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-2016/75

eTravel SAC/EAC/BAC V2.0 with Filter 5.0 on MultiApp V3 - Configuration SAC référence T1033550

Paris, le 14 novembre 2016

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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2016/75

Nom du produit

eTravel SAC/EAC/BAC V2.0 with Filter 5.0 on MultiApp V3 – Configuration SAC

Référence/version du produit

T1033550

Conformité à un profil de protection

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

EAL5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Gemalto

**6 rue de la Verrerie,
92197 Meudon cedex, France**

Infineon Technologies AG

Am Campeon 1-12, 85579 Neubiberg, Allemagne

Commanditaire

Gemalto

**6 rue de la Verrerie,
92197 Meudon cedex, France**

Centre d'évaluation

Serma Safety & Security

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

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL2.

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 « eTravel SAC/EAC/BAC V2.0 with Filter 5.0 on MultiApp V3 - Configuration SAC, référence T1033550 » développé *GEMALTO* et *INFINEON TECHNOLOGIES AG*.

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.

Le 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 au profil de protection [PP EAC PACE].

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 les éléments présents dans la réponse que donne le produit suite à la commande GET DATA pour le tag '9F 7F' appliquée au fichier de données CPLC (voir [GUIDES]) :

- IC FABRICATOR = **40 90** (*INFINEON*) ;
- IC TYPE = **71 64** (SLE78CLX1600P) ;
- OPERATING SYSTEM IDENTIFIER = **D0 01 9D** ;
- CONFIGURATION = **01** (application IAS ECC V4.3.2.A présente dans l'environnement de la TOE) ;
- OPERATING SYSTEM RELEASE LEVEL = **05 00**.

1.2.3. Services de sécurité

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 ;

- la protection, en intégrité et en confidentialité, à l'aide du mécanisme de *Secure Messaging*, des données lues ;
- l'authentification du microcontrôleur par le mécanisme optionnel *Active Authentication* ;
- l'authentification entre le document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme SAC (*Supplemental Access Control*).

1.2.4. Architecture

L'architecture du produit est résumée par la figure ci-dessous :

