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-2012/31

Application eTravel EAC 1.4 avec AA, configuration BAC avec AMD 113v3, masquée sur composants IFX M7820 A11

(eTravel EAC 1.4 with AA application, BAC configuration with AMD 113v3 embedded on IFX M7820 A11 components)

Paris, le 6 juillet 2012

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-2012/31

Nom du produit

Application eTravel EAC 1.4 avec AA, configuration BAC avec AMD 113v3, masquée sur composants IFX M7820 A11

Référence/version du produit

Version de l'application et de la plateforme : 023078 / 023079
Version de l'AMD (patch) : 113v3
Version du composant IFX M7820 A11 : SLE78CLXxxxxP / SLE78CLXxxxxPM

Conformité à un profil de protection

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

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

Développeurs

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

THALES (TCS – CNES)

18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, 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. Identification du produit 7
1.2.2. Services de sécurité 8
1.2.3. Architecture 9
1.2.4. Cycle de vie 10
1.2.5. 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 LES REFERENTIELS TECHNIQUES DE L'ANSSI 15
2.4. ANALYSE DU GENERATEUR D'ALEAS 16

3. LA CERTIFICATION 17

3.1. CONCLUSION 17
3.2. RESTRICTIONS D'USAGE 17
3.3. RECONNAISSANCE DU CERTIFICAT 18
3.3.1. Reconnaissance européenne (SOG-IS) 18
3.3.2. Reconnaissance internationale critères communs (CCRA) 18

ANNEXE 1. NIVEAU D'EVALUATION DU PRODUIT 19

ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE 20

ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION 22

1. Le produit

1.1. Présentation du produit

Le produit évalué est le passeport électronique intitulé « Application eTravel EAC 1.4 avec AA, configuration BAC avec AMD 113v3, masquée sur composants IFX M7820 A11 ». La version de l'application et de la plateforme est 023078 pour SLE78CLXxxxxP et 023079 pour SLE78CLXxxxxPM, la version de l'AMD (patch dans la terminologie Multos) est 113v3 quelle que soit la variante du composant, les variantes des composants M7820 A11 utilisées sont SLE78CLXxxxxP / SLE78CLXxxxxPM. Ce produit est développé par Gemalto et Infineon Technologies AG.

Le produit évalué est de type « carte à puce » avec et sans contact. Il implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (ICAO). Ce produit est 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.

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

1.2. Description du produit

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]. Elle comprend la fonctionnalité additionnelle « *Active Authentication* ».

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 détaillés au chapitre « 1.1 ST Identification » de la [ST]. Ces éléments sont obtenus en réponse à la commande GET DATA avec le tag 9F7F (voir [GUIDES]) :

Description	Length (byte)	Value for v1.0
IC Fabricator	2	'40 90' (IFX)
IC Type	2	'XX XX' (see below)
Operating System Identifier	3	''02 30 78' (G230-ML3-78) '02 30 79' (G230M-ML3-79)
RFU	1	'00'
Operating System release level	2	'01 13'
IC Fabrication Date	2	'YYDD'
IC Serial Number	4	YYYYYYYY
IC Batch Identifier	2	YYYY
IC Module Fabricator	2	'40 90'
IC Module Packaging Date	2	YYDD
ICC Manufacturer	2	'ZZ ZZ'
IC Embedding Date	2	'YYDD'
IC Pre-personalizer	2	'ZZ ZZ'
IC Pre-personalization Date	2	'YYDD'
IC Pre-personalization Equipment Identifier	4	'00 00 00 00'
IC Personalizer	*2*	*'ZZ ZZ'*
IC Personalization Date	*2*	*'YYDD'*
IC Personalization Equipment Identifier	*4*	*'ZZ ZZ ZZ ZZ'*

Table 1: Card Production Life Cycle Data

Les différentes valeurs de « IC Type » désignent les variantes des familles P et PM :

Chip type/size	P	PM (Mifare)
78CLX1600	78A4h	79A5h
78CLX1440	78A0h	79A2h
78CLX1280	78A7h	NA
78CLX800	78A9h	79ABh
78CLX480	78AFh	79B0h
78CLX360	78B1h	79B2h

Ces variantes de composants diffèrent uniquement par leur taille mémoire et par la présence ou non de l'interface Mifare.

