



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-2014/06

Plateforme Java Card en configuration ouverte de la carte à puce MultiApp V3 masquée sur le composant M7820 A11

(Version du patch : 1.5)

Paris, le 3 février 2014

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

Contre-amiral Dominique RIBAN
[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-2014/06

Nom du produit

**Plateforme Java Card en configuration ouverte de
la carte à puce MultiApp V3 masquée sur le
composant M7820 A11**

Référence/version du produit

**Version de la plateforme Java Card MultiApp : 3.0
Version du patch : 1.5**

Conformité à un profil de protection

**ANSSI-CC-PP-2010/03-M01 [PP JCS]
Java Card System – Open Configuration, version 3.0**

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

**EAL 5 augmenté
ALC_DVS.2, AVA_VAN.5**

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

Serma Technologies
14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

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>Introduction</i>	6
1.2.2. <i>Identification du produit</i>	6
1.2.3. <i>Services de sécurité</i>	7
1.2.4. <i>Architecture</i>	8
1.2.5. <i>Cycle de vie</i>	8
1.2.6. <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	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	16
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	16
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	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

L'évaluation porte sur la plateforme ouverte Java Card du produit « MultiApp V3 » qui est une carte à puce pouvant être en mode contact ou sans-contact. Le produit est développé par la société Gemalto et embarqué sur le microcontrôleur M7820 A11 fabriqué par la société Infineon Technologies.

La plateforme ouverte Java Card est destinée à fournir des services de sécurité aux applets qui seront installées sur la carte.

D'autres applications, en dehors du périmètre de cette évaluation, sont embarquées dans la ROM du produit (voir [GUIDES]), notamment :

- l'application native passeport eTravel EAC ;
- l'application native passeport eTravel SAC ;
- l'applet IAS Classic v4 destinée à faire de la signature électronique ;
- l'application « MOCA Server » (application de *Match On Card*).

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 JCS]. Bien que le [PP JCS] réclame une conformité démontrable, la conformité stricte de la cible de sécurité [ST] au [PP JCS] a été choisie afin que des objectifs sur l'environnement opérationnel du [PP JCS] soient inclus dans les objectifs sur la TOE (*Target of Evaluation* – Cible d'évaluation). Autrement dit, dans cette [ST], la TOE réalise davantage que ce qui est requis par le [PP JCS].

1.2.2. 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 donnée par le produit à la commande GET DATA (voir [GUIDES]). La commande GET DATA permet aussi à l'utilisateur d'identifier quelles applications sont actives dans le produit à sa disposition.



Sur le produit utilisé lors de l'évaluation, la commande GET DATA pour le tag '01 03' donne la réponse '**B0 85 43 3F x1 15 40 90 71 64** 00 A0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00', dont les éléments d'identification sont les suivants :

Nom de la famille	Java Card	B0
Nom du système d'exploitation	MultiApp ID	85
Numéro du masque	G260	43
Nom du produit	MultiApp ID V3.0 Combi 160K	3F
Configurations du produit	Configuration Plateforme Java Card ouverte seule	x1 = 11
	Configuration Plateforme Java Card ouverte + applet IAS activée	x1 = 31
	Configuration Plateforme Java Card ouverte + application eTravel activée	x1 = 51
	Configuration Plateforme Java Card ouverte + application eTravel + applet IAS activées	x1 = 71
Version du patch	Version 1.5	15
Fabricant du microcontrôleur	Infineon	40 90
Version du microcontrôleur	SLE78CLX1600P	71 64

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par la plateforme ouverte Java Card sont :

- l'initialisation du *Card Manager* et la gestion du cycle de vie de la carte ;
- l'installation, le chargement et « l'extradition » d'applets par le *Card Manager* (« l'extradition » permet de modifier le domaine de sécurité associé à une application) ;
- la suppression d'applications sous le contrôle du *Card Manager* ;
- le pare-feu permettant le cloisonnement des applets ;
- l'interface de programmation permettant d'opérer de manière sûre les applications.

Les services de sécurité offerts par le microcontrôleur sont :

- SF_DPM : la gestion sécurisée du cycle de vie ;
- SF_PS : la protection contre les écoutes illicites (« *snooping* ») ;
- SF_PMA : la protection contre les attaques par fautes ;
- SF_PLA : la protection contre les attaques logiques ;
- SF_CS : le support cryptographique.

