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

Rapport de certification ANSSI-CC-2010/06

Produit eTravel EAC v1.0 (version 01.03) sur composant SLE66CLX800PE

Paris, le 24 mars 2010

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

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-2010/06

Nom du produit

Produit eTravel EAC v1.0 (version 01.03) sur composant SLE66CLX800PE

Référence/version du produit

T1002880 avec *softmask* S1040453 révision B2

Conformité à un profil de protection

BSI-PP-0017-2005 [PP BAC]

Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Basic Access Control

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 4 augmenté

ADV_IMP.2, ALC_DVS.2

Développeur(s)

Gemalto SA

6 rue de la verrerie, 92197 Meudon, France

Infineon Technologies AG

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

Commanditaire

Gemalto SA

6 rue de la verrerie, 92197 Meudon, France

Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 75, mél : e.francois@serma.com

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, publié au Journal officiel de la République française. 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

L'évaluation porte sur l'application e-passport en configuration BAC (*Basic Access Control*) du produit « eTravel EAC v1.0 (version 01 03) » développée par la société Gemalto et embarquée sur le microcontrôleur SLE66CLX800PE fabriqué par la société Infineon Technologies AG.

Le produit est une carte à puce sans contact comportant un logiciel destiné à vérifier l'authenticité du document de voyage et à identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection, et permettant, conformément aux spécifications de l'Organisation de l'Aviation Civile Internationale (OACI) :

- de protéger en intégrité les données stockées du porteur du document de voyage : nation ou organisation émettrice, numéro de document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, photo du visage du porteur, données d'information optionnelles, données biométriques complémentaires du porteur et diverses données permettant de gérer la sécurité du document ;
- d'authentifier le porteur du document de voyage et le système d'inspection (terminal de lecture des documents de voyage), préalablement à tout contrôle aux frontières, à l'aide du mécanisme *Basic Access Control* (ou BAC) ;
- de protéger en intégrité et en confidentialité les données lues à l'aide du mécanisme *secure messaging* ;
- de vérifier l'authenticité de la puce à l'aide du mécanisme *Active Authentication* si celui-ci a été activé en phase de pré-personnalisation à la demande du client.

Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels, de cartes plastiques, etc. Ils peuvent être intégrés sous forme de module, d'inlay ou de datapage.

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 est conforme au profil de protection [PP BAC].

1.2.1. Identification du produit

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

La version certifiée de ce produit est constituée des éléments suivants :

Eléments de configuration		**Origine**
Nom commercial	eTravel v1.0	Gemalto
Référence de la TOE (label interne)	T1002880 avec softmask S1040453 révision B2	Gemalto
Référence de la TOE (label de l'IC)	SLE66CLX800PE	Infineon Technologies
Référence du système d'exploitation	1.0	Gemalto
Référence du softmask	SM 0103	Gemalto
Identification de l'IC	SLE66CLX800PE m1581 e13/a14	Infineon Technologies

Ces éléments sont identifiables à l'aide de la commande « GET DATA » comme indiqué dans le guide d'administration (cf. [GUIDES]) :

- IC FABRICATOR = **40 90** (Infineon)
- IC TYPE = **68 00** (SLE66CLX800PE)
- OPERATING SYSTEM RELEASE LEVEL = **01 03**

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 le microcontrôleur sont :
- contrôle des conditions de fonctionnement ;
- gestion des phases de vie avec protection du mode de test ;
- protection contre les écoutes illicites ;
- chiffrement des données et masquage des données ;
- génération de nombres aléatoires ;
- auto-test des fonctions de sécurité du microcontrôleur ;
- notification en cas d'attaque physique ;
- unité de gestion de la mémoire ;
- support cryptographique.

1.2.3. Architecture

Le produit est constitué du microcontrôleur, du logiciel embarqué comprenant les tests et la gestion des commandes et des données, et de la structure logique des données.

