POLITIQUE DE CERTIFICATION

Certificats KWA pour PDF

AUTORITE DE CERTIFICATION KEYNECTIS K.Websign® CDS CA

Date :	09 Novembre 2009
Version :	1.0
Référence :	PC/KEY/K-Web/KEYNECTIS/KWA-KEYNECTIS CDS
OID :	1.3.6.1.4.1.22234.2.8.3.1

HISTORIQUE DES MODIFICATIONS

Historique du document :				
Date	Version	Rédacteur	Objet	Statut
06/11/2009	0.1	DM/JYF/MQ	Rédaction	Projet
09/11/2009	1.0	JYF	Validation du document pour diffusion	Diffusable

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

SOMMAIRE

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com

S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

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.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com

S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

1 INTRODUCTION

1.1 Présentation générale de la politique de certification

Ce document constitue la politique de certification de la société KEYNECTIS agissant en tant qu'Autorité de Certification (ci-après désignée « AC ») pour les besoins de sécurisation des applications web de ses clients ayant souscrit au Service K.Websign®, ci-après « Clients K.Websign® », mis à disposition par la société KEYNECTIS, incluant la fonctionnalité 'Signature électronique embarquée'.

Les certificats électroniques émis et gérés conformément à la présente politique de certification, ci-après désignés dans le présent document « certificats KWA CDS », sont délivrés aux utilisateurs des applications web proposées par les Clients K.Websign® utilisant le Service K.Websign® (ci-après « les Utilisateurs »).

Les certificats KWA CDS seront utilisés pour des besoins de signature électronique de documents électroniques sous format PDF localement présents sur le site web du Client K.Websign®, échangés et signés entre ce dernier et ses propres clients, partenaires ou toute autre personne ; la signature apposée sur le document manifestant ainsi leur consentement respectif. A chaque signature de document sous forme électronique entre le Client K.Websign® et l'Utilisateur, il sera associé un identifiant unique par le biais du Certificat KWA CDS.

Cette politique de certification a pour objet de décrire dans le cadre du service K.Websign® :

- les engagements de l'AC relatifs à l'émission et à la gestion des Certificats KWA CDS, 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,
- les engagements de l'AE relatifs à la définition des règles d'émission des Certificats KWA CDS et à leur bonne application,
- les conditions d'utilisation des Certificats KWA CDS.

Les intervenants suivants doivent prendre connaissance de la présente Politique de certification et s'y soumettre :

- tout Utilisateur à savoir toute personne utilisant pour son propre compte ou pour le compte d'une entité qu'elle est habilitée à représenter, le site web du Client K.Websign® et souhaitant signer un document sous forme électronique sous format PDF proposé par le Client K.Websign®,
- tout Client K.Websign® lié contractuellement à KEYNECTIS pour l'utilisation du service K.Websign®, notamment dans le cadre de ses engagements en qualité d'Autorité d'enregistrement habilitée par KEYNECTIS,
- l'Autorité de Certification KEYNECTIS délivrant les Certificats KWA CDS dans le cadre du service K.Websign® pour les besoins de ses Clients,
- toute personne ou entité souhaitant se fier valablement à un Certificat KWA CDS délivré par l'AC KEYNECTIS émettrice dudit certificat.

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 SGDN-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 1.3.6.1.4.1.22234.2.8.3.1

La déclaration des pratiques de certification correspondante est référencée par l'OID 1.3.6.1.4.1.22234.2.8.4.1

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 KWA K.Websign KEYNECTIS CDS » et de « DPC KWA-K.Websign KEYNECTIS CDS », pour les Certificats émis par l'AC KEYNECTS KWEBSIGN CDS CA.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

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 KWA CDS repose sur la mise en œuvre et l'exploitation d'une Infrastructure de Clés Publiques (ICP).

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 KWA tout au long de leur cycle de vie (génération, diffusion, renouvellement, révocation,...) dans le cadre du Service K.Websign®.

La décomposition en fonctions de l'ICP est présentée dans le cadre de ce chapitre.

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

- Fonction de demande de certificat : cette fonction reçoit les informations d'identification et/ou d'authentification du Demandeur d'un certificat, ainsi qu'éventuellement d'autres attributs spécifiques, avant de transmettre la demande correspondante à la fonction adéquate de l'ICP.

  Dans le cadre de la présente PC, la fonction de demande de certificat KWA CDS est mise en œuvre par l'Application K.Websign®, dès lors que la demande d'émission du certificat a été réalisée et validée par l'AE à savoir le Client K.Websign®.

- Fonction de génération de certificat : cette fonction génère les certificats (création du gabarit, signature électronique avec la clé privée de l'AC) à partir des informations transmises par l'AE et de la clé publique de l'Utilisateur provenant de la fonction de génération de la bi-clé cryptographique de l'Utilisateur.

- Dans le cadre de la présente PC, cette fonction de génération des certificats est assurée par la société KEYNECTIS en tant qu'Autorité de certification.

- Fonction de génération de la bi-clé cryptographique de l'Utilisateur : cette fonction génère la bi-clé cryptographique à destination de l'Utilisateur et la prépare en vue de la mise à disposition du contrôle de l'Utilisateur pour une seule opération de signature.

  Dans le cadre de la présente PC, cette fonction est assurée par la société KEYNECTIS par le biais d'un module HSM hébergé sur l'Application K.Websign®.

- Fonction de mise à disposition du certificat : cette fonction met sous le contrôle de l'Utilisateur son certificat associé à la biclé générée précédemment.

  Dans le cadre de la présente PC, cette fonction est assurée par la société KEYNECTIS.

- Fonction de publication : cette fonction met à disposition des différentes parties concernées, les politiques et pratiques publiées par l'AC, les certificats d'AC et toute autre information pertinente destinée aux Utilisateurs. Dans le cadre de la présente PC, cette fonction est assurée par la société KEYNECTIS étant précisé que pour ce qui concerne les règles et conditions relatives à la délivrance du Certificat KWA CDS, cette partie est assurée par l'Autorité d'enregistrement à savoir le Client K.Websign®.

- Fonction de gestion des révocations de certificat : cette fonction n'est pas implémentée du fait de la durée très brève des Certificats KWA CDS.

- Fonction d'information sur l'état des certificats : cette fonction fournit aux Applications utilisatrices 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.

