTIS par envoi d'un mail signé ou d'un courrier papier. La réception de cette acceptation vaut ouverture du service K.Websign.

4.1.4 Acceptation du certificat

Après acceptation par l'AE de la demande de certificat et transmission à l'AC, le demandeur reçoit son certificat sous forme d'un fichier P12 protégé par un Password. La remise du certificat à l'AE par le service client KEYNECTIS vaut acceptation tacite du certificat.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

4.2 Révocation d'un certificat

4.2.1 Causes possibles de révocation

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

- les informations du porteur figurant dans son certificat ne sont plus en conformité avec l'identité ou l'utilisation prévue dans le certificat, ceci avant l'expiration normale du certificat ;
- il a été démontré que le porteur n'a pas respecté les règles applicables d'utilisation du certificat ;
- il a été démontré une fraude dans le dossier de demande de certificat ;
- la clé privée du porteur est suspectée de compromission, est compromise, est perdue ou est volée ;
- le porteur ou une autre composante autorisée en fait la demande ;
- le certificat de l'AC est révoqué (ce qui entraîne la révocation de tous les certificats signés par la clé privée correspondante) ;
- la fermeture du service K.Websign®

Lorsqu'une des circonstances ci-dessus se réalise et que l'AC en a eu connaissance, le certificat concerné doit être révoqué et le numéro de série placé dans la Liste de Certificats Révoqués (LCR).

4.2.2 Origines d'une demande de révocation

Les entités qui peuvent demander la révocation d'un certificat sont les suivantes :

- le porteur ou KEYNECTIS au nom duquel le certificat a été émis
- l'AE de l'AC ;
- le responsable du Département de KEYNECTIS dont dépend le porteur du certificat, avec validation de la demande par l'AA
- l'AC émettrice du certificat ou l'une de ses composantes (AE) avec validation de la demande par l'AA

4.2.3 Processus de demande de révocation

La composante saisie par le porteur de la demande de révocation doit :

- Contrôler l'authenticité et l'intégrité de la demande de révocation et des informations fournies ;
- Transmettre la demande à l'AC afin d'effectuer la révocation.

Toute demande de révocation d'un certificat, qu'elle que soit l'entité qui en est à l'origine, doit être réalisée en utilisant le formulaire de révocation de certificat. Le formulaire une fois complété et signé sera transmis à la composante habilitée.

4.2.4 Procédure et délai de traitement d'une demande de révocation

A la réception de la demande de révocation conforme et authentifié par l'AC, l'AC révoque le certificat en faisant placer le numéro de série du certificat dans une liste de révocation. Le propriétaire du certificat, et le cas échéant le demandeur de la révocation s'il ne s'agit pas de la même personne, sera informé par mail du bon déroulement de la révocation.

Dès que le porteur ou une personne autorisée a connaissance qu'une des causes possibles de révocation est effective il doit formuler sa demande de révocation sans délai.

Toute demande de révocation d'un certificat porteur doit être traitée dans un délai inférieur à 3 jours ouvrés, ce délai s'entend entre la réception de la demande de révocation authentifiée et la mise à disposition de l'information de révocation auprès de utilisateurs.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

4.2.5 Publication des causes de révocation de certificat

La demande de révocation est enregistrée dans les journaux d'évènements avec suffisamment d'informations (à préciser dans la DPC) sur les causes initiales ayant entraîné la révocation du certificat. Les causes de révocation ne seront pas publiées dans la CRL.

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

L'utilisateur d'un certificat KWS est tenu de vérifier, avant son utilisation, l'état des certificats de l'ensemble de la chaîne de certification correspondante. La méthode utilisée (LCR) est à l'appréciation de l'AC selon leur disponibilité et les contraintes liées à son application.

4.2.7 Fréquence d'établissement des LCR

Les CRL sont émises toutes les 24 heures. Les LCR sont des LCR V2.

4.2.8 Délai maximum de publication d'une LCR

La CRL est publiée avec un délai maximum de 2 heures suite à génération.

4.3 Renouvellement d'un certificat Modification d'un certificat de porteur

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

A titre informatif, l'opération de renouvellement de certificat correspondant à la délivrance d'un nouveau certificat pour lequel seules les dates de validité sont modifiées et où toutes les autres informations sont identiques au certificat précédent y compris la clé publique du porteur, n'est pas autorisée par la présente politique de certification. Les certificats et les bi-clés doivent avoir la même durée de vie, il ne peut donc y avoir de renouvellement de certificat sans renouvellement de bi-clés.

Les bi-clés des porteurs et les certificats correspondants seront renouvelés tous les trois ans.

Lors des renouvellements de bi-clés et des certificats correspondants et si le DN ne doit pas être modifié, il appartient au porteur d'un certificat Personnel KEYNECTIS de formuler auprès de l'AE une demande de renouvellement par la délivrance d'un nouveau certificat en lui remettant le formulaire DDNC complété et signé.