1.2.4. Architecture

La plateforme Java Card de la carte MultiApp V3 est constituée des éléments suivants :

- le microcontrôleur M7820 A11, offrant les fonctionnalités matérielles (gestion de la mémoire et gestion des entrées/sorties), et sa librairie cryptographique ;
- une partie native composée des éléments suivants :
 - o un gestionnaire de mémoire *Memory Manager* ;
 - o un gestionnaire de communication *Communication (I/O)* ;
 - o un gestionnaire de librairies cryptographiques *Crypto Libs* ;
- un système Java Card (JCS : *Java Card System*) composé des éléments suivants :
 - o un environnement *Runtime* (JCRE) ;
 - o une machine virtuelle Java (*Virtual Machine*) ;
 - o une interface de programmation (API) contenant notamment le paquet propriétaire « *com.gemalto.javacardx.pace* » ;
 - o un gestionnaire d'applications (*Card Manager*).

Cette architecture est résumée dans la figure suivante :

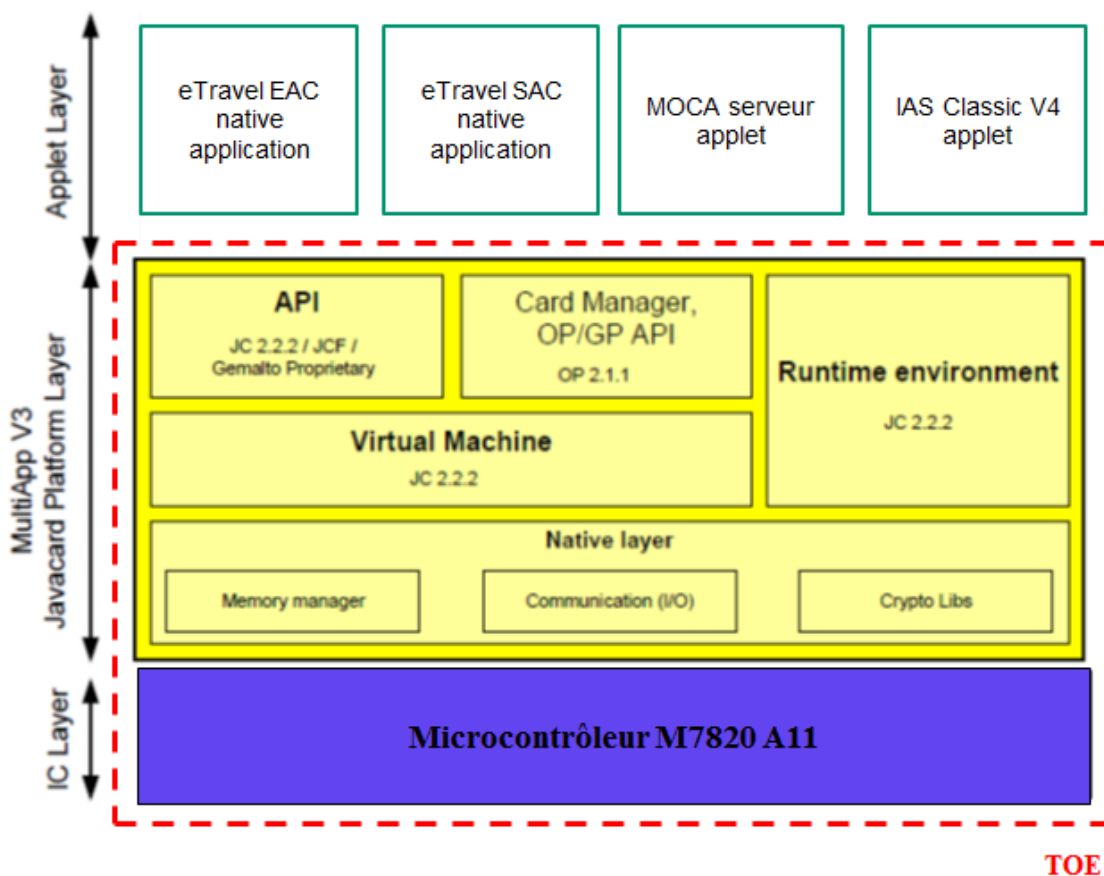


Figure 1 - Architecture et périmètre de la TOE

1.2.5. Cycle de vie

Le produit est proposé avec trois cycles de vie possibles qui sont explicités ci-après.

