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-2012/46

eTravel EAC version 1.1 avec AA (version 01 03), configuration BAC, sur composant P5CD080

Paris, le 30 novembre 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-2012/46

Nom du produit

eTravel EAC version 1.1 avec AA (version 01 03), configuration BAC, sur composant P5CD080

Référence/version du produit

T1003327 avec softmask S1051194 révision 01 03

Conformité à un profil de protection

BSI-CC-PP-0055-2009, [PP BAC], version 1.10

CC Protection Profile – Machine Readable Travel Document with ICAO application, Basic Access Control

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2

Développeur(s)

Gemalto	NXP Semiconductors GmbH
6 rue de la Verrerie **92197 Meudon cedex** **France**	**Box 54 02 40** **22502 Hamburg** **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 6

1.1. PRESENTATION DU PRODUIT 6
1.2. DESCRIPTION DU PRODUIT 6
1.2.1. Introduction 6
1.2.2. Identification du produit 7
1.2.3. Services de sécurité 7
1.2.4. Architecture 8
1.2.5. Cycle de vie 8
1.2.6. Configuration évaluée 13

2. L'EVALUATION 14

2.1. REFERENTIELS D'EVALUATION 14
2.2. TRAVAUX D'EVALUATION 14
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LE REFERENTIEL TECHNIQUE DE L'ANSSI 14
2.4. ANALYSE DU GENERATEUR D'ALEAS 14

3. LA CERTIFICATION 15

3.1. CONCLUSION 15
3.2. RESTRICTIONS D'USAGE 15
3.3. RECONNAISSANCE DU CERTIFICAT 15
3.3.1. Reconnaissance européenne (SOG-IS) 15
3.3.2. Reconnaissance internationale critères communs (CCRA) 16

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 17

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 18

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 20

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte « eTravel EAC v1.1 avec Active Authentication (version 01 03), en configuration BAC (« *Basic Access Control* »), sur composant P5CD080 » développée par la société Gemalto. Le microcontrôleur est développé et fabriqué par la société NXP Semiconductors.

Le produit est une carte à puce sans contact comportant un logiciel destiné à permettre la vérification de l'authenticité du document de voyage et l'identification de 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* » ;
- 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* ».

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

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 BAC].

1.2.2. 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 EAC v1.1 with AA (version 01 03)	Gemalto
Référence de la TOE (label interne)	T1003327 avec softmask S1051194 révision 01 03	Gemalto
Référence du système d'exploitation	1.1	Gemalto
Référence du softmask	01 03	Gemalto
Identification de l'IC	P5CD080 V0B	NXP Semiconductors

Ces éléments sont identifiables à l'aide de la commande « GET DATA », pour le tag '9F 7F', comme indiqué dans le guide d'administration (cf. [GUIDES]) :

- IC FABRICATOR = **40 70** (NXP Semiconductors) ;
- IC TYPE = **50 80** (P5CD080) ;
- OPERATING SYSTEM IDENTIFIER = **D0 00 67** ;
- OPERATING SYSTEM RELEASE LEVEL = **01 03**.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :
- contrôle d'accès ;
- mécanisme d'authentification mutuelle ;
- mécanisme de « *Secure Messaging* » ;
- mécanisme d'« *Active Authentication* ».

Les principaux services de sécurité fournis par le microcontrôleur sont :
- génération de nombres aléatoires ;
- coprocesseur triple-DES ;
- coprocesseur AES ;
- contrôle des conditions de fonctionnement ;
- protection contre les modifications physiques ;
- protection logique ;
- protection du mode de contrôle ;
- contrôle d'accès aux mémoires ;
- fonctions spéciales de contrôle de l'accès aux registres.

1.2.4. Architecture

Le produit est constitué du microcontrôleur P5CD080, du logiciel embarqué, comprenant les tests et la gestion des commandes et des données, et de la structure logique des données.

La figure 1 résume l'architecture du produit évalué :

