Certificat électronique RGS

Edition du 25 avril 2013

1. Généralités

Le SDITEC a fait l'acquisition de certificats électroniques de niveau RGS 2 étoiles (**) et 3 (***) étoiles conformes aux critères définis dans le Référentiel Général de Sécurité (RGS) institué par le décret n°2010-112 du 2 février 2010. Ces certificats sont classés PRIS V2.1.
Ces certificats sont utilisés pour réaliser des opérations d'authentification forte ainsi que des opérations de signature électronique.
Conformément aux exigences du RGS pour des certificats de niveau **et ***, ces derniers sont délivrés sur un support de type clé cryptographique au format USB.
Les certificats peuvent être utilisés dans des environnements Windows XP, Windows Vista et Windows 7, Macintosh Leopard et Snow Leopard avec les navigateurs Internet Explorer 7.0 ou supérieur, Firefox 3.6 ou supérieur et Safari.

2. Présentation des certificats K.SIGN®

La société KEYNECTIS est Tiers de Confiance, éditeur et opérateur de services de confiance et de certification électronique. Keynectis participe activement au développement des moyens de signature électronique, de l'émission de certificats à l' horodatage, la validation de signature ou la gestion de la preuve électronique.
Pour ce faire Keynectis s'appuie sur son infrastructure de haute sécurité certifiée PSCE et sur son IGC Sequoia®certifiée CC EAL4 + sous qualification standard pour l'hébergement et l'opération des services de fourniture certificats électroniques.

K.Sign® est une gamme de certificat sur carte à puce qui se décline sous 3 formats selon le type de certificat supporté. La gestion de ces certificats se faisant à travers l'IGC Sequoia®certifiée CC EAL4 +.

Durée de Vie des Certificats

Les certificats ont une durée de vie **de 3 ans**.
En cas de perte ou de vol ou de besoin de réaffectation un forfait remplacement vous est proposé permettant le remplacement complet pendant les deux premières années d'un certificat émis (Même date de fin de validité)

Supports Physiques des Certificats

Support Gemalto Classic TPC IM CC certifié Critères Communs EAL4+ / PPSSCD, totalement compatible avec le référencement RGS ** et ***.
Les certificats RGS ** et *** sont réalisés après vérification d'informations fournies par le demandeur (Personne Physique ou Morale) et la délivrance se fait par envoi séparé avec face à face conformément à la politique de certification agrée par L'ANSSI

Les livrables K.Sign® for PDF se composent d'un tokens USB (contenant les certificats de personnes prêts à l'emploi). Les opérations de fabrication sont réalisées au sein du Bunker sécurisé de KEYNECTIS

Un droit d'accès au serveur OCSP de KEYNECTIS.

Un droit d'accès au serveur d'horodatage de KEYNECTIS, lors de chaque signature, assujetti à un droit de tirage de jetons d'horodatage par certificat.

Ce support cryptographique contient l'ensemble des certificats d'AC suivants : Certificat KEYNECTIS ROOT CA, KEYNECTIS ICS CA, KEYNECTIS ICS ADVANCED Class 3 CA (signé par l'AC KEYNECTIS ROOT CA), Class 2 Primary CA et le certificat ICS Advanced Class 3 délivré par l'AC Class 2 Primary CA.

- **Environnements supportés pour la signature et l'Authentification**

Ci-dessous une matrice de conformité pour les différents couple OS/Navigateur supportés.

	Windows XP	Windows Vista	Windows 7	Macintosh
IE 6 et +	OUI	OUI	OUI	OUI
Firefox 1.0.6 et +	OUI	OUI	OUI	OUI
Safari	OUI	OUI	OUI	OUI