Il est par la suite procédé à l'application de la procédure de demande initiale de certificat prévue et définie au § 4.1, § 4.2, § 4.3 et § 4.4.

4.4 Suspension d'un certificat de porteur

Sans objet.

4.5 Fonction d'information sur l'état des certificats

L'autorité de certification fournit aux utilisateurs de certificats les informations leur permettant de vérifier et de valider, préalablement à son utilisation, le statut d'un certificat et de l'ensemble de la chaîne de certification correspondante.

La CRL est publiée avec un délai maximum de 24 heures maximum suite à génération.

4.6 Séquestre et recouvrement de clés

5 LE SEQUESTRE ET LE RECOUVREMENT DE CLES PRIVEES DES PORTEURS NE SONT PAS AUTORISES PAR LA PRESENTE POLITIQUE DE CERTIFICATION.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

MESURES DE SECURITE NON TECHNIQUES DES OPERATIONS

5.1 Mesures de sécurité physique

5.1.1 Situation géographique

Le site d'exploitation de l'autorité de certification est situé à Paris (FRANCE) dans les locaux de la société KEYNECTIS. La construction du site respecte les règlements et normes en vigueur et son installation tient compte des résultats de l'analyse de risque, du métier d'opérateur de certification selon la méthode EBIOS, par exemple certaines exigences spécifiques de type inondation, explosion (proximité d'une zone d'usines ou d'entrepôts de produits chimiques,...) réalisées par KEYNECTIS.

5.1.2 Accès physique

Afin de limiter l'accès aux applications et aux informations de l'ICP et afin d'assurer la disponibilité du système de l'AC, KEYNECTIS a mis en place un périmètre de sécurité opéré pour ses besoins. La mise en œuvre de ce périmètre permet de respecter les principes de séparation des rôles de confiance telle que prévus dans cette PC.

Les accès au site des composantes d'AC et d'AE sont limités aux seules personnes nécessaires à la réalisation des services et selon leur besoin d'en connaître. Les accès sont nominatifs et leur traçabilité accès est assurée. La sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion passifs et actifs. Tout évènement de sécurité fait l'objet d'un enregistrement et d'un traitement.

Le système d'information supportant les services de certification est installé au sein du périmètre de sécurité de KEYNECTIS.

5.1.3 Energie et air conditionné

Des systèmes de protection de l'alimentation électrique et de génération d'air conditionné sont mis en œuvre par KEYNECTIS afin d'assurer la continuité des services délivrés.

Les matériels utilisés pour la réalisation des services sont opérés dans le respect des conditions définies par leurs fournisseurs et ou constructeurs.

5.1.4 Exposition aux liquides

Les systèmes de KEYNECTIS sont implantés de telle manière qu'ils ne sont pas sensibles aux inondations et autres projections et écoulements de liquides.

5.1.5 Prévention et protection incendie

Les moyens de prévention et de lutte contre les incendies mis en œuvre par KEYNECTIS permettent de respecter les exigences et les engagements pris par l'AC dans sa PC, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.6 Mise hors service des supports

En fin de vie, les supports seront soit détruits soit réinitialisés en vue d'une réutilisation.

5.1.7 Sauvegardes hors site

L'AC réalise des sauvegardes hors site, en s'appuyant sur les procédures convenues avec Keynectis, permettant une reprise rapide des fonctions de gestion des révocation et d'information sur l'état des certificats suite à la

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

survenance d'un sinistre ou d'un événement affectant gravement et de manière durable la réalisation de ces fonctions.

Les précisions quant aux modalités des sauvegardes des informations sont fournies dans la DPC.

5.2 Mesures de sécurité procédurales

5.2.1 Rôles de confiance

Afin de veiller à la séparation des tâches critiques, il est fait distinction de cinq rôles fonctionnels au sein des composantes de l'ICP.

Il s'agit des rôles fonctionnels suivants :

- **Ingénieur système** : il est chargé de la mise en service et de la maintenance du système
- **Responsable de sécurité** : il est chargé de la gestion de la sécurité au niveau du système ainsi que de l'exploitation et de la sauvegarde des fichiers d'audit du système
- **Administrateur de composante** : il est chargé au sein de la composante à laquelle il est rattaché de la mise en œuvre de la politique de certification et de la déclaration des pratiques de certification de l'ICP.
- **Opérateur** : il est chargé de l'exploitation du système et des applications pour les fonctions mises en œuvre par la composante.
- **Responsable qualité** : il est chargé d'assurer la cohérence des actions des différents rôles décrits précédemment et la qualité des fonctions fournies par la composante par rapport à la politique de certification, à la déclaration des pratiques de certification et à la politique de sécurité de la composante.

En plus de ces rôles de confiance au sein de chaque composante de l'IGC, en fonction de l'organisation de l'IGC et des outils mis en œuvre, l'AC peut être amenée à distinguer d'autres rôles de confiance, comme ceux de porteurs de parts de secrets d'IGC.

