



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-2011/16

Applet IAS Classic v3 sur carte à puce MultiApp V2 masquée sur composants de la famille SLE66

Paris, le 18 août 2011

*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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CC-2011/16

Nom du produit

**Applet IAS Classic v3 sur carte à puce MultiApp V2
masquée sur composants de la famille SLE66**

Référence/version du produit

**Version du masque : 1.0
Version plateforme Java Card MultiApp : 2.0
Version du patch : 2.7**

Conformité à un profil de protection

**[BSI-PP-0005-2002],
Protection Profile – Secure Signature-Creation Device Type 2, version 1.04

[BSI-PP-0006-2002],
Protection Profile – Secure Signature-Creation Device Type 3, version 1.05**

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

Accords de reconnaissance applicables



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. <i>Identification du produit</i>	6
1.2.2. <i>Services de sécurité</i>	8
1.2.3. <i>Architecture</i>	9
1.2.4. <i>Cycle de vie</i>	9
1.2.5. <i>Configuration évaluée</i>	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.....	15
3. LA CERTIFICATION	16
3.1. CONCLUSION	16
3.2. RESTRICTIONS D’USAGE.....	16
3.3. RECONNAISSANCE DU CERTIFICAT	16
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	16
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	17
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT.....	18
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	19
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	21

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce « MultiApp v2 », pouvant être en mode contact ou dual. Le produit est développé par la société Gemalto et embarqué sur l'un des microcontrôleurs SLE66CLX360PEM m1588 k11/a15, SLE66CLX360PE m1587 k11/a15, SLE66CLX800PEM m1580 k11/a15, SLE66CLX800PE m1581 k11/a15, SLE66CX800PE m1599 k11/a15, SLE66CLX1440PEM m2090/a13, SLE66CLX1440PE m2091/a13 ou SLE66CX1440PE m2093/a13 fabriqués par la société Infineon Technologies AG.

Le produit évalué est composé :

- de l'applet IAS Classic v3 qui permet à l'utilisateur de signer électroniquement des données ;
- de la plateforme ouverte JavaCard MultiApp version 2.0 qui permet de charger des applets, durant la phase opérationnelle. Cette plateforme est certifiée par ailleurs sous la référence [ANSSI-CC-2011/10]

D'autres applications, en dehors du périmètre de cette évaluation, sont embarquées dans la ROM du produit, notamment l'application native eTravel EAC qui réalise les fonctions du passeport 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 est conforme aux profils de protection [BSI-PP-0005-2002] et [BSI-PP-0006-2002], adaptés à la version 3.1 des CC (ces PP ayant été rédigés selon la version 2.1 des CC).

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]).

Sur les produits utilisés lors de l'évaluation la commande GET DATA pour le tag 01 03 a donné la réponse suivante :

- **B0 85 xx yy vv 27 40 90 00 zz uu 00** 00

dont les éléments d'identification sont les suivants :

Microcontrôleurs de la famille SLE66C(L)X800 :

Nom de la famille	Java Card	B0
Nom du système d'exploitation	MultiApp ID v2.0	85
Numéro du masque	G211	2F
Nom du produit	Generic G211	29
Configuration du produit	vv = '0 1 i i 0 0 0 1' en binaire où i prend indifféremment pour valeur 0 ou 1	
Version du patch	version 2.7	27
Fabriquant du microcontrôleur	Infineon	40 90
Famille du microcontrôleur	SLE66C(L)X800	00 CF
Identifiant du sous-masque	SLE66CLX800PEM (G211)	00 00 pour G211
	SLE66CLX800PE (G211A)	0A 00 pour G211A
	SLE66CX800PE (G211B)	0B 00 pour G211B

Microcontrôleurs de la famille SLE66CLX360 :

