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-2011/80

Mécanisme SAC de l'application eTravel EAC v1.3 chargée sur la carte à puce MultiApp V2 SAC (PACE) masquée sur le composant SLE66CLX1440PE m2091/a13

Paris, le 7 février 2012

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

Patrick Pailloux
[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-2011/80

Nom du produit

Mécanisme SAC de l'application eTravel EAC v1.3 chargée sur la carte à puce MultiApp V2 SAC (PACE) masquée sur le composant SLE66CLX1440PE m2091/a13

Référence/version du produit

Version du masque : 1.0

Version plateforme Java Card MultiApp : 2.0

Version du patch : 3.0

Conformité à un profil de protection

ANSSI-CC-PP-2010/06, [PP SAC], version 1.00

Protection Profile – Machine Readable Travel Document – SAC (PACE V2) Supplemental Access Control

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeur(s)

Gemalto

6 rue de la Verrerie,
92197 Meudon cedex, France

Infineon Technologies AG

AIM CC SM PS – Am Campeon 1-12,
85579 Neubiberg, Allemagne

Commanditaire

Gemalto

6 rue de la Verrerie,
92197 Meudon cedex, France

Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, 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 « MultiApp v2 SAC (PACE) », pouvant être en mode contact ou dual. Le produit est développé par la société Gemalto et embarqué sur le microcontrôleur SLE66CLX1440PE m2091/a13 fabriqué par la société Infineon Technologies AG.

Le produit évalué est composé :

- de l'application native eTravel EAC v1.3, comportant le mécanisme SAC, qui réalise les fonctions du passeport électronique ;
- de la plateforme ouverte JavaCard MultiApp v2.0, qui permet de charger des applets, durant la phase opérationnelle. Cette plateforme est certifiée par ailleurs sous la référence [ANSSI-CC-2011/10].

Deux autres applications, en dehors du périmètre de cette évaluation, sont embarquées dans la ROM du produit. Il s'agit de l'applet IAS Classic, destinée à faire de la signature électronique, et de l'applet MPCOS qui est une application de fidélité et de porte-monnaie électronique.

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.
Cette cible de sécurité [ST] est strictement conforme au profil de protection [PP SAC].

1.2.1. 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 (cf. [GUIDES]).

La commande GET DATA pour le tag '01 03' donne la réponse '**B0 85 2E 35 11 30 40 90 00 E9 0A 00** 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00', dont les éléments d'identification sont les suivants :

Nom de la famille	Java Card	**B0**
Nom du système d'exploitation	MultiApp ID v2.0	**85**
Numéro du masque	G207	**2E**
Nom du produit	G207 SAC	**35**
Configuration du produit	Configuration certifiée	**11**
Version du patch	version 3.0	**30**
Fabriquant du microcontrôleur	Infineon	**40 90**
Version du microcontrôleur	SLE66CLX1440	**00 E9**
Identifiant du sous-masque	SLE66CLX1440PE (G207A)	**0A 00**

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par ce produit sont :

- fiabilité ;
- contrôle d'accès ;
- mécanisme d'authentification mutuelle ;
- mécanisme de « *secure messaging* ».

Les services de sécurité offerts par les microcontrôleurs sont :

- SEF.1 : contrôle des conditions de fonctionnement ;
- SEF.2 : gestion des phases de vie avec protection du mode de test ;
- SEF.3 : protection contre les écoutes illicites ;
- SEF.4 : chiffrement des données et masquage des données ;
- SEF.5 : génération de nombres aléatoires ;
- SEF.6 : auto-test des fonctions de sécurité du microcontrôleur ;
- SEF.7 : notification en cas d'attaque physique ;
- SEF.8 : unité de gestion de la mémoire ;
- SEF.9 : support cryptographique.