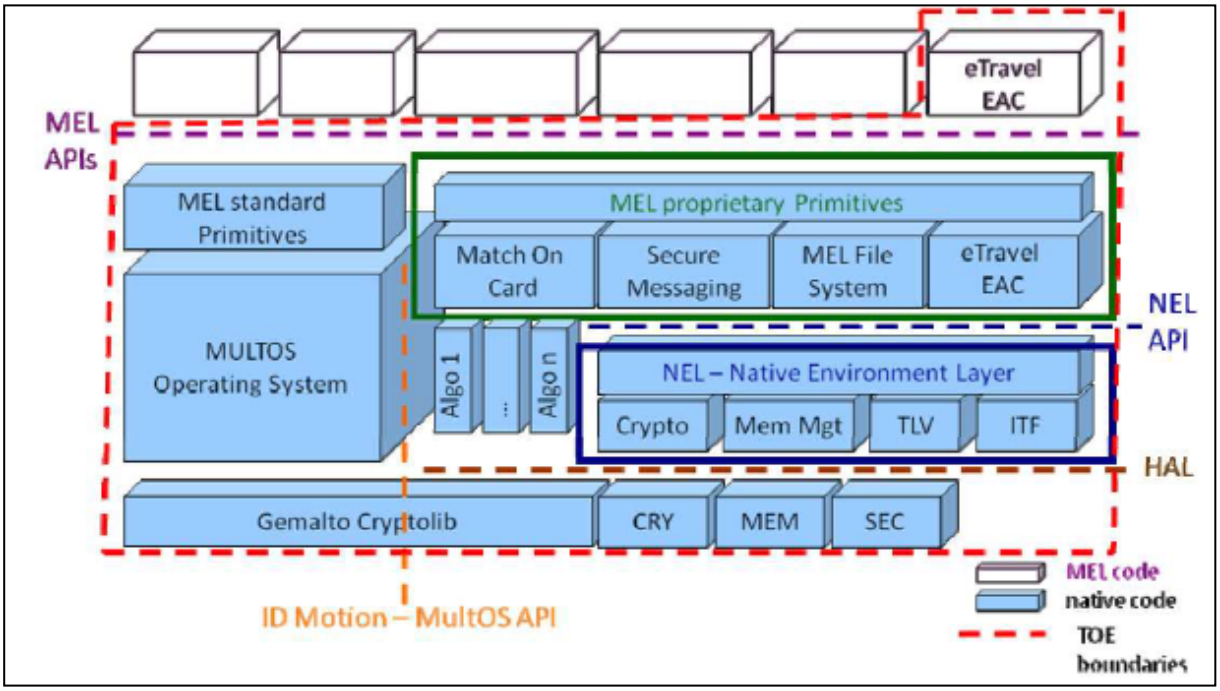
1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection de l'intégrité des données du porteur, stockées dans la carte grâce au système de contrôle d'accès n'acceptant qu'une seule écriture et grâce à des moyens physiques offerts par le composant ;
- l'authentification, lors du contrôle aux frontières, entre le document de voyage et le système d'inspection (terminal de lecture des documents de voyage) à l'aide du mécanisme *Basic Access Control ;*
- la vérification de l'authenticité du microcontrôleur à l'aide du mécanisme *Active Authentication* (si activé) ; ce mécanisme peut être effectué avec du RSA ou de l'ECC ;
- la protection des échanges avec le système d'inspection grâce à un mécanisme de canal sécurisé.

