PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2015/39

Application eTravel EAC v2.1, en configuration EAC et SAC, sur la plateforme ouverte ou fermée MultiApp V3.1 masquée sur le composant P60D144PVA

(Version du patch : 1.3)

Paris, le 28 septembre 2015

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

Guillaume POUPARD
[ORIGINAL SIGNE]

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2015/39

Nom du produit

Application eTravel EAC v2.1, en configuration EAC et SAC, sur la plateforme ouverte ou fermée MultiApp V3.1 masquée sur le composant P60D144PVA

Référence/version du produit

Version de l'application eTravel EAC : 2.1

Version de la plateforme Java Card MultiApp : 3.1 Version du patch : 1.3

Conformité à un profil de protection

BSI-CC-PP-0056-V2, [PP EAC PACE], version 1.3.1

Machine Readable Travel Document with ICAO Application,

BSI-CC-PP-0068-V2, [PP SAC], version 1.0

Machine Readable Travel Document using Standard Inspection Procedure with PACE

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Gemalto

6 rue de la Verrerie,
92197 Meudon cedex, France

NXP Semiconductors

Box 54 02 40,
D-22502 Hambourg, Allemagne

Commanditaire

Gemalto

6 rue de la Verrerie,
92197 Meudon cedex, France

Centre d'évaluation

Serma Technologies

14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL4.

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 modifié. Ce décret indique que :

- L'agence nationale de la sécurité des systèmes d'information élabore les **rapports de certification**. Ces rapports précisent les caractéristiques des objectifs de sécurité proposés. Ils peuvent comporter tout avertissement que ses rédacteurs estiment utile de mentionner pour des raisons de sécurité. Ils sont, au choix des commanditaires, communiqués ou non à des tiers ou rendus publics (article 7).
- Les **certificats** délivrés par le Premier ministre attestent que l'exemplaire des produits ou systèmes soumis à évaluation répond aux caractéristiques de sécurité spécifiées. Ils attestent également que les évaluations ont été conduites conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises (article 8).

Les procédures de certification sont disponibles sur le site Internet www.ssi.gouv.fr.

Table des matières

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce ouverte ou fermée « MultiApp v3.1 », pouvant être en mode contact ou sans contact. Le produit est développé par la société *GEMALTO* et embarqué sur le microcontrôleur P60D144PVA fabriqué par la société *NXP SEMICONDUCTORS.*

Le produit implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (ICAO). Ce produit 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.

La cible d'évaluation est composée :
- des applications natives eTravel EAC et SAC qui réalisent les fonctions de passeport électronique ;
- de la plateforme ouverte ou fermée Java Card MultiApp V3.1. Cette plateforme est certifiée par ailleurs sous la référence [ANSSI-CC-2015/15].

D'autres applications, en dehors du périmètre de cette évaluation, sont embarquées dans la ROM du produit, notamment :
- l'applet IAS Classic v4.2 destinée à faire de la signature électronique ;
- l'application « MOCA Server » v1.0 (application de *Match On Card*).

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels. Ils peuvent être intégrés sous forme de module ou d'inlay. Le produit final peut être un passeport, une carte plastique, etc.

1.2. Description du produit

1.2.1. Introduction

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est strictement conforme aux profils de protection [PP EAC PACE] et [PP SAC].

1.2.2. Identification du produit

Les éléments constitutifs du produit sont identifiés dans la liste de configuration [CONF].

La version certifiée du produit est identifiable par la réponse que donne le produit à la commande *GET DATA* pour le tag '9F 7F'. Les éléments d'identification sont les suivants :

- fabriquant du microcontrôleur : '47 90' (NXP Semiconductors) ;
- type de microcontrôleur : '6A 15' (P60D144PVA) ;
- identification du système d'exploitation : 'D0 02 0C' ;
- configuration certifiée : '00' (pour plateforme fermée) ou '01' (pour la plateforme ouverte) ;
- version du système d'exploitation : '01 03' (version 1.3).

Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le document [App_list] qui liste les applications et les paquetages (*packages)* inclus dans le produit, associés à leurs noms et AID[1].
La commande *GET STATUS* permet à l'utilisateur du produit de vérifier quelles applications et quels *packages* sont installés dans le produit à sa disposition.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- ceux de la plateforme Java Card en configuration ouverte de la carte à puce MultiApp V3.1 certifiée sous la référence [ANSSI-CC-2015/15] (si la plateforme est en configuration ouverte) ;
- 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 ;
- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de *Secure Messaging*, des données lues ;
- la validation de la chaîne de certificats ;
- l'authentification du microcontrôleur par le mécanisme optionnel *Active Authentication* ;
- l'authentification forte entre le microcontrôleur et le système d'inspection par le mécanisme EAC (*Extended Access Control*, en configuration *EAC on SAC*) préalablement à tout accès aux données biométriques.

[1] *Application Identifier.*

1.2.4. Architecture

Le produit est une carte à puce constituée :

- du composant P60D144PVA fabriqué par *NXP SEMICONDUCTORS* ;
- d'un système d'exploitation sous forme d'une plateforme ouverte ou fermée Java Card : MultiApp V3.1 ;
- des applications natives passeport eTravel EAC et SAC (en configuration « EAC *on* SAC ») ;
- de l'applet IAS Classic de signature électronique, en dehors du périmètre de l'évaluation et non fonctionnelle ;
- de l'application « MOCA Server » destinée à faire du *Match On Card*, en dehors du périmètre de l'évaluation et non fonctionnelle.

Les applications déjà chargées dans le produit sont toutes identifiées dans le document [App_list].
Bien que ces applications standards ne soient pas incluses dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [NOTE.10]. En effet, ces applications standards ont été vérifiées conformément aux contraintes de développements d'applications décrites dans le guide [AGD-Dev_Basic].

1.2.5. Cycle de vie

Le produit est proposé avec trois cycles de vie possibles qui sont explicités ci-après.

Pour chacun des cycles de vie, l'évaluation se limite aux étapes 1 à 5 correspondant aux phases 1 et 2, respectivement phase de développement et phase de fabrication.

Cycle de vie n° 1 : Initialisation du module sur le site de Gemalto :

