PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Le Directeur général

Paris, le 01 FEV. 2021
N° 217 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT AU NIVEAU RENFORCE

Digital Identity on MultiApp v4.0.1 platform
with Filter Set 1.0 - PACE, EAC en version 1.0

THALES DIS

RCS 562 113 530

6 rue de la Verrerie
92190 MEUDON
France

Pièces constitutives de la décision de qualification :

Fiche 1 : Description du produit.

Fiche 2 : Conditions et limites de la qualification.

Fiche 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 la décision du 22 octobre 2014 portant délégation de signature (secrétariat général de la défense et de la sécurité nationale) ;

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

Vu le dossier de demande de qualification d'un produit fourni par la société *THALES DIS*, reçu le 18 septembre 2019,

Décide :

Art. 1er – Le produit fourni par la société *THALES DIS* portant le nom « Digital Identity on MultiApp v4.0.1 platform with Filter Set 1.0 - PACE, EAC » en version 1.0 respecte les règles fixées par le décret n° 2010-112 du 2 février 2010 et est qualifié au niveau renforcé sous réserve du respect des conditions et limites d'utilisation énoncées en fiche 2.

Art. 2 – La présente décision est valable pour une durée de 3 ans.

Art. 3 – Le maintien de cette décision est conditionné au respect des règles relatives au suivi de la qualification établies dans le processus de qualification d'un produit.

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

Fiche 1

Description du produit.

Désignation et versions

Le produit qualifié est la solution « Digital Identity on MultiApp v4.0.1 platform with Filter Set 1.0 - PACE, EAC » en version 1.0 fournie par l'entreprise *THALES DIS* dans la configuration conforme aux profils de protection *« Machine readable travel document with ICAO application Extended Access Control with PACE »*, réf. BSI-CC-PP-0056-V2-2012-MA-02 et *« Machine readable travel document using standard inspection procedure with PACE »*, réf. BSI-CC-PP-0068-V2-2011-MA-01.

Présentation générale

Ce produit implémente les fonctions de document de voyage électronique, conformément aux spécifications de l'organisation de l'aviation civile internationale (OACI)[1] et européenne [CE_MRTD]. Il permet la vérification de l'authenticité du document de voyage et l'identification de son porteur lors du contrôle frontalier à l'aide d'un système d'inspection.

En outre, ce produit étant multi applicatif, il est possible de combiner sur la même puce des applications d'identité électronique offrant un haut niveau de protection des données personnelles et des applications de document de voyage. En particulier ce produit implémente les fonctions nécessaires à la carte nationale d'identité numérique.

Les principaux services de sécurité fournis par le produit sont :

- la protection en intégrité des données du porteur stockées dans la carte : nations ou organisations émettrices, numéro du document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait, autres données optionnelles, données biométriques additionnelles et autres données permettant de gérer la sécurité du document de voyage ;
- le contrôle d'accès aux données du porteur stockées dans la carte ;
- l'authentification du microcontrôleur par le mécanisme « Active Authentication » ou « Chip Authentication » ;
- l'authentification forte (avec validation de la chaîne de certificats) entre le microcontrôleur et le système d'inspection par le mécanisme EAC (« Extended Access Control ») ;
- le mécanisme « Password Authenticated Connection Establishment » (PACE) pour l'authentification entre le microcontrôleur et le système d'inspection, et l'établissement d'un canal sécurisé fort (« Secure Messaging ») ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de « Secure Messaging », des données lues.

[1] Encore appelée ICAO : *International Civil Aviation Organization.*

Fiche 2

Conditions et limites de la qualification.

Conditions

La décision de qualification est valide sous réserve du respect des conditions énoncées ci-après.

C1. Les restrictions d'usage figurant aux chapitres 2.3 et 3.2 des rapports de certification [CERTIF] de l'application « *Digital Identity* » et de la plateforme Multiapp v 4.0.1 [CERT_PF] sont bien respectées, en particulier l'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [CDS].