La figure suivante résume l'architecture du produit évalué :

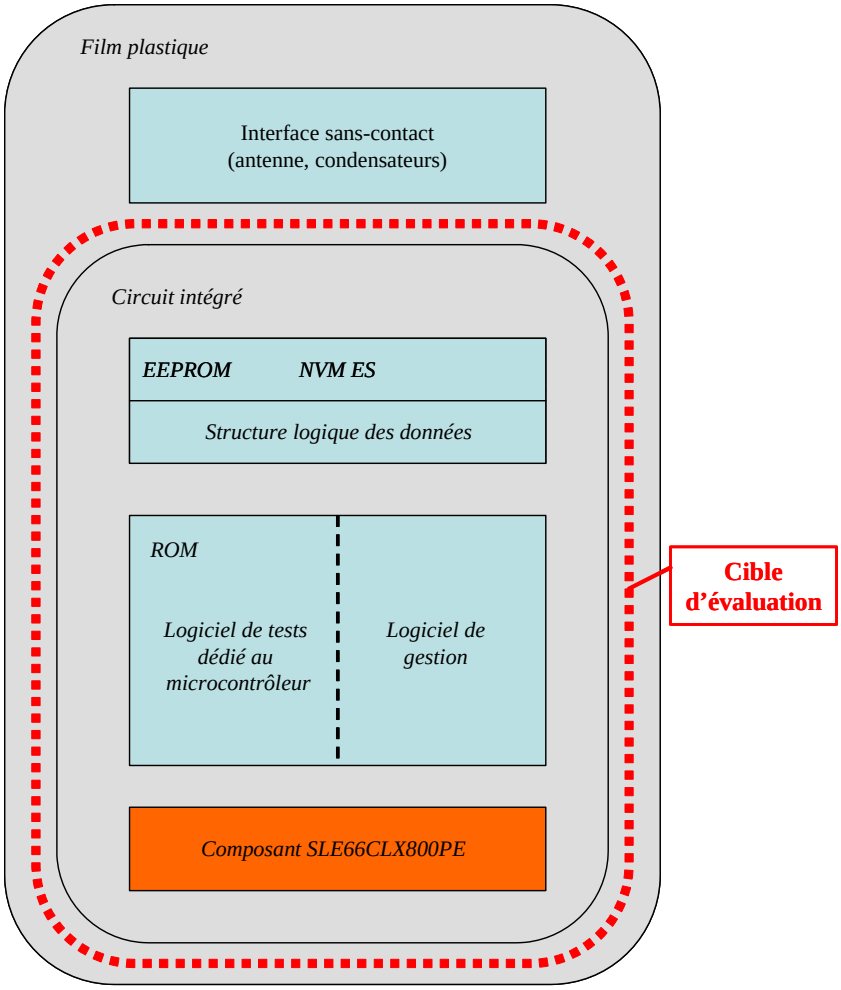

Figure 1 - Architecture du produit

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.