1.2.3. Architecture

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

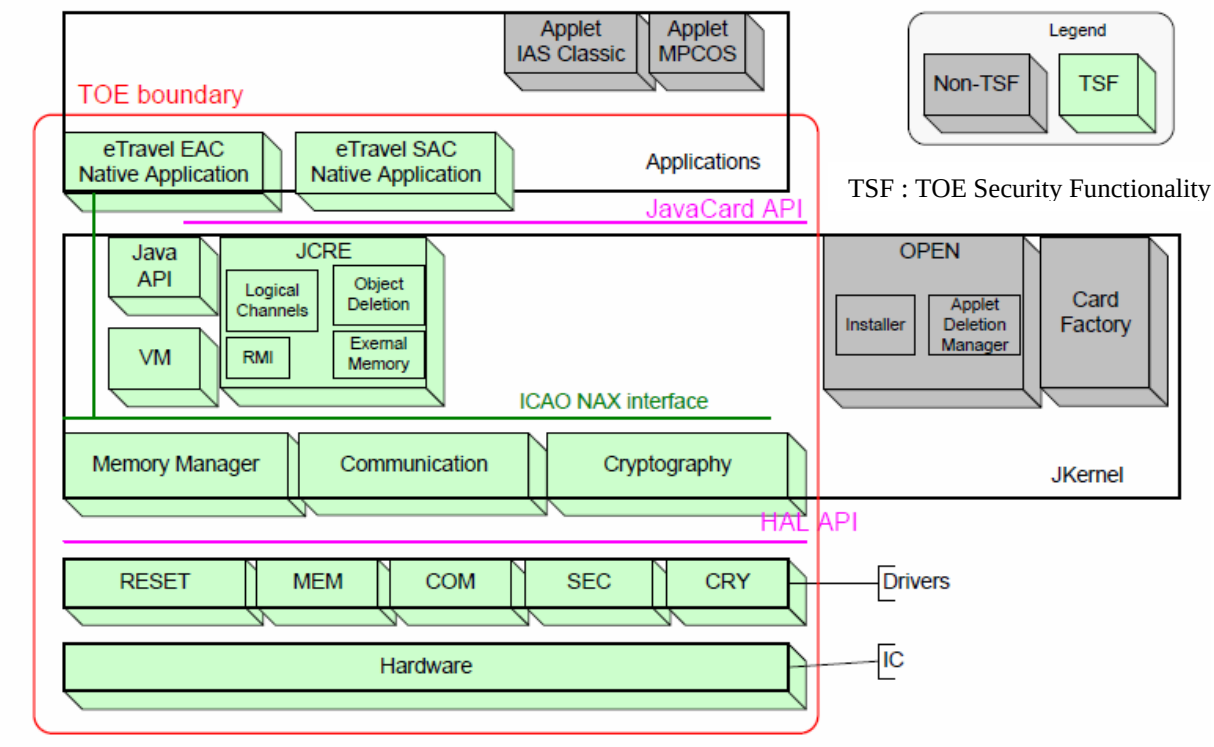

Figure 1 - Architecture et périmètre de la TOE

Le produit est une carte à puce constituée :

- du composant SLE66CLX1440PE m2091/a13 fabriqué par Infineon Technologies ;
- d'un système d'exploitation sous forme d'une plateforme ouverte JavaCard : MultiApp version 2.0 ;
- de l'application native passeport eTravel EAC version 1.3, comportant le mécanisme SAC ;
- de l'applet IAS Classic de signature électronique, en dehors du périmètre de l'évaluation ;
- de l'applet MPCOS (*Multi-application Payment Chip Operating System*), en dehors du périmètre de l'évaluation.

1.2.4. Cycle de vie

Le produit a trois cycles de vie possibles, qui sont explicités ci-dessous.

Pour chacun des cycles de vie, l'évaluation se limite aux étapes allant jusqu'à la fabrication de l'inlay, fabrication non incluse.