Nom de la famille	Java Card	B0
Nom du système d'exploitation	MultiApp ID v2.0	85
Numéro du masque	G210	30
Nom du produit	Generic G210	30
Configuration du produit	vv = '0 1 i i 0 0 0 1' en binaire où i prend indifféremment pour valeur 0 ou 1	
Version du patch	version 2.7	27
Fabriquant du microcontrôleur	Infineon	40 90
Version du microcontrôleur	SLE66CLX360	00 CE
Identifiant du sous-masque	SLE66CLX360PEM (G210)	00 00 pour G210
	SLE66CLX360PE (G210A)	0A 00 pour G210A

Microcontrôleurs de la famille SLE66C(L)X1440 :

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	Generic G207	28
Configuration du produit	vv = '0 1 i i 0 0 0 1' en binaire où i prend indifféremment pour valeur 0 ou 1	
Version du patch	version 2.7	27
Fabriquant du microcontrôleur	Infineon	40 90
Version du microcontrôleur	SLE66C(L)X1440	00 E9
Identifiant du sous-masque	SLE66CLX1440PEM (G207)	00 00 pour G207
	SLE66CLX1440PE (G207A)	0A 00 pour G207A
	SLE66CX1440PE (G207B)	0B 00 pour G207B

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par ce produit sont :

- authentification du signataire par un code PIN ;
- génération des données de création et de vérification de signature ;
- import et stockage des données de création de signature ;
- export des données de vérification de signature ;
- création d'une signature électronique.

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

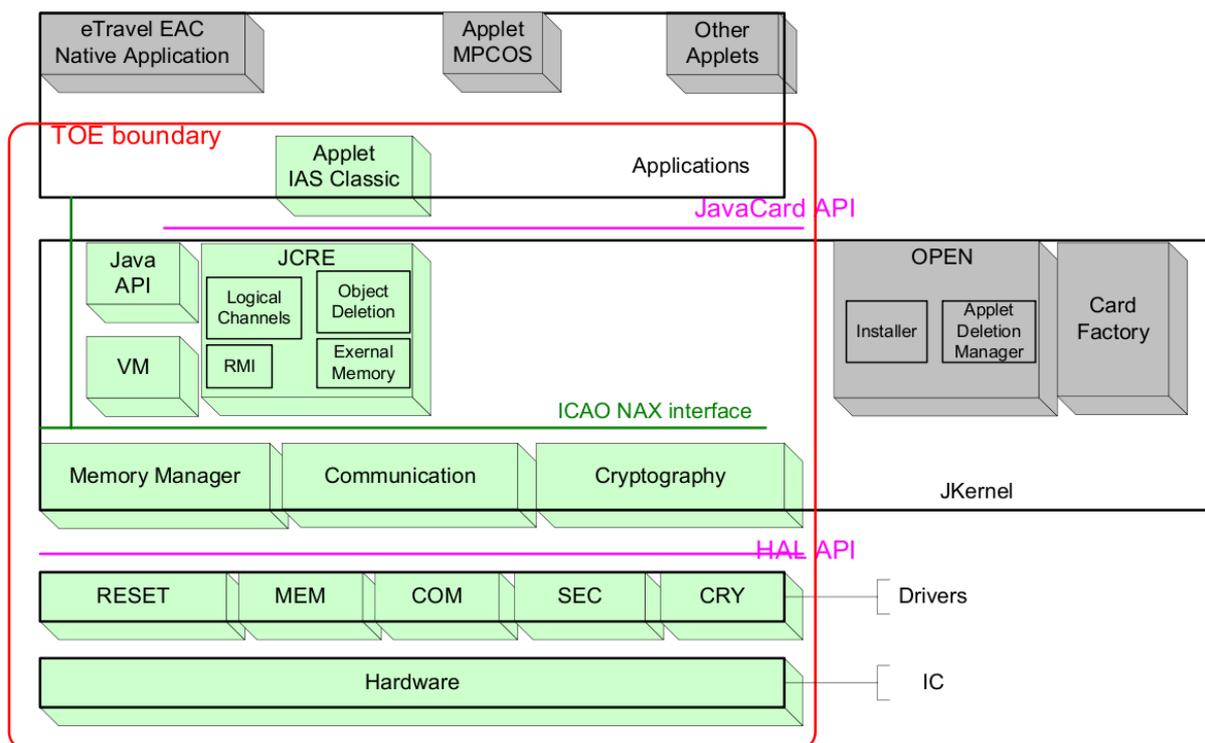


Figure 1 – Architecture et périmètre de la TOE

Le produit est une carte à puce constituée :

