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

Bureau Qualifications et agréments

Paris, le 06 DEC. 2017
N° 6124 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT

OBERTHUR TECHNOLOGIES

RCS 340 709 534
420, rue d' Estienne d' Orves
92700 COLOMBES
France

Pièces constitutives de la décision de qualification :

Fiche n°1 : Description du produit

Fiche n°2 : Conditions et restrictions de la qualification.

Fiche n°3 : Base documentaire de la qualification.

Le directeur général de l'Agence nationale de la sécurité des systèmes d'information,

Vu l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives, notamment son article 9 ;

Vu le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n°

2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

Vu le décret n° 2009-834 du 7 juillet 2009 modifié portant création d'un service à compétence nationale dénommé « agence nationale de la sécurité des systèmes d'information », notamment son article 1er ;

Vu le décret du 27 mars 2014 portant nomination du directeur général de l'Agence nationale de la sécurité des systèmes d'information – M. POUPARD (Guillaume) ;

Vu l'arrêté du 13 juin 2017 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques ;

Vu le processus de qualification d'un produit, référence QUAL-PROD-PROCESS, version en vigueur ;

Vu le rapport de certification selon les Critères Communs, référence ANSSI-CC-2013/70, du 14 février 2014 ;

Vu la décision de qualification au niveau renforcé, note n°5258 du 10 décembre 2014 ;

Vu le dossier de demande de qualification fourni par *OBERTHUR TECHNOLOGIES* ;

Vu l'analyse de sécurité fournie par *IDEMIA/OBERTHUR TECHNOLOGIES*,

Décide :

Art. 1 – Le produit fourni par la société *OBERTHUR TECHNOLOGIES* portant le nom « *Carte IAS ECC v1.0.1 : applet version 6179 sur ID-One Cosmo v7.0.1-n R2.0, masquée sur composants NXP P5CC081 et P5CD081, en configuration Standard ou Standard Dual* », respecte les règles fixées par le décret n°2010-112 du 2 février 2010 et est qualifié au niveau standard sous réserve du respect des conditions et restrictions d'utilisation énoncées en fiche n°2.

Art. 2 – Le produit est un dispositif de création de signature et de cachet électronique satisfaisant les exigences du référentiel général de sécurité pour le niveau deux étoiles (**).

Art. 3 – La présente décision est conditionnée au respect par la société *OBERTHUR TECHNOLOGIES* des engagements relatifs au processus de qualification d'un produit, pris par la société au titre de sa demande de qualification.

Art. 4 – La présente décision est valable pour une durée de 3 ans.

Guillaume POUPARD
Directeur général de l'agence nationale
de la sécurité des systèmes d'information

Fiche n°1

Description du produit

Ce produit est développé par la société *OBERTHUR TECHNOLOGIES*. Il offre en particulier les fonctionnalités de création de signature électronique qualifiée et de création de cachet électronique qualifié :

- la génération et l'import de clés de signature et de cachet électronique ;
- la création de signature et de cachet électronique.
- l'initialisation, la gestion et le déblocage du code PIN.

Fiche n°2

Conditions et restrictions de la qualification

Lors de la mise en œuvre du produit, l'autorité d'emploi doit s'assurer que les conditions et restrictions énoncées dans le présente fiche sont respectées.

Conditions

C1. Les restrictions d'usage figurant aux chapitres 2 3 et 3.2 du rapport de certification [4] sont respectées.

C2. Les guides d'installation [6] et [7], d'administration [9] et d'utilisation [10] sont respectés.

C3. Chaque clé cryptographique doit être dédiée à un usage unique (signature, authentification, etc.).

C4. Le module des clés RSA doit avoir une taille d'au moins 2048 bits pour une utilisation ne dépassant pas 2030.

C5. L'exposant public des clés RSA doit être strictement supérieur à 2^{16}.

C6. L'échange de clés Diffie-Hellman dans Z/pZ ne doit pas être utilisé pour des valeurs de p de taille inférieure à 2048 bits ;

C7. L'échange de clés Diffie-Hellman dans le corps des entiers modulo p utilisant des sous-groupes dont l'ordre est multiple d'un nombre premier p ne doit pas être utilisé pour des valeurs de p de taille inférieure à 200 bits.

Restrictions

R1. Le produit n'est plus agréé pour la protection de clés cryptographiques de niveau *Diffusion Restreinte* ou équivalents : *Restreint OTAN/NATO Restricted, Retreint UE/UE Restricted* ou *Diffusion Restreinte EUROCOR.*

R2. La fonction de hachage SHA-1 ne doit pas être utilisée pour les mécanismes de signature.

R3. Le mécanisme d'authentification symétrique basé sur l'algorithme 3DES-CBC doit être utilisé uniquement avec des aléas d'une taille d'au moins 8 octets, et la même clé ne peut effectuer que 2^{27} authentifications au maximum.

R4. L'algorithme de MAC DES-CBC-MAC ne doit pas être utilisé pour calculer plus de 2^{27} MAC avec la même clé.

R5. Le schéma de signature PKCS#1v1.5 pour l'authentification client/serveur n'est pas conforme au référentiel cryptographique de l'ANSSI [1] et ne doit pas être mis en œuvre s'il est utilisé sans hachage pour la signature de données dont la taille atteint ou dépasse un tiers de celle du module.

R6. Le mécanisme RSA-PKCS#1v1.5 pour le déchiffrement de clés symétriques chiffrées à l'aide d'une clé asymétrique n'est pas conforme au référentiel cryptographique de l'ANSSI [1] et ne doit pas être mis en œuvre.

Fiche n°3

Base documentaire de la qualification

Cadre réglementaire

[1]. Référentiel Général de Sécurité, version en vigueur et notamment son annexe « Règles et recommandations concernant la gestion des clés utilisées dans les mécanismes cryptographiques ».

Documents rédigés par l'ANSSI

[2]. Processus de qualification d'un produit, référence QUAL-PROD-PROCESS, version en vigueur.

[3]. Cotation de mécanismes cryptographiques - Qualification EUTERPE, référence : N°722/ANSSI/ACE/LCC, ANSSI.

[4]. Rapport de certification « Carte IAS ECC v1.0.1 : applet version 6179 sur ID-One Cosmo v7.0.1-n R2.0, masquée sur composants NXP P5CC081 et P5CD081, en configuration Standard ou Standard Dual », référence ANSSI-CC-2013/70, du 14 février 2014.

Documents rédigés par le fournisseur de produit

[5]. Euterpe on Terpsichore (NXP) Security target, version 8, référence : FQR : 110 5165, Oberthur Technologies.

[6]. ID-One Cosmo V7.0.1-n R2.0 Pre-Perso Guide, version 2, référence : FQR 110 6407, Oberthur Technologies.

[7]. ID-One Cosmo V7.0.1-n R2.0 Reference Guide, version 2, référence : FQR 110 6408, Oberthur Technologies.

[8]. Euterpe on Terpsichore AGD_PRE, version 7, référence : FQR : 110 5171, Oberthur Technologies.

[9]. Euterpe on Terpsichore AGD_OPE, version 5, référence : FQR : 110 5170, Oberthur Technologies.

Autres

[10]. Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0005-2002T.

[11]. Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. Certifié par le BSI sous la référence BSI-PP-0006-2002T.