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

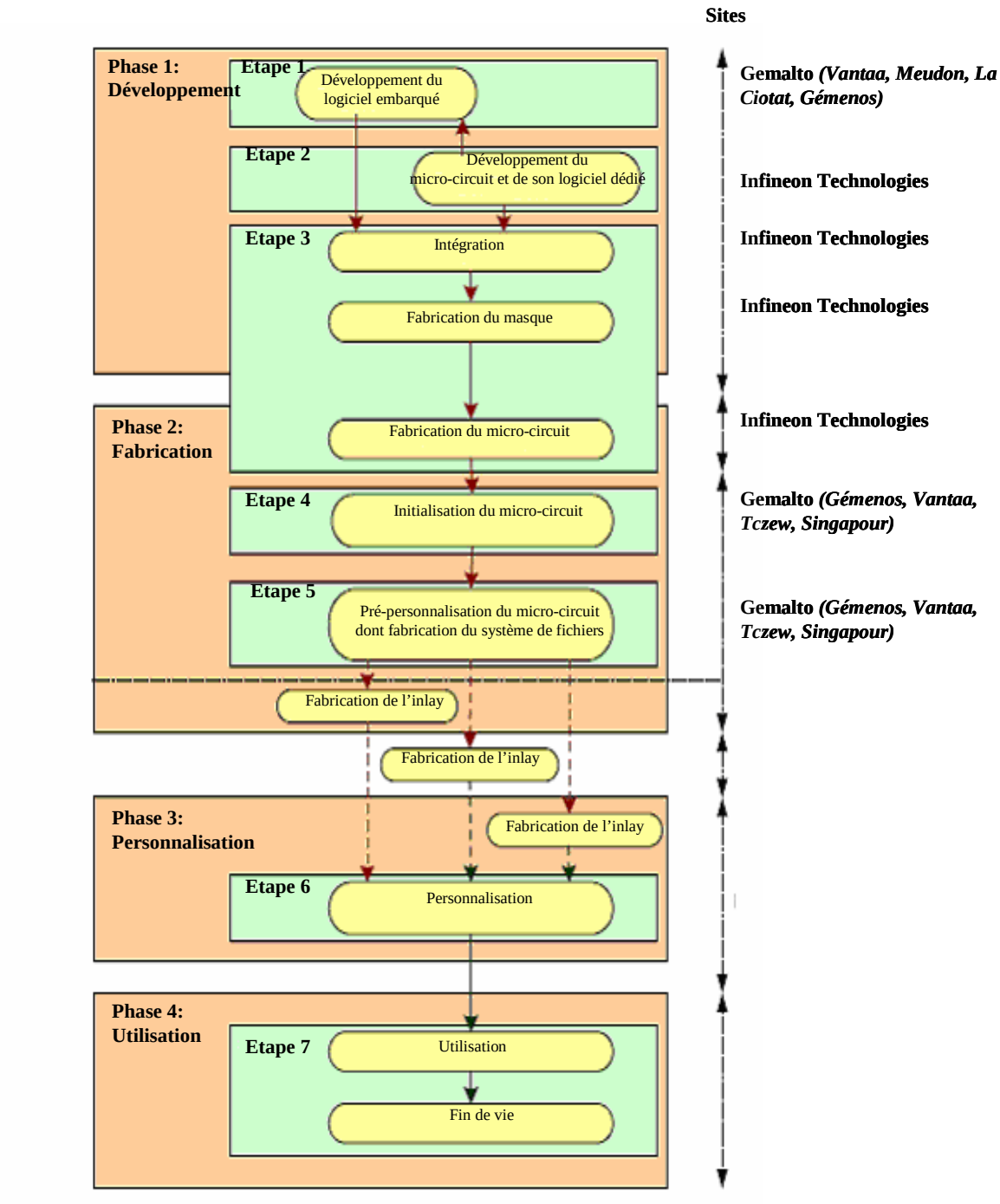

Figure 2 - Cycle de vie n° 1 : Initialisation du module sur le site de Gemalto

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 :