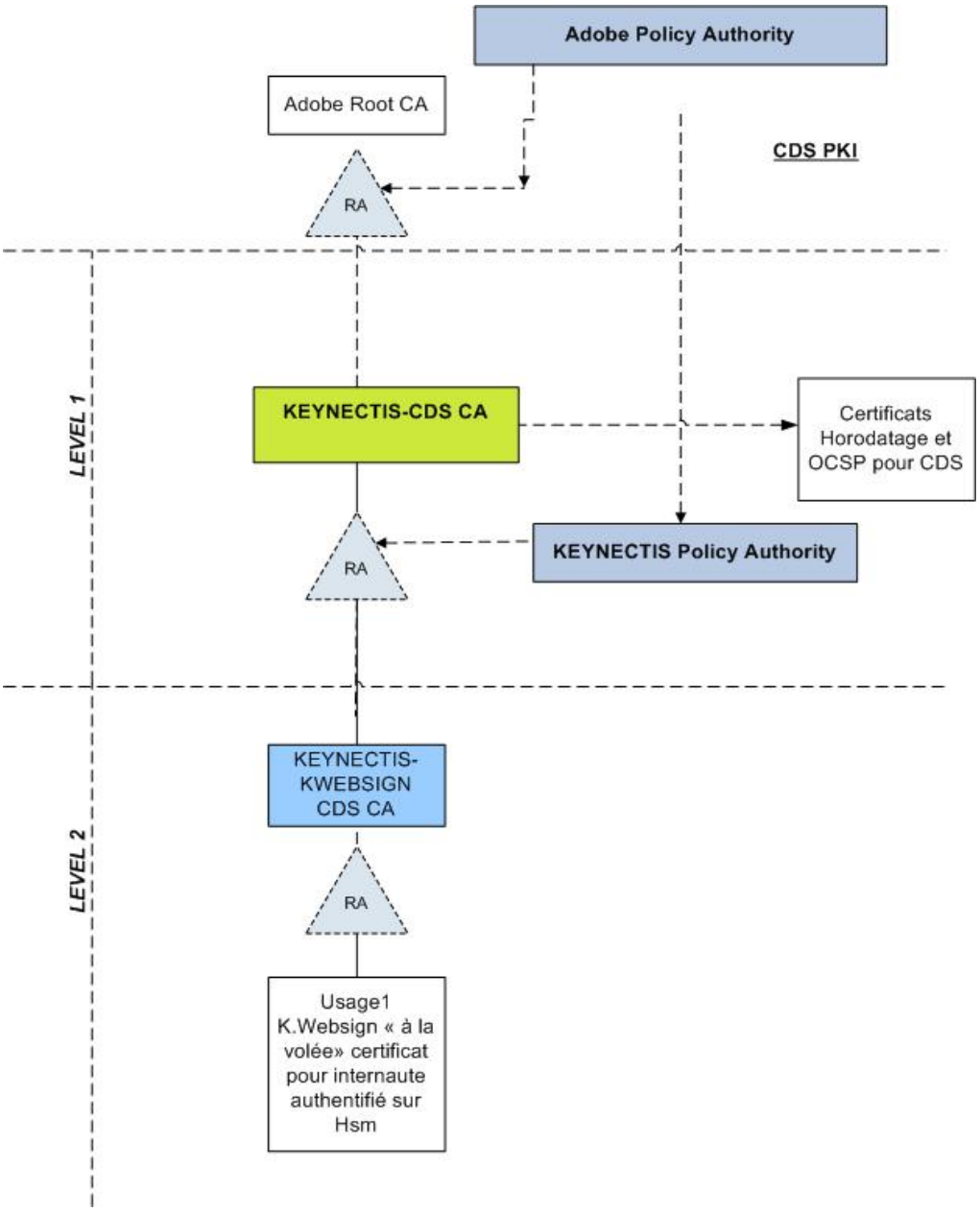
Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

1.3.1 L'Autorité de Certification (AC)

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 KWA CDS. A ce titre, elle assure la gestion de leur cycle de vie tout en délégant aux Clients K.Websign® la définition des règles applicables en matière d'enregistrement des demandes d'émission de Certificat KWA CDS et la validation des demandes d'émission de Certificat KWA CDS.

L'autorité de certification KEYNECTIS est une autorité de certification fille rattachée à une hiérarchie de certification Adobe conformément au schéma ci-dessous.



Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

Les exigences qui incombent à l'AC en tant que responsable de l'ensemble de l'ICP dans le cadre de ses fonctions opérationnelles, qu'elle assume directement ou qu'elle confie à des entités externes, sont les suivantes :

- Rendre accessible l'ensemble des prestations déclarées dans sa PC aux Utilisateurs et aux Applications utilisatrices qui gèrent et mettent œuvre les certificats KWA CDS ;
- S'assurer que les exigences de la PC et les procédures de la DPC associée sont appliquées par chacune des composantes de l'ICP ;
- Mener une analyse de risques permettant de déterminer les objectifs de sécurité propres à couvrir les risques métiers de l'ensemble de l'ICP 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 Utilisateurs puisque cette partie est confiée aux Clients K.Websign ® ;
- Mettre en œuvre les différentes fonctions identifiées dans sa PC, notamment en matière de génération des certificats, 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 Utilisateurs et aux Applications utilisatrices.

1.3.2 L'Autorité d'Enregistrement (AE)

L'AE a pour rôle de vérifier l'identité du Demandeur de Certificat KWA CDS afin de valider la demande d'émission du Certificat KWA CDS.

L'AE est désignée et habilitée par l'AC par voie contractuelle. Par conséquent, l'AE applique des procédures d'identification des personnes physiques ou morales, conformément aux règles définies par elle-même en fonction de ses besoins notamment dans le Protocole de consentement. Son rôle est d'établir que le demandeur justifie de l'identité et des qualités qui seront indiquées dans le Certificat. Ces procédures d'identification sont variables selon le niveau de confiance que l'AE entend apporter à cette vérification.

L'AE assure plus précisément les tâches suivantes :

- la prise en compte et la vérification des informations du Demandeur de certificat lors de la demande de certificat KWA conformément aux procédures définies ;
- l'établissement et la transmission de la demande de certificat à l'AC après vérification de l'identité selon les procédures applicables au travers de l'appel du Module TransID et conformément à la Politique de Gestion de Preuves associée ;
- la conservation et la protection en confidentialité et en intégrité des données personnelles d'identification de l'Utilisateur, y compris lors des échanges de ces données avec les autres fonctions de l'ICP.