Pour chacun des cycles de vie, l'évaluation se limite aux étapes 1 à 5 correspondant aux phases 1 et 2, respectivement phase de développement et phase de fabrication.

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

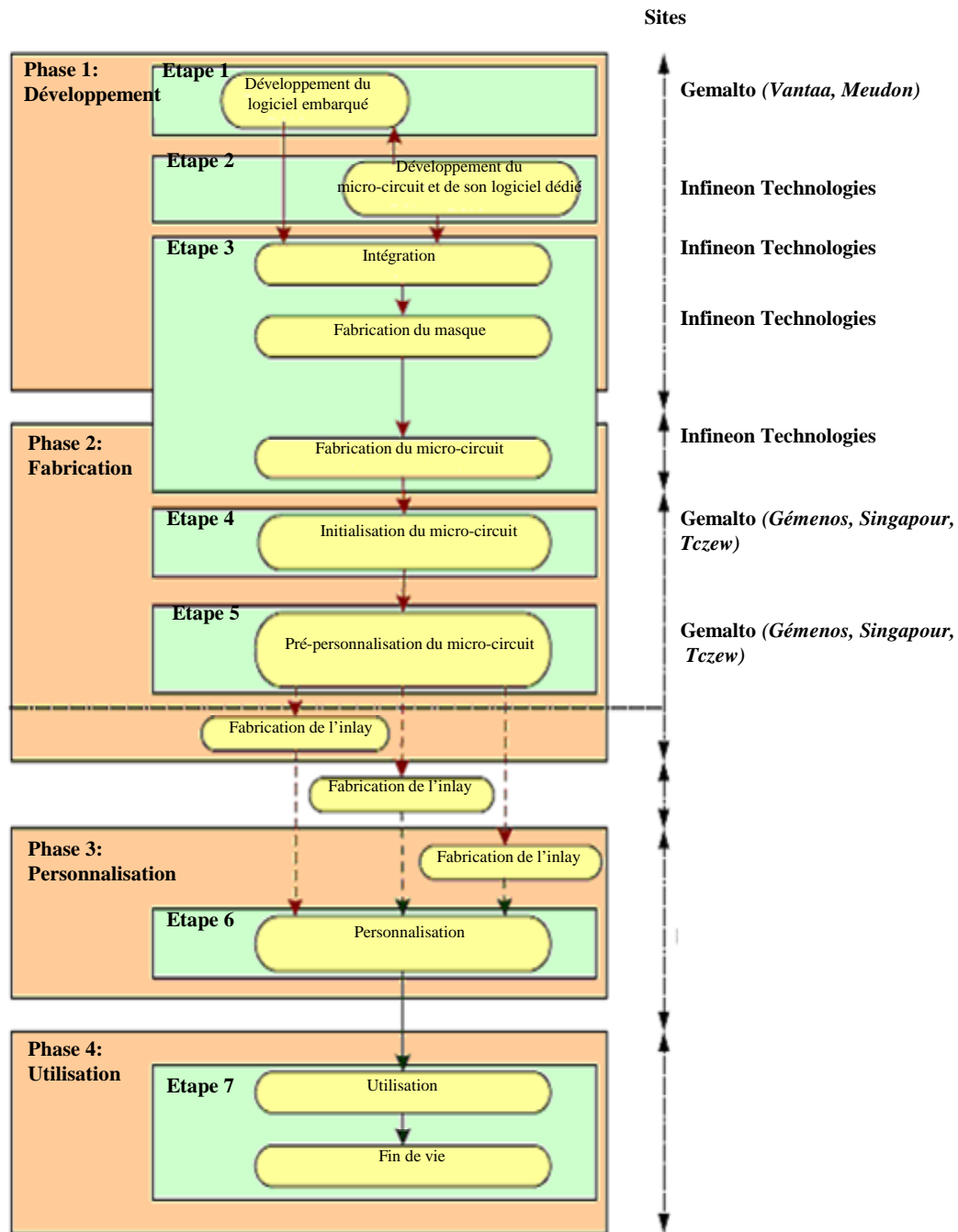


Figure 2 - Cycle de vie n° 1 : Initialisation du module sur le site de Gemalto

Le cycle de vie n° 1 décrit le cycle de vie standard. Le module est fabriqué sur le site du fondeur. Il est ensuite envoyé sur le site de Gemalto où il est initialisé et pré-personnalisé. Puis il est envoyé au personnalisateur, soit directement et dans ce cas le personnalisateur fabrique l'inlay, soit après que Gemalto ait fabriqué l'inlay, soit après être passé par le fabricant d'inlays (autre que Gemalto).