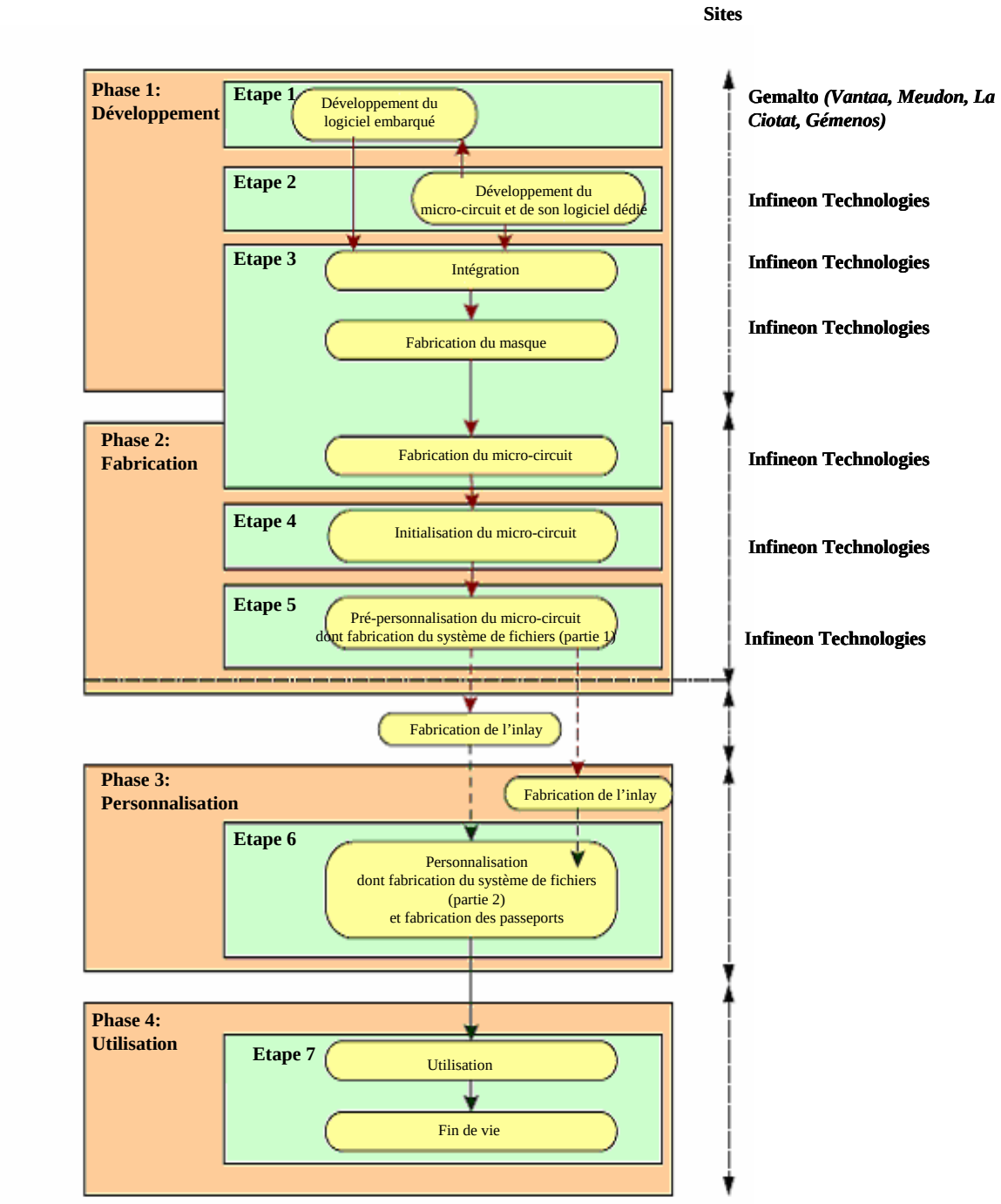

Figure 3 - Cycle de vie n° 2 : Initialisation du module sur le site du fondeur

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. La création des fichiers est initialisée par le fondeur et complétée par le personnalisateur.