- d'un composant de la famille SLE66 fabriqué par Infineon Technologies ;
- d'un système d'exploitation sous forme d'une plateforme ouverte JavaCard : MultiApp version 2.0 ;
- de l'applet IAS Classic v3 permettant de signer électroniquement des données ;
- de l'application native passeport eTravel EAC, 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 s'est limitée aux étapes allant jusqu'à la fabrication de l'inlay.

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

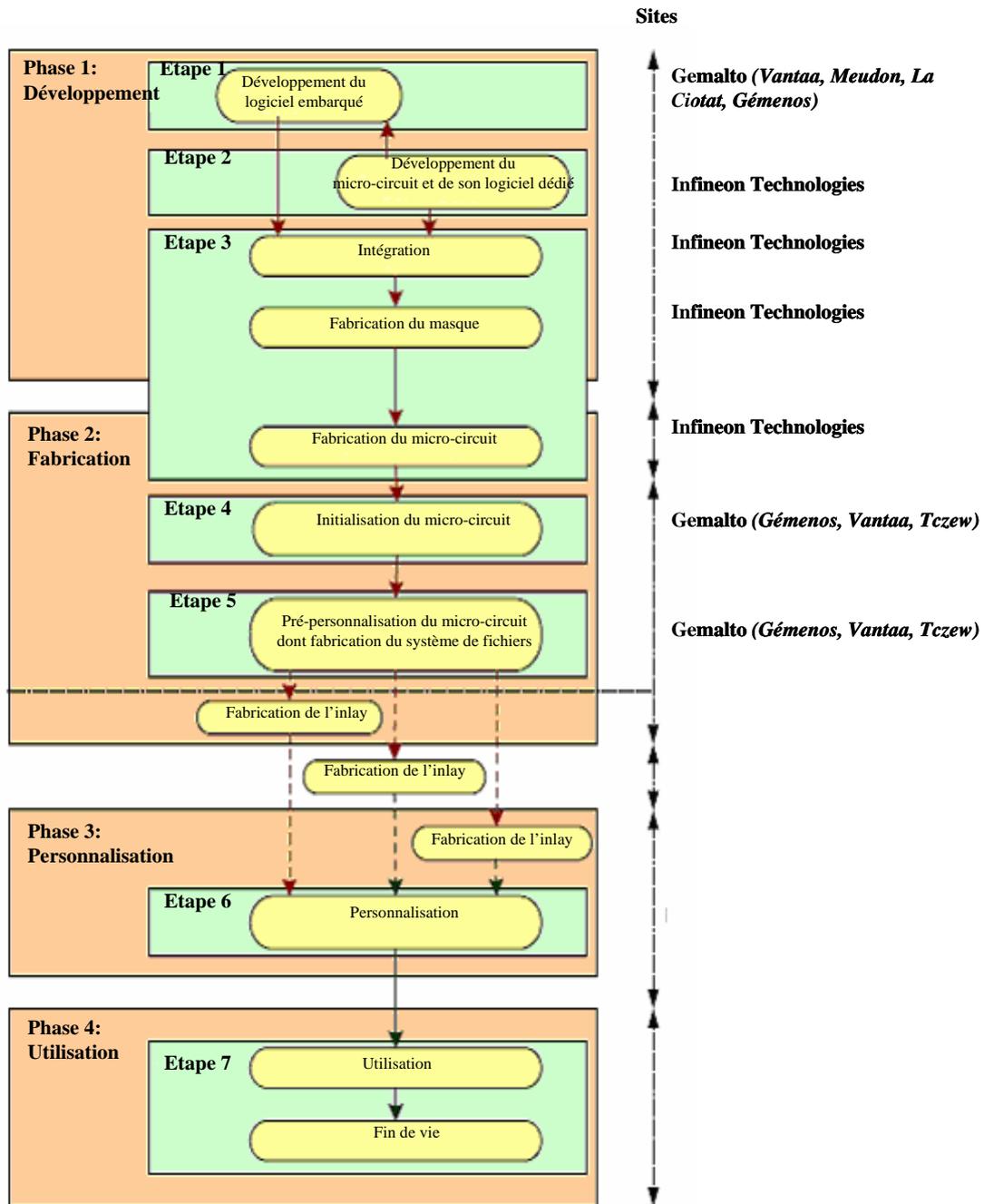


Figure 2 - Cycle de vie n° 1 : Initialisation du module sur le site de Gemalto

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 fabricant d'inlays.

