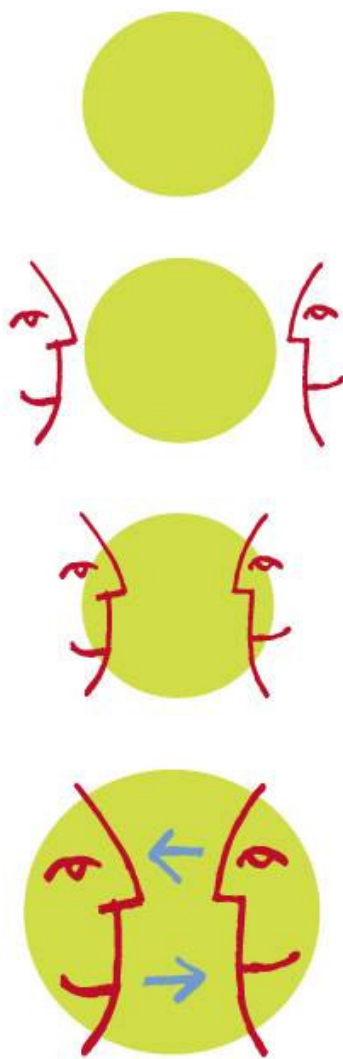


La Politique de Certification KWS Service K.WEBSIGN®



KEYNECTIS

www.keynectis.com

SOMMAIRE

1	QU'EST-CE QU'UNE POLITIQUE DE CERTIFICATION ?	3
2	QUEL EST LE ROLE DE LA POLITIQUE DE CERTIFICATION KWS POUR LE SERVICE K.WEBSIGN® ?	3
3	QUELS SONT LES USAGES ET APPLICATIONS CONCERNES PAR LA POLITIQUE DE CERTIFICATION KWS - « K.WEBSIGN® » ?	4



1 QU'EST-CE QU'UNE POLITIQUE DE CERTIFICATION ?

La mise en œuvre d'un service de certification électronique pour la délivrance et la gestion de certificats électroniques implique la rédaction et la diffusion d'un document dénommé « Politique de Certification » qui a pour objectifs principaux de :

- décrire le contexte général (modalités de demande et de délivrance des certificats électroniques, conditions d'utilisation des certificats électroniques et applications auxquelles les certificats sont destinés) dans lequel s'applique la Politique de Certification ;
- présenter l'entité Autorité de Certification en charge d'émettre les certificats ;
- présenter la communauté de porteurs des certificats électroniques ainsi que les tiers utilisateurs de certificats électroniques ;
- décrire toutes les opérations relatives à la vie d'un certificat, depuis son émission jusqu'à sa fin de vie (expiration ou révocation).

La Politique de Certification est un document public. Il doit pouvoir être consulté par tous, notamment par les porteurs de certificats, et par les personnes destinataires de données qui vont fonder leur confiance sur les certificats à savoir les tiers utilisateurs de certificats.

2 QUEL EST LE ROLE DE LA POLITIQUE DE CERTIFICATION KWS POUR LE SERVICE K.WEBSIGN® ?

La Politique de Certification KWS, ci-après dénommée « PC KWS », de la société KEYNECTIS a pour objet de décrire les procédures mises en place pour l'émission et la gestion des certificats électroniques KWS dans le cadre et pour les besoins du service K.Websign®.

Les certificats électroniques KWS sont délivrés par KEYNECTIS en qualité d'Autorité de Certification aux serveurs web désignés par ses clients (ci-après « Organisme client ») pour les besoins de l'utilisation du service K.Websign®.

Les certificats KWS seront utilisés pour des besoins de chiffrement et de signature électronique de documents sous format XML localement présents sur un site web de l'Organisme client. Ces documents ainsi traités sont ensuite transmis à la plateforme K.Websign® avec un numéro de transaction unique. Les certificats KWS comporteront par conséquent l'identification de l'Organisme client et l'identité du serveur web faisant appel au service K.Websign®.

L'Autorité de Certification KEYNECTIS KWS émet 3 types de certificats KWS :

- Certificat KWS_signature : a pour objet de désigner l'Organisme client lors de l'utilisation de l'application web par ses propres clients, partenaires, fournisseurs ci-après « l'Utilisateur » pour la signature de données électroniques ;
- Certificat KWS_intégrité : a pour objet de garantir l'intégrité du document présenté par l'Organisme client en charge de la gestion de l'application web sur laquelle se connecte l'Utilisateur ;
- Certificat KWS_chiffrement : a pour objet de distribuer des clefs de chiffrement entre l'application de l'Organisme client et la plateforme K.Websign® et ce afin de protéger la confidentialité des données échangées dans le cadre du service K.Websign® pour la constitution du fichier de preuve¹.

¹ Le fichier de preuve désigne l'ensemble des éléments créés lors de la réalisation de la transaction entre l'Organisme Client et l'Utilisateur, puis conservé pendant un délai conforme aux exigences légales ou indiqué par l'Organisme Client, permettant ainsi d'assurer la traçabilité de la réalisation de la transaction conclue conformément au Service K.Websign®.

3 QUELS SONT LES USAGES ET APPLICATIONS CONCERNES PAR LA POLITIQUE DE CERTIFICATION KWS - « K.WEBSIGN® » ?

Il est précisé que l'Organisme client peut utiliser le service K.Websign® pour toutes applications métier ou pour tout type de document sous forme électronique de son choix.

KEYNECTIS intervient lors de la création technique du fichier de preuve associé à la transaction électronique réalisée entre l'Organisme client et l'Utilisateur conformément à la Politique de Gestion de Preuve K.Websign®.

Les certificats KWS_signature et KWS_intégrité comportent l'identification de l'Organisme client et de la machine sur laquelle s'exécute l'application de création des données qui vont être soumises à signature de l'Utilisateur avec l'aide du Certificat KWA. Ces certificats garantissent l'identité de l'Organisme client et l'intégrité du document présenté à l'Utilisateur et soumis à signature si ce dernier y consent.