1.2.3. Architecture

L'architecture logicielle est illustrée dans la figure suivante :



Le produit est une carte à puce constituée :

- du microcontrôleur M7820 A11 sous la forme d'une de ses variantes par famille (voir liste plus haut au chapitre 1.2.1 Identification du produit) ;
- de la plateforme Multos « ID Motion V1 platform » en version 023078 pour la famille SLE78CLXxxxxP et 023079 pour la famille SLE78CLXxxxxPM et en configuration fermée ;
- du patch « AMD » en version 113v3 ;
- de l'application passeport électronique « eTravel EAC 1.4 with AA application » en configuration BAC (la plateforme et l'application ont le même identifiant de version).

D'autres applications, en dehors du périmètre de cette évaluation, sont embarquées dans la mémoire du produit mais ne sont pas actives dans la configuration évaluée.

1.2.4. Cycle de vie

Le produit a trois cycles de vie possibles, tous basés sur celui décrit dans [PP BAC]. Ils sont détaillés au chapitre « 1.8 TOE Life-cycle » de la [ST]. Une illustration de chacun de ces cycles de vie est donnée ci-après.

Le cycle de vie n° 1 correspond à « l'initialisation du module sur le site de Gemalto », c'est le cycle de vie standard (livraison de modules) :

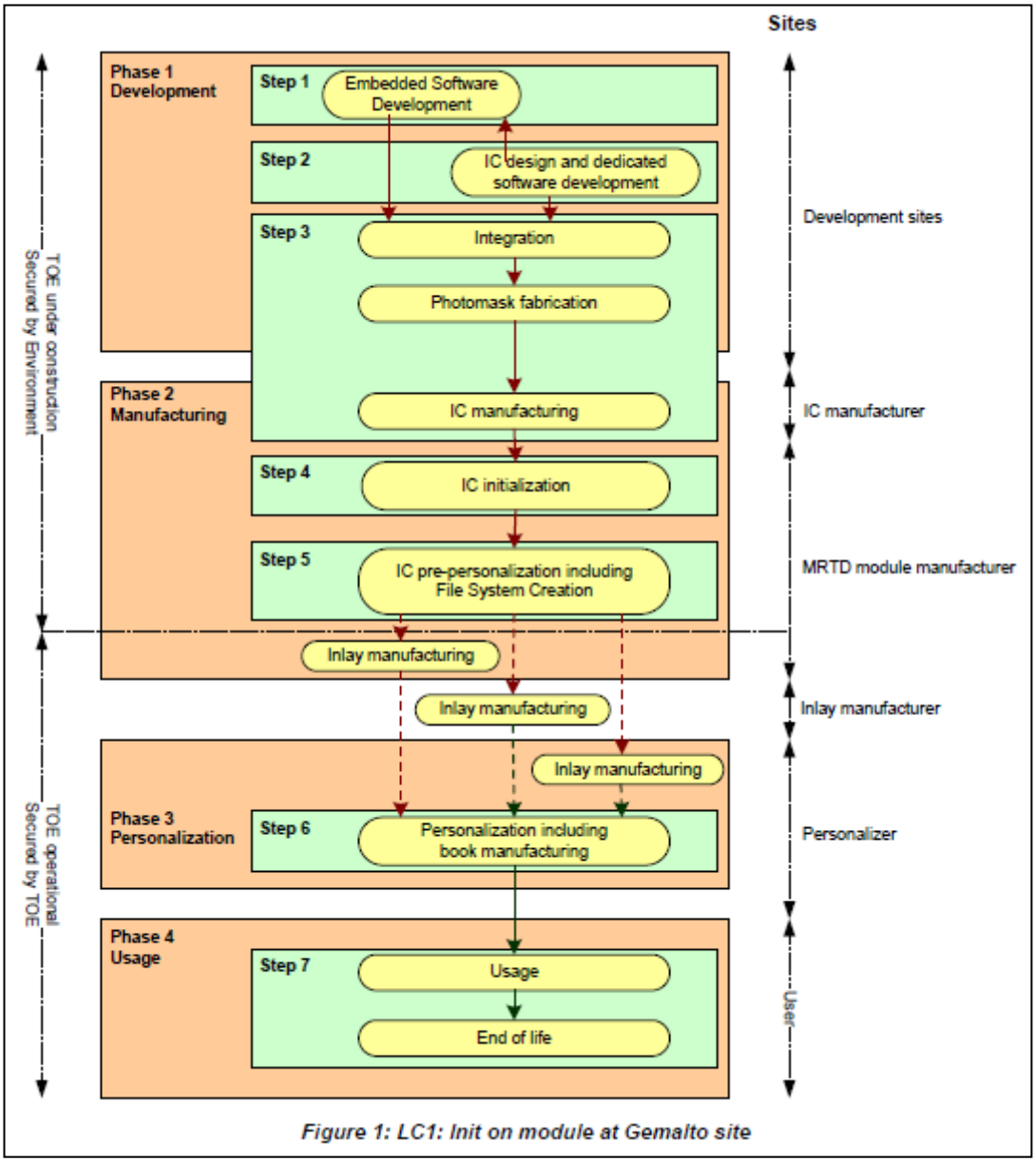


Figure 1: LC1: Init on module at Gemalto site

Le point de livraison est situé après l'étape 5. Toutes les étapes qui précèdent ce point de livraison ont été prises en compte durant la présente évaluation au travers des activités ALC, le cas échéant en réutilisant les résultats obtenus lors de l'évaluation du composant sous-jacent. L'étape 6 a été prise en compte durant l'évaluation au travers des guides (activités AGD). Les tests ont porté sur les fonctionnalités du produit disponibles aux étapes 6 et 7 (activités ATE et AVA).

Le cycle de vie n°2 correspond à « l'initialisation du module sur le site du fondeur », c'est le cycle de vie adapté lorsque la livraison de *wafers* est souhaitée (au lieu de modules) :