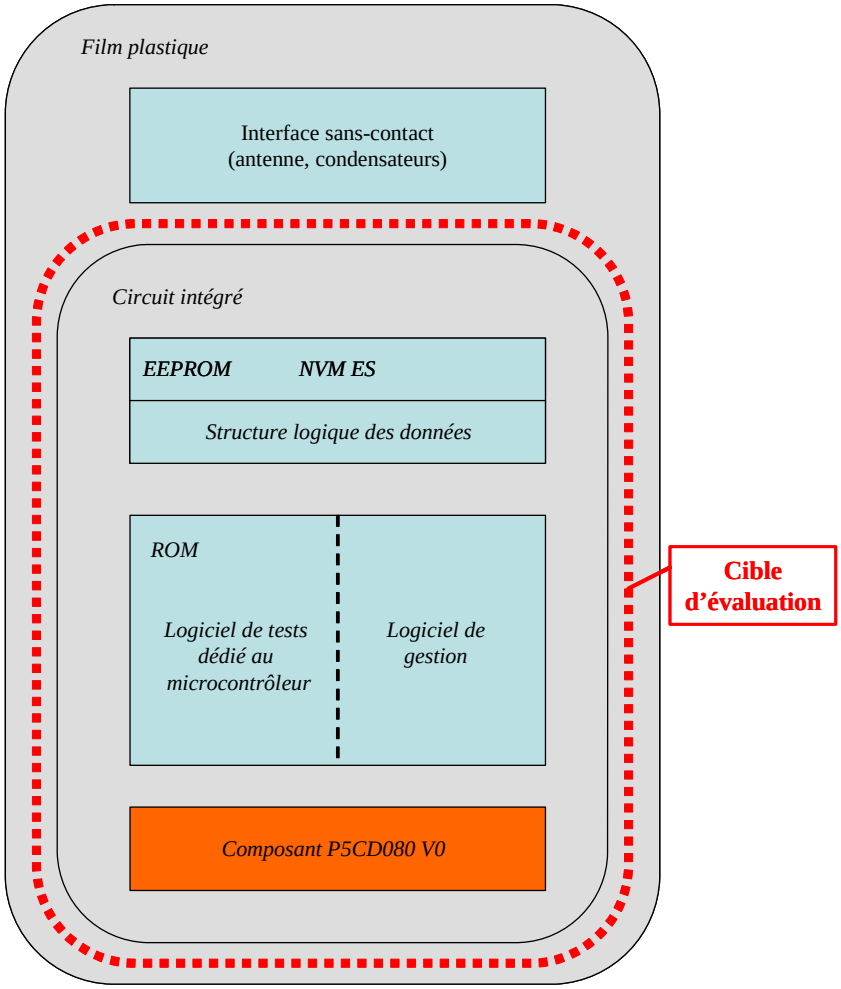

Figure 1 - Architecture du produit

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 phases 1 et 2, fabrication de l'inlay non incluse.