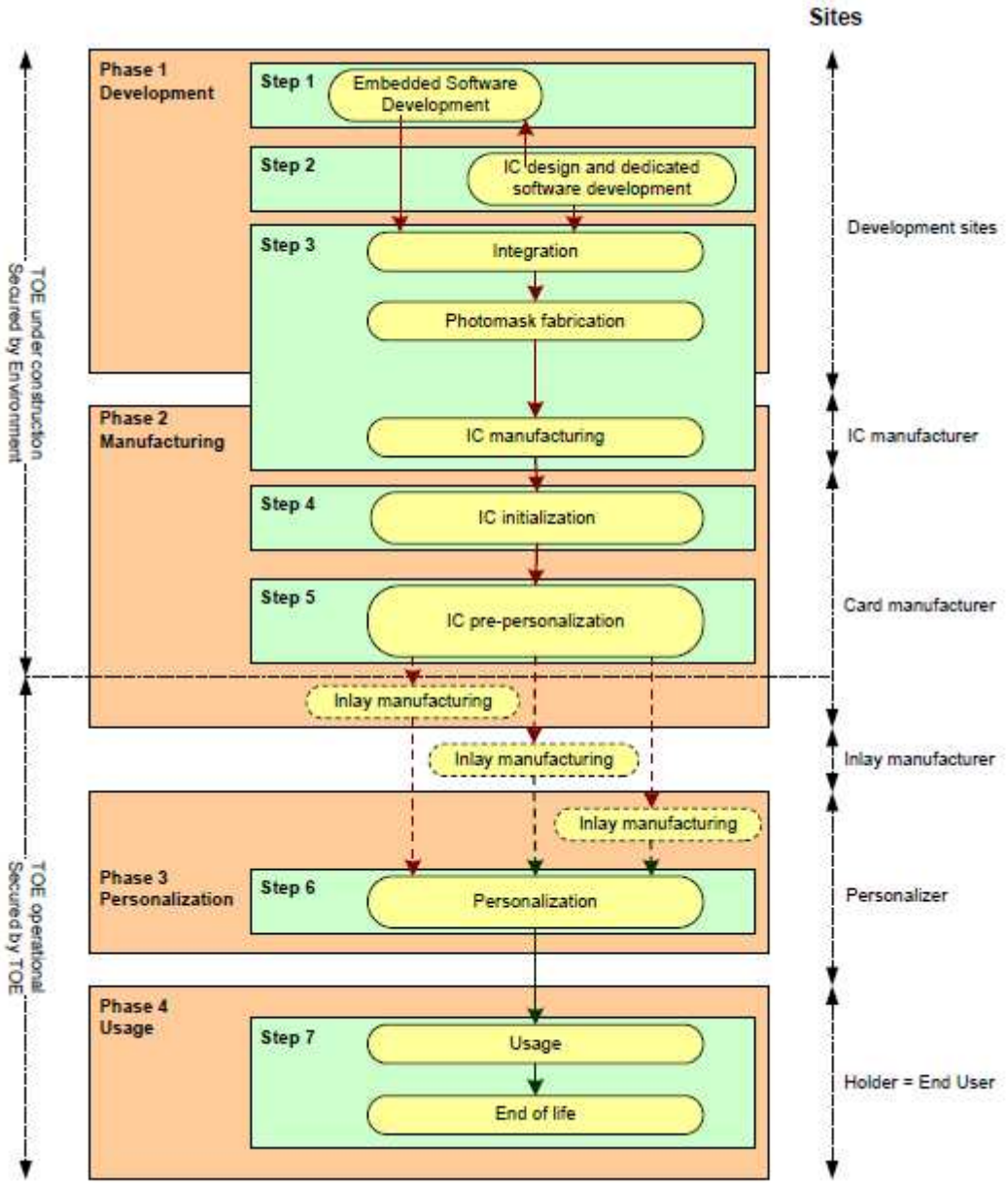

Figure 1 - Cycle de vie n° 1 : Initialisation du module sur le site de Gemalto

Le cycle de vie n° 1 décrit le cycle de vie standard. Le module est fabriqué sur le site du fondeur. Il est ensuite envoyé sur le site de Gemalto où il est initialisé et pré-personnalisé. Puis il est envoyé au personnalisateur, soit directement et dans ce cas le personnalisateur fabrique l'*inlay*, soit après que Gemalto ait fabriqué l'*inlay*, soit après être passé par le fabricant d'*inlays* (autre que Gemalto).

Cycle de vie n° 2 : Initialisation du module sur le site du fondeur :