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

5.2.2 Nombre de personnes nécessaires à l'exécution de tâches sensibles

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

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

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

5.2.3 Identification et authentification des rôles

Chaque entité opérant une composante de l'IGC a fait vérifier l'identité et les autorisations de tout membre de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu au sein de l'IGC.

Ces contrôles sont décrits dans la DPC de l'AC et sont conformes à la politique de sécurité de la composante.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

Chaque attribution d'un rôle à un membre du personnel de l'IGC est notifiée par écrit.

5.3 Mesures de sécurité vis-à-vis du personnel

5.3.1 Qualifications, compétence et habilitations requises

Chaque personne amenée à travailler au sein des composantes de l'ICP est soumise à une clause de confidentialité vis-à-vis de son employeur. Il est également vérifié que les attributions de ces personnes correspondent à leurs compétences professionnelles.

Toute personne intervenant dans les procédures de certification de l'ICP est informée de ses responsabilités relatives aux services de l'ICP et des procédures liées à la sécurité du système et au contrôle du personnel.

5.3.2 Procédures de vérification des antécédents

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

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

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

5.3.3 Exigences en matière de formation initiale

Le personnel a été préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en œuvre et qu'il doit respecter, correspondants à la composante au sein de laquelle il opère.

Les personnels ont eu connaissance et compris les implications des opérations dont ils ont la responsabilité.

5.3.4 Exigences et fréquence en matière de formation continue

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation, etc. en fonction de la nature de ces évolutions.

5.3.5 Gestion des métiers

Des précisions sont fournies dans la DPC fournie par KEYNECTIS

5.3.6 Sanctions en cas d'actions non autorisées

Des précisions sont fournies dans la DPC.

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

Des précisions sont fournies dans la DPC.

5.3.8 Documentation fournie au personnel

Des précisions sont fournies dans la DPC.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

5.4 Procédures de constitution des données d'audit

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

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

5.4.1 Type d'événements à enregistrer

Chaque entité opérant une composante de l'ICP journalise les événements concernant les systèmes liés aux fonctions qu'elle met en oeuvre dans le cadre de l'ICP :

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- événements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres événements sont également recueillis. Il s'agit de événements concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques aux zones sensibles ;
- les actions de maintenance et de changements de la configuration des systèmes ;
- les changements apportés au personnel ayant des rôles de confiance ;
- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,...).

En plus de ces exigences de journalisation communes à toutes les composantes et à toutes les fonctions de l'ICP, des événements spécifiques aux différentes fonctions de l'ICP sont également journalisés, notamment :

- réception d'une demande de certificat (initiale et renouvellement) ;
- validation / rejet d'une demande de certificat ;
- événements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...) ;
- génération des certificats des porteurs ;
- transmission des certificats aux porteurs et, selon les cas, acceptations / rejets par les porteurs ;
- publication et mise à jour des informations liées à l'AC ;
- réception d'une demande de révocation ;
- validation / rejet d'une demande de révocation ;
- génération puis publication des LCR .

Chaque enregistrement d'un événement dans un journal contient les champs suivants :

- type de l'évènement ;
- nom de l'exécutant ou référence du système déclenchant l'évènement ;
- date et heure de l'évènement ;
- résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant figure explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement pourra également contenir les champs suivants :

- destinataire de l'opération ;
- nom du demandeur de l'opération ou référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'évènement ;
- toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

5.4.2 Processus de journalisation

Les opérations de journalisation sont effectuées au cours du processus considéré.

En cas de saisie manuelle, l'écriture se fera, sauf exception, le même jour ouvré que l'évènement.

Des précisions sont fournies dans la DPC.

5.4.3 Protection des journaux d'évènements

La journalisation doit être conçue et mise en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.

Les journaux d'évènements doivent être protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non)

La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.4 Procédures de sauvegarde des journaux d'évènements

Chaque entité opérant une composante de l'IGC met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences de la présente PC Type et en fonction des résultats de l'analyse de risque de l'AC.

5.4.5 Système de collecte des journaux d'évènements

Des précisions sont fournies dans la DPC.

5.4.6 Evaluation des vulnérabilités

Chaque entité opérant une composante de l'ICP est en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

Les journaux d'évènements sont contrôlés régulièrement afin d'identifier des anomalies liées à des tentatives en échec.

Les journaux sont analysés dans leur totalité au moins à une fréquence mensuelle. Cette analyse donnera lieu à un résumé dans lequel les éléments importants sont identifiés, analysés et expliqués. Le résumé doit faire apparaître les anomalies et les falsifications constatées. Il est transmis régulièrement à l'AC.