Cycle de vie n° 3 : Initialisation sur inlay sur le site du fondeur :

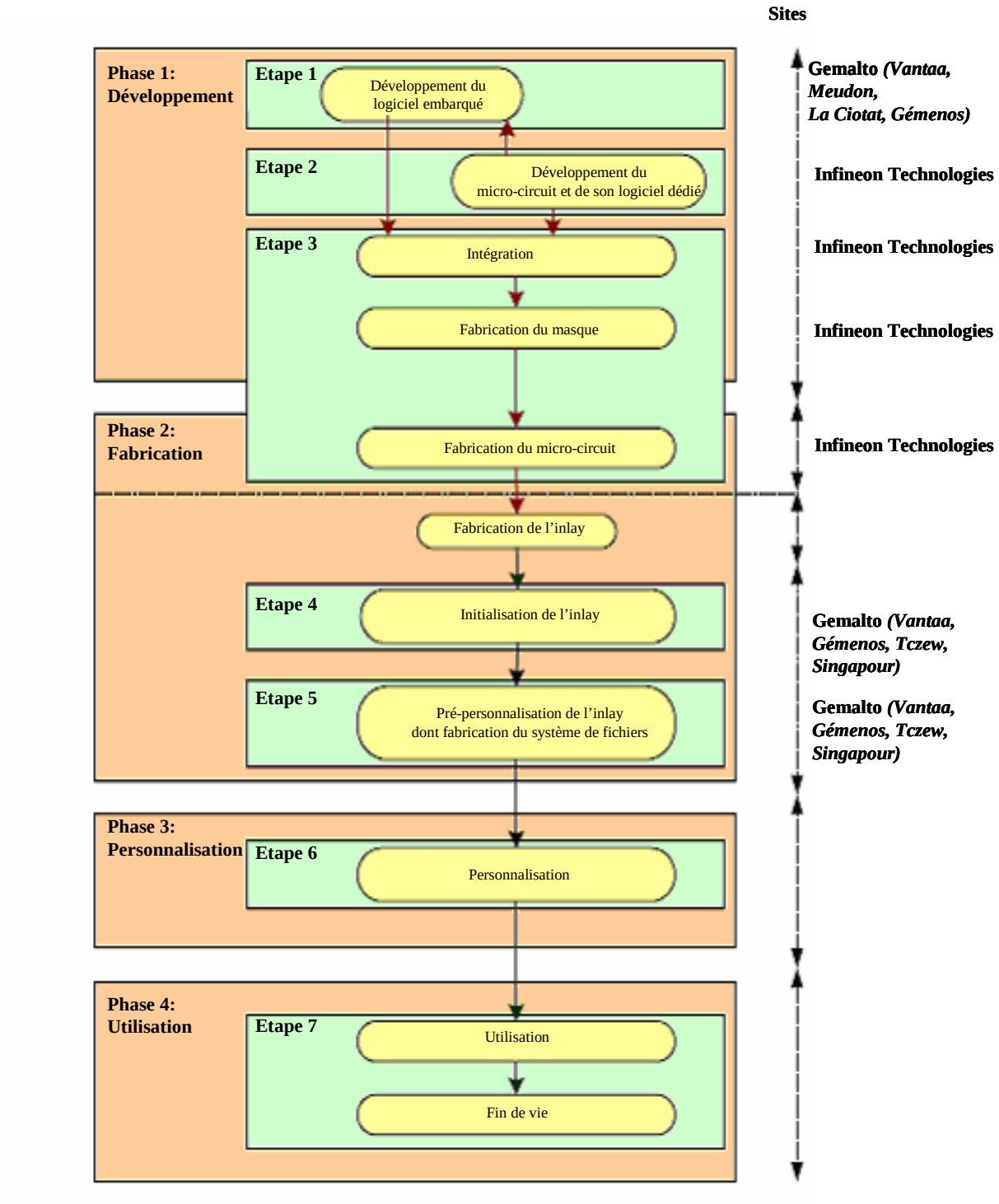

Figure 4 - Cycle de vie n° 3 : Initialisation sur inlay sur le site de Gemalto

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 le module au fabricant d'inlays.