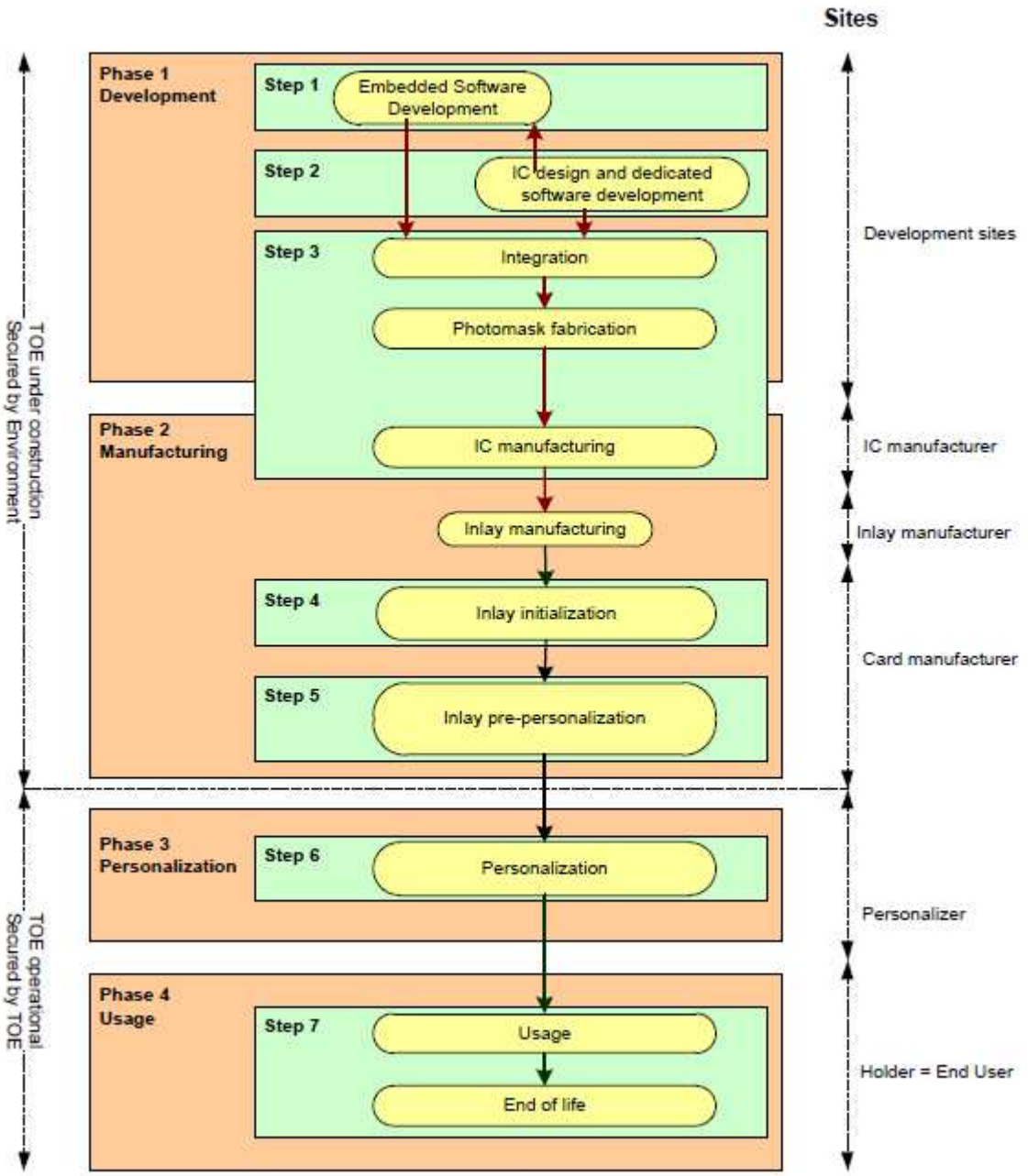

Figure 2 - Cycle de vie n° 2 : Initialisation du module sur le site du fondeur

Le cycle de vie n° 2 correspond au cas où le client souhaite recevoir les *wafers* directement du fondeur. Dans ce cas, l'initialisation et la pré-personnalisation, qui incluent des opérations sensibles telles que le chargement de patchs, sont réalisées sur le site du fondeur.

Cycle de vie n° 3 : Initialisation sur *inlay* sur le site de Gemalto :