5.5 Archivage des données

L'archivage des données permet d'assurer la pérennité des journaux constitués par les différentes composantes de l'ICP.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

5.5.1 Type de données archivées

Les données archivées au niveau de chaque composante, sont les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;
- les politiques de certification ;
- les déclarations des pratiques de certification ;
- les accords contractuels avec d'autres AC, le cas échéant ;
- les certificats et LCR tels qu'émis ou publiés ;
- les journaux d'évènements des différentes entités de l'ICP.

5.5.2 Période de conservation des archives

Certificats et LCR émis par l'AC

Les certificats de clés de porteurs et d'AC, ainsi que les LCR / LAR produites, sont archivés 10 ans après l'expiration de ces certificats.

Journaux d'évènements

Les journaux d'évènements traités au § 5.4 sont archivés pendant 10 ans après leur génération. L'intégrité des enregistrements est assurée tout au long de leur cycle de vie.

Autres journaux

Aucune exigence n'est stipulée.

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives et leurs sauvegardes seront :

- protégées en intégrité ;
- accessibles aux personnes autorisées ;
- en mesure de pouvoir être relues et exploitées.

5.5.4 Procédures de sauvegardes des archives

Des précisions sont fournies dans la DPC.

5.5.5 Exigences d'horodatage des données

Des précisions sont fournies dans la DPC.

5.5.6 Système de collecte des archives

Des précisions sont fournies dans la DPC.

5.5.7 Procédures de récupération et de vérification des archives

Les archives papier sont récupérables dans un délai inférieur ou égal à 48 heures ouvrées. Les sauvegardes électroniques sont récupérables dans un délai inférieur ou égal à 48 heures ouvrées.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

5.6 Changement de clé d'AC

L'AC ne peut pas générer de certificats dont la date de fin de validité serait postérieure à la date d'expiration du certificat correspondant de l'AC. Pour cela la période de validité de ce certificat de l'AC doit être supérieure à celle des certificats qu'elle signe.

Au regard de la date de fin de validité de ce certificat, son renouvellement doit être demandé dans un délai au moins égal à la durée de vie des certificats signés par la clé privée correspondante.

Dès qu'une nouvelle bi-clé d'AC est générée, seule la nouvelle clé privée doit être utilisée pour signer des certificats.

Le certificat d'AC précédent reste utilisable dans le cadre des opérations de gestion de la validité des certificats émis sous cette clé et ce au moins jusqu'à ce que tous les certificats signés avec la clé privée correspondante aient expiré.

5.7 Reprise suite à compromission et sinistre

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

Des procédures et des moyens de remontée et de traitement des incidents sont mis en place par chacune des entités opérant une composante de l'ICP, notamment au travers de la sensibilisation et de la formation de son personnel et au travers de l'analyse des différents journaux d'évènements.

5.7.2 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et/ou données) et en cas de compromission de la clé privée d'une composante

Chaque composante de l'ICP dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'ICP découlant de la présente politique de certification et des résultats de l'analyse de risque de l'ICP, notamment en ce qui concerne les fonctions liées à la publication et / ou liées à la révocation des certificats. Dans le cas de compromission d'une clé d'AC, le certificat correspondant doit être immédiatement révoqué.

5.7.3 Capacités de continuité d'activité suite à un sinistre

Les différentes composantes de l'ICP disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences de la politique de certification.

5.8 Fin de vie de l'ICP

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

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

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

Transfert d'activité ou cessation d'activité affectant une composante de l'ICP

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

- Mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des certificats des porteurs et des informations relatives aux certificats).

- Assurer la continuité de la révocation (prise en compte d'une demande de révocation et publication des LCR), conformément aux exigences de disponibilité pour ces fonctions définies dans la présente politique de certification.

Cessation d'activité affectant l'AC

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de certificats donnée seulement).

La cessation partielle d'activité doit être progressive de telle sorte que seules les obligations visées aux 1), 2), et 3) ci-dessous soient à exécuter par l'AC, ou une entité tierce qui reprend les activités, lors de l'expiration du dernier certificat émis par elle.

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

Lors de l'arrêt du service, l'AC doit :

- 1) s'interdire de transmettre la clé privée lui ayant permis d'émettre des certificats ;
- 2) prendre toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;
- 3) révoquer son certificat.

6 MESURES DE SECURITE TECHNIQUES ET LOGIQUES

6.1 Génération et installation de biclés

6.1.1 Génération des bi-clés

6.1.1.1 Clés d'AC

La génération des clés de signature de l'AC est réalisée dans un environnement sécurisé.

Les clés de signature d'AC sont générées et mises en œuvre dans un module cryptographique certifié au niveau EAL 4+ selon les critères communs.

La génération des clés de signature d'AC est effectuée lors d'une cérémonie de clés, par des personnels dans des rôles de confiance et selon un processus défini au préalable. Des précisions quant aux modalités de génération des clés sont fournies dans la DPC notamment sur le rôle des porteurs de secret.