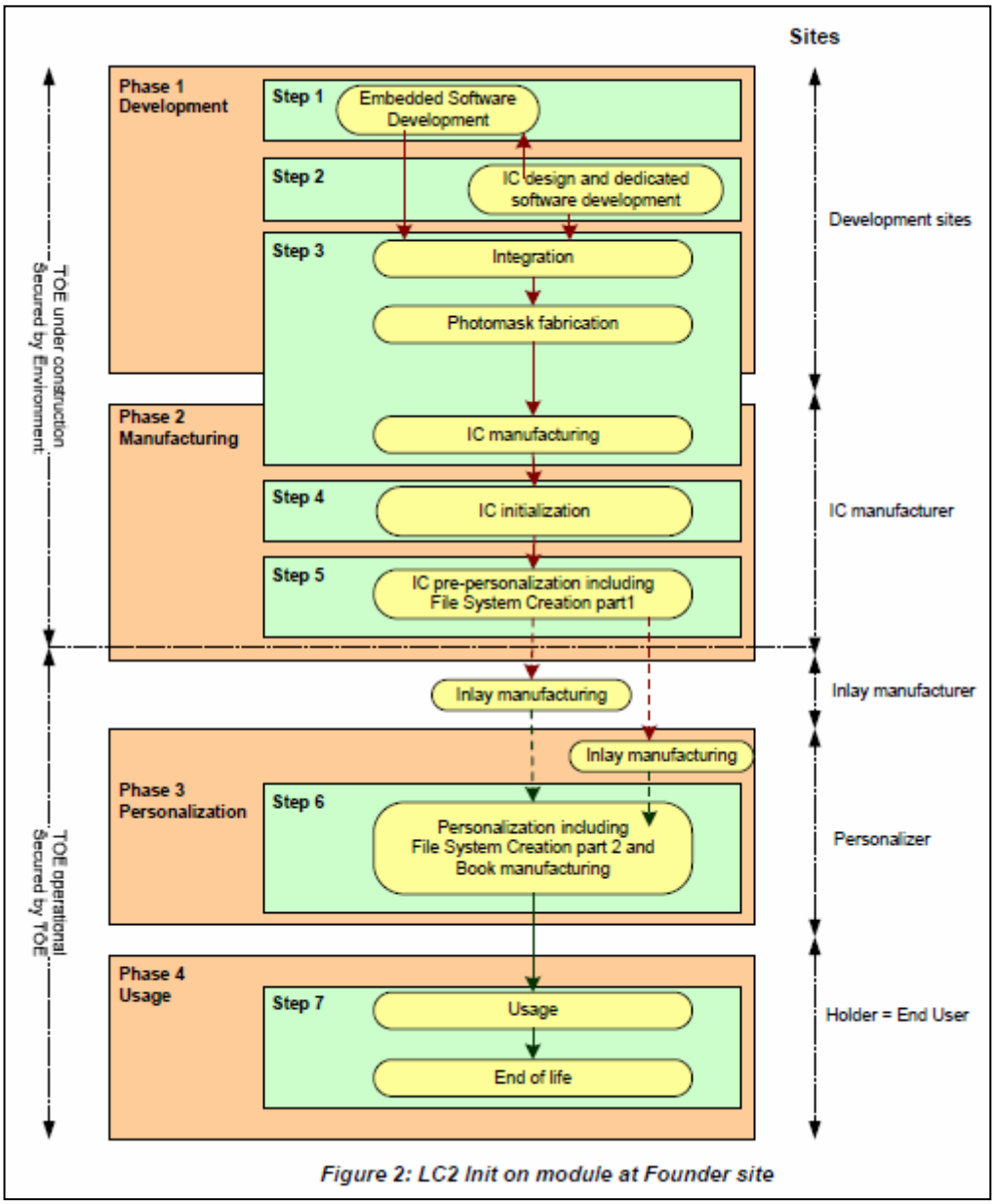


Figure 2: LC2 Init on module at Founder site

Dans cette variante de cycle de vie, seule la première partie de la pré-personnalisation (correspondant aux opérations sensibles de la pré-personnalisation) est effectuée à l'étape 5. La seconde partie de la pré-personnalisation (correspondant à des opérations nécessaires pour la personnalisation) est couverte par les activités AGD tout comme le reste des opérations de la personnalisation (étape 6).

Le cycle de vie n°3 correspond à « l'initialisation sur « *inlay* » sur le site de Gemalto », c'est le cycle de vie adaptée lorsque la livraison de *inlays* est souhaitée (au lieu de modules) :