L'AE assure le lien entre l'AC et l'Utilisateur. Elle est dépositaire des informations personnelles de l'Utilisateur, qu'elle ait ou non eu un contact physique avec celui-ci au cours de la procédure d'identification.

L'AC assure un devoir de contrôle et d'audit de l'AE, conformément aux engagements contractuels mis en place entre l'AE et l'AC et aux dispositions des présentes.

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

- Coordination des demandes d'identification électronique ;
- Vérification des caractéristiques d'identification des Demandeurs de Certificats KWA CDS ;
- Transmission des données d'authentification de l'Utilisateur à l'AE ;
- Gestion et protection des données personnelles des Utilisateurs ;
- Administration, exploitation et protection des moyens techniques mis à la disposition de l'AE par l'AC et utilisés par ladite AE pour remplir ces missions.

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

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

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

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 KWA CDS. Sa responsabilité se limite au respect des procédures que l'AC définit afin de répondre aux exigences de la présente politique de certification.
Dans la présente Politique de Certification, son rôle et ses obligations ne sont pas distingués de ceux de l'AC, car KEYNECTIS est son propre opérateur de certification.

1.3.4 Utilisateur

Dans le cadre de la présente Politique de Certification, l'Utilisateur est la personne physique préalablement identifiée par le Client K.Websign® dont le nom est inscrit dans le Certificat KWA CDS, et souhaitant apposer sa signature sur le document électronique proposé par une application web du Client K.Websign®.
Le certificat KWA CDS contient le numéro unique de la Transaction objet de l'émission du certificat.
L'Utilisateur agit pour son propre compte ou le cas échéant est habilité à agir pour celui de la personne morale qu'il représente, dans le cadre de la signature des documents électroniques proposés par le Client K.Websign® au travers de son Application web. L'identité de l'Utilisateur est reconnue et validée préalablement par le Client K.Websign® en sa qualité d'AE.

1.3.5 Application utilisatrice du Certificat KWA CDS

L'Application utilisatrice du Certificat KWA CDS se définit comme l'ensemble des intervenants utilisant et se fiant aux Certificats émis par l'AC dans le cadre du Service K.Websign®. A cette fin, elle se fonde sur la chaîne de confiance mise en place pour chacun des certificats. Cette chaîne de confiance, composée du certificat KWA CDS et de(s) certificat(s) d'AC de niveau supérieur est prise comme référence pour l'opération de validation de la signature.

Les applications utilisatrices du Certificat KWA CDS sont :

- Une application web déclarée par le Client K.Websign ayant pour fonction de présenter et de proposer à la signature de l'Utilisateur un document non modifiable (signé par un certificat d'Organisme Client) et l'associer à un numéro de transaction unique (TransNUM),
- Une application de visualisation du contenu des Fichiers de Preuve apte à vérifier la signature électronique apposée par l'Utilisateur au moyen du Certificat KWA CDS.
- Tous les logiciels de visualisation des documents PDF de la sociéte Adobe®

Dans le cadre des présentes, le Client K.Websign® pour pouvoir réaliser les demandes de certificats dans la hiérarchie Adobe® Certified Document Service (CDS) a de plus l'obligation de réaliser la première signature du document PDF en utilisant un logiciel de signature de la société Adobe de type Live Cycle Digital Signature ou Acrobat et ce conformément la PC de la société ADOBE dont l'OID est : 1.2.840.113583.1.2.1, disponible sur l'Url Suivante: https://www.adobe.com/misc/pki/cds_cp.html

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

1.4.1 Champ d'application

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

- la qualité de l'exploitation et du maintien de la sécurité technique de la plateforme technique émettant les certificats ;
- le mode d'enregistrement de l'Utilisateur pour l'émission des Certificats, à savoir la détermination et la mise en application des règles d'identification des Demandeurs de Certificats.

1.4.2 Usages autorisés

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

Les Certificats KWA CDS émis dans le cadre de cette présente politique de certification sont utilisés uniquement dans le cadre des applications web des Clients K.Websign® utilisant le Service K.Websign® mis à leur disposition par KEYNECTIS et qui incluse la fonctionnalité 'Signature électronique embarquée'.

Le Certificat KWA CDS n'est utilisé par l'Utilisateur que pour signer un document électronique présenté par un Client K.Websign® sur le site web de ce dernier, et ce afin de manifester son accord sur les termes contenus dans le document.

1.4.3 Usages interdits

Il s'agit de tout usage qui ne figure pas dans la liste des usages autorisés indiqués ci-dessus ou de tout usage non licite et/ou non légal.
L'AC décline toute responsabilité dans le cas où l'Utilisateur utiliserait son certificat à d'autres fins que celles autorisées au présent article. Pour le cas où les certificats KWA CDS seraient amenés à être utilisés dans le cadre de nouvelles applications, la présente Politique de certification sera revue afin que le présent paragraphe les mentionne de façon explicite.

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 (AA) de l'AC. 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 échéance régulière, sur la nécessité d'apporter des modifications à la Politique de Certification.

1.5.2 Point de contact

L'AA de l'AC est l'entité à contacter pour toutes questions concernant la présente Politique de Certification.

Le représentant habilité de cette AA est :
Monsieur Jean-Yves Faurois
Directeur Qualité & Sécurité de KEYNECTIS
KEYNECTIS – 11-13 rue René Jacques – 92131 Issy les Moulineaux cedex
Téléphone : (33) (0)1.55.64.22.00
Fax : (33) (0)1.55.64.22.01

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 pour la partie relevant de l'AC sur la base, en particulier, de leur capacité à faire l'évaluation de la sécurité. Pour la partie relevant de l'AE, la personne habilitée à déterminer la conformité de la déclaration des pratiques de certification avec la présente politique de certification est désignée par l'Organisme client sur la base, en particulier, de leur capacité à faire l'évaluation de la sécurité.

1.6 Acronymes et définitions

1.6.1 Liste des acronymes

AA	Autorité administrative
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)
CDS	Certified Document Service
DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information du SGDN

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

DPC	Déclaration des Pratiques de Certification
ICP	Infrastructure à Clés Publiques
IETF	Internet Engineering Task Force
LCR ou CRL	Liste des Certificats Révoqués ou (Certificate Revocation List)
OC	Opérateur de Certification
PC	Politique de certification
URL	Uniform Resource Locator

1.6.2 Définitions

Les termes qui suivent auront la signification suivante lorsqu'ils sont utilisés avec une majuscule dans la présente Politique de certification.