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

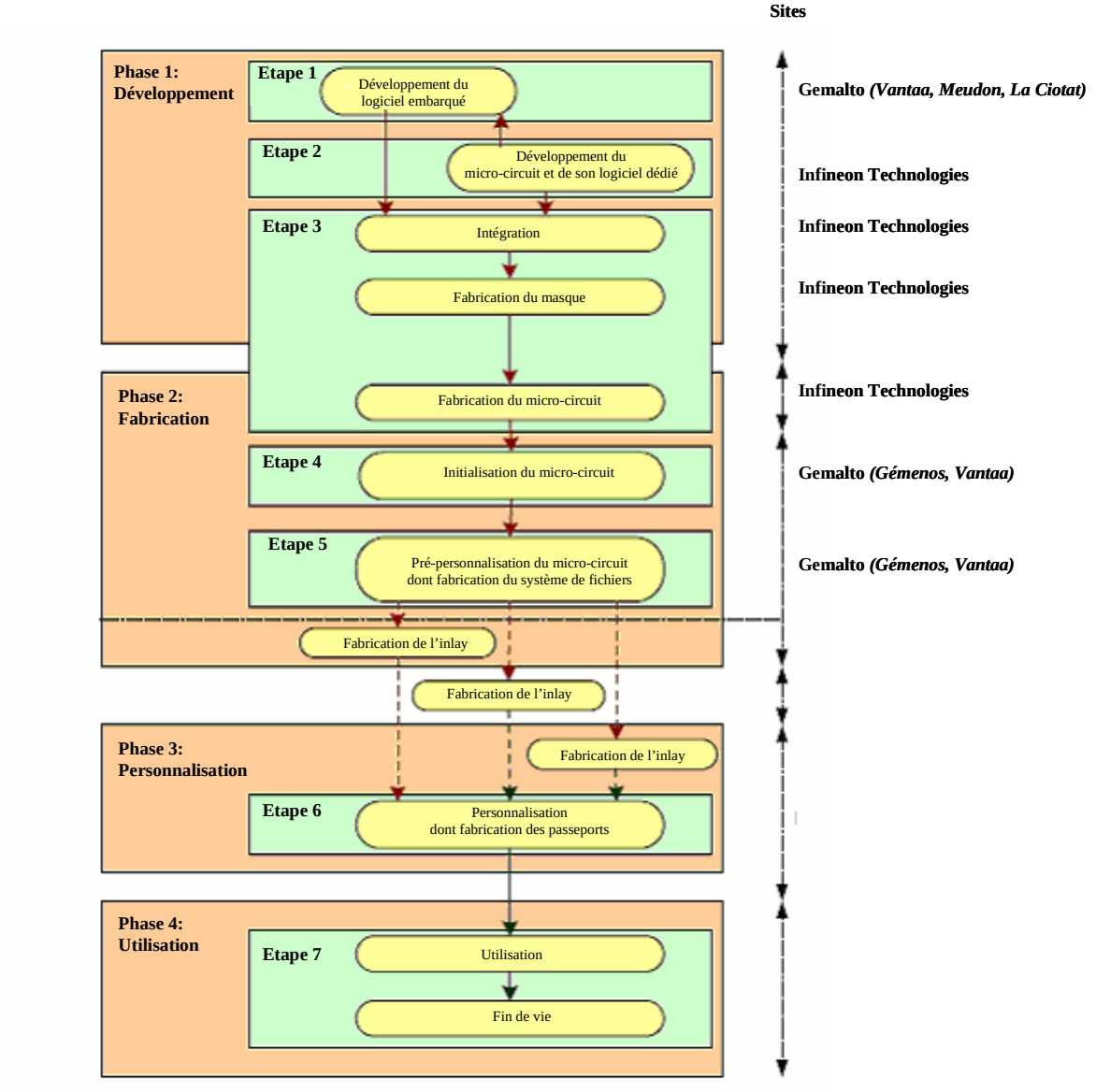

Figure 2 - Cycle de vie n° 1 : Initialisation du module sur le site de Gemalto

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, soit après être passé par le fabriquant d'inlays.