Le produit est développé et fabriqué sur les sites suivants :

Gemalto

Turvalaaksonkaari 2
FI-01741 Vantaa
Finlande

Gemalto

6 Rue de la verrerie
92190 Meudon
France

Gemalto

Avenue du Jujubier
ZI Athelia IV
13705 La Ciotat
France

Gemalto

Avenue du Pic de Bertagne
13881 Gémenos
France

Gemalto

Ul. Skarszewska 2
83-110 Tczew
Pologne

Gemalto

12 Ayer Rajah Crescent
Singapor 139941
Singapour

Le microcontrôleur est développé et fabriqué par Infineon Technologies AG. Les sites de développement et de fabrication du microcontrôleur sont détaillés dans le rapport de certification dont la référence est [BSI-DSZ-CC-0523-2008].

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.

1.2.5. Configuration évaluée

Le certificat porte sur le mécanisme SAC de l'application native eTravel EAC version 1.3 chargée sur la plateforme ouverte JavaCard de la carte à puce MultiApp V2 SAC (PACE) masquée sur le composant SLE66CLX1440PE m2091/a13, telle que présentée plus haut, au paragraphe 1.2.1.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [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 ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués.

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 SLE66CLX1440PE m2091/a12 a été certifié au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conformément au profil de protection [BSI-PP-0002-2001], le 6 novembre 2008, sous la référence [BSI-DSZ-CC-0523-2008].

Le microcontrôleur SLE66CLX1440PE m2091/a13 utilisé dans le cadre de cette évaluation, et dont les différences avec le microcontrôleur certifié sous la référence [BSI-DSZ-CC-0523-2008] n'ont pas d'impact sur la sécurité, a été ré-évalué au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4 et fait l'objet d'un rapport de maintenance daté du 9 juin 2009 référencé [BSI-DSZ-CC-0523-2008-MA-01].

Le microcontrôleur SLE66CLX1440PE m2091/a12 a été ré-évalué et certifié au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conformément au profil de protection [BSI-PP-0002-2001], le 1er octobre 2010, sous la référence [BSI-DSZ-CC-0630-2010].

L'évaluation s'appuie sur les résultats de l'évaluation de la « Plateforme JavaCard en configuration ouverte de la carte à puce MultiApp V2 masquée sur composants de la famille SLE66 » certifiée le 28 avril 2011 sous la référence [ANSSI-CC-2011/10].

L'évaluation s'appuie sur les résultats de l'évaluation de l' « Application eTravel EAC sur carte MultiApp V2 masquée sur composants de la famille SLE66 » certifiée le 3 juin 2011 sous la référence [ANSSI-CC-2011/12].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 17 août 2011, 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 le référentiel technique de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique [REF-CRY] de l'ANSSI 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 visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (cf. [BSI-DSZ-CC-0523-2008] et [BSI-DSZ-CC-0630-2010]).

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 mécanisme SAC de l'application eTravel EAC v1.3 chargée sur la carte à puce MultiApp V2 SAC (PACE) masquée sur le composant SLE66CLX1440PE m2091/a13 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

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. 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.

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[1], des certificats Critères Communs. 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 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 4+	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	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	3	Basic 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	4	Problem tracking configuration management 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	1	Well-defined development tools
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	1	Testing: basic 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 : - MutiApp v2 PACE Cyllene2 : eTravel SAC Security Target Référence : D1191367 Version 1.0 du 21 juin 2011 Gemalto Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - MultiApp v2 Pace – SAC – Common Criteria / ISO 15408 – Security Target – Public version – EAL4+ Référence : ST_D1250513 Version 1.1 du 30 janvier 2012 Gemalto
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – CYLLENE2 Project Référence : CYLLENE2_ETR_MRTD_v1.0 Version 1.0 du 17 août 2011 Serma Technologies
[CONF]	Listes de configuration : - MultiApp V2 Cyllene : ALC Configuration List Référence : D1154123 Version 0.7 du 26 novembre 2010 Gemalto - MultiApp V2 PACE Cyllene2 : ALC Configuration List Référence : D1192591_CL_MultiAppV2Pace_Cyllene2 Version 0.6 du 30 juin 2011 Gemalto
[GUIDES]	Guide d'installation du produit : - MultiApp V2 Pace MRTD Cyllene2 : Preparation procedures Référence : D1191507_PRE_MRTD_MultiAppV2Pace_Cyllene2 Version 0.7 du 28 juin 2011 Gemalto Guide d'initialisation du produit : - Card Initialization Specification for MultiApp ID v2.0 SAC : G207x Generic Products Référence : D1201935 Version 1.4 du 23 juin 2011 Gemalto