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

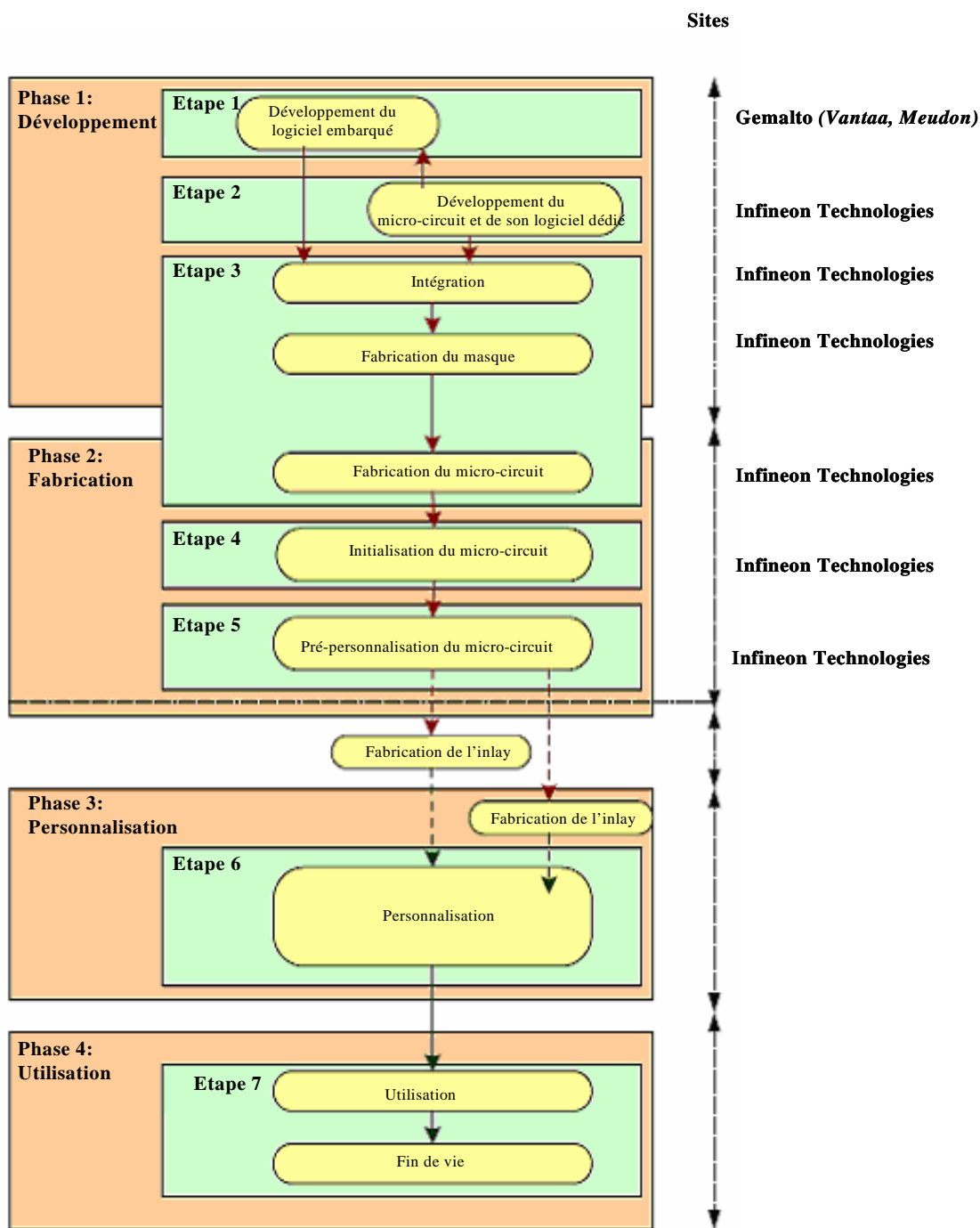


Figure 3 - Cycle de vie n° 2 : Initialisation du module sur le site du fondeur

Le cycle de vie n° 2 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 patches, sont réalisées sur le site du fondeur.

