Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

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

Paris, le 11 JAN 2016

N°69 /ANSSI/SDE/PSS/BQA

QUALIFICATION AU NIVEAU RENFORCÉ

Carte VITALE 2 - Application ADELE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.4 avec correctif version 4

MORPHO / ST MICROELECTRONICS

Annexe : Références de la qualification.

Le produit « *Carte VITALE 2 - Application ADELE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.4 avec correctif version 4* » développé par *MORPHO* et *STMICROELECTRONICS* fournit des services de signature électronique : génération, destruction et chargement de bi-clés de signature électronique, création de signature électronique.

Eu égard au rapport de certification [10], à la cotation cryptographique [9] et conformément au processus de qualification [1], j'atteste que ce produit atteint le niveau de qualification renforcé, sous réserve :

- du respect des restrictions d'usage figurant aux chapitres 2.3 et 3.2 des rapports de certification [10] ;
- du respect des condition suivantes concernant le choix et le dimensionnement des mécanismes cryptographiques :
  - la taille des modules RSA doit être d'au moins 2048 bits pour une utilisation jusqu'en 2030 et 3072 bits au-delà ;
  - la taille des courbes elliptiques ECDSA doit être d'au moins 200 bits pour une utilisation jusqu'en 2020 et 256 bits au-delà ;
  - il est recommandé d'utiliser un exposant public strictement supérieur à 2^{16} ;
  - une même clé cryptographique chargée dans la carte à puce ne doit être affectée qu'à un seul usage ;
  - la fonction de hachage SHA-2 doit être utilisée dans les calculs de signature.

La conformité du produit aux profils de protection [4], [5], [6] et [7] 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 [2] 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 ADELE ne soient employées que dans des mécanismes respectivement d'authentification et de signature électronique.

Cette qualification est valable pour une durée de 3 ans. Elle pourra être prolongée par la mise sous surveillance du produit certifié.

Contre-amiral Dominique RIBAN
Directeur général adjoint

Annexe

Références de la qualification

[1]. Processus de qualification au niveau renforcé, version 2.0 (disponible sur www.ssi.gouv.fr).

[2]. Référentiel Général de Sécurité, version 2.0 du 13/06/2014, et notamment ses annexes [RGS_A3] et [RGS_A4] (fonction de sécurité « Authentification » et « Signature », version 3.0 du 27 février 2014).

[3]. Security target for ADELE application, reference : 0000081295, version 09, 02/10/2015.

[4]. Protection Profile - Protection Profile Embedded software for Smart Secure Devices Basic and Extended configurations – Basic configuration, version 1.0, 1er décembre 2009. Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2009_02.

[5]. Protection Profile, Security IC Platform Protection Profile, version 1.0, juin 2007. Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.

[6]. Profil de Protection « Protection Profile – Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001 ». Certifié par le BSI sous la référence BSI-PP-0005-2002.

[7]. Profil de protection « Protection Profile – Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001 ». Certifié par le BSI sous la référence BSIPP-0006-2002.

[8]. Rapport technique d'évaluation : Rapport Technique d'Evaluation/Evaluation Technical Report, référence LETI.CESTI.HYR.RTE.001,version 1.1, 06/10/2015.

[9]. Cotation des mécanismes cryptographiques, référence LETI.CESTI.HYR.RT.01, version 1.0, 02/07/2015.

[10]. Rapport de certification ANSSI-CC-2015/35 du 23/10/2015. « Carte VITALE 2 - Application ADELE : Composant SB23ZL48 masqué par le logiciel SESAM VITALE v1.0.4 avec correctif version 4 ».