	Guide de personnalisation du produit : - ICAO-SAC module (PACE) – Personalization Guide Référence : D1225570 Version du 27 juin 2011 Gemalto Guide d'utilisation du produit : - MultiApp V2 Pace Cyllene2 : Operational User Guide Référence : D1191508_OPE_MRTD_MultiAppV2Pace_Cyllene2 Version 0.7 du 1er juillet 2011 Gemalto
[ANSSI-CC-2011/10]	Plateforme JavaCard en configuration ouverte de la carte à puce MultiApp V2 masquée sur composants de la famille SLE66. *Certifié par l'ANSSI le 28 avril 2011 sous la référence ANSSI-CC-2011/10.*
[ANSSI-CC-2011/12]	Application eTravel EAC sur carte MultiApp V2 masquée sur composants de la famille SLE66. *Certifié par l'ANSSI le 3 juin 2011 sous la référence ANSSI-CC-2011/12.*
[BSI-PP-0002-2001]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001*.
[PP SAC]	Protection Profile - Machine Readable Travel Document – SAC (PACE V2) Supplemental Access Control, version 1.00, 21 Septembre 2010. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/06.*
[BSI-DSZ-CC-0523-2008]	Infineon Smart Card IC (Security Controller) SLE66CLX1600PEM / m1590-a12, SLE66CLX1600PE / m1596-a12, SLE66CLX1600PES / m1597-a12, SLE66CX1600PE / m1598-a12, SLE66CLX1440PEM / m2090-a12, SLE66CLX1440PE / m2091-a12, SLE66CLX1440PES / m2092-a12, SLE66CX1440PE / m2093-a12, SLE66CLX1280PEM / m2094-a12, SLE66CLX1280PE / m2095-a12, SLE66CLX1280PES / m2096-a12, SLE66CX1280PE / m2097-a12, all optional with RSA2048 V1.5 and ECC V1.1 and all with specific IC dedicated software. *Certifié par le BSI le 6 novembre 2008.*

[BSI-DSZ-CC-0630-2010]	Infineon Smart Card IC (Security Controller) SLE66CLX1600PEM / m1590-a12, SLE66CLX1600PE / m1596-a12, SLE66CLX1600PES / m1597-a12, SLE66CX1600PE / m1598-a12, SLE66CLX1440PEM / m2090-a12, SLE66CLX1440PE / m2091-a12, SLE66CLX1440PES / m2092-a12, SLE66CX1440PE / m2093-a12, SLE66CLX1280PEM / m2094-a12, SLE66CLX1280PE / m2095-a12, SLE66CLX1280PES / m2096-a12, SLE66CX1280PE / m2097-a12, all optional with RSA V1.6 and EC V1.1 and SHA-2 V1.0 and all with specific IC dedicated software. *Certifié par le BSI le 1er octobre 2010.*
[BSI-DSZ-CC-0523-2008-MA-01]	Infineon Smart Card IC (Security Controller) SLE66CLX1600PEM / m1590-a13, SLE66CLX1600PE / m1596-a13, SLE66CLX1600PES / m1597-a13, SLE66CX1600PE / m1598-a13, SLE66CLX1440PEM / m2090-a13, SLE66CLX1440PE / m2091-a13, SLE66CLX1440PES / m2092-a13, SLE66CX1440PE / m2093-a13, SLE66CLX1280PEM / m2094-a13, SLE66CLX1280PE / m2095-a13, SLE66CLX1280PES / m2096-a13, SLE66CX1280PE / m2097-a13, all optional with RSA2048 V1.5 and ECC V1.1 and all with specific IC dedicated software. *Maintenu par le BSI le 9 juin 2009.*

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, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2009-03-001 version 2.7 revision 1, March 2009.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.
[REF-CRY]	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, voir www.ssi.gouv.fr