Cycle de vie n° 3 : Initialisation sur *inlay* sur le site de Gemalto :

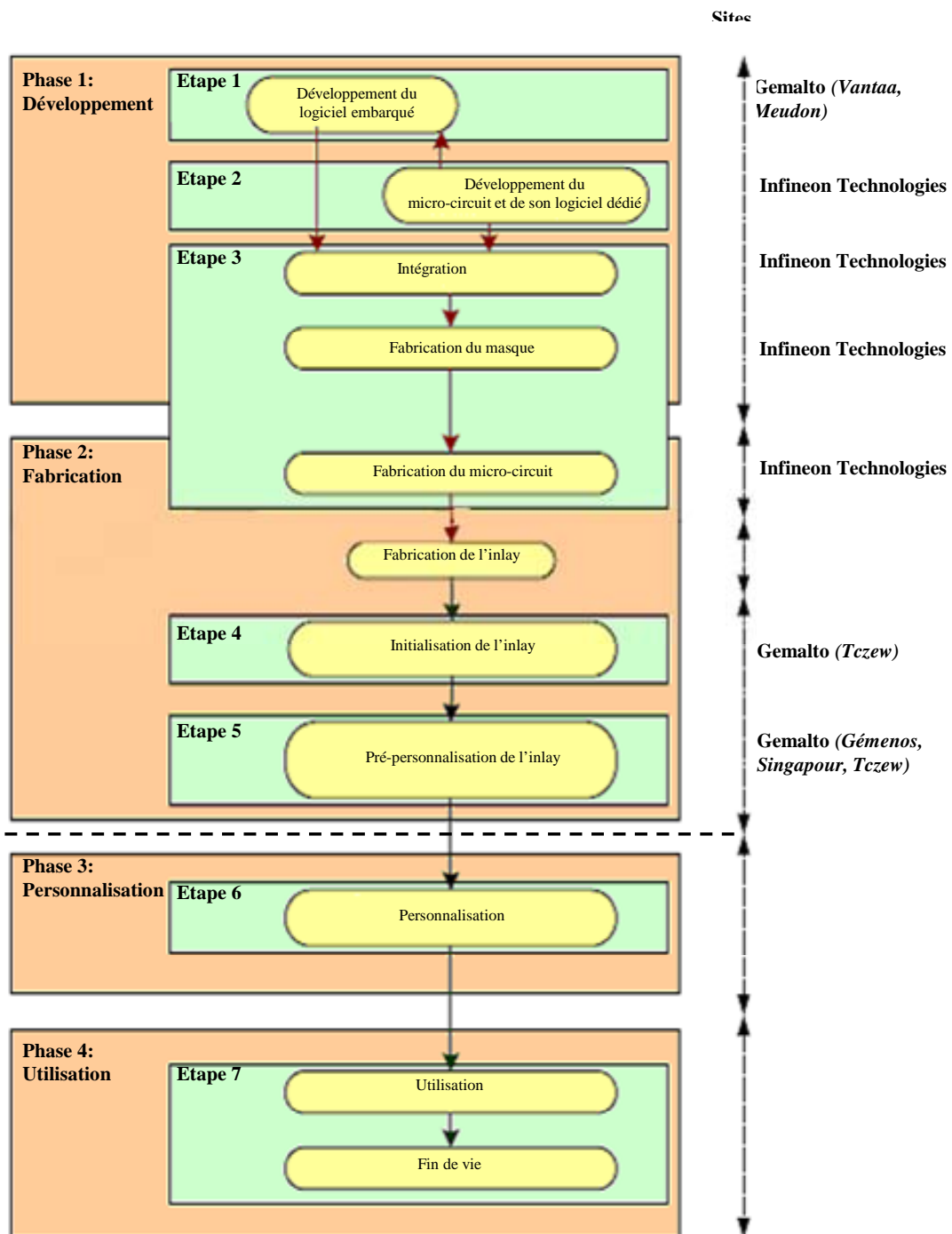


Figure 4 - Cycle de vie n° 3 : Initialisation sur *inlay* sur le site de Gemalto

Le cycle de vie n° 3 correspond au cas où Gemalto souhaite recevoir du fondeur des *inlays* plutôt que des modules. Dans ce cas, le fondeur envoie les *inlays* à Gemalto.