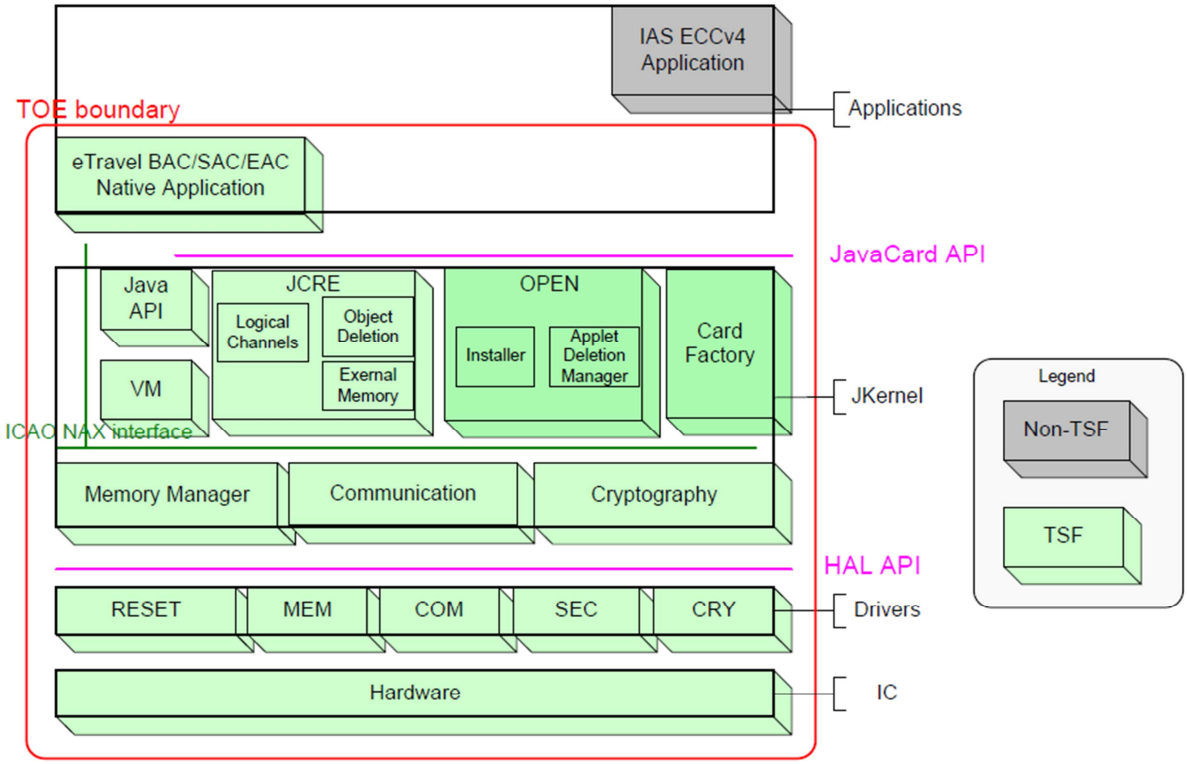

Figure 1 - Architecture et périmètre de la TOE

Le produit est une carte à puce constituée :

- du composant SLE78CLX1600P ;
- de la plateforme ouverte Java Card, en configuration fermée, MultiApp V3 ;
- de l'application native eTravel BAC/SAC/EAC V2 associée au patch v5.0, en configuration SAC (*Supplemental Access Control*) ;
- de l'applet de signature électronique IAS ECC V4.3.2.A, en dehors du périmètre de l'évaluation.