Adobe® Certified Document Services ou CDS : désigne le programme Adobe mettant à disposition un ensemble de fonctions de signature électronique au sein du format PDF permettant à toute personne recevant un document d'en vérifier l'intégrité et d'identifier son auteur de façon certaine avec les produits Adobe Reader ou Acrobat. Les certificats utilisés doivent être conformes aux exigences des politiques de certification approuvées par le département de sécurité de la société Adobe et de KEYNECTIS.

Application utilisatrice : désigne un service applicatif du Client K.Websign® utilisant et exploitant les Certificats émis par l'Autorité de certification pour des besoins de signature de données électroniques par l'Utilisateur.

Application K.Websign® : désigne l'ensemble cohérent d'informations et de programmes informatiques de KEYNECTIS hébergé sur les matériels de KEYNECTIS mis à disposition des Clients K.Websign® et ayant pour objet de fournir un service de génération de Fichier de preuve associé aux Transactions réalisées.

Application web : désigne un ensemble d'applications informatiques du Client K.Websign® susceptible de faire appel au Service K.Websign® proposé et hébergé par KEYNECTIS. Plus particulièrement, ce terme désigne l'ensemble cohérent d'informations et de programmes informatiques du Client K.Websign® ayant pour objet de mettre à disposition de l'Utilisateur un service de Transactions conformément au Protocole de consentement défini par le Client K.Websign®.

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 et des Applications utilisatrices 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 les données propres à l'Utilisateur. L'AE est une composante de l'ICP qui dépend d'au moins d'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 l'ICP :

- 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 application à des fins de déchiffrement de données ou informations 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.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

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 de l'Utilisateur,
- la clé publique de l'Utilisateur,
- 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 KWA CDS : désigne des certificats de signature utilisés pour la signature par l'Utilisateur de documents sous forme électronique crées et signés par le Client K.Websign®. Leur caractéristique principale est d'avoir une existence éphémère permettant leur génération à la volée et de contenir une information unique (le TransNUM) référençant et identifiant le document à signer.

Certificat KWS : désigne selon les cas des certificats de chiffrement, d'intégrité ou de signature. Ces certificats seront utilisés soit pour la signature des Données métier, soit pour le transport des BLOB entre la plateforme Web du Client K.Websign® et le site de KEYNECTIS fournisseur du Service K.Websign®.

Clé publique : désigne une clé mathématique (constituée en même temps qu'une clé associée et liée mathématiquement à une clé privée) rendue publique et qui est utilisée pour vérifier la signature numérique d'une donnée reçue, qui a été préalablement signée avec une clé privée.

Clé privée : désigne une clé mathématique associé à la Clé publique, qui reste sous l'autorité de l'Utilisateur et qui sert à signer les données électroniques.

Client K.Websign® : désigne l'entité ayant contracté avec KEYNECTIS pour l'utilisation du Service K.Websign® et qui dans le cadre des présentes exerce la fonction d'Autorité d'Enregistrement.

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

Composante de l'ICP : 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'ICP. 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 : désigne l'ensemble de données structurées pouvant faire l'objet de traitement informatique par les applications informatiques du Client K.Websign®.

Données d'activation : désigne les données ou actions associées à un Utilisateur permettant de mettre en œuvre sa clé privée. Dans le cas d'un Certificat KWA, ces données ou actions sont définies par le Protocole de consentement du Client K.Websign® et la Politique de Gestion de Preuves.

Données métier : désigne le document électronique sous un format PDF ou XML élaboré par le Client K.Websign®.

Données métier signées : désigne les Données métier auxquelles a été apposée une signature électronique avec un certificat KWS. Ces Données métier signées sont ensuite présentées à l'Utilisateur qui y apposera sa signature s'il y consent.

Enregistrement (d'un Utilisateur) : 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 KWA.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

Enveloppe Sécurisée : désigne l'ensemble des éléments crées en suite de la réalisation de la Transaction entre le Client K.Websign® et l'Utilisateur et lors de la fabrication d'un accusé réception par K.Websign®, condensé dans un BLOB signé et chiffré.

Fichier de preuve : désigne conformément aux procédures décrites dans la Politique de Gestion de Preuves K.Websign® l'ensemble des éléments crées lors de la réalisation de la Transaction entre le Client K.Websign® et l'Utilisateur, puis conservé pendant un délai conforme aux exigences légales, permettant ainsi d'assurer la traçabilité de la réalisation de la Transaction.

Horodatage : désigne l'ensemble des prestations nécessaires à la datation des événements réalisés.

Infrastructure à Clés Publiques (**ICP**) : désigne un ensemble de moyens techniques, humains, organisationnels, documentaires et contractuels pour assurer, avec des systèmes de cryptographie asymétrique, un environnement sécurisé aux échanges électroniques. L'ICP gère le cycle de vie d'un Certificat à savoir sa génération, sa distribution, sa gestion et son archivage.

Intégrité : désigne la propriété d'exactitude et de complétude des données. Dans le cadre des présentes, cette propriété est mise en œuvre soit au moyen de certificat électronique KWS de signature ou d'intégrité pour les données stockées, soit au moyen de certificat électronique de contrôle d'accès (SSL) pour les données échangées.

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 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.

Politique de Certification (PC) : désigne l'ensemble des règles énoncées et publiées par l'AC décrivant les caractéristiques générales des Certificats qu'elle délivre. Ce document décrit les obligations et responsabilités de l'AC, de l'AE, des Utilisateurs et de toutes les composantes de l'ICP intervenant dans l'ensemble du cycle de vie d'un Certificat.

Politique de Gestion de Preuves (PGP) : désigne le document décrivant le processus technique de signature d'un document sous forme électronique, puis de création et de la conservation du Fichier de preuve dans le cadre du Service K.Websign®.

Protocole de consentement : désigne le document dans lequel le Client K.Websign® précise l'ensemble des règles pour une Application web donnée utilisant le Service K.Websign® à savoir (i) la définition des actions à réaliser par l'Utilisateur pour signer le document proposé par le Client K.Websign®, (ii) les modalités de transfert de l'identification de l'Utilisateur par le Client K.Websign® vers l'Application K.Websign®, (iii) les modalités de contrôle par le Service K.Websign® des informations saisies par l'Utilisateur par comparaison aux informations fournies par le Client K.Websign® pour chaque transaction, et (iv) le type de fichier soumis par le Client K.Websign® à signature (XML/PDF…).