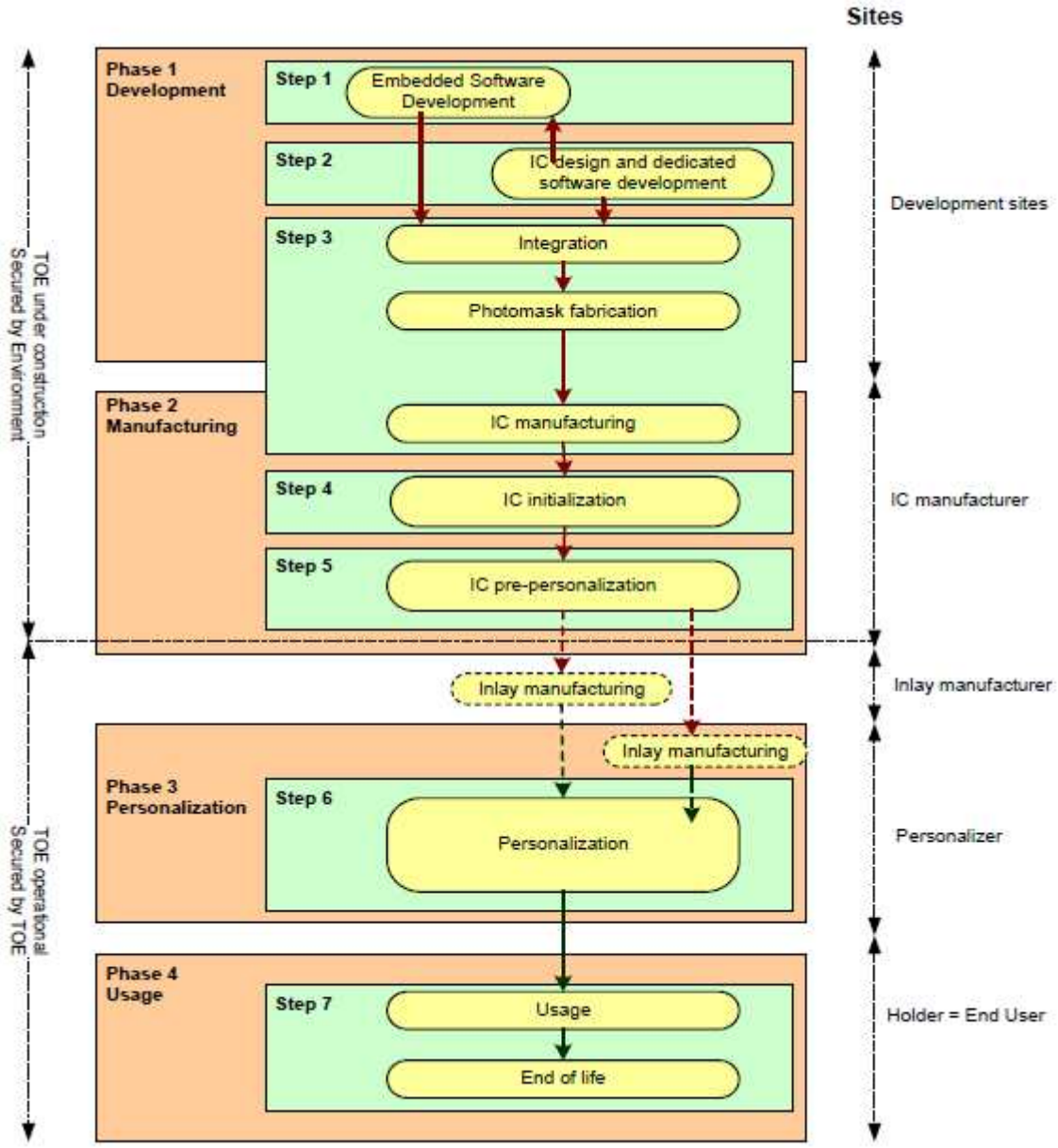

Figure 3 - Cycle de vie n° 3 : Initialisation sur *inlay* sur le site de Gemalto

Le cycle de vie n° 3 correspond au cas où Gemalto souhaite recevoir du fondeur des *inlays* plutôt que des modules. Dans ce cas, le fondeur envoie les *inlays* à Gemalto.

Le produit a été développé sur les sites suivants :

Gemalto

Myllynkivenkuja 4
FI-01620 Vantaa
Finlande

Gemalto

12 Ayer Rajah Crescent
Singapor 139941
Singapour

Gemalto

6 Rue de la Verrerie
92190 Meudon
France

Gemalto

Avenue du Pic de Bertagne
13881 Gémenos
France

Gemalto

Avenue du Jujubier, ZI Athelia IV,
16705 La Ciotat
France

Gemalto

Ul. Skarszewska 2
33-110 Tczew
Pologne

Le microcontrôleur est développé et fabriqué par NXP Semiconductors. Les sites de développement et de fabrication du microcontrôleur sont détaillés dans le rapport de certification dont la référence est [BSI-DSZ-CC-0845-V2-2013].

Les « administrateurs du produit » sont les nations ou organisations émettrices du document de voyage.
Les « utilisateurs du produit » sont les voyageurs et les systèmes d'inspection pendant la phase d'utilisation.

Le guide [AGD-OPE] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.
Par ailleurs, les guides [AGD-Dev_Basic] et [AGD-Dev_Sec] décrivent les règles de développement des applications destinées à être chargées sur cette carte ; le guide [AGD-OPE-VA] décrit les règles de vérification qui doivent être appliquées par l'autorité de vérification.

Pour l'évaluation, l'évaluateur a aussi considéré comme administrateurs du produit le pré-personnalisateur, le personnalisateur et le gestionnaire de la carte chargés de l'administration de la carte, et comme utilisateurs du produit les développeurs des applications à charger sur la plateforme.

1.2.6. Configuration évaluée

Le certificat porte sur l'application eTravel EAC v2.1 (avec mécanisme d'*Active Authentication*), sur la plateforme ouverte ou fermée MultiApp V3.1 masquée sur le composant P60D144PVA, telle que présentée plus haut au paragraphe 1.2.4.

Ce rapport de certification porte sur la configuration incluant les mécanismes suivants :
- *Extended Access Control* ;
- *Supplemental Access Control* ;
- *Active Authentication*.