C2. Les guides d'installation [GUIDE_INSTALL], d'utilisation de l'application « *Digital Identity* » [GUIDE_UTIL] et de la plateforme Multiapp v 4.0.1 [GUIDE_PF] sont mis en œuvre lors du déploiement, de la configuration et de l'utilisation du produit tout le long de son cycle de vie ainsi que le cas échéant pour le développement d'applications complémentaires sur la plateforme.

C3. La dernière version du Byte Code Verifier est utilisée pour vérifier toutes les applications installées sur la plateforme Multiapp v 4.0.1 conformément aux guides [GUIDE_PF].

C4. Les fonctions de hachage SHA-256, SHA-384 et SHA-512 peuvent être utilisées pour les mécanismes de signature.

C5. Le mécanisme de génération de nombres aléatoires basé sur l'AES-128 peut être utilisé.

C6. Le mécanisme de l'AA (« Active Authentication ») utilisant le RSA peut être utilisé :
- si la taille minimale du module et de l'exposant privé RSA est de 2048 bits pour une utilisation jusqu'en 2030 et de 3072 bits pour une utilisation au-delà de 2030 ;
- si l'exposant privé a la même longueur que le module ;
- si la valeur de l'exposant public est supérieure ou égale à $2^{16}+1$;
- si les modules p et q ont la même taille ;
- si la bi-clé de signature est dédiée au mécanisme de l'AA.

C7. Le mécanisme de l'AA utilisant ECDSA peut être utilisé :
- si les courbes utilisées sont conformes au référentiel [RGS] ;
- si la longueur des clés est d'au moins 256 bits ;
- si la bi-clé de signature est dédiée au mécanisme de l'AA.

C8. Le mécanisme de génération de clés asymétriques de type RSA peut être utilisé si la génération de nombres aléatoires basée sur l'AES-128 est employée.

C9. Le mécanisme de génération de clés asymétriques de type « courbes elliptiques » peut être utilisé si la génération de nombres aléatoires basée sur l'AES-128 est employée.

C10. Le CAN (« Card Access Number ») doit avoir une longueur minimum de 3 octets.

C11. Le mécanisme PACE (« Password Authenticated Connection Establishment ») employant l'échange de clés Diffie-Hellman peut être mis en œuvre si la taille minimale du module et de l'exposant privé RSA est de 2048 bits pour une utilisation jusqu'en 2030 et de 3072 bits pour une utilisation au-delà de 2030.

C12. Le mécanisme PACE basé sur les courbes elliptiques sur GF(p) peut être mis en œuvre :
- si les courbes utilisées sont conformes au référentiel [RGS] ;
- si la longueur des clés est d'au moins 256 bits.

C13. Le mécanisme de l'EAC (« Extended Access Control ») utilisant le RSA peut être mis en œuvre :
- si la taille minimale du module et de l'exposant privé RSA est de 2048 bits pour une utilisation jusqu'en 2030 et de 3072 bits pour une utilisation au-delà de 2030 ;
- si l'exposant privé a la même longueur que le module.

C14. Le mécanisme de l'EAC utilisant les courbes elliptiques peut être employé :
- si les courbes utilisées sont conformes au référentiel [RGS] ;

- si la longueur des clés est d'au moins 256 bits.

C15. Le mécanisme de confidentialité du Secure Messaging employant l'AES peut être utilisé.

C16. Le mécanisme d'intégrité du Secure Messaging employant l'AES peut être utilisé à condition que moins de 2^{27} calculs de MACs soient effectués par ce mécanisme pour une clé donnée.

C17. Le protocole SCP03 peut être utilisé pour la phase de personnalisation du produit.

C18. Le mécanisme de dérivation de la clé d'initialisation de PACE pour authentifier le porteur peut être utilisé, à condition que le code PIN soit composé d'au moins 4 chiffres avec un nombre d'essais inférieur ou égal à 3 et que le code PUK ait une entropie de 128 bits.

Limites

L1. Seules les fonctions décrites dans la fiche 1 sont couvertes par la présente décision de qualification.

L2. Les fonctions de hachage SHA-1 et SHA-224 ne doivent pas être utilisées pour les mécanismes de signature.

