



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-2008/01**

Ce certificat est fondé sur le rapport de certification DCSSI 2007/18

#### **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 Morpho-Citiz32, référence MC32/P5CC036V1D/1.0.0, développée par **Sagem Défense Sécurité**, aux exigences définies par l'article 3.1 du décret 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 1<sup>er</sup> février 2008

Le Directeur central de la sécurité des  
systèmes d'information  
Patrick Pailloux  
[ORIGINAL SIGNE]

*Ce certificat est émis conformément au décret 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, publié au journal officiel de la République française le 19 avril 2002. Il est délivré conformément aux règles énoncées dans la procédure SIG-P-01 « Certification de conformité des dispositifs de création de signature électronique », publiée sur [www.ssi.gouv.fr](http://www.ssi.gouv.fr).*

*Ce certificat comporte 2 pages.*

## Références

[1]	Rapport de certification DCSSI 2007/18.
[2]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard – Version 1.10 – Note N°724/SGDN/DCSSI/SDS/Crypto du 13 mars 2006.

## Conditions d'utilisation

La conformité de la Carte Morpho-Citiz32, référence MC32/P5CC036V1D/1.0.0, aux exigences définies par l'article 3.1 du décret 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 n'est valable que lorsque le produit est configuré de manière à respecter les conditions spécifiées dans la partie 3.2 du rapport de certification [1] et les règles suivantes :

- Les algorithmes cryptographiques mis en œuvre par le dispositif doivent se conformer aux recommandations indiquées dans le document [2]. Notamment :
  - la taille du module RSA doit être supérieure ou égale à 1536 bits ;
  - la fonction de hachage utilisée est SHA-2<sup>1</sup>.
- Les clés RSA utilisées doivent être spécifiques à l'application de création de signature (i.e. typées « digital signature only »).
- La carte Morpho-Citiz32 propose une fonction de déblocage du PIN (activable ou non). Cette fonction doit être désactivée afin que, conformément aux exigences relatives à la signature électronique, le dispositif de signature reste sous contrôle exclusif de l'utilisateur.



---

<sup>1</sup> La carte Morpho-Citiz32 propose également la fonction de hachage SHA-1. Au jour de publication de ce certificat, la résistance aux collisions de cette fonction est remise en cause par une attaque théorique. Il existe un risque de mise en œuvre pratique de cette attaque, ce qui compromettrait le mécanisme de signature. La DCSSI déconseille donc l'utilisation de cette fonction.