Les cérémonies de clés se déroulent sous le contrôle d'au moins deux personnes dans des rôles de confiance et en présence de témoins dont au moins un sont externes à l'AC et sont impartiaux. Les témoins attestent, de façon objective et factuelle, du déroulement de la cérémonie par rapport au script préalablement défini. Un officier public (huissier ou notaire) atteste du déroulement selon les conditions définies au préalables.

6.1.1.2 Clés de porteur de certificat KWS

La génération est effectuée dans un dispositif logiciel sur les machines off-line de KEYNECTIS dans ses locaux et en présence des porteurs de certificats.

6.1.2 Transmission de la clé privée à son propriétaire

La clé privée doit être transmise au porteur de manière sécurisée, afin d'en assurer la confidentialité et l'intégrité entre le module de génération de clé et le porteur. Les clés sont protégées en confidentialité à l'aide d'une enveloppe P12 dont le mot de passe est choisi par l'AE.

6.1.3 Transmission de la clé publique à l'AC

La clé publique du porteur est transmise vers l'AC en étant protégée en intégrité sous un format Pkcs#10.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

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

Les clés publiques de vérification de signature de l'AC sont diffusées auprès des utilisateurs de certificats KWS par un moyen qui en assure l'intégrité de bout en bout et qui permet d'authentifier l'AC émettrice.

La clé publique de l'AC ainsi que les informations correspondantes (certificats, empreintes numériques, déclaration d'appartenance) sont disponibles et sont récupérables facilement par les utilisateurs de certificats.

6.1.5 Taille des clés

La taille des clés est de 2048 bits pour l'algorithme RSA pour les certificats KWS et AC.

6.1.6 Contrôle de la qualité des paramètres des clés

L'équipement de génération des bi-clés d'AC utilise des paramètres respectant les normes de sécurité propres à l'algorithme correspondant à la bi-clé.

6.1.7 Objectifs d'usage de la clé

L'utilisation de la clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats et de LCR.

L'utilisation d'une clé privée d'AC et du certificat associé est strictement limitée à la signature de certificats et de LCR.

6.2 Mesures de sécurité pour la protection des clés privées

6.2.1 Standards et mesures de sécurité pour les modules cryptographiques

6.2.1.1 Module AC

Le module cryptographique de l'AC est un HSM évalué certifié EAL 4+ ou FIPS 140-1 level 3.

6.2.1.2 Module porteur

Le module cryptographique est logiciel pour les clés KWS, il est installé sur le site de [entité cliente] qui en assure la sécurité.

6.2.2 Contrôle de la clé privée d'AC par plusieurs personnes

Le contrôle de la clé privée de signature de l'AC est assuré par un outil mettant en œuvre le partage des secrets.

6.2.3 Séquestre de la clé privée

Ni les clés privées d'AC, ni les clés privées des porteurs ne sont séquestrées.

6.2.4 Copie de secours de la clé privée

Les clés privées des porteurs ne font l'objet d'aucune copie de secours.

La clé privée d'AC fait l'objet d'une copie de sauvegarde. Tout transfert de clé privée de l'AC se fait sous forme chiffrée.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

6.2.5 Archivage de la clé privée

Les clés privées de l'AC et des porteurs ne sont pas archivées.

6.2.6 Méthode d'activation de la clé privée

6.2.6.1 Clé d'AC

L'activation des clés privées d'AC dans le module cryptographique est contrôlée via des données d'activation et fait intervenir au moins deux personnes dans des rôles de confiance

6.2.6.2 Clé KWS

Les clés sont activées, uniquement par le porteur, chaque fois, ou par un procédé apportant un degré d'assurance équivalent, lors de son action à signer les preuves et les blobs ainsi qu'au déchiffrement des blobs. La DPC précise la mise en œuvre des clés privées KWS.

6.2.7 Méthode de destruction des clés privées

En fin de vie d'une clé privée d'AC, normale ou anticipée (révocation), cette clé sera détruite ainsi que toute copie de sauvegarde et tout élément permettant éventuellement de la reconstituer.

Les clés des porteurs sont détruites après leur utilisation dans une signature.

6.3 Autres aspects de la gestion des bi-clés

6.3.1 Archivage des clés publiques

Les clés publiques de l'AC et des porteurs sont archivées dans le cadre de l'archivage des certificats correspondants.

6.3.2 Durée de vie des biclés et des certificats

Les bi-clés et les certificats des porteurs KWS utilisables dans le cadre de la présente politique de certification ont une durée de vie similaire, soit une durée de validité de 3 ans.

6.4 Données d'activation

6.4.1 Données d'activation correspondant à la clé privée de l'AC

Les données d'activation de la clé privée de l'AC sont des secrets détenus par des porteurs de secret.

6.4.2 Données d'activation correspondant à la clé privée KWS du porteur

Les données d'activation de la clé du porteur KWS sont choisies par l'organisme client.