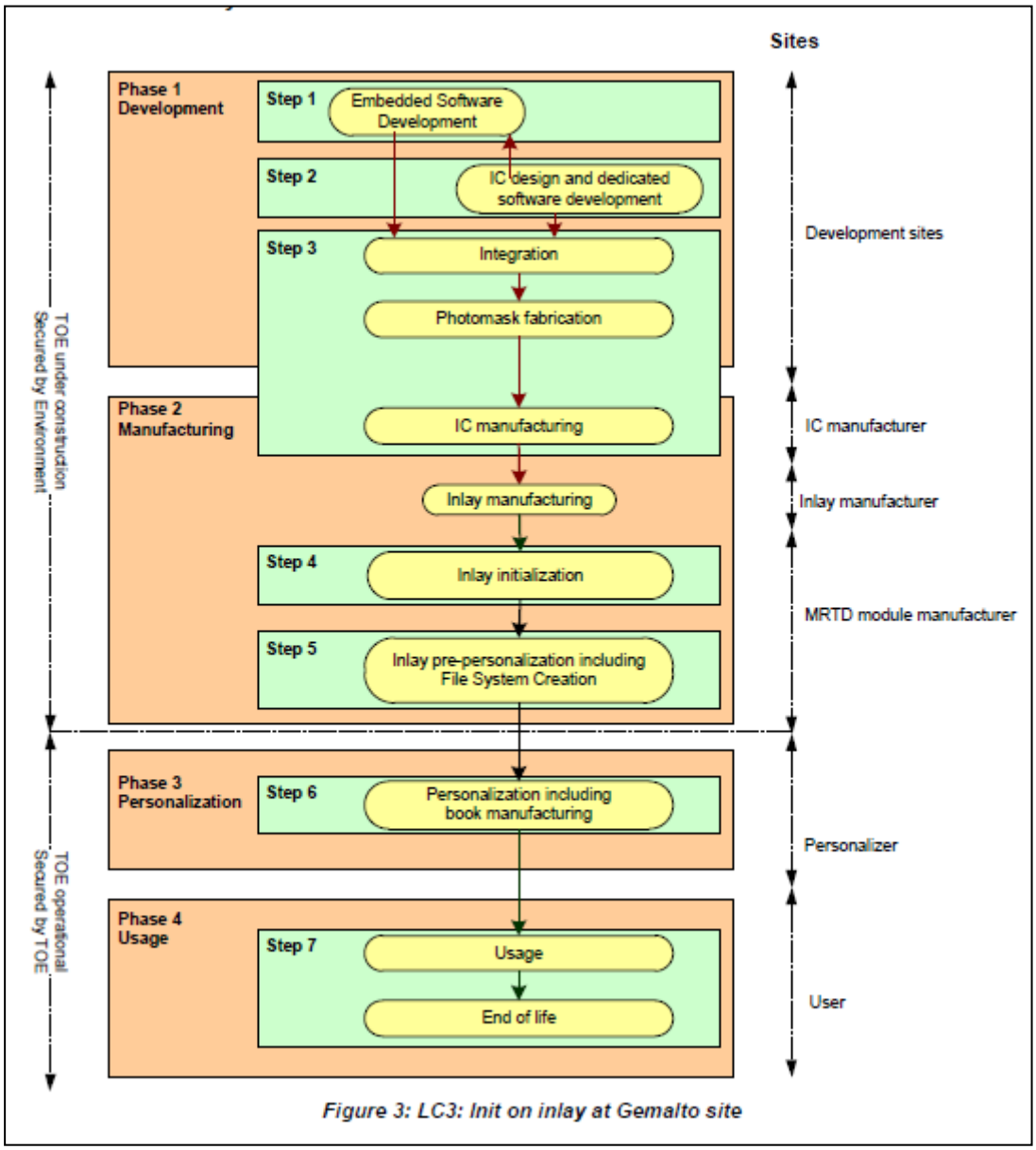


Figure 3: LC3: Init on inlay at Gemalto site

Dans cette variante de cycle de vie, les opérations de pré-personnalisation et de fabrication de l'inlay sont effectuées à l'étape 5, elles ont été prises en compte durant la présente évaluation au travers des activités ALC.

Le produit a été développé et fabriqué durant les étapes 1 à 5 sur les sites suivants :

Gemalto - Meudon

6 Rue de la verrerie
92190 Meudon
France

Multos international - Sydney

Level 14, the Zenith - Tower B, 821 Pacific Highway
Chatswood NSW 2067
Australia

Gemalto - Vantaa

Turvalaaksonkaari 2
FI-01741 Vantaa
Finlande

Gemalto - Gemenos

Avenue du Pic de Bertagne
13881 Gémenos
France

Gemalto - Tczew

Ul. Skarszewska 2
83-110 Tczew
Pologne

Gemalto - Singapour

12 Ayer Rajah Crescent
Singapor 139941
Singapour

Le microcontrôleur a été développé et fabriqué par Infineon Technologies AG sur ses sites (voir [BSI-DSZ-CC-0813-2012]).

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit l'agent de personnalisation (qui agit pour le compte des nations ou organisations émettrices) et le système d'inspection (qui est utilisé lors des contrôles aux frontières). Par ailleurs, l'évaluateur a considéré comme utilisateur du produit le détenteur du document de voyage contenant le produit. Ces rôles sont détaillés dans la [ST] au chapitre « 3.1.2 Subjects ».

1.2.5. Configuration évaluée

Le certificat porte sur la configuration telle que présentée au chapitre « 1.2.3 Architecture».