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

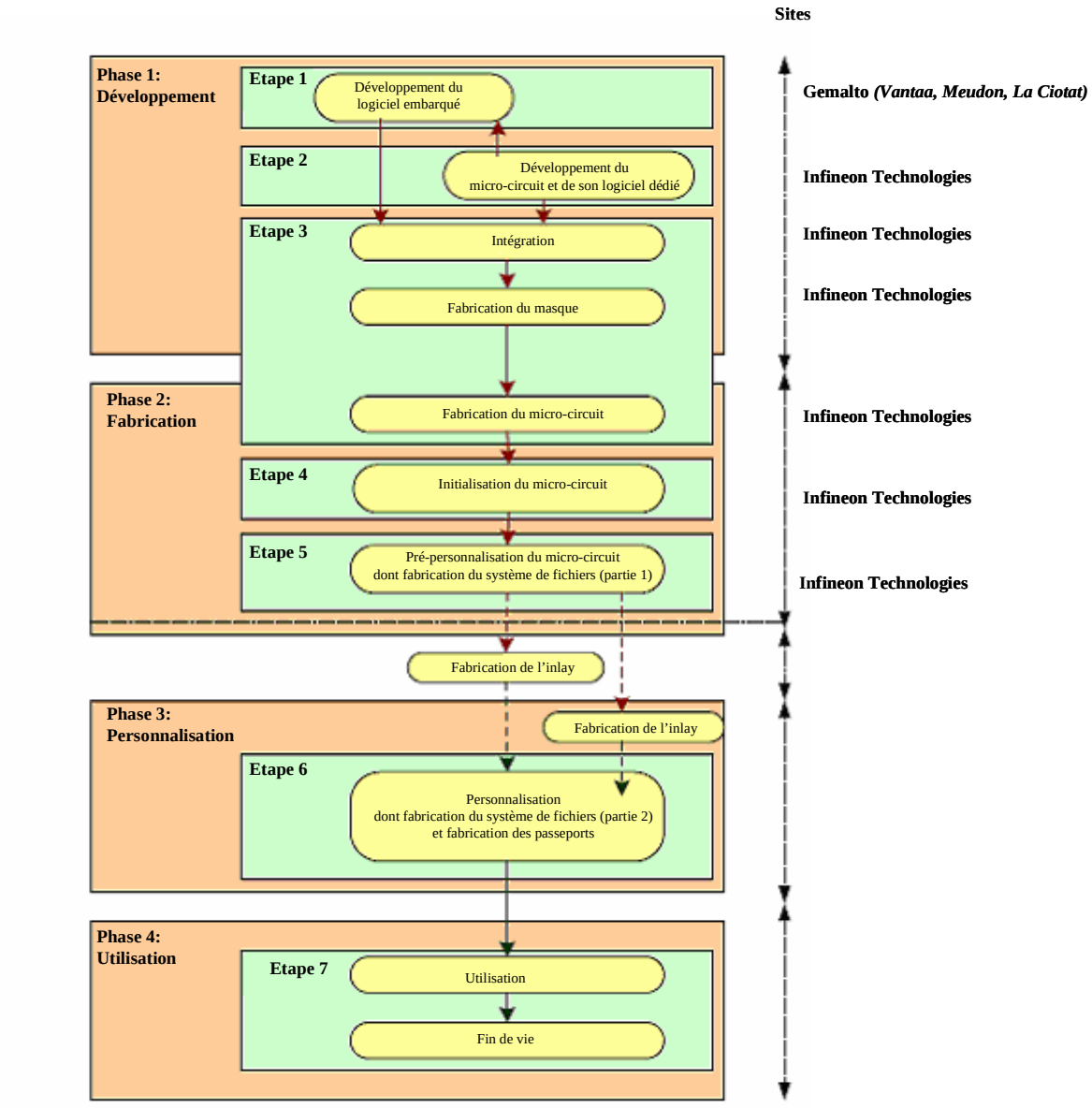

Figure 3 - Cycle de vie n° 2 : Initialisation du module sur le site du fondeur

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 :