1.2.5. Cycle de vie

Le produit a 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*

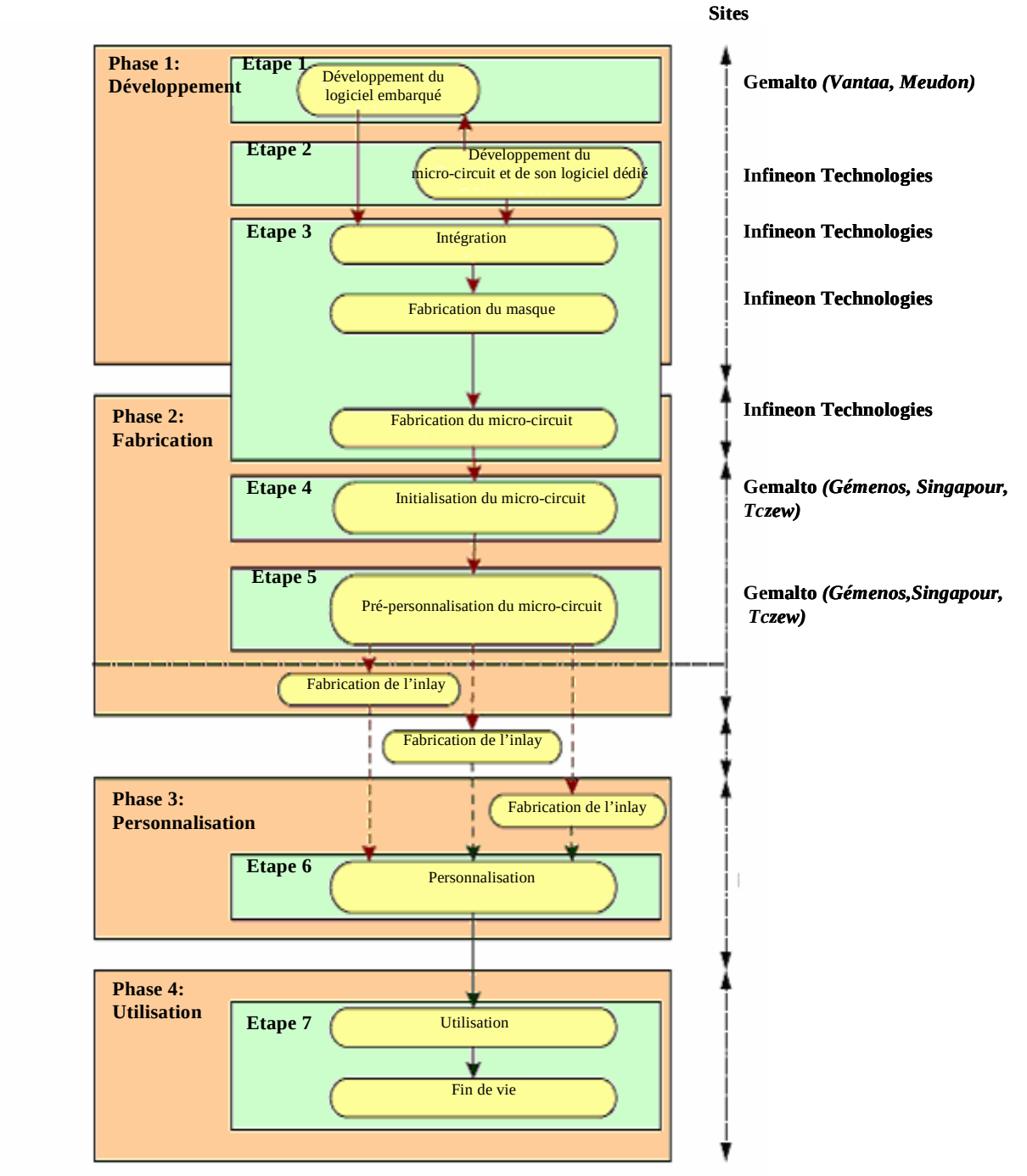

Figure 2 - Cycle de vie n° 1 : Initialisation du module sur le site de *GEMALTO*

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*.