L'évaluateur a testé la plateforme Java Card masquée sur le composant P60D144PVA.

Le mécanisme PACE d'authentification mutuelle entre la carte et le terminal a été évalué de façon à être utilisable par toute autre application sur la plateforme.

La configuration ouverte du produit a été évaluée conformément à [NOTE.10] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification et réalisé selon les processus audités ne remet pas en cause le présent rapport de certification.
Toutes les applications identifiées dans [App_list] ont été vérifiées conformément aux contraintes décrites dans [AGD-OPE_VA].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC], à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur « P60D144PVA » au niveau EAL6 augmenté des composants ALC_FLR.1 et ASE_TSS.2, conforme au profil de protection [BSI-PP-0035-2007]. Ce microcontrôleur a été certifié le 19 décembre 2013 sous la référence [BSI-DSZ-CC-0845-V2-2013].

L'évaluation s'appuie sur les résultats d'évaluation du produit « Application eTravel EAC v2.1, en configuration EAC et SAC, sur la plateforme ouverte MultiApp V3.1 masquée sur le composant P60D080PVC patch 1.4 » certifié le 12 février 2015 sous la référence [ANSSI-CC-2015/01] et sur les résultats d'évaluation du produit « Plateforme Java Card en configuration ouverte de la carte à puce MultiApp V3.1 masquée sur le composant P60D144PVA patch 1.3 » certifié le 31 août 2015 sous la référence [ANSSI-CC-2015/15].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 6 mai 2015, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée conformément aux référentiels techniques de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] qui atteste que les mécanismes analysés sont conformes aux exigences des

référentiels techniques de l'ANSSI ([REF]) sous réserve de prendre en compte les recommandations se trouvant dans les guides (voir [GUIDES]).

Quoi qu'il en soit, les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI. Ces résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [BSI-DSZ-CC-0845-V2-2013]).

Par ailleurs, comme requis dans le référentiel cryptographique de l'ANSSI ([REF]), la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique.

Les résultats ont été pris en compte dans l'analyse de vulnérabilité indépendante réalisée par l'évaluateur et n'ont pas permis de mettre en évidence de vulnérabilité exploitable pour le niveau AVA_VAN.5 visé.

3. La certification

3.1. Conclusion

L'évaluation a été conduite conformément aux règles et normes en vigueur, avec la compétence et l'impartialité requises pour un centre d'évaluation agréé. L'ensemble des travaux d'évaluation réalisés permet la délivrance d'un certificat conformément au décret 2002-535.

Ce certificat atteste que le produit « Application eTravel EAC v2.1, en configuration EAC et SAC, sur la plateforme ouverte ou fermée MultiApp V3.1 masquée sur le composant P60D144PVA, patch 1.3 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

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 [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doivent respectées les contraintes de développement de la plateforme (guides [AGD-Dev_Basic] et [AGD-Dev_Sec] selon la sensibilité de l'application considérées ;
- les autorités de vérification doivent appliquer le guide [AGD-OPE_VA].

Les recommandations du chapitre « 2.3 Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI » du présent rapport devront également être mises en œuvre.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puces et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CCRA [CC RA].