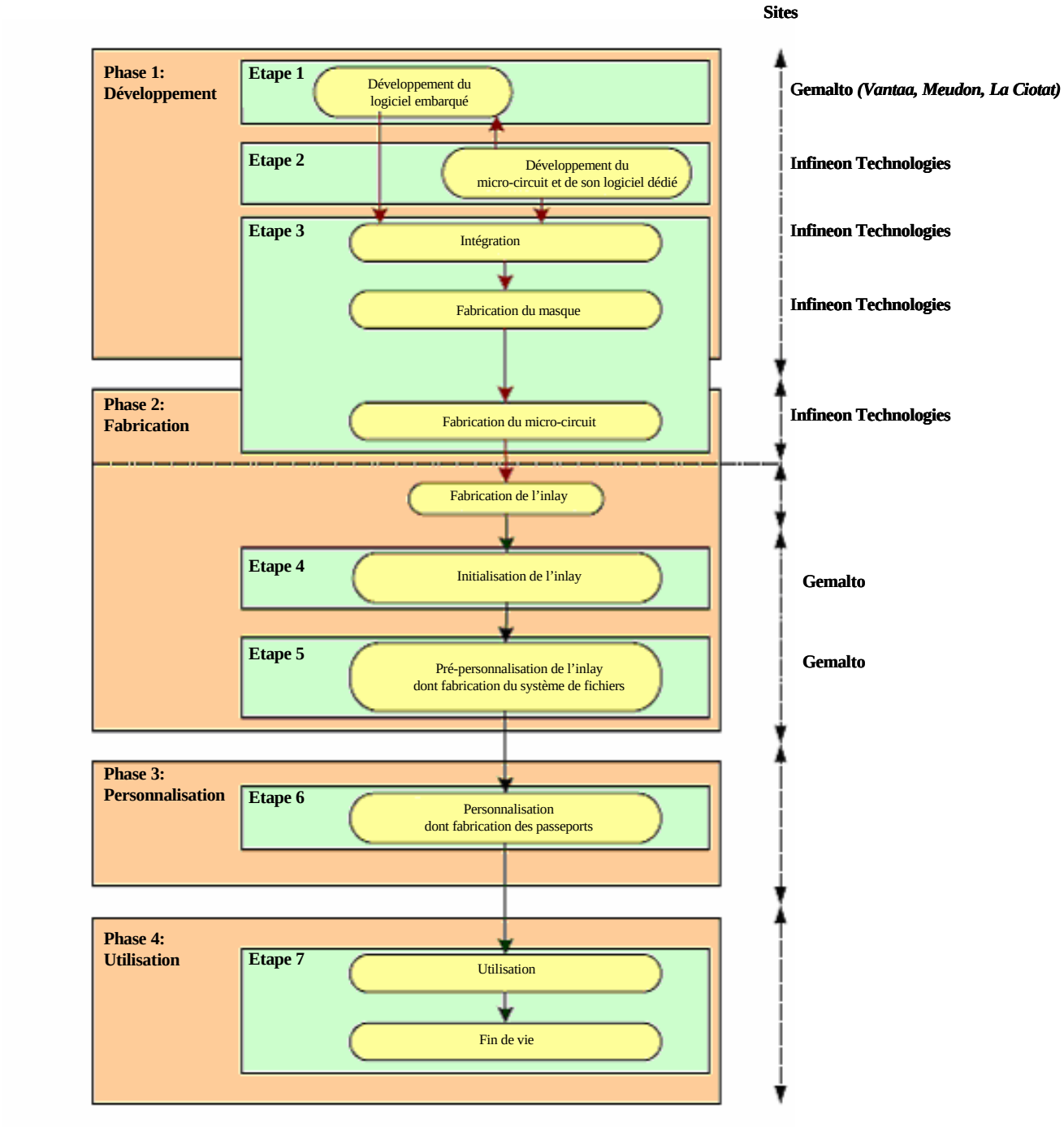

Figure 4 - Cycle de vie n° 3 : Initialisation sur inlay sur le site de Gemalto

Le cycle de vie n° 3 est une 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 fabriquant d'inlays.

Le logiciel est développé 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

Le composant est développé et fabriqué par Infineon Technologies AG. Les sites de développement et de fabrication de la puce Infineon SLE66CLX800PE sont détaillés dans le rapport de certification dont la référence est [BSI-DSZ-CC-0482-2008].

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

Ce rapport de certification porte sur la configuration incluant le mécanisme *Basic Access Control*.
L'antenne et la phase de fabrication du document de voyage lui-même ne sont pas incluses dans le périmètre d'évaluation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par l'ANSSI et compatibles avec le document [AIS 34], 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.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur SLE66CLX800PE / m1581 - e13/a14 au niveau EAL5, augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, et conforme au profil de protection [PP0002]. Le microcontrôleur SLE66CLX800PE / m1581 - e13/a14 a été certifié le 7 mai 2008 sous la référence [BSI-DSZ-CC-0482-2008].