L3. Le mécanisme PACE utilisant le TDES ne doit pas être mis en œuvre.

L4. Le mécanisme de confidentialité et le mécanisme d'intégrité du Secure Messaging utilisant le TDES ne doivent pas être utilisés.

L5. Les protocoles SCP01 et SCP02 ne doivent pas être utilisés.

Fiche 3

Base documentaire de la qualification

Cadre réglementaire

[PROCESS_QUALIF_PROD]	Processus de qualification d'un produit, note n° 274/ANSSI/SDE du 12 janvier 2017, référence QUAL-PROD-PROCESS, version en vigueur. Disponible sur https://www.ssi.gouv.fr/qualification-processus
[RGS]	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. Disponible sur https://www.legifrance.fr.
[CE_MRTD]	Règlement n° 2252/2004 du Parlement européen et du Conseil du 13 décembre 2004 établissant des normes pour les éléments de sécurité et les éléments biométriques intégrés dans les passeports et les documents de voyage délivrés par les États membres.

Documents rédigés par le centre d'évaluation

[RTE]	Rapport technique d'évaluation, - référence : ROBINC_ETR_v1.1 ; - version : 1.1 ; - en date du 10 novembre 2020.

Documents rédigés par l'Agence nationale de la sécurité des systèmes d'information

[CERTIF]	Rapport de certification : - Digital Identity on MultiApp v4.0.1 platform with Filter Set 1.0 - PACE, EAC (version 1.0), 18/12/2020, ANSSI-CC-2020/49.
[CERT_PF]	Rapport de certification : - MultiApp v4.0.1 with Filter Set 1.0 Java Card Open Platform on M7892 G12 chip, 17/11/2020, ANSSI-CC-2020/42.
[CRYPTO]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, annexée au Référentiel général de sécurité (RGS_B1), disponible sur www.ssi.gouv.fr. - version : 2.03 - en date du : 21 février 2014

Guides d'utilisation et documentations techniques de l'industriel

[GUIDE_PF]	Titre - Rules for applications on Multiapp certified product: qualification level, référence D1484823, version 1.2, janvier 2019, THALES DIS ; - Guidance for secure application development on Multiapp platforms, référence : D1390326, version A01, mars 2018, THALES DIS ; - Verification process of Gemalto non sensitive applet: qualification level, référence D1484874, version 1.0, décembre 2018, THALES DIS ; - Verification process of Third Party non sensitive applet : qualification level, référence D1484875, version 1.2, février 2019, THALES DIS ; - MultiApp V4.0.1 with filter Set 1.0 AGD_PRE document – Javacard Platform, référence D1431347, version 1.1, 14/2/2020, THALES DIS ; - MultiApp V4.0.1 with filter set 1.0 Javacard Platform - AGD_OPE document, référence D1432683, version 1.11, 24/09/2020, THALES DIS ;

	- CNIe – Electronic Personalization Specification and Application Administration Service, reference D1518028, version 1.4, 7/2/2020, THALES DIS ; - MultiApp ID Operating System Application Service – Reference Manual, reference D1519213C, 22/09/2020, THALES DIS.
[GUIDE_INSTALL]	Titre - MultiApp V4.0.1: AGD PRE document - eTravel v2.2 & Digital identity on MultiApp v4.0.1 with filter set 1.0, référence D1433280, version 1.2, 3/4/2020, THALES DIS ; - MultiApp V4.0.1: AGD PRE document - eTravel v2.2 & Digital identity 1.0 on MultiApp v4.0.1 with filter set 1.0, référence D1433279, version 1.2, 5/3/2020, THALES DIS.
[GUIDE_UTIL]	Titre - eTravel v2.2 with Filter 1.0, reference D1516624B, 27/2/2020, THALES DIS.
[CDS]	Cible de sécurité : - Digital Identity on MultiApp v4.0.1 platform with Filter Set 1.0, PACE, EAC Security Target-Public version, référence D1516266_LITE, version 1.4, 24/09/2020, THALES DIS.

Diffusion interne (par messagerie)

ANSSI DIR – SDE/PSS – SDE/DAT – chrono informatique.