Service de certification électronique : désigne l'ensemble des prestations réalisées par l'Autorité de Certification pour l'émission de Certificats en appliquant des procédures stipulées dans la Politique de Certification et dans ses engagements contractuels le cas échéant vis à vis des Utilisateurs.

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

Service K.Websign® : désigne le service de KEYNECTIS mis à disposition de ses clients, constitué notamment de l'Application K.Websign®, dont l'objet est de permettre à ses clients à partir de leur portail web de proposer à leurs propres clients, fournisseurs ou toute autre personne un service de signature de document sous forme électronique à partir d'une Signature électronique associée à un certificat à usage unique d'une durée limitée émis

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

pour chaque transaction et de constituer pour archivage électronique un Fichier de preuve relatif à la Transaction réalisée en ligne.

Signature électronique : désigne, aux termes de l'article 1316-4 du Code civil, « *l'usage d'un procédé fiable d'identification garantissant son lien avec l'acte auquel elle s'attache* » et a pour objet d'identifier la personne qui l'appose et de manifester le consentement du signataire aux obligations qui découlent de l'acte signé.

Signature électronique embarquée : désigne une fonctionnalité additionnelle du Service K.Websign permettant d'intégrer la signature électronique de l'Utilisateur, et le cas échéant de l'Organisme Client, dans un document sous format PDF. Dans ce cas, les Certificats de signature utilisés sont émis par l'Autorité de certification de KEYNECTIS ayant été référencée par Adobe® dans le cadre du programme CDS. Il est précisé que cette fonctionnalité additionnelle de Signature électronique embarquée dans un document sous format PDF est associée à un service de validation OSCP du certificat signataire et d'horodatage de la signature lors de l'utilisation du certificat pour signature du document sous forme électronique. Cette fonctionnalité additionnelle est liée au choix du service de certification mis à disposition du Client par Keynectis et communiqué à Keynectis lors de la mise en production de l'application du Client utilisant le service K.Websign.

Transaction électronique : désigne l'échange électronique entre le Client K.Websign® et l'Utilisateur au cours duquel le Client K.Websign® lui propose pour signature un document sous forme électronique.

TransID : désigne le module logiciel fourni par KEYNECTIS au Client K.Websign® (dans le cadre du Service K.Websign®) pour générer une Enveloppe Sécurisée. Il permet de créer un identifiant TransNUM dans un BLOB ainsi que de signer et chiffrer un BLOB.

TransNUM: désigne un numéro de référence unique généré par l'Application web du Client K.Websign® permettant de lier un document électronique, sur lequel est apposée une signature électronique, à l'Utilisateur préalablement identifié par l'Application web.

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

Utilisateur : désigne une personne physique, connue du Client K.Websign®, identifiée dans le certificat KWA, qui appose sa signature électronique sur le document sous forme électronique proposé par l'Application web du Client K.Websign® permettant ainsi d'y associer un numéro unique de transaction. L'Utilisateur est appelé **Demandeur de certificat** lors de sa demande de Certificat et avant l'émission du Certificat.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

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 ICP une fonction de publication et une fonction d'information sur l'état des certificats.

2.2 Types d'informations publiées

L'AC publie la présente Politique de certification et les informations concernant la révocation des Certificats.

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 KWA CDS

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 certificats d'AC utilisables pour la validation des certificats KWA CDS sont publiés par l'AC au profit 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'ICP.

2.4.1 Politique de certification

La présente Politique de certification est consultable à l'adresse précisée dans le champ policy Qualifier de chaque Certificat sous forme d'un OID.

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.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

3 IDENTIFICATION ET VERIFICATION D'IDENTITE POUR LA DELIVRANCE DE CERTIFICAT

Le présent chapitre indique les dispositions prises par l'AC en matière d'enregistrement des demandes de Certificats, étant précisé que la majeure partie des procédures de demandes d'émission des Certificats sont laissées à la discrétion du Client K.Websign® en sa qualité d'AE.

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 l'Utilisateur (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 Utilisation de noms explicites

Les noms choisis pour désigner les Utilisateurs doivent être explicites.
Un DN de certificat KWA CDS comporte notamment les éléments suivants:

- l'identification de l'entité Organisme Client
- le TransNUM

Le DN est construit à partir des nom, prénom et adresse email extraits des bases informatiques détenues par le Client K.Websign® et collectés lors de l'enregistrement pour inscription de l'Utilisateur à l'Application web du Client K.Websign®

3.1.3 Anonymisation des Utilisateurs

L'utilisation d'un pseudonyme ou d'un identifiant anonyme pour désigner un Utilisateur n'est pas autorisée par la présente Politique de Certification.

3.1.4 Règles d'interprétation des différentes formes de nom

Les principes applicables sont ceux définies par les Clients K.Websign® en leur qualité d'AE.

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 Utilisateur au sein de l'ICP grâce à l'utilisation du numéro unique de transaction, le TransNUM, pour les certificats KWA CDS.

3.1.6 Procédure de règlement des différends au sujet des noms

L'AE est responsable de l'unicité des noms de ses Utilisateurs et de la résolution des litiges portant sur la revendication d'utilisation d'un nom. Les principes applicables sont ceux définies par les Clients K.Websign® en leur qualité d'AE. Tout différend portant sur ce point devra être soumis à l'AA responsable de la présente Politique de Certification.

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

3.2.1 Vérification de l'identité d'un Utilisateur

L'enregistrement d'un Utilisateur pour l'émission du Certificat KWA se fait directement auprès de l'AE.

Les règles de vérification d'identité du Demandeur de Certificat sont laissées à la discrétion de l'AE qui est en charge de la gestion des utilisateurs de ses Applications web.

La procédure d'identification, d'authentification et de validation de la demande d'émission d'un certificat est décrite dans la Politique de Gestion de Preuves, dans le Protocole de consentement utilisé pour chaque Application utilisatrice des Certificats KWA et complétée par l'AE par une procédure propre à son métier.

La méthode d'attribution de cette identité est par conséquent définie par le Client K.Websign® qui enregistre l'ensemble de ses Utilisateurs avec ses données d'identité.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

3.2.2 Méthode de vérification de la possession de la clé privée

Pour les Certificats KWA, la preuve de la possession de la clé privée correspondant au Certificat KWA utilisé pour la signature est apportée par les moyens techniques et organisationnels définis dans le Protocole de consentement utilisé et appliqué dans le cadre du Service K.Websign® lors de la demande de certificat.

3.3 Authentification et validation d'une demande de révocation

Sans objet dans le cadre de la présente Politique de Certification car il n'y a pas de possibilité de révocation des Certificats KWA.