6.5 Mesures de sécurité des systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est défini dans la DPC de l'AC. Il répond aux objectifs de sécurité suivants:

- identification et authentification des personnels de l'OSC et de l'AE pour l'accès au système ;
- gestion de sessions d'utilisation ;
- protection contre les virus informatiques, toutes formes de logiciels compromettant ou non-autorisés et mises à jour des logiciels ;

- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- protection du réseau contre l'intrusion ;
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent ;
- fonctions d'audits (non-répudiation et nature des actions effectuées) ;
- éventuellement, gestion des reprises sur erreur.

Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires qui seront alors définies par [entité cliente].

Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) sont mis en place.

6.6 Mesures de sécurité du système durant son cycle de vie

6.6.1 Mesures de sécurité liées au développement des systèmes

L'implémentation du système permettant de mettre en œuvre les composantes de l'ICP est documentée. La configuration du système des composantes de l'ICP ainsi que toute modification et mise à niveau est documentée et contrôlée par KEYNECTIS

6.6.2 Gestion de la sécurité

Toute évolution significative d'un système d'une composante de l'ICP est signalée par la composante à l'AC pour validation. Elle est documentée et apparaît dans les procédures de fonctionnement interne de la composante concernée,.

6.7 Mesures de sécurité réseau

L'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.

De plus, les échanges entre composantes au sein de l'IGC mettent en œuvre des mesures particulières en fonction du niveau de sensibilité des informations (utilisation de réseaux séparés / isolés, mise en œuvre de mécanismes cryptographiques à l'aide de clés d'infrastructure et de contrôle, etc.) définies par l'opérateur KEYNECTIS.

6.8 Mesures de sécurité pour les modules cryptographiques

Les modules cryptographiques utilisés par l'AC sont certifiés au niveau EAL 4+ selon les critères communs.

Ils sont manipulés selon et bénéficient de mesures de protection spécifiques, sous la responsabilité d'un acteur de confiance.

7 PROFILS DES CERTIFICATS ET DES LISTES DE CERTIFICATS REVOQUES

7.1 Profil des certificats

Ils incluent les champs de base définis dans la recommandation X.509 v1 :

- Numéro de version ;
- Numéro de série,
- Emetteur ;
- Identifiant et paramètre de l'algorithme ;
- Validité ;
- Subject Public Key Info ;
- Subject.

7.1.1 Numéro de version

Les certificats utilisés sont les certificats X509 v3 spécifiés dans la norme [9594-8].

7.1.2 Extensions du certificat

Les extensions utilisées sont au minimum :

- Authority Key Identifier (non critique) ;
- Key usage (non critique) ;
- SubjectKeyIdentifier (non critique) ;
- CRL Distribution Points (non critique) ;
- Basic Constraints (non critique).

7.1.3 OID des algorithmes

Les certificats, en fonction de l'algorithme de signature, doivent contenir un identificateur d'algorithme qui est inscrit auprès d'un registre (par exemple un registre international tel que celui de l'ISO).

7.1.4 Forme des noms

Les noms respectent les règles édictées au § 3.1.1.

Certificat de base	Valeur
Version	2 (=version 3)
Serial number	Défini par l'outil
Taille de la clé	2048
Durée de validité	2 ans
Issuer DN	O=KEYNECTIS OU=KWEBSIGN CN=AC KEYNECTIS KWEBSIGN 1 C=FR
Subject DN	C=FR O=<Organisme client > OU= < N° Siren organisme -XXXXX> Trois valeurs possibles de XXX: N° d'organisme émetteur-chiffrement N° d'organisme émetteur-intégrité N° d'organisme émetteur-signature

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

	OU=<Nom du serveur métier ou Département > CN=<Nom machine ou Département ou signataire > E=<adresse email > email associable au CN ci dessus
NotBefore	YYMMDDHHMMSS
NotAfter	YYMMDDHHMMSS
Public Key Algorithm	sha1WithRSAEncryption (1.2.840.113549.1.1.5)
Parameters	NULL

7.1.5 Contraintes sur les noms

Cf. 7.1.4.

7.1.6 OID des PC

Le certificat contient l'OID de la présente PC.

7.1.7 Utilisation de l'extension "contraintes de politique"

Cf. DPC..

7.1.8 Sémantique et syntaxe des qualifiants de politique

Cf. DPC.

7.1.9 Sémantiques de traitement des extensions critiques de la PC

Cf. DPC.

7.2 Profil de LCR

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

- **version** : version de la liste de Certificats révoqués X.509.
- **signature** : identifiant de l'algorithme de signature de l'AC XXX
- **issuer** : nom de l'AC XXX
- **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** : extension non proposée par la LCR de l'AC XXX
- **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 ;
- **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.

8 AUDIT DE CONFORMITE ET AUTRES EVALUATIONS

Les audits et les évaluations concernent les audits que l'AC diligente afin de s'assurer que l'ensemble de son IGC est bien conforme aux engagements affichés dans la présente PC et aux pratiques identifiées dans la DPC correspondante.

