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 Qualification et Agrément

Paris, le 12 JUIL. 2017
N° 3420 /ANSSI/SDE

DECISION DE QUALIFICATION D'UN PRODUIT
AU NIVEAU RENFORCE

***eTravel* 2.2**
en configuration EAC sur SAC sur plate-forme *MultiApp* v4.0,
embarqué sur le microcontrôleur M7892 G12
Gemalto / Infineon Technologies

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 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 [**RGS**] ;

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 le rapport de certification [**Certif**] ;

Décide :

Art. 1er – Le produit *eTravel* 2.2 en configuration EAC sur SAC sur plate-forme *MultiApp* v4.0 de *Gemalto*, embarqué sur le microcontrôleur M7892 G12 d'*Infineon Technologies*, respecte les règles fixées par le décret n° 2010-112 du 2 février 2010 ainsi que le processus de qualification d'un produit [***Process-Qualif-Prod***] 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 trois ans**.

Art. 3. – La prolongation de cette décision est conditionnée à la mise sous surveillance du produit certifié.

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

Fiche 1

Description du produit

Désignation et version

Le produit qualifié est le produit *eTravel* 2.2 en configuration EAC ou SAC sur plate-forme *MultiApp* v4.0 de *Gemalto* embarqué sur le microcontrôleur M7892 G12 d'*Infineon Technologies*.

Présentation générale

Le produit qualifié est une carte à puce, en mode contact ou sans contact.

Il 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.

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

Fiche 2

Conditions et limites de la qualification

La décision de qualification est valide sous réserve du respect des conditions énoncées ci-après. Lors de la mise en œuvre du produit, l'autorité d'emploi doit s'assurer que :

C1. les restrictions d'usage figurant aux chapitres 2.3 et 3.2 du rapport de certification [**CERTIF**] soient bien respectées, à savoir :

- lors de la personnalisation, les valeurs « *Security Attributes* » indiquées dans [**UM**] doivent être utilisées afin que les conditions d'accès soient celles recherchées pour une configuration mettant en œuvre les fonctionnalités SAC, AA (optionnel) et EAC ;
- toutes les applications chargées sur ce produit doivent respecter les contraintes de développement de la plateforme (guides [**PLF_BADR**] et [**PLF_SADR**]) selon la sensibilité de l'application considérée ;
- les autorités de vérification doivent appliquer les guides [**PLF_GTO_VAR**] et [**PLF_THIRD_VAR**] ;
- la protection du chargement de toutes les applications sur ce produit doit être activée conformément aux indications de [**PLF_AGD_PRE**].

C2. les guides d'installation, d'administration et utilisateur [**GUIDES**] sont mis en œuvre lors du déploiement, de la configuration et de l'utilisation du produit tout le long de son cycle de vie ;

C3. l'utilisateur du produit s'assure du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [**CDS**] ;

C4. les conditions suivantes relatives au choix et au dimensionnement des mécanismes cryptographiques sont respectées :

- le bit le plus significatif de chaque nombre premier « p » et « n » utilisé pour la génération de clé doit être fixé à 1 ;
- l'algorithme de hachage doit être choisi en relation avec la taille de clés des courbes elliptiques ou de l'algorithme RSA si applicable, comme par exemple, l'usage du SHA-256 avec des clés ECC de 256 bits ;
- les modules utilisés avec les algorithmes *Diffie-Hellman* et RSA doivent être de longueurs au moins égales à 2048 bits, pour une utilisation ne devant pas dépasser 2030, et 3072 bits au-delà. L'ordre des sous-groupes utilisés avec *Diffie-Hellman* doit être multiple d'un nombre premier d'au moins 200 bits et la conformité des paramètres de domaine avec la RFC 2785 doit être utilisée ;
- dans le cas des courbes elliptiques, pour une utilisation ne devant pas dépasser 2020, on emploiera des sous-groupes dont l'ordre est multiple d'un nombre premier d'au moins 200 bits (256 bits au-delà de 2020) ;
- l'algorithme TDES (Triple DES) deux clés est utilisable au plus tard jusqu'en 2020 ; dans le cas de l'utilisation de l'algorithme TDES, la même clé ne peut être utilisée pour chiffrer plus de 2^{27} blocks.