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

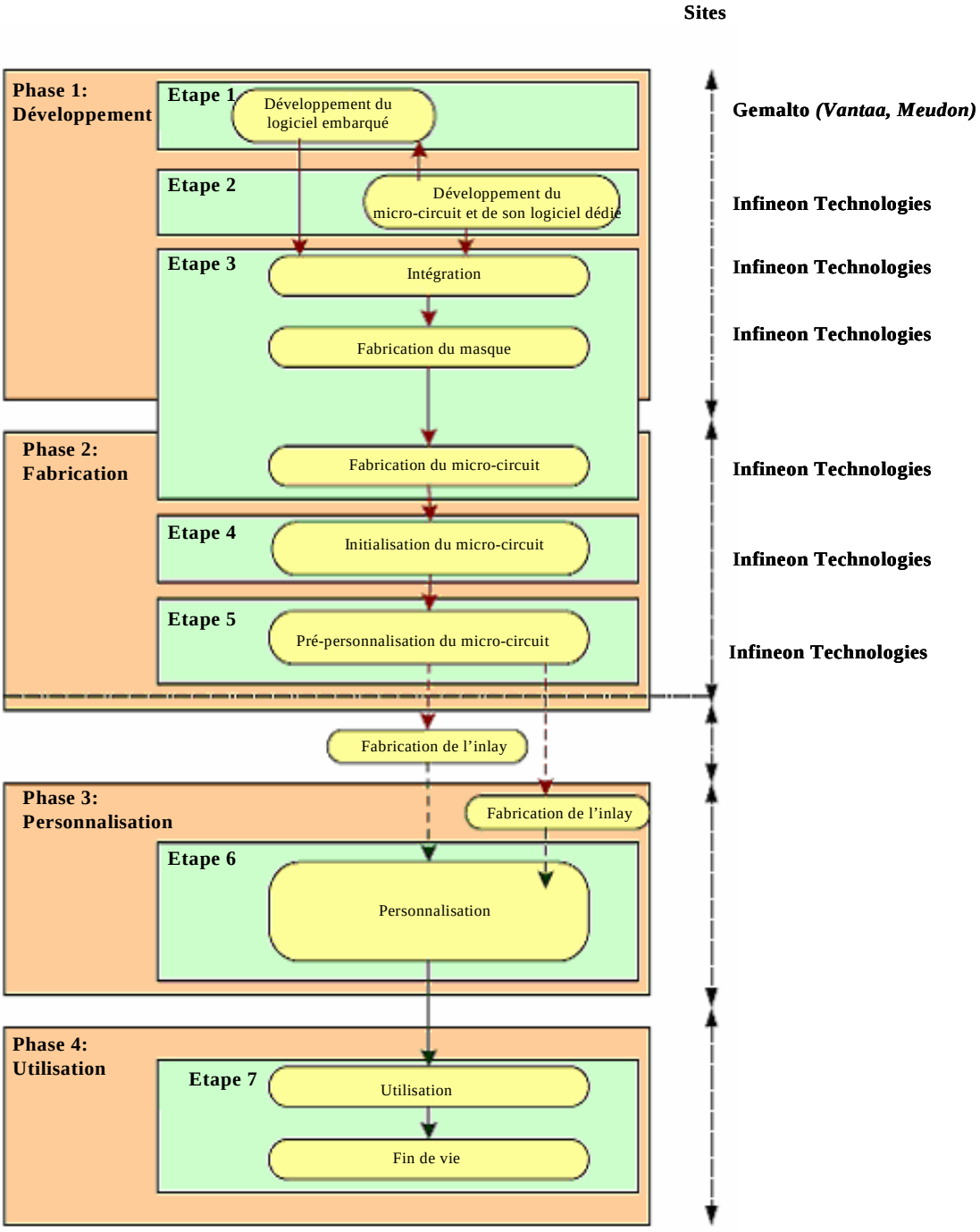

Figure 3 - Cycle de vie n° 2 : Initialisation du module sur le site du fondeur

Le cycle de vie n° 2 est une alternative au cycle de vie n° 1. Il décrit le cycle de vie correspondant 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*

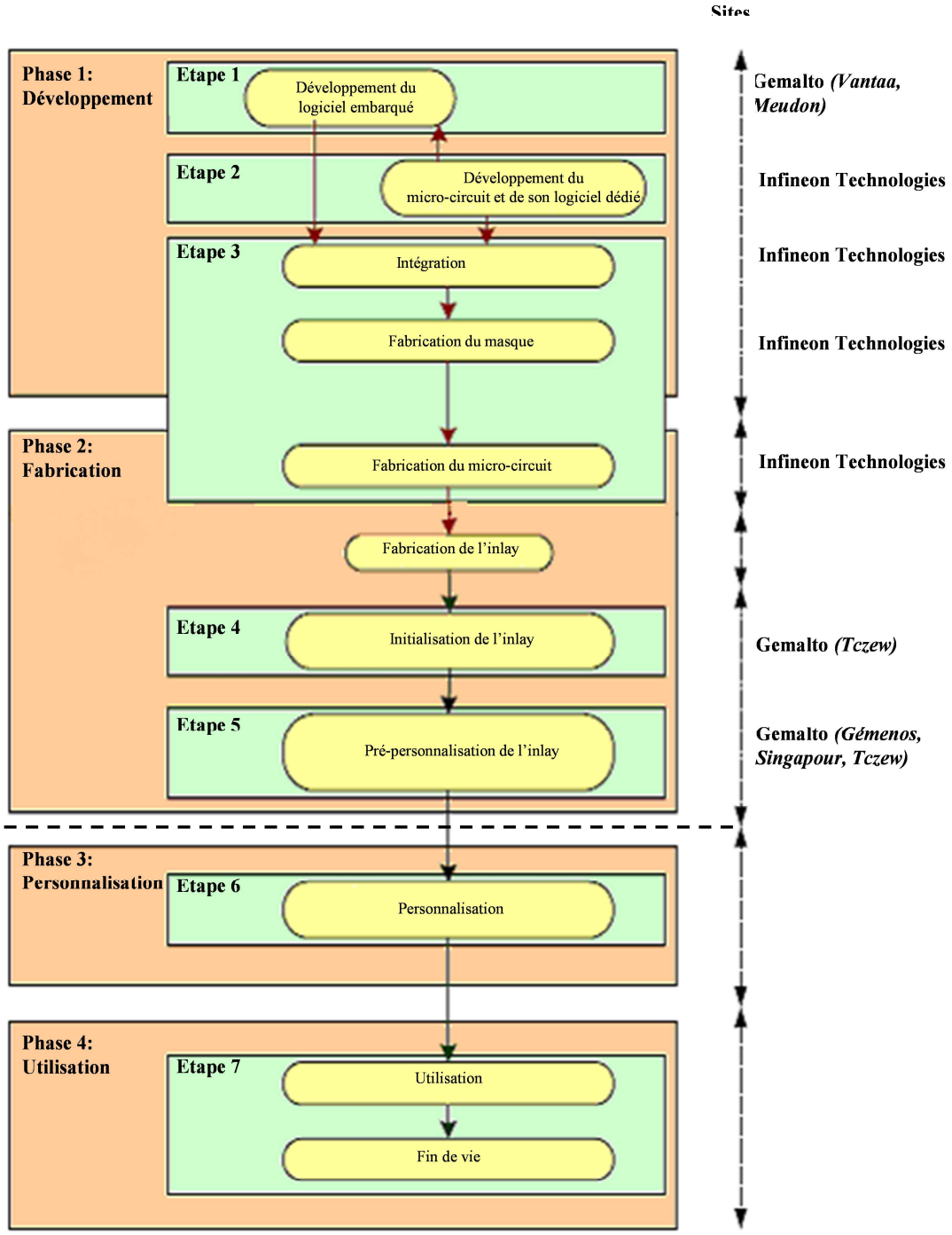

Figure 4 - Cycle de vie n° 3 : Initialisation sur *inlay* sur le site de *GEMALTO*