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[2], des certificats Critères Communs. Pour les évaluations enregistrées avant septembre 2014, la reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.
[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant
ADV Développement	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	Well-structured internals
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	4	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	1	1	1	1	1	1	1	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	1	2	3	4	4	5	5	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	5	Development tools CM coverage
	ALC_DEL		1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - MultiApp V31 Delphes31 : eTravel EAC Security Target, version 1.0, reference D1361392, 23 avril 2015, Gemalto. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite - MultiApp V3.1 eTravel EAC on PACE, référence : D1361392, version 1.0p, avril 2015, Gemalto.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - DELPHES31 Project, référence DELPHES31_ETR_MRTD-144K_v1.0, version 1.0, 6 mai 2015, Serma Technologies.
[ANA-CRY]	Rapport d'analyse des mécanismes cryptographiques : - Cryptographic Mechanisms Evaluation Report DELPHES 31 – MRTD Project, référence : DELPHES31_MRTD_cryptography_v1.0, Version : 1.0, 14 janvier 2014, Serma Technologies.
[CONF]	Liste de configuration du produit : - LIS: Configuration List for MRTD on MPH149, référence : D1362170, version 1.0 du 28 avril 2015, Gemalto. Liste des applications et packages vérifiés [App_list] : - Card Initialisation Specification – MultiApp v3.1 : MPH149 Filter01, référence : D1325691, version 1.8, 26 novembre 2014, Gemalto.
[GUIDES]	Guide d'installation du produit [AGD_PRE] : - Etravel EAC 2.1 – AGD_PRE document, référence : D1297092, version 1.1 du 10 octobre 2014, Gemalto. Guide d'administration du produit [AGD_OPE] : - Etravel EAC 2.1 – Operational User Guide, référence D1297093, version 1.2 du 10 octobre 2014, Gemalto. Guide d'utilisation du produit : - eTravel v2.x EAC –CC Certified – Reference manual, reference : D1280261A du 9 janvier 2015, Gemalto ; - Guide de développement d'applications [AGD-Dev_Basic] : Rules for applications on Multiapp certified product, référence D1280572, version A00 de décembre 2012, Gemalto ; - Guide de développement d'applications sécurisées [AGD-Dev_Sec] : Guidance for secure application development on Multiapp platforms, référence : D1280580, version A00 de décembre 2012, Gemalto ;

	- Guide pour l'autorité de vérification [AGD_OPE_VA] : Verification process of Third Party non sensitive applet loaded in POST-issuance, référence D1322491, version A00 de février 2014, Gemalto.
[PP EAC PACE]	Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control with PACE (EAC PP), version 1.3.1, 22 mars 2012. *Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 26 mars 2012 sous la référence BSI-CC-PP-0056-V2-2012-MA-01.*
[PP SAC]	Protection Profile, Machine Readable Travel Document using Standard Inspection Procedure with PACE, Version 1.0, 2 novembre 2011. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0068-V2-2011*
[BSI-PP-0035-2007]	Security IC Platform Protection Profile, version 1.0, août 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*
[BSI-DSZ-CC-0845-V2-2013]	NXP Secure Smart Card Controller P60x144/080PVA/PVA(Y) with IC Dedicated Software FW5.0 *Certifié par le BSI le 19 décembre 2013 sous la référence BSI-DSZ-CC-0845-V2-2013.*
[ANSSI-CC-2015/01]	Application eTravel EAC v2.1, en configuration EAC et SAC, sur la plateforme ouverte MultiApp V3.1 masquée sur le composant P60D080PVC, patch 1.4. *Certifié par l'ANSSI le 12 février 2015 sous la référence ANSSI-CC-2015/01.*
[ANSSI-CC-2015/15]	Plateforme Java Card en configuration ouverte de la carte à puce MultiApp V3.1 masquée sur le composant P60D144PVA patch 1.3. *Certifié par l'ANSSI le 31 août 2015 sous la référence ANSSI-CC-2015/15.*

Annexe 3. Références liées à la certification

<table>
<tr><td colspan="2">Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.</td></tr>
<tr><td>[CER/P/01]</td><td>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.</td></tr>
<tr><td>[CC]</td><td>Common Criteria for Information Technology Security Evaluation :
Part 1: Introduction and general model,
September 2012, version 3.1, revision 4, ref CCMB-2012-09-001;
Part 2: Security functional components,
September 2012, version 3.1, revision 4, ref CCMB-2012-09-002;
Part 3: Security assurance components,
September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.</td></tr>
<tr><td>[CEM]</td><td>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology,
September 2012, version 3.1, révision 4, ref CCMB-2012-09-004.</td></tr>
<tr><td>[JIWG IC] *</td><td>Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.</td></tr>
<tr><td>[JIWG AP] *</td><td>Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, January 2013.</td></tr>
<tr><td>[COMP] *</td><td>Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.</td></tr>
<tr><td>[NOTE.10]</td><td>« Note d'application - Certification d'applications sur "plateformes ouvertes cloisonnantes" », référence ANSSI-CC-NOTE-10/1.0, voir www.ssi.gouv.fr.</td></tr>
<tr><td>[CC RA]</td><td>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.</td></tr>
<tr><td>[SOG-IS]</td><td>« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.</td></tr>
<tr><td rowspan="2">[REF]</td><td>Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr.</td></tr>
<tr><td>Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.</td></tr>
</table>

	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), voir www.ssi.gouv.fr.

*Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.