



PREMIER MINISTRE

Schéma français d'évaluation et de certification de la sécurité des technologies de l'information

En application de la réglementation relative à la signature électronique

CERTIFICAT DE CONFORMITE SSCD-2010/01

Ce certificat est fondé sur le rapport de certification ANSSI-CC 2009/56

DISPOSITIF SÉCURISÉ DE CRÉATION DE SIGNATURE ÉLECTRONIQUE

(fonctions : génération des données de création et de vérification de signature, création de signature)

Ce certificat atteste la conformité de la **Carte à puce Multiapp ID IAS ECC** développée par **Gemalto SA**, aux exigences définies par l'article 3.I du décret n° 2001-272 du 30 mars 2001 modifié pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique.

Paris, le 12 mars 2010

Le directeur général de l'agence nationale de
la sécurité des systèmes d'information
Patrick Pailloux
[ORIGINAL SIGNE]

Conformément au 1° de l'article 3.II du décret n° 2001-272 du 30 mars 2001, ce certificat est émis par l'Agence nationale de la sécurité des systèmes d'information dans les conditions prévues au décret n° 2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et systèmes des technologies de l'information. La procédure de délivrance de ces certificats de conformité fait l'objet du document de procédure SIG-P-01 « Certification de conformité des dispositifs de création de signature électronique », publié sur www.ssi.gouv.fr.

Ce certificat comporte 2 pages.

Références

[1]	Rapport de certification ANSSI-CC 2009/56, publié sur www.ssi.gouv.fr .
[2]	RGS_B_1, Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010, publié sur www.ssi.gouv.fr .

Conditions de validité

Le certificat de conformité de la Carte à puce « Multiapp ID IAS ECC, applet de signature v4.2.7.A chargée sur plate-forme Java Card Multiapp v1.0 avec correctif v1.2 masquée sur microcontrôleur NXP P5CD144 VOB » aux exigences définies par l'article 3.I du décret n° 2001-272 du 30 mars 2001, n'est valable que lorsque ce produit est configuré et utilisé dans les conditions suivantes :

- Les restrictions d'usage spécifiées dans la partie 3.2 du rapport de certification [1] doivent être respectées.
- Les algorithmes cryptographiques mis en œuvre par le dispositif doivent se conformer aux règles indiquées dans le document [2], notamment :
 - la taille du module RSA doit être égale à 2048 bits pour une utilisation jusqu'en 2020 ;
 - la fonction de hachage utilisée doit être le SHA256.
- Les clés RSA utilisées doivent être spécifiques à l'application de création de signature (i.e. typées « digital signature only »).
- Les mécanismes de déblocage de la carte suite à des présentations erronées du PIN de signature peuvent poser un problème concernant le respect de l'exigence de contrôle exclusif par l'utilisateur de son dispositif de signature (cf. la définition d'une signature électronique sécurisée à l'article 1^{er} du décret n° 2001-272). Le déblocage ne devrait être possible que si les conditions de sécurité (environnementales et techniques) concernant la mise en œuvre de cette fonction sont au moins équivalentes à celles existantes lors de l'enregistrement de l'utilisateur auprès de l'autorité d'enregistrement (vérification de l'identité en particulier). En cas de doute (qui pourrait remettre en cause la fiabilité de la signature électronique au sens de l'article 2 du décret n° 2001-272), il est recommandé que cette fonction de déblocage de la carte soit rendue inopérante lors de la personnalisation de la carte.

