



PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, 22 MARS 2010
N° 675 /ANSSI/SR/RGL

QUALIFICATION AU NIVEAU RENFORCÉ

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
GEMALTO / NXP SEMICONDUCTORS

Références :

- [1]. Carte à puce « Multiapp ID IAS ECC » masquée sur microcontrôleur NXP P5CD144 VOB - Rapport de certification ANSSI-CC-2009/56 du 17 février 2010.
- [2]. Cotation de mécanismes cryptographiques, projet MISTRAL, n° 2356/SGDN/ANSSI/DR du 22 septembre 2009.
- [3]. Processus de qualification au niveau renforcé, version 1.0 (disponible sur www.ssi.gouv.fr).
- [4]. Carte européenne pour les applications de services électroniques et d'identité électroniques, IAS ECC (Identification Authentification Signature / carte européenne du citoyen), version 1.0.1 du 21 mars 2008.
- [5]. Profil de protection « Secure Signature-Creation Device Type 2 », version 1.04 du 25 juillet 2001.
- [6]. Profil de protection « Secure Signature-Creation Device Type 3 », version 1.05 du 25 juillet 2001.
- [7]. Référentiel Général de Sécurité, version 0.99, et notamment ses annexes [RGS_A_2] (Fonction de sécurité « Authentification », version 2.3 du 11 février 2010) et [RGS_A_3] (fonction de sécurité « Signature », version 2.3 du 11 février 2010).

La carte à puce « Multiapp ID IAS ECC » masquée sur microcontrôleur NXP, destinée à être utilisée dans le cadre de l'administration électronique, répond aux caractéristiques des dispositifs sécurisés de création de signature électronique, dont les fonctionnalités applicatives sont offertes par l'application IAS ECC [4], laquelle couvre les domaines de l'identité, de l'authentification, de la signature électronique et du stockage de données.

Eu égard aux rapports de certification [1] et de cotation cryptographique [2], et conformément au processus de qualification [3], j'atteste que ce produit atteint le niveau de qualification renforcé, sous réserve de l'utilisation de clés d'au moins 2048 bits pour RSA.

La conformité du produit aux profils de protection [5] et [6] ainsi qu'aux spécifications IAS ECC [4] permet d'attester de l'aptitude du produit à satisfaire les exigences du niveau trois étoiles (***) des fonctions de sécurité « Authentification » et « Signature » du RGS [7] pour ce qui concerne respectivement le dispositif d'authentification et le dispositif sécurisé de création de signature, sous réserve que les clés d'authentification et de signature utilisées par l'application IAS ECC ne soient employées que dans des mécanismes respectivement d'authentification et de signature électronique.

Le produit est également déclaré apte à la génération et à la protection de clés du niveau Diffusion Restreinte, ou classifiées au niveau Diffusion Restreinte OTAN ou Restreint UE.

Cette qualification est valable pour une durée de 1 an. Elle pourra être prolongée par la mise sous surveillance du produit certifié.



Patrick PAILLOUX
directeur général