L'évaluation s'appuie sur les résultats d'évaluation du produit « eTravel EAC v1.0 (version 01 03) sur SLE66CLX800PE m1581 e13/a14 » certifié le 27 juillet sous la référence ANSSI-2009/17 (cf. [2009/17]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 5 novembre 2009, 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 [REF-CRY] n'a pas été réalisée par l'ANSSI. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VLA visé.

2.4. Analyse du générateur d'aléas

Le générateur d'aléas du produit était en dehors du périmètre de l'évaluation et n'a pas été analysé.

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 l'application e-passeport en configuration BAC du produit « eTravel EAC version 1.0 (version 01 03) sur composant SLE66CLX800PE » 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 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 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 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. 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'Espagne, la Finlande, la France, la Grèce, 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 4+	Intitulé du composant
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2	**1**	Partial CM automation
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Configuration support and acceptance procedures
	ACM_SCP			**1**	**2**	**3**	3	3	**2**	Problem tracking CM coverage
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**2**	Detection of modification
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**2**	Fully defined external interfaces
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**1**	Informal TOE security policy model
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				**1**	**2**	2	**3**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-level 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_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**2**	Validation of analysis
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**2**	Independent vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - eTravel v1.0 MAÏA3 BAC Security Target, Référence : D1104528, version 1.0 du 19 octobre 2009, Gemalto Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - eTravel v1.0 MAÏA3 BAC Security Target, Référence : D1131804, version 1.0 du 11 janvier 2010, Gemalto
[RTE]	Evaluation Technical Report – MAÏA3 Project – BAC configuration, Référence : MAIA3_ETR_BAC_v1.1, version 1.1, Serma Technologies
[2009/17]	Rapport de certification ANSSI-2009/17 – « eTravel EAC version 1.0 (version 01 03) sur composant SLE66CLX800PE m1581 e13/a14 », 27 juillet 2009, SGDN/ANSSI
[CONF]	eTravel v1.0 MAÏA3 : Configuration list, Référence : D1107039, version 0.5, Gemalto
[GUIDES]	Guide d'administration du produit : - MAÏA3 – Administrator guide, Référence : D1094049_AGD_ADM_eTravel_V1.0_MAÏA3, Version 0.7, Gemalto Guide d'utilisation du produit : - MAÏA3 – User guide, Référence : D1094048_AGD_USR_eTravel_V1.0_MAÏA3, Version 0.5, Gemalto
[PP0002]	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 BAC]	Protection Profile - Machine Readable Travel Document with "ICAO Application", Basic Access Control, version 1.0, 18 Août 2005. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0017-2005.*
[BSI-DSZ-CC-0482-2008]	BSI-DSZ-CC-0482-2008 for SLE66CLX800PE / m1581-e13/a14, SLE66CLX800PEM / m1580-e13/a14, SLE66CLX800PES / m1582-e13/a14, SLE66CX800PE / m1599-e13/a14, SLE66CLX360PE / m1587-e13/a14, SLE66CLX360PEM / m1588-e13/a14, SLE66CLX360PES / m1589-e13/a14, SLE66CLX180PE / m2080-a14, SLE66CLX180PEM / m2081-a14, SLE66CLX120PE / m2082-a14, SLE66CLX120PEM / m2083-a14, all optional with RSA2048 V1.5 and ECC V1.1 and all with specific IC

	dedicated software from Infineon Technologies AG. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 7 mai 2008 sous la référence BSI-DSZ-CC-0482-2008.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 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, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2008-04-001 version 2.5 revision 1, April 2008.
[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 2.0, April 1999, Management Committee of Agreement Group.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.11 du 24 octobre 2008, SGDN/DCSSI, voir www.ssi.gouv.fr

[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, BSI (Bundesamt für Sicherheit in der Informationstechnik)