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

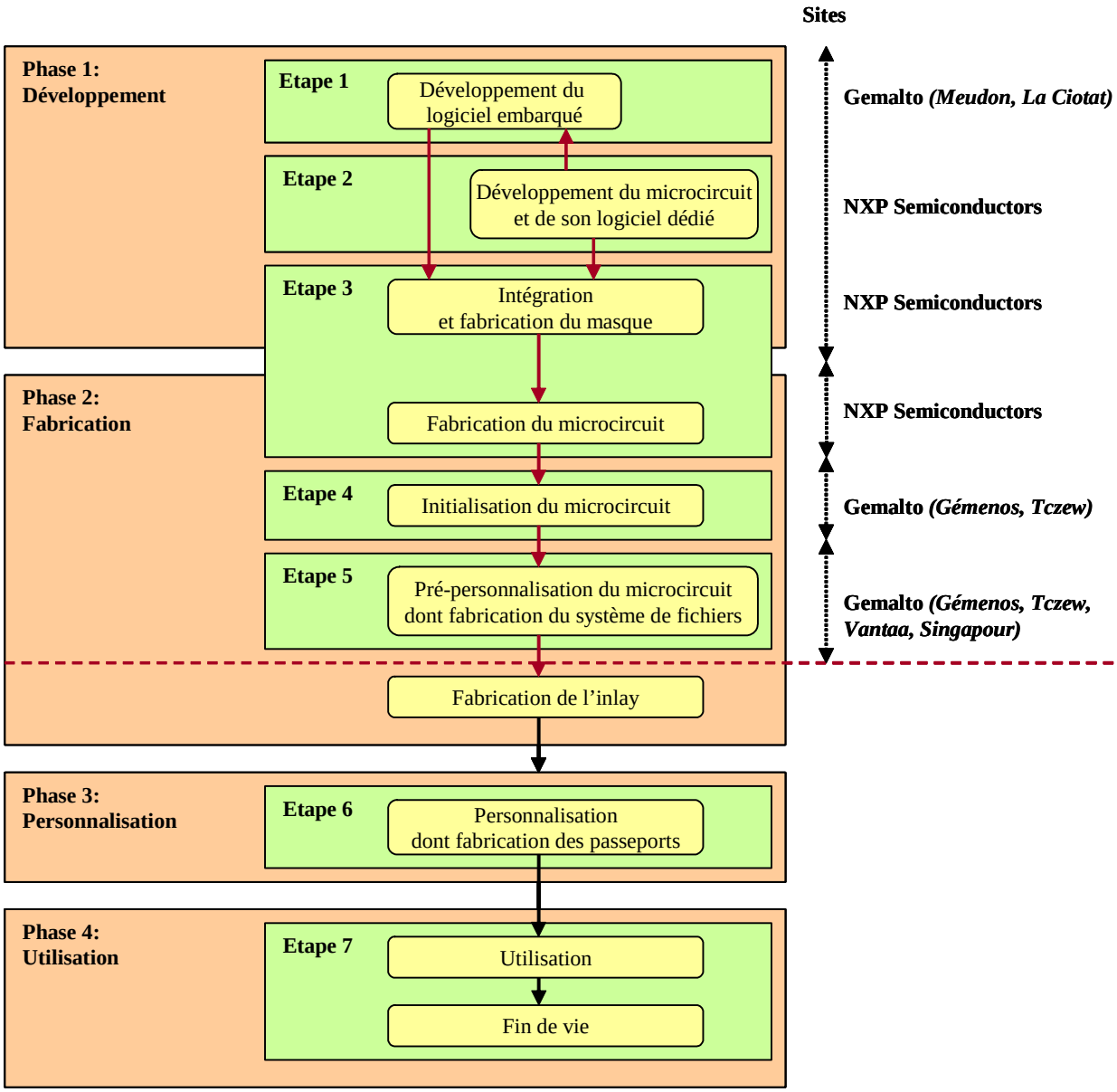

Figure 2 - Cycle de vie n° 1 : Initialisation du module sur le site de Gemalto

Le cycle de vie n° 1 correspond au 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 qui fabrique l'inlay.