3.4 Authentification d'une demande de renouvellement

Sans objet dans le cadre de la présente Politique de Certification car il n'y a pas de possibilité de renouvellement des Certificats KWA.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

4 EXIGENCES OPERATIONNELLES SUR LE CYCLE DE VIE DES CERTIFICATS

Le présent chapitre précise les pratiques opérationnelles appliquées par l'ICP pour la gestion des Biclés et des Certificats.

4.1 Demande de Certificat

Un certificat KWA CDS ne peut être demandé par le Client K.Websign® en qualité d'AE que pour procéder à la signature par l'Utilisateur de Données métiers signées et présentées par le Client K.Websign®.
Cette opération déclenche une ouverture de session sur la plate-forme K.Websign® qui est authentifiée par l'Application web au moyen du protocole SSL V2.
L'ouverture de cette session entraîne la transmission du formulaire de demande de certificat KWA CDS à l'AC du Service K.Websign® de KEYNECTIS.

4.1.1 Processus de demande d'un Certificat

Suite à la vérification d'identité de l'Utilisateur réalisée l'AE, cette dernière transmet la demande d'émission de certificat à l'Application K.Websign®. Cette demande de certificat contient le TransNUM et l'identité de l'Utilisateur.
L'Application K.Websign® demande au Demandeur de Certificat KWA CDS de fournir des informations précisées dans le cadre d'un Protocole de consentement afin de déclencher:

- la génération d'une bi-clé cryptographique par un logiciel ou bien d'une carte cryptographique ;
- la demande associée de certificat KWA CDS auprès de l'AC en utilisant une requête signée et chiffrée au moyen de Certificats KWS.

4.1.2 Traitement d'une demande de Certificat

Après la vérification réussie par l'AC de l'intégrité et de l'identité du Demandeur, puis des droits de l'AE à demander un Certificat KWA CDS, le Certificat KWA CDS contenant les informations relatives à l'Utilisateur et à l'AE sera émis par l'AC.

L'AC génère et signe un certificat KWA CDS d'une durée de validité de un à cinq minutes contenant les données du DN précisée au § 3.1.2.

4.2 Emission d'un Certificat

4.2.1 Délivrance du Certificat

Compte tenu des modalités de fonctionnement du Service K.Websign®, le Certificat n'est pas publié ni remis à l'Utilisateur.
En cas de rejet de la demande de certificat KWA CDS par l'Application K.Websign®, cette dernière en informe le Demandeur en justifiant le rejet par un code retour qui provoque la destruction de la Bi-clé cryptographique et rétablit la liaison vers l'Application web.

4.2.2 Acceptation du Certificat

L'acceptation du Certificat par l'Utilisateur est tacite car elle est subordonnée à l'utilisation du Certificat KWA CDS pour la signature du document PDF sous forme électronique présenté par le Client K.Websign®.

4.3 Révocation d'un Certificat

Compte tenu de la brève durée de vie d'un certificat KWA CDS, il n'y a pas de fonction de révocation des Certificats.

4.4 Renouvellement d'un Certificat

Compte tenu de la brève durée de vie d'un certificat KWA CDS, il n'y a pas de fonction de renouvellement des Certificats.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

4.5 Suspension et/ou modification d'un Certificat

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

4.6 Fonction d'information sur l'état des Certificats

Une Liste de Certificats Révoqués d'une durée de validité de 7 jours est publiée avec un délai maximum de 24 heures maximum.

4.7 Séquestre et recouvrement de clés

Le séquestre et le recouvrement de clés privées ne sont pas autorisés par la présente Politique de certification.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

5 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 en région parisienne (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 risques, 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.
Le site d'implantation de l'AE est choisi par le client K.Websign®.

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 d'exploitation 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 Politique de Certification.

Les accès au site des composantes d'OC, 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 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'informations supportant les Services de certification électronique (hors AE) 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 et des révocations 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 certificats suite à la 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

Les personnels doivent avoir connaissance et comprendre les implications des opérations dont ils ont la responsabilité.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

Les rôles de confiance sont classés en trois groupes :

- Les personnels d'exploitation, dont la responsabilité est le maintien de l'ICP en conditions opérationnelles ;
- Les personnels d'administration, dont la responsabilité est l'administration technique des composantes de l'ICP ;
- Les personnels de la sécurité, dont la responsabilité est de réaliser les opérations de vérification de la bonne application des mesures et de la cohérence de fonctionnement de la composante d'ICP.

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.

5.2.3 Identification et authentification des rôles

Chaque entité opérant une composante de l'ICP 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 ;
- Eventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu au sein de l'ICP.

Ces contrôles sont décrits dans la DPC de l'AC et de l'AE et sont conformes à la politique de sécurité de la composante. Chaque attribution d'un rôle à un membre du personnel de l'ICP lui 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'ICP 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, il est notamment vérifié que chaque personne n'a pas fait l'objet de condamnation de justice en contradiction avec leurs attributions.
Les personnes ayant un rôle de confiance ne doivent pas souffrir de conflit d'intérêts préjudiciables à l'impartialité de leurs tâches.
Ces vérifications sont menées préalablement à l'affectation 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.
Le personnel a eu connaissance et compris les implications des opérations dont il a 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

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

Des précisions sont fournies dans la DPC.

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.

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 évènements concernant les systèmes liés aux fonctions qu'elle met en œuvre 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 ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements sont également recueillis. Il s'agit des évènements 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 Utilisateurs,...).

En plus de ces exigences de journalisation communes à toutes les composantes et à toutes les fonctions de l'ICP, des évènements 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 ;
- évènements liés aux clés de signature et aux certificats d'AC (génération (cérémonie des clés), sauvegarde / récupération, révocation, renouvellement, destruction,...) ;
- génération des certificats KWA ;
- transmission des certificats aux Utilisateurs et, selon les cas, acceptations / rejets par les Utilisateurs ;
- publication et mise à jour des informations liées à l'AC ;
- génération puis publication des LCR.

Chaque enregistrement d'un évènement 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.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

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'événements

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'événements

Chaque entité opérant une composante de l'ICP 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 et en fonction des résultats de l'analyse de risques de l'AC.

5.4.5 Système de collecte des journaux d'événements

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.

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

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

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

Journaux d'événements
Les journaux d'évènements traités au chapitre 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
Sans objet.

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.

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

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

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 KWA 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).