8.1 Fréquences et / ou circonstances des évaluations

L'AC procède régulièrement ou en tant que de besoin à des contrôles de conformité de l'ensemble de son IGC.

8.2 Identités / qualifications des évaluateurs

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

8.3 Relations entre évaluateurs et entités évaluées

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

8.4 Sujets couverts par les évaluations

Les contrôles de conformité portent sur une ou plusieurs composantes de l'IGC (contrôles ponctuels) et visent à vérifier le respect des engagements et pratiques définies dans la présente PC et dans la DPC associée.

8.5 Actions prises suite aux conclusions des évaluations

A l'issue d'un contrôle de conformité, l'équipe d'audit rend à l'AC un avis parmi les suivants : "réussite", "échec", "à confirmer".

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

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

8.6 Communication des résultats

Les résultats des audits de conformité sont conservés par l'AC. Ils sont communiqués par l'AC aux composantes concernées suite à l'audit.

9 DISPOSITIONS DE PORTEE GENERALE

9.1 Barèmes des prix

9.1.1 Tarifs pour la fourniture ou le renouvellement de certificats

Cette exigence est couverte par la politique commerciale de l'AC.

9.1.2 Tarifs pour accéder aux certificats

Cette exigence est couverte par la politique commerciale de l'AC.

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

Cette exigence est couverte par la politique commerciale de l'AC.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

9.1.4 Tarifs pour d'autres services

Cette exigence est couverte par la politique commerciale de l'AC.

9.1.5 Politique de remboursement

Cette exigence est couverte par la politique commerciale de l'AC.

9.2 Responsabilité financière

9.2.1 Couverture par les assurances

Cette exigence est couverte par la politique commerciale de l'AC.

9.2.2 Autres ressources

Sans objet.

9.2.3 Couverture et garantie concernant les entités utilisatrices

Sans objet.

9.3 Loi applicable et juridictions compétentes

Les dispositions de la politique de certification sont régies par le droit français.

En cas de litige relatif à l'interprétation, la formation ou l'exécution de la présente politique, et faute de parvenir à un accord amiable, tout différend sera porté devant les tribunaux compétents de Paris.

9.4 Droits de propriété intellectuelle

Tous les droits de propriété intellectuelle détenus par l'IGC sont protégés par la loi, règlement et autres conventions internationales applicables.

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.

9.5 Politique de confidentialité

9.5.1 Types d'informations considérées comme confidentielles

Les informations suivantes sont considérées comme confidentielles :

- La DPC de l'AC
- Les clés privées des porteurs de certificats
- Les données d'activation associées aux clés privées des porteurs de certificat
- Les journaux d'événements des composantes de l'AC et de l'AE
- Les données liées à l'enregistrement du porteur et notamment les données personnelles

9.5.2 Délivrance aux autorités habilitées

Les procédures de l'AC relatives au traitement de la confidentialité doivent être conformes à la législation française.

9.6 Protection des données personnelles

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 collectés, détenus ou transmis par l'AC ou par l'AE dans le cadre de la délivrance d'un certificat.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

Les porteurs disposent d'un droit d'accès et de rectification des données collectées par l'AC ou l'AE pour l'émission du certificat et la gestion de son cycle de vie. Ce droit peut s'exercer auprès de l'AA.

Toutes les données collectées et détenues par l'AC sont considérées comme confidentielles, hormis les données figurant dans le certificat.

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.

9.7 Durée et fin anticipée de validité de la politique de certification

9.7.1 Durée de validité

La politique de certification de l'AC restera en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette politique de certification.

9.7.2 Fin anticipée de validité

La publication d'une nouvelle version de la présente politique de certification n'impose pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité.

9.7.3 Effets de la fin de validité et clauses restant applicables

Certaines fonctions de l'ICP, notamment d'archivage, de protection des données confidentielles seront maintenues jusqu'à leur terme.

9.8 Administration de la politique de certification

Le présent article indique les dispositions prises par l'AC en matière d'administration et de gestion de la présente politique de certification.

9.8.1 Délai de préavis

KEYNECTIS informera les porteurs de certificats et l'AC en respectant un préavis de trente (30) jours calendaires, avant de procéder à tout changement de la présente politique de certification susceptible de produire un effet majeur sur lesdits porteurs et utilisateurs.

L'AC informera les porteurs et les utilisateurs de certificats en respectant un préavis de quinze (15) jours calendaires avant de procéder à tout changement de la présente politique de certification susceptible de produire un effet mineur sur lesdits porteurs et utilisateurs.

L'AC peut modifier la présente politique sans préavis lorsque, selon l'évaluation du responsable de la Politique de Certification, ces modifications n'ont aucun impact sur elle.