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

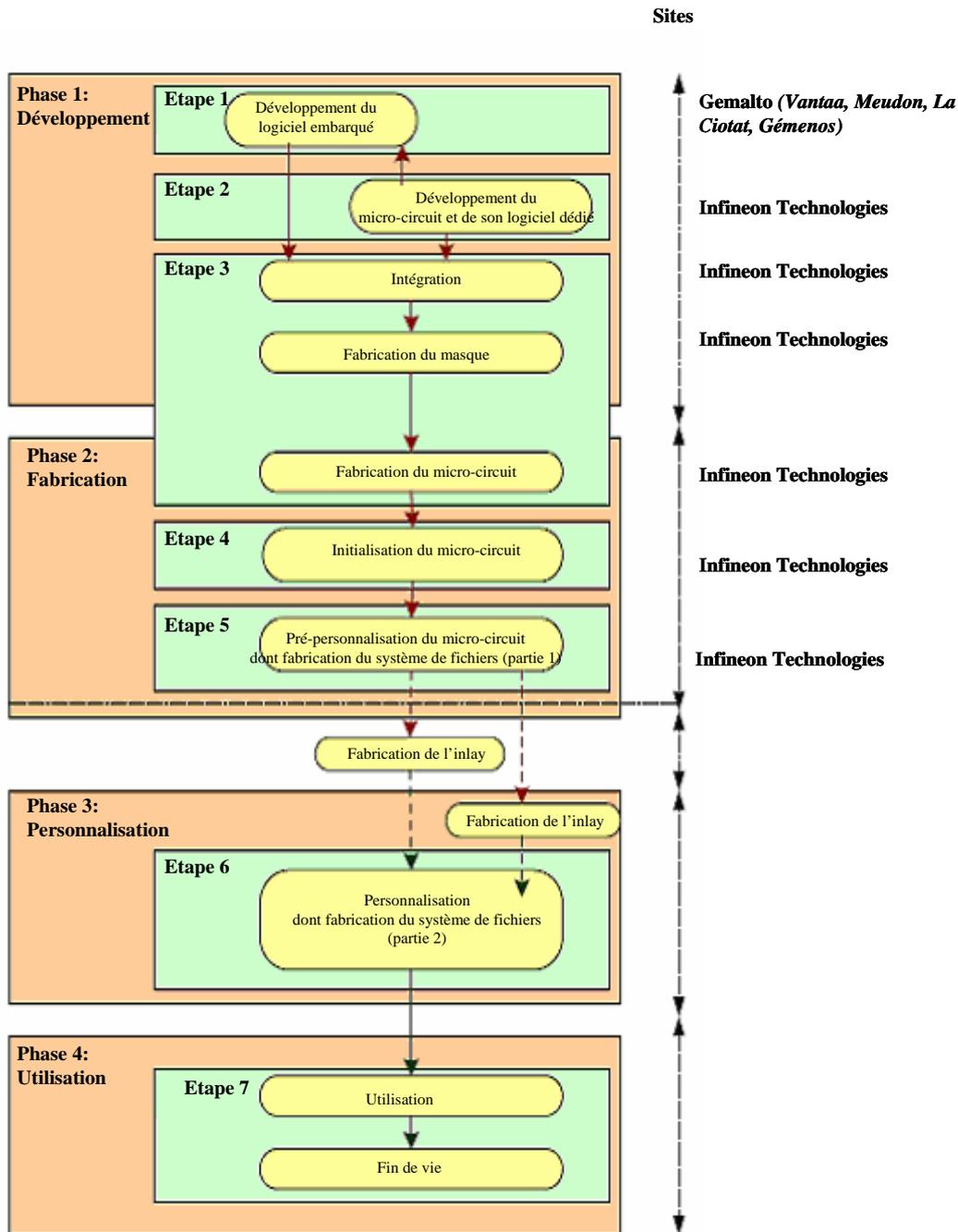


Figure 3 - Cycle de vie n° 2 : Initialisation du module sur le site du fondeur

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 patches, 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 :