C5. Le mécanisme *Active Authentification* permettant l'authentification du microcontrôleur est activé.

Limite

La décision de qualification ne couvre pas les *applets* **supplémentaires** même lorsque celles-ci respectent les contraintes et exigences de la présente décision.

Fiche 3

Base documentaire de la qualification

Cadre réglementaire

[PROCESS_ QUALIF_PROD]	Processus de qualification d'un produit, version 1.0 du 06 janvier 2017. Disponible sur http://www.ssi.gouv.fr.
[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.
[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 : *SERMA SAFETY & SECURITY*

[RTE]	Rapport technique d'évaluation, *MINORIS MRTD project* - référence : *MINORIS-MRTD_ETR_*v1.1 - version : 1.1 - en date du : 21 février 2017
[CRYPTO_RE]	*Cryptographic Mechanisms Evaluation Report – MINORIS MRTD project* : - référence : *MINORIS-MRTD_ETR_*v1.0 ; - version : 1.0 ; - en date du : 4 août 2016.

Référentiels et standards

[PP_MRTD]	Profil de protection, *Security IC plateform protection profile with augmentation packages :* - version : 1.0 ; - certifié par le *Bundesamt für Sicherheit in der Informationstechnik* (BSI) ; - référence : BSI-PP-0084-2014 ; - en date du : 13 janvier 2014. Profil de protection, *Machine readable travel document using standard inspection procedure with PACE (PACE PP) :* - version : 1.0 ; - certifié par le BSI ; - référence : BSI-CC-PP-0068-v2-2011 ; - en date du : 2 novembre 2011. Profil de protection, *Machine readable travel document with ICAO application "extended access control" with PACE (EAC PP) :* - version: 1.3.1 ; - certifié et maintenu par le BSI ; - référence : BSI-CC-PP-0056-v2-2012-MA-01 ; - en date du : 26 mars 2012.

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

[CERTIF]	Rapport de certification, référence : ANSSI-CC-2017/20, en date du : 13 avril 2017.

Guides d'utilisation et documentations techniques de l'industriel

[CDS]	*MINORIS – MULTIAPP v4 ETRAVEL 2.2 EAC on SAC Security Target :* - référence : D1384181 ; - version : 1.1 ;

- en date du : 2 février 2017.

[GUIDES]

[AGD_PRE]	- *ETRAVEL* EAC 2.2, *Preparative Guide*, référence D1391898, version 1.0 du 7 avril 2016, GEMALTO ;
[UM]	- *ETRAVEL* EAC 2.2, *CC Certified, reference Manual*, réference D1392378A du 1er juillet 2016, *GEMALTO* ;
[PM]	- *Global Dispatcher Personalization Applet User Guide*, référence D1390286A du 26 février 2016, *GEMALTO* ;
[AGD_OPE]	- *ETRAVEL* EAC 2.2 *Operational User Guide*, référence D1391899, version 1.0 du 7 avril 2016, *GEMALTO* ;

[GUIDES_PLF]

[PLF_BADR]	- *Rules for applications on MULTIAPP certified product* ; référence D1390963, version 1.1 de juin 2016, *GEMALTO* ;
[PLF_SADR]	- *Guidance for secure application development on MULTIAPP platforms*, référence D1390326, version A01 de février 2016, *GEMALTO* ;
[PLF_GTO_VA]	- *Verification process of GEMALTO non sensitive applet*, référence D1390670, version A01 de février 2016, *GEMALTO* ;
[PLF_THIRD_VA]	- *Verification process of Third Party non sensitive applet*, référence D1390671, version A01 de février 16, *GEMALTO* ;
[PLF_AGD_PRE]	- *MULTIAPP* V4, *Preparative Guide*, référence D1390316, version 1.1 du 6 juin 2016, *GEMALTO* ;
[PLF_AGD_OPE]	- *MULTIAPP* V4, *Operational User Guide*, référence D1390321,version 1.2 du 15 février 2017, *GEMALTO*.