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 et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [CC 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 intitulé « *Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software* » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [BSI-PP-0035-2007]. Ce microcontrôleur a été certifié par le BSI (voir [BSI-DSZ-CC-0813-2012]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 29 juin 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 les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques a été réalisée conformément au référentiel technique de l'ANSSI [REF-CRY]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY] qui atteste que les mécanismes analysés sont conformes au référentiel [REF-CRY] sous réserve de prendre en compte les conclusions suivantes :

- concernant l'application de passeport électronique eTravel :
  - la longueur du modulo RSA, utilisée dans le cadre d'une signature RSA, doit être égale à 2 048 bits ;
  - la longueur de la clé ECDSA, utilisée dans le cadre d'une signature ECDSA, doit être égale à 224 bits pour une utilisation ne dépassant pas 2020 ;
  - la longueur du modulo premier Diffie-Hellmann, utilisée dans le cadre du protocole « *Chip Authentication* », doit être égale à 2 048 bits ;
  - l'algorithme de négociation de clés ECDH doit utiliser des courbes elliptiques avec une taille de 256, 320 ou 384 bits ;
  - dans le cadre du protocole « *Terminal authentication* » :
    - l'utilisation du mécanisme « *RSA 2048 bits – PKCS #1 v2.1 SHA-256* » est reconnu conforme ;
    - l'utilisation du mécanisme « *ECDSA at least 256 bits length of the curve – with SHA-256* » est reconnu conforme ;
- concernant globalement le produit :
  - le bit relatif à la vérification de signature doit être initialisé en mémoire statique de l'application ;
  - la clé mère ISK ne doit pas être utilisée directement et doit être diversifiée pour chaque puce en phase de personnalisation.

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

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

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires du produit génère les aléas par retraitement algorithmique de nature cryptographique des aléas générés par le composant.

Le mécanisme de retraitement a été analysé au titre de la cotation des mécanismes cryptographiques (voir chapitre précédent « 2.3 Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI »), et atteint le niveau K3-DRNG selon la méthodologie [AIS 20].

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

3. La certification

3.1. Conclusion

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

Ce certificat atteste que le produit « Application eTravel EAC 1.4 avec AA, configuration BAC avec AMD 113v3, masquée sur composants IFX M7820 A11», 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 Description du produit » 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]. Il devra également suivre les recommandations données au chapitre « 2.3 Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI » plus haut s'il utilise le produit dans un contexte de qualification.

3.3. Reconnaissance du certificat

3.3.1. Reconnaissance européenne (SOG-IS)

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

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

3.3.2. Reconnaissance internationale critères communs (CCRA)

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

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

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

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 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 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: security enforcing modules
	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 1.4: BAC Security Target, référence ST_D1251495, version 1.6.2, Gemalto. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - eTravel EAC 1.4: BAC - Security Target, référence ST_D1251495-Pub, date 29 juin 2012, Gemalto.
[RTE]	Rapport technique d'évaluation : - Evaluation technical report - Project: E-TRAVEL, référence ETV_ETR, version 1.0r3, THALES-CEACI.
[ANA-CRY]	Rapport d'analyse cryptographique de l'évaluateur : - Evaluation Report - Project: E-TRAVEL - Cryptographic Analysis référence ETV_ER, version 3.0, THALES-CEACI.
[CONF]	Liste de configuration du produit : - LIS: Configuration List Doc, référence LIS CC Etravel Standalone V2, date 29/06/2012, Gemalto.
[GUIDES]	Guide de préparation du produit : - eTravel EAC: Preparation procedures, référence AGD_PRE_eTravel_D1251497, version 1.0, Gemalto. Guide d'opération du produit : - eTravel EAC: Operational User Guide, référence AGD_OPE_eTravel_D1251498, version 1.1, 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-PP-0055-2009.*
[BSI-PP-0035-2007]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*

[BSI-DSZ-CC-0813-2012]	Certificat BSI délivré le 6 juin 2012 pour le produit : « *Infineon smart card IC (Security Controller) M7820 A11 with optional RSA2048/4096 v1.02.008, EC v1.02.008, SHA-2 v1.01 and Toolbox v1.02.008 libraries and with specific IC dedicated software* »

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.

[AIS 20]	AIS20 Functionality classes and evaluation methodology for deterministic number generators, AIS20 version 1, 2 décembre 1999, BSI (Bundesamt für Sicherheit in der Informationstechnik).