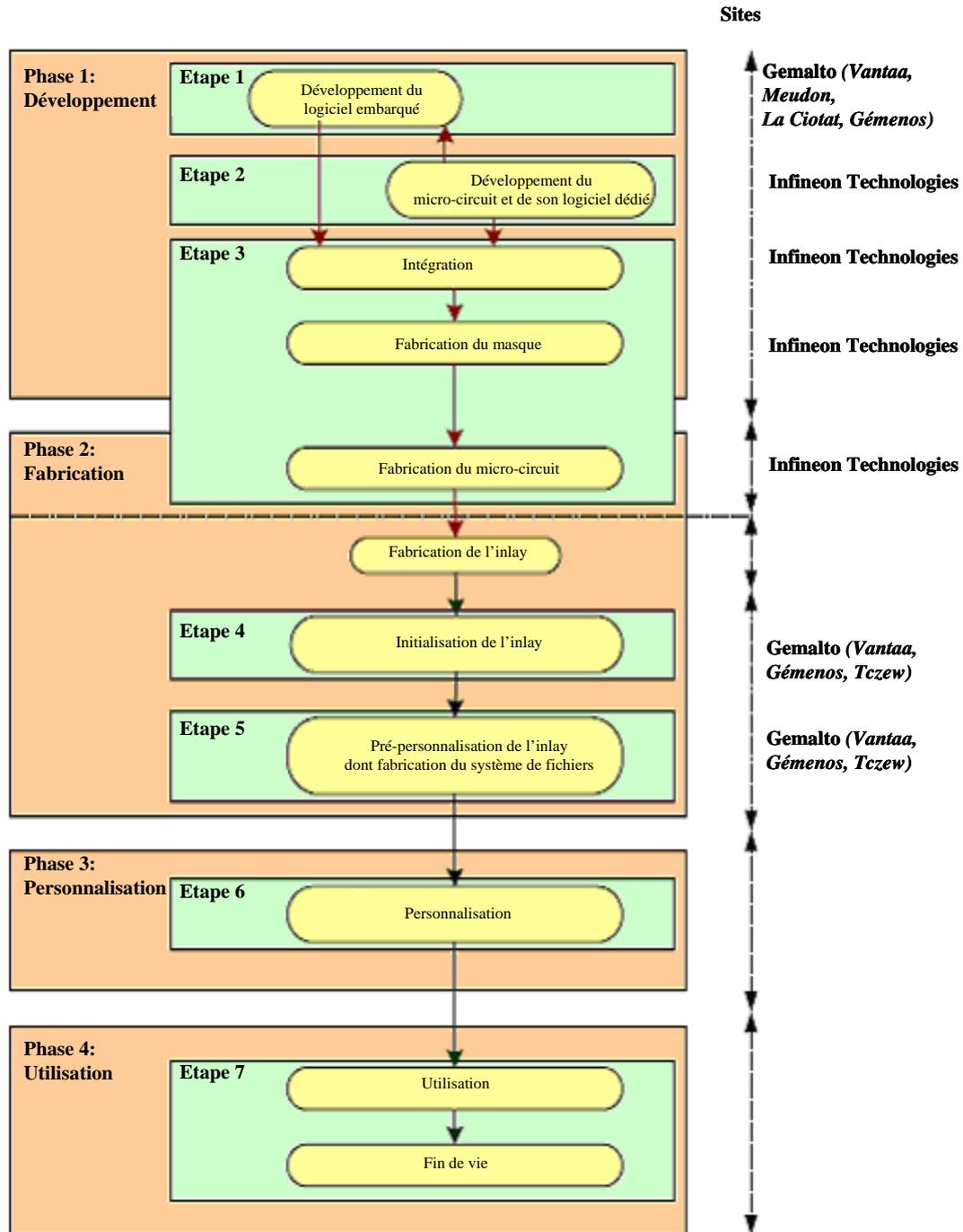


Figure 4 - Cycle de vie n° 3 : Initialisation sur inlay sur le site de Gemalto

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

Les composants sont développés et fabriqués par Infineon Technologies AG. Les sites de développement et de fabrication des puces Infineon sont détaillés dans les rapports de certification dont les références sont :

- [BSI-DSZ-CC-0523-2008] (pour les microcontrôleurs SLE66CLX1440PEM, SLE66CLX1440PE et SLE66CX1440PE) ;
- [BSI-DSZ-CC-0626-2009] (pour les microcontrôleurs SLE66CLX360PEM, SLE66CLX360PE, SLE66CLX800PEM, SLE66CLX800PE et SLE66CX800PE).

1.2.5. Configuration évaluée

Le certificat porte sur l'applet IAS Classic v3, version 1.0, chargée sur la plateforme ouverte JavaCard de la carte à puce MultiApp V2 masquée sur composants de la famille SLE66, telle que présentée plus haut, au paragraphe 1.2.1.

L'évaluateur a testé le produit sur les composants SLE66CLX800PEM et SLE66CLX1440PEM. Ces composants sont représentatifs de l'ensemble des références des composants à inclure dans la certification.

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.

Cette évaluation a ainsi pris en compte les résultats des évaluations des microcontrôleurs.

Les microcontrôleurs SLE66CLX1440PEM m2090/a12, SLE66CLX1440PE m2091/a12 et SLE66CX1440PE m2093/a12 ont été certifiés 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].

Les microcontrôleurs SLE66CLX1440PEM m2090/a13, SLE66CLX1440PE m2091/a13 et SLE66CX1440PE m2093/a13, utilisés dans le cadre de cette évaluation, et dont les différences avec les microcontrôleurs certifiés sous la référence [BSI-DSZ-CC-0523-2008] n'ont pas d'impact sur la sécurité, ont été ré-évalués au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4 et font l'objet d'un rapport de maintenance daté du 9 juin 2009 référencé [BSI-DSZ-CC-0523-2008-MA-01].

Les microcontrôleurs SLE66CLX360PEM, SLE66CLX360PE, SLE66CLX800PEM, SLE66CLX800PE et SLE66CX800PE ont été certifiés 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 19 novembre 2009, sous la référence [BSI-DSZ-CC-0626-2009].

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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 11 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 les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI [REF-CRY], [REF-KEY] et [REF-AUT] 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 des évaluations des microcontrôleurs (cf. [BSI-DSZ-CC-0523-2008] et [BSI-DSZ-CC-0626-2009]).