L'AC KEYNECTIS est attachée à une ICP dont la racine est ADOBE ROOT CA, Les conditions de cessation d'activité de cette dernière qui affecteront l'AC KEYNECTIS KWEBSIGN CDS CA sont décrites dans la politique de certification de la société ADOBE dont l'OID est : 1.2.840.113583.1.2.1, disponible sur l'Url suivante: https://www.adobe.com/misc/pki/cds_cp.html

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.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

6 MESURES DE SECURITE TECHNIQUES ET LOGIQUES

6.1 Génération et installation de bi-clés

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.

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 préalable.

6.1.1.2 Clés de certificat KWA CDS

La génération des clés d'un Certificat KWA CDS est effectuée par l'Application K.Websign®, à l'aide d'un module cryptographique hardware, suite à la saisie d'informations et d'actions définies dans des Protocoles de consentement décrivant les règles de validation de ces informations communiquées par le Client K.Websign®.

6.1.2 Transmission de la clé privée à son propriétaire

La clé privée KWA CDS de l'Utilisateur n'est jamais transmise, elle est détruite immédiatement après son utilisation,

6.1.3 Transmission de la clé publique KWA à l'AC

La clé publique KWA CDS est transmise vers l'AC sous un format PKCS#10.

6.1.4 Taille des clés

La taille des clés de l'Utilisateur est de 2048 bits pour l'algorithme RSA.
La taille des bi-clés d'AC est de 2048 bits pour l'algorithme RSA.

6.1.5 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. Il est certifié EAL4+ selon les critères communs.

6.1.6 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 de la clé privée KWA CDS et du certificat associé est strictement limitée aux usages indiqués dans la présente PC.

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+ selon les critères communs.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

6.2.1.2 Module Utilisateur

Le module cryptographique pour les clés KWA CDS est installé au sein du centre de production sécurisé de KEYNECTIS dont les accès sont restreints. Le module cryptographique pour les clés d'AC est supporté par du matériel dont l'accès est contrôlé.

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 Utilisateurs ne sont séquestrées.

6.2.4 Copie de secours de la clé privée

Les clés privées des Utilisateurs 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.

6.2.5 Archivage de la clé privée

Les clés privées de l'AC et des Utilisateurs 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 de l'Utilisateur KWA CDS

Les clés sont activées une fois uniquement par l'Utilisateur lors de son acceptation à signer les Données métier signées conformément au Protocole de consentement du Client K.Websign®.

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 Utilisateurs sont détruites après leur utilisation dans une signature (Usage Unique).

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 Utilisateurs sont archivées dans le cadre de l'archivage des certificats correspondants.

6.3.2 Durée de vie des bi-clés et des certificats

La durée de vie des bi-clés et des certificats KWA est de 1à 5 minutes.

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 secrets.

6.4.2 Données d'activation correspondant à la clé privée KWA

Le protocole d'activation de la clé du Certificat KWA est choisi par le Client K.Websign®.

6.5 Mesures de sécurité des systèmes informatiques

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

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

- Identification et authentification des personnels de l'OC 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) ;
- Eventuellement, gestion des reprises sur erreur.

Les applications utilisant les services des composantes peuvent requérir des besoins de sécurité complémentaires qui seront alors définies par le Client K.Websign®.
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'ICP.
De plus, les échanges entre composantes au sein de l'ICP 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.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

7 PROFILS DES CERTIFICATS ET DES LISTES DE CERTIFICATS REVOQUES

7.1 Profil des certificats

Les certificats émis par l'AC contiennent les champs primaires et les extensions suivantes :

Certificat de base	**Valeur**
Version	2 (=version 3)
Serial number	Défini par l'outil
Taille de la clé	2048
Durée de validité	**5 minutes**
Issuer DN	CN = KEYNECTIS K.Websign CDS OU = KEYNECTIS for Adobe O = KEYNECTIS C = FR
Subject DN	C=FR O=KWEBSIGN OU= <Nom convivial de l'AE> (Valeur du champ Authority lors de l'appel de TransID associé à un organisme client provenant d'une table de la plateforme) OU=<&TransNUM> La variable TransNUM OU =<Autres informations d'identité> CN=<& Prénom NOM utilisateur> la variable nom prénom E=<& Email utilisateur> la variable email
NotBefore	YYMMDDHHMMSS
NotAfter	YYMMDDHHMMSS (+ 5 minutes)
Public Key Algorithm	sha1WithRSAEncryption (1.2.840.113549.1.1.5)
Parameters	NULL

Extensions standards	**OID**	**Inclure**	**Critique**	**Valeur**
Authority Info Access	(1.3.6.1.5.5.7.1.1)			n/a
Authority Key Identifier	{id-ce 35}	**X**	**FALSE**	
Methods of generate key ID				**Methode 1**
Select AKI Fields				**Key Identifier**
Basic Constraint	{id-ce 19}	**X**	**TRUE**	
CA				**False**
Maximum Path Length				**n/a**
Certificate Policies	{id-ce 32}	**X**	**FALSE**	
policyIdentifiers				1.3.6.1.4.1.22234.2.8.3.1
policyQualifiers				n/a
CPSpointer				n/a
OID				{id-qt-cps] [1.3.6.1.5.5.7.2.1]
value				**URI=** http://www.keynectis.com/PC/
User Notice				n/a
OID				n/a
value				n/a
noticeRef				n/a
organization				n/a
noticeNumbers				n/a

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

explicitText				This certificate has been issued in accordance with the Adobe CDS CPS and KEYNECTIS CDS CPS OID 1.3.6.1.4.1.22234.2.8.3.1
CRL Distribution Points	{id-ce 31}	**X**	**FALSE**	
distributionPoint				**URI=** http://crl.certificat.com/KEYNECTIS/AC_KEYNECTIS_KWA_KWEBSIGN.CDScrl
reasons				n/a
cRLIssuer				n/a
Extended Key Usage	{id-ce 37}			n/a
Issuer Alternative Name	{id-ce 18}			n/a
Subject Alternative Name				
Key Usage	{id-ce 15}	**X**	**TRUE**	
Digital Signature				**Set**
Non Repudiation				**Set**
Key Encipherment				**Clear**
Data Encipherment				**clear**
Key Agreement				**Clear**
Key CertSign				**Clear**
Key CRL Sign				**Clear**
Private Key Usage Period	{id-ce 16}			n/a
Subject Key Identifier	{id-ce 14}	**X**	**FALSE**	
Methods of generating key ID				**Methode 1**
Other Extensions				