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

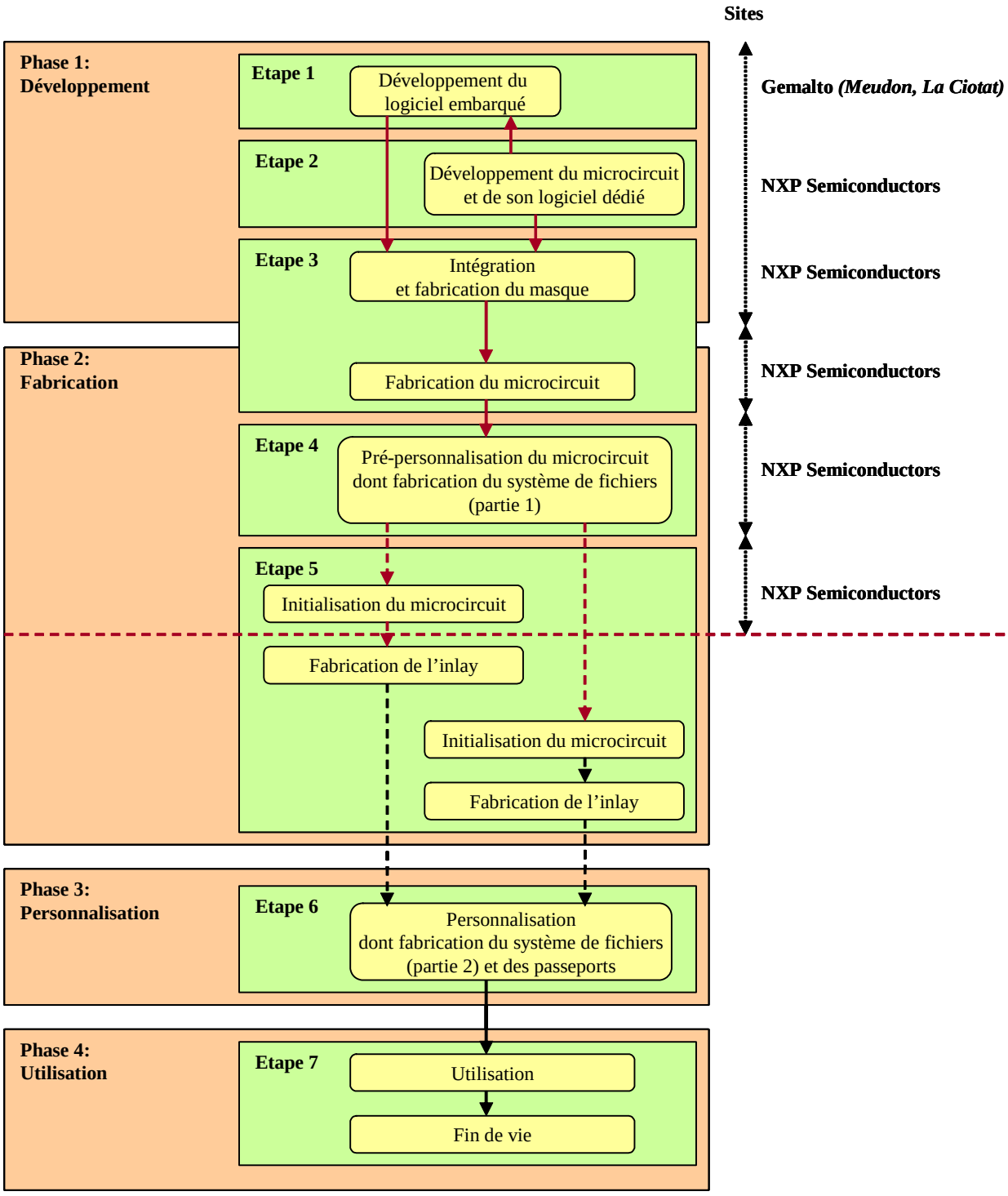

Figure 3 - Cycle de vie n° 2 : Initialisation du module sur le site du fondeur

Le cycle de vie n° 2 est une variante du cycle de vie n° 1. Il 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. 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 :