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'applet IAS Classic v3 de la carte à puce MultiApp V2 masquée sur les composants de la famille SLE66 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'accord¹, 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 signataires¹, 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	1	Security architecture description	
	ADV_FSP	1	2	3	4	5	5	6	4	4	Complete functional specification	
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF	
	ADV_INT					2	3	3				
	ADV_SPM						1	1				
	ADV_TDS		1	2	3	4	5	6	3	3	Basic modular design	
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance	
	AGD_PRE	1	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	4	Production support, acceptance procedures and automation	
	ALC_CMS	1	2	3	4	5	5	5	4	4	Problem tracking CM coverage	
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures	
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures	
	ALC_FLR											
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model	
	ALC_TAT				1	2	3	3	1	1	Well-defined development tools	
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims	
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition	
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction	
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives	
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements	
	ASE_SPD		1	1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage	
	ATE_DPT			1	1	3	3	4	1	1	Testing: basic design	
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing	
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample	
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis	

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - MultiApp V2 Cyllene : IAS Classic V3 Security Target Référence : D1132887 Version 1.1 du 7 juillet 2011 Gemalto <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - MultiApp V2 – IAS Classic V3 – Common Criteria / ISO 15408 – Security Target – Public version – EAL4+ Référence : D1201112 Version 1.1 du 8 juin 2011 Gemalto
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation Technical Report – CYLLENE Project Référence : CYLLENE_ETR_IAS_v1.2 Version 1.2 du 11 août 2011 Serma Technologies
[ANSSI-CC-2011/10]	<p>Rapport de certification ANSSI-CC-2011/10 – « Plateforme JavaCard en configuration ouverte de la carte à puce MultiApp V2 masquée sur composants de la famille SLE66 » <i>Certifié par l'ANSSI le 28 avril 2011.</i></p>
[CONF]	<p>Liste de configuration :</p> <ul style="list-style-type: none"> - MultiApp V2 Cyllene : ALC Configuration List Référence : D1154123 Version 0.7 du 26 novembre 2010 Gemalto
[GUIDES]	<p>Guide d'administration du produit :</p> <ul style="list-style-type: none"> - MultiApp v2 – CYLLENE : IAS Preparation procedures Référence : D1144772 Version 0.7 du 28 mars 2011 Gemalto <p>Guide d'utilisation du produit :</p> <ul style="list-style-type: none"> - MultiAppID v2 – CYLLENE : Operational User Guide Référence : D1144771 Version 0.6 du 28 mars 2011 Gemalto - IAS Classic Applet V3 – Reference Manual Référence : DOC116499F du 20 avril 2010 Gemalto
[BSI-PP-0005-2002]	<p>Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0005-2002.</i></p>

[BSI-PP-0006-2002]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. <i>Certifié par le BSI sous la référence BSI-PP-0006-2002.</i>
[BSI-PP-0002-2001]	Protection Profile, Smart card IC Platform Protection Profile Version: 1.0, July 2001. <i>Certifié par le BSI sous la référence BSI-PP-0002-2001.</i>
[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. <i>Certifié par le BSI le 6 novembre 2008.</i>
[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. <i>Maintenu par le BSI le 9 juin 2009.</i>
[BSI-DSZ-CC-0626-2009]	Infineon Smart Card IC (Security Controller) SLE66CLX800PE m1581-k11/a15, SLE66CLX800PEM m1580-k11/a15, SLE66CLX800PES m1582-k11/a15, SLE66CX800PE m1599-k11/a15, SLE66CLX360PE m1587-k11/a15, SLE66CLX360PEM m1588-k11/a15, SLE66CLX360PES m1589-k11/a15, SLE66CLX180PE m2080-a15, SLE66CLX180PEM m2081-a15, SLE66CLX120PE m2082-a15, SLE66CLX120PEM m2083-a15 all with optional libraries RSA V1.6 and EC V1.1 and SHA-2 V1.0 all with specific IC dedicated software. <i>Certifié par le BSI le 19 novembre 2009.</i>

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, voir www.ssi.gouv.fr
[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008, voir www.ssi.gouv.fr
[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010, voir www.ssi.gouv.fr