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
- **issuer** : nom de l'AC
- **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
- **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.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

Caractéristiques de la CRL :	Périodicité de mise à jour : 24 heures Durée de validité (en jours) : 7 Version de la CRL (v1 ou v2) : v2 Extensions : Numéro de la CRL + AKI URL http de publication : http://crl.certificat.com/KEYNECTIS/AC_KEYNECTIS_KWEBSIGN_CDS.crl URL LDAP de publication : Nom DNS=directory.certplus.com Adresse d'annuaire : CN= AC_KEYNECTIS_KWEBSIGN_CDS O=KEYNECTIS OU= KWEBSIGN_CDS C=FR

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

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 ICP 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 ICP. Le Client K.Websign® procède régulièrement ou en tant que de besoin à des contrôles de conformité de l'ensemble de l'AE

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.
Le contrôle de l'AE sera assigné par KEYNECTIS 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'ICP 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'ICP (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 son rapport. L'AC, en fonction des résultats pour l'AE, en concertation avec le Client K.Websign® décide des actions à mener afin de se remettre en conformité avec le référentiel documentaire applicable et du délai imparti.

8.6 Communication des résultats

Les résultats des audits de conformité sont conservés par l'AC et le Client K.Websign®. Ils sont communiqués par l'AC et le Client K.Websign® aux composantes concernées suite à l'audit.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

9 DISPOSITIONS DE PORTEE GENERALE

9.1 Barèmes des prix

Les dispositions relatives aux conditions financières du Service de certification électronique prévu aux présentes sont prévues dans les documents contractuels conclus entre l'AC et l'AE d'une part et l'AE et les Utilisateurs d'autre part.

9.2 Responsabilité financière

Les dispositions relatives aux assurances du Service de certification électronique prévu aux présentes sont prévues dans les documents contractuels conclus entre l'AC et l'AE d'une part et l'AE et les Utilisateurs d'autre part.

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'ICP 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
- Les clés privées des Utilisateurs
- Les données d'activation associées aux clés privées des Utilisateurs
- Les journaux d'événements des composantes de l'AC et de l'AE
- Les données liées à l'enregistrement de l'Utilisateur 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 à caractère personnel

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.

Les Utilisateurs 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.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

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

L'AC informera les Utilisateurs et les Clients K.Websign® 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.
L'AC informera les Utilisateurs et les Clients K.Websign® 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.
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 les Utilisateurs et les Clients K.Websign®.

9.8.2 Forme de diffusion des avis

Dans les cas de modification soumise à préavis, l'AC avise les Utilisateurs et les Clients K.Websign® 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.

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 d'Utilisateurs ou de Clients K.Websign®, le responsable de la politique de certification 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 à l'adresse URL suivante : www.keynectis.com/PC/. 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,

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

- 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 et l'organisme de qualification, et le cas échéant remédier aux non-conformités qui pourraient être révélées,
- respecter les accords ou documents qui les lient entre elles ou aux Utilisateurs,
- documenter leurs procédures internes de fonctionnement à l'attention de leur personnel respectif ayant à en connaître dans le cadre des fonctions qui lui sont dévolues en qualité de composante de l'ICP,
- 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 qu'elle a émis un certificat pour un Utilisateur donné et que cet Utilisateur 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 Utilisateurs 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 et des Utilisateurs.
Par conséquent, toute AE habilitée par l'AC doit se conformer à l'ensemble des exigences de la présente Politique de Certification, ainsi qu'à des procédures internes qu'elle formalise notamment dans le cadre de la détermination des règles d'identification des Demandeurs de Certificats pour la délivrance des Certificats KWA.
Le Client K.Websign® doit mettre en place des procédures d'identification des Utilisateurs suffisantes lors de la génération du Certificat KWA associé à la Signature et contrôler de manière périodique et régulière les éléments d'identification des Utilisateurs.
L'Autorité d'enregistrement doit veiller à la protection des éléments cryptographiques mis en œuvre pour les besoins du Service K.Websign®.

9.10.3 Utilisateur

L'Utilisateur doit se conformer à toutes les exigences de la présente politique de certification et des procédures internes formalisées et communiquées par l'AC ou par l'AE. L'Utilisateur 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.

L'Utilisateur 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 Applications utilisatrices de certificats

Les 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 KWA 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.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318

9.11 Limite de responsabilité

L'AC n'est tenue qu'à une obligation de moyens pour la mise en œuvre et l'exploitation des Services de certification électronique qu'elle fournit dans le cadre du Service K.Websign®.

L'enregistrement des Demandeurs par le Client K.Websign® pour émission des Certificats KWA par KEYNECTIS dans le cadre du Service K.Websign® est le fait exclusif du Client K.Websign®. Aucune vérification des données d'identification n'est effectuée par KEYNECTIS. En conséquence de quoi KEYNECTIS décline toute responsabilité quant à l'exactitude des données d'identification des Demandeurs de Certificats communiquées par le Client et contenues dans les Certificats.

Pour le cas où la responsabilité de KEYNECTIS serait engagée en qualité d'Autorité de Certification en cas de manquement du Client à l'une de ses obligations au titre d'Autorité d'Enregistrement, le Client se subrogerait à KEYNECTIS pour tout règlement des différends ou toute action judicaire de la part d'un Utilisateur ou d'un tiers.

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 également toute responsabilité à l'égard du choix de l'acte ou du type du contrat proposé par le Client K.Websign pour signature au moyen du Certificat KWA délivré dans le cadre du Service K.Websign®.

L'AC ne pourra en aucun cas être tenue pour responsable des préjudices indirects, ceux-ci n'étant en aucun cas préqualifiés par avance par les présentes.

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.

La responsabilité de l'AC retenue en cas de préjudice subi par une des composantes de l'ICP (AE, Utilisateur, Applications utilisatrices) dans le cadre des présentes est limitée pour chaque période annuelle pour l'ensemble des préjudices subis pour chaque Client K.Websign® et ses Applications y afférentes, au montant précisé dans le contrat conclu avec le Client K.Websign® concerné.

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.

Siège social : 11-13 rue René Jacques • 92131 Issy les Moulineaux Cedex • France • Tél. +33 (0)1 55 64 22 00 • Fax : +33 (0)1 55 64 22 01 • www.keynectis.com
S.A. au capital de 6.986.000 Euros • R.C.S. Nanterre B 478 217 318 • TVA Intra communautaire FR 44 478 217 318