9.8.2 Forme de diffusion des avis

Dans les cas de modification soumise à préavis, l'AC avise les porteurs et les utilisateurs des modifications apportées à la présente politique de certification, par tous moyens à sa convenance dont notamment le site web de l'AC et la messagerie électronique, en fonction de la portée des modifications. Les avis de modification impactant les AC tierces leur sont expressément communiqués.

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

9.8.3 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 porteurs ou d'utilisateurs, le responsable de la politique peut, à sa discrétion, instituer une nouvelle politique avec un nouvel identificateur d'objet (OID).

9.9 Procédures d'informations

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

La présente Politique de Certification est publiée et accessible aux porteurs et utilisateurs à l'adresse URL suivante : <https://www.keynectis.com/PC/ACKEYNECTISKWEBSIGN1KWS.pdf>. Une copie peut également être obtenue par courrier électronique, sur demande auprès de l'AA.

9.10 Rôles et obligations de l'ICP et de ses composantes

Les obligations communes aux composantes de l'ICP sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- n'utiliser leurs clés cryptographiques (publiques, privées et/ou secrètes) qu'aux fins prévues lors de leur émission et avec les outils spécifiés dans les conditions fixées par la PC de l'AC et les documents qui en découlent,
- respecter et appliquer la partie de la DPC leur incombant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par l'AC (cf. chapitre VIII) et l'organisme de qualification,
- respecter les accords ou documents qui les lient entre elles ou aux porteurs,
- documenter leurs procédures internes de fonctionnement,
- mettre en oeuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.

9.10.1 Autorité de certification

L'AC a notamment pour obligation de :

- Pouvoir démontrer aux utilisateurs de ses certificats qu'elle a émis un certificat pour un porteur donné et que ce porteur a accepté le certificat, conformément aux exigences du § 4.1.
- Garantir et maintenir la cohérence de sa DPC avec la PC.
- Prendre toutes les mesures raisonnables pour s'assurer que ses porteurs sont informés de leurs droits et obligations en ce qui concerne l'utilisation et la gestion des clés, des certificats ou encore de l'équipement et des logiciels utilisés aux fins de l'ICP.
- Publier les informations précisées au § 2.2.
- Respecter ou de faire respecter par les composantes de l'AC, les obligations de journalisation et d'archivage.

L'AC est responsable de la bonne application de sa politique de certification et reconnaît avoir à sa charge un devoir général de surveillance, quant à la sécurité et l'intégrité des certificats délivrés par elle-même ou l'une de ses composantes.

9.10.2 Autorités d'enregistrement

L'AE a pour rôle de vérifier l'identité du demandeur de certificat conformément à ses engagements pris vis-à-vis de l'AC ;

	POLITIQUE DE CERTIFICATION K.Websign®	Date :	24 Janvier 2007
	AUTORITE DE CERTIFICATION AC KEYNECTIS KWebsign 1	OID :	1.3.6.1.4.1.22234.2.3.3.3.1.
		Version :	1.01

9.10.3 Porteurs de certificats

Le porteur doit se conformer à toutes les exigences de la présente politique de certification et des procédures internes formalisées par l'AC. Le porteur 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.

Le porteur doit notamment :

- communiquer des informations exactes et à jour lors de la demande;
- protéger ses données d'activation et, le cas échéant, les mettre en oeuvre ;
- respecter les conditions d'utilisation de sa clé privée et du certificat correspondant ;

9.10.4 Utilisateurs de certificats

Les personnes ou applications utilisant les certificats doivent :

- vérifier et respecter l'usage pour lequel un certificat a été émis ;
- vérifier la validité du certificat ;
- pour chaque certificat de la chaîne de certification, du certificat du porteur jusqu'à l'AC, vérifier la signature numérique de l'AC émettrice du certificat considéré et contrôler la validité de ce certificat (dates de validité, statut de révocation) ;
- vérifier et respecter les obligations des utilisateurs de certificats exprimées dans la présente politique de certification.

9.11 Limite de responsabilité

L'AC n'est tenue qu'à une obligation de moyen pour la mise en œuvre des services de certification qu'elle fournit.

Seule la responsabilité de l'AC peut être mise en cause en cas de non-respect des dispositions prévues par les présentes.

L'AC décline toute responsabilité à l'égard de l'usage qui est fait des certificats KWA qu'elle a émis dans des conditions et à des fins autres que celles prévues dans la présente politique de certification que dans tout autre document contractuel applicable associé.

L'AC décline toute responsabilité quant aux conséquences des retards ou pertes que pourraient subir dans leur transmission tous messages électroniques, lettres, documents, et quant aux retards, à l'altération ou autres erreurs pouvant se produire dans la transmission de toute télécommunication.

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

De façon expresse, sont considérés comme cas de force majeure ou cas fortuit, outre ceux habituellement retenus par la jurisprudence des cours et tribunaux français, les conflits sociaux, la défaillance du réseau ou des installations ou réseaux de télécommunications externes.