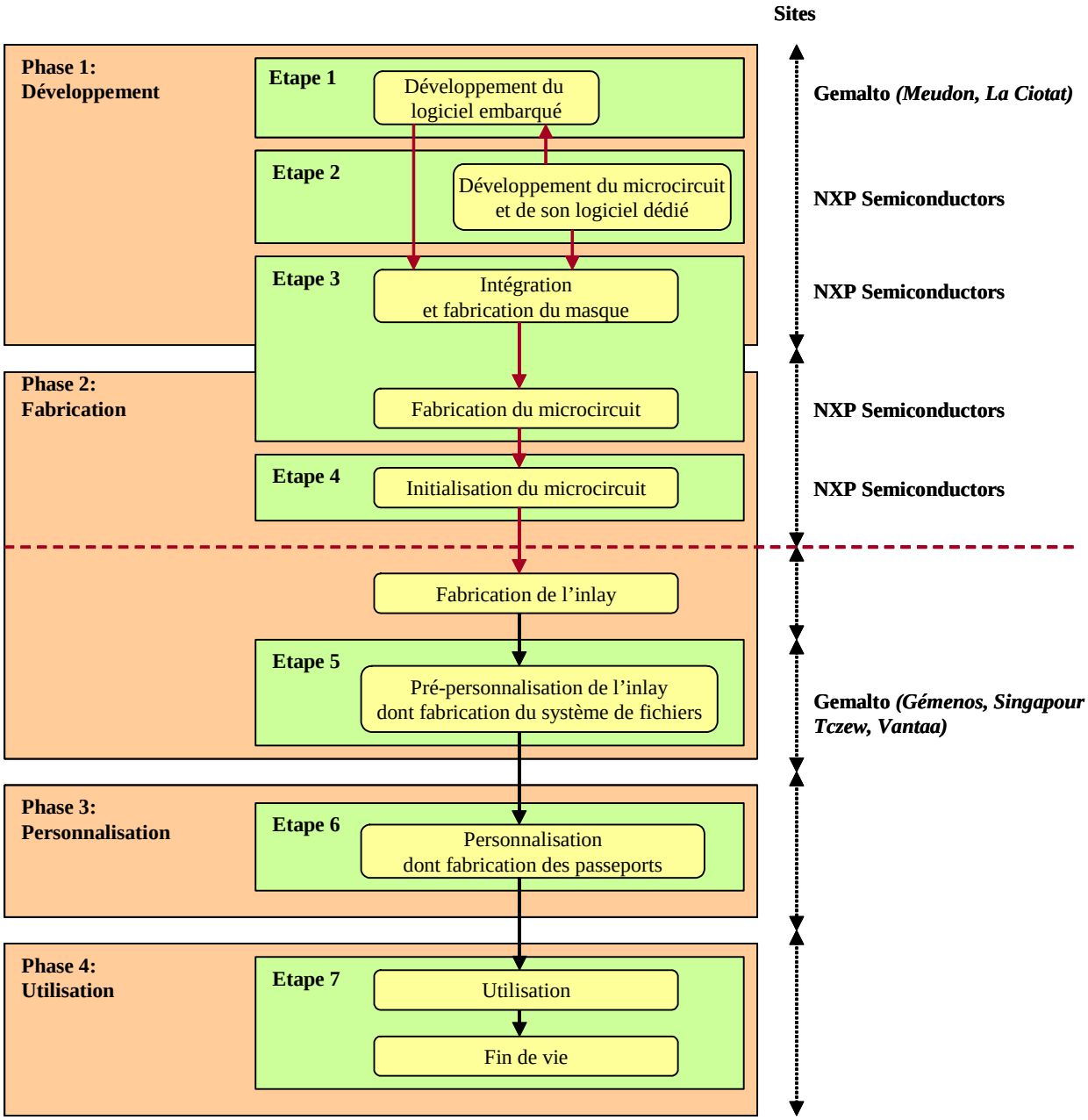

Figure 4 - Cycle de vie n° 3 : Initialisation sur inlay sur le site de Gemalto

Le cycle de vie n° 3 est une autre variante du cycle de vie n° 1. Il correspond au cas où Gemalto souhaite recevoir des inlays plutôt que des modules. Dans ce cas, c'est le fondeur qui envoie les modules au fabricant d'inlays.

Le produit est développé et fabriqué sur les sites suivants :

Gemalto

Turvalaaksontie 1
FI-01740 Vantaa
Finlande

Gemalto

Myllynkivenkuja 4
FI-01740 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
283-110 Tczew
Pologne

Gemalto

12 Ayer Rajah Crescent
Singapor 139941
Singapour

Le microcontrôleur P5CD080 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-0700-2011].

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 le produit « eTravel EAC v1.1 (avec mécanisme d'« *Active Authentication* »), en configuration BAC, sur composant P5CD080 », tel que présenté au paragraphe 1.2.2.

Ce rapport de certification porte sur la configuration incluant les mécanismes suivants :

- « *Basic Access Control* » ;
- « *Active Authentication* ».

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 3.1 révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour répondre aux spécificités des cartes à puce, les guides [CC 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 « P5CD080 V0B » au niveau EAL5 augmentée des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4 conformément au profil de protection [PP0002]. Ce microcontrôleur a été certifié le 25 octobre 2011 sous la référence [BSI-DSZ-CC-0700-2011].

L'évaluation s'appuie sur les résultats de l'évaluation du produit « eTravel EAC v1.1 (version 01 02) sur composants P5CD080 et P5CD144 » certifié le 18 décembre 2008 sous la référence [DCSSI-2008/45].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 29 octobre 2012, 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 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 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-0700-2011]).

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 EAC version 1.1 avec AA (version 01 03), configuration BAC, sur composant P5CD080 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté du composant ALC_DVS.2.

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 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 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	**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	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - eTravel EAC v1.1 with AA Maia4 : BAC Security Target Référence : D1239132 Version 1.1 du 26 octobre 2012 Gemalto. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - eTravel EAC v1.1 with AA – BAC – Common Criteria / ISO 15408 – Security Target – Public version – EAL4+. Référence : D1276271 Version 1.0 du 25 octobre 2012 Gemalto.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – MAIA4 Project Référence : MAIA4_ETR_BAC_v1.0 Version 1.0 du 29 octobre 2012 Serma Technologies.
[CONF]	Liste de configuration : - eTravel v1.1 Maia4 – Configuration List Référence : D1240330 Version 0.7 du 17 septembre 2012 Gemalto.
[GUIDES]	Guide d'administration du produit : - Maia4 AGD: Preparative procedures, Référence : D1239135, Version 1.0 du 17 septembre 2012, Gemalto. Guide d'utilisation du produit : - eTravel v1.1 Maia4 AGD: Operational procedures, Référence : D1239138, Version 1.1 du 7 septembre 2012, Gemalto.
[PP BAC]	Protection Profile - Machine Readable Travel Document with "ICAO Application", Basic Access Control, version 1.10, 25 Mars 2009. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-CC-PP-0055-2009.*
[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.*

[BSI-DSZ-CC-0700-2011]	« NXP Secure Smart Card Controller P5CD080V0B, P5CC080V0B, P5CN080V0B and P5CC073V0B each with specific IC Dedicated Software ». *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 25 octobre 2011 sous la référence BSI-DSZ-CC-0700-2011*.
[DCSSI-2008/45]	« eTravel EAC version 1.1 (version 01 02) sur composants P5CD080 et P5CD144. ». *Certifié par l'ANSSI le 18 décembre 2008 sous la référence DCSSI-2008/45*.

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.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.
[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]	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.