Le cycle de vie n° 3 est une autre alternative au cycle de vie n° 1. Il décrit le cycle de vie correspondant 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

Ul. Skarszewska 2
33-110 Tczew
Pologne

Le microcontrôleur est développé et fabriqué par *INFINEON TECHNOLOGIES AG*. Les sites de développement, de fabrication, d'initialisation et de pré-personnalisation du microcontrôleur sont détaillés dans le rapport de certification dont la référence est [BSI-DSZ-CC-0829-V2-2015].

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.

1.2.6. Configuration évaluée

Le certificat porte sur l'application eTravel BAC/SAC/EAC v2.0, en configuration SAC (avec mécanisme d'*Active Authentication*), sur la carte à puce MultiApp V3 masquée sur le composant M7820 A11, telle que présentée plus haut au paragraphe 1.2.4.
Ce rapport de certification porte sur la configuration incluant les mécanismes suivants :

- *Supplemental Access Control* ;
- *Active Authentication.*

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [CC], et 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 et validées par l'ANSSI 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.

Le microcontrôleur M7820 A11 a été certifié au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conformément au profil de protection [PP0035], le 3 août 2015, sous la référence [BSI-DSZ-CC-0829-V2-2015].

L'évaluation s'appuie sur les résultats d'évaluation du produit « Application eTravel EAC v2.0, en configuration SAC, sur la carte à puce fermée MultiApp V3 masquée sur le composant M7820 A11 (Version du patch : 5.0) » certifié le 16 septembre 2014 sous la référence [ANSSI-CC-2014/62].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 27 octobre 2016, 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 selon le référentiel technique de l'ANSSI [REF], n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction 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-0829-V2-2015]).

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 « eTravel SAC/EAC/BAC V2.0 with Filter 5.0 on MultiApp V3 - Configuration SAC, référence T1033550 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL5 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].

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 lorsque les dépendances CC sont satisfaites. 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].

[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.

L'accord « Common Criteria Recognition Arrangement » permet la reconnaissance, par les pays signataires[1], des certificats Critères Communs.
La reconnaissance s'applique jusqu'aux composants d'assurance du niveau CC EAL2 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 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, le Qatar, 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 : - « CAPRI: eTravel v2.0 SAC with PACE DH Security Target », référence D1392953,version 1.8. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « eTravel v2.0 SAC with PACE DH - Security Target Lite », référence D1392953,version 1.8p.
[RTE]	Rapport technique d'évaluation : - « Evaluation Technical Report - CAPRI Project », référence CAPRI_ETR_v1.1 version 1.1.
[CONF]	Liste de configuration du produit : - « LIS: Configuration List for MRTD ALONE in xml file (plus cyllene3_DH_Filter51-dev.txt extcrat from MKS) », référence CYLLENE3_DH_Document Delivery Status 2014-06-06_V1.xml, version 06/06/14 ; - « Anomaly List Report », référence R0R21013_007_ALR_Serma, version 7 ; - « MultiApp ID V3.0 Software for FilterV1.xCard Project Configuration Check », référence R0A21013_002_SCK, version 1.4
[GUIDES]	Guide d'installation du produit : - eTravel EAC_Reference_Manual, reference D1280261A, version version du 27 juin 2014.
[PP SAC]	Protection Profile – Machine Readable Travel Document using Standard Inspection Procedure with PACE (PACE PP), version 1.0 du 2 novembre 2011. *Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0068-V2-2011 le 10 novembre 2011.*
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 august 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*
[BSI-DSZ-CC-0829-V2-2015]	Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software. *Certifié par le BSI le 3 août 2015 sous la référence* BSI-DSZ-CC-0829-V2-2015.

[ANSSI-CC-2014/62]	Application eTravel EAC v2.0, en configuration SAC, sur la carte à puce fermée MultiApp V3 masquée sur le composant M7820 A11 (Version du patch : 5.0) *Certifié par l'ANSSI le 16 septembre 2014 sous la référence [ANSSI-CC-2014/61.*

Annexe 3. Références liées à la certification

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.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001; Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.4, août 2015.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
	<Si nécessaire> 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.

	<Si nécessaire> 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.