Le produit a été développé sur les sites suivants :

Gemalto

Myllynkivenkuja 4
FI-01620 Vantaa
Finlande

Gemalto

12 Ayer Rajah Crescent
Singapor 139941
Singapour

Gemalto

6 Rue de la Verrerie
92190 Meudon
France

Gemalto

Avenue du Pic de Bertagne
13881 Gémenos
France

Gemalto

Ul. Skarszewska 2
33-110 Tczew
Pologne

Le microcontrôleur est développé et fabriqué par Infineon Technologies. Les sites de développement et de fabrication du microcontrôleur sont détaillés dans le rapport de certification dont la référence est [BSI-DSZ-CC-0829-2012].

Le cycle de vie de la plateforme Java Card (la TOE) est une partie du cycle de vie du produit.

Il est composé de quatre étapes :

- développement ;
- stockage, pré-personnalisation et test ;
- personnalisation et test ;
- usage final.

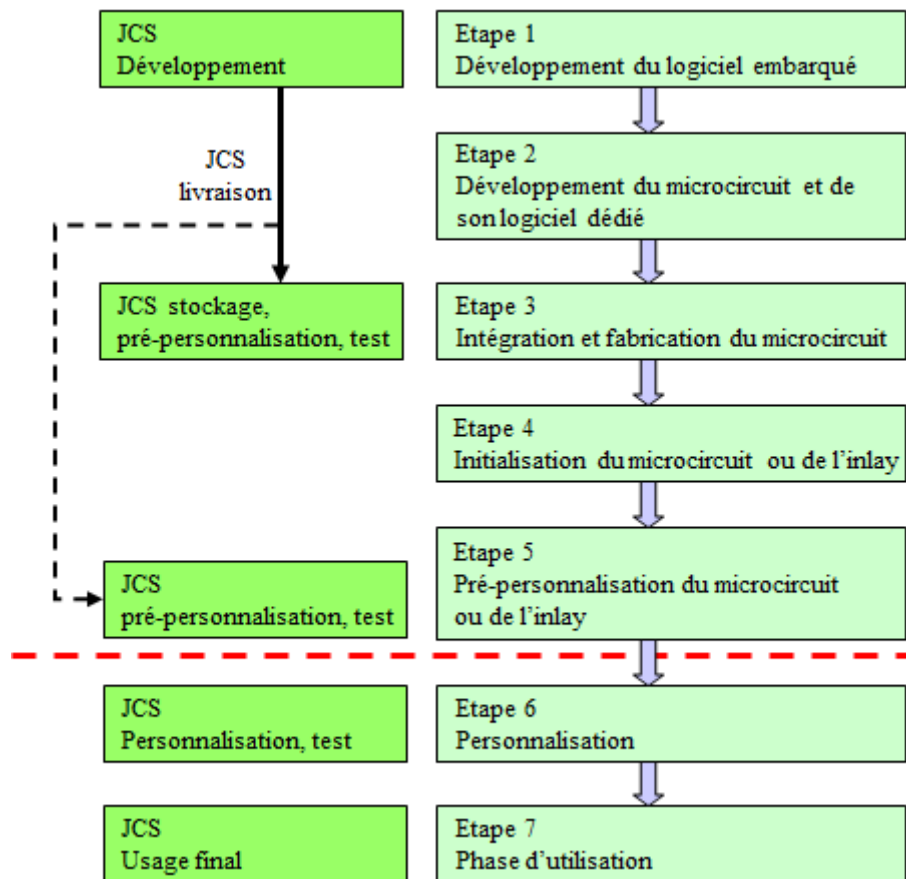


Figure 5 - Cycle de vie de la plateforme Java Card dans le cycle de vie du produit

Pour l'évaluation, l'évaluateur a considéré comme administrateurs du produit le pré-personnalisateur, le personnalisateur et le gestionnaire de la carte chargés de l'administration de la carte, et comme utilisateurs du produit les développeurs des applications à charger sur la plateforme.

1.2.6. Configuration évaluée

Le certificat porte sur la plateforme ouverte Java Card seule, telle que présentée plus haut, au paragraphe « 1.2.4 Architecture », et configurée conformément au guide de personnalisation (voir [GUIDES]). La plateforme ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications réalisé selon les processus audités ne remet pas en cause le présent rapport de certification.

L'évaluateur a testé la plateforme Java Card masquée sur le composant M7820 A11 dans sa version SLE78CLX1600P.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 4** [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 [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.

Le microcontrôleur M7820 A11 a été certifié au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conformément au profil de protection [BSI-PP-0035-2007], le 5 septembre 2012 sous la référence [BSI-DSZ-CC-0829-2012].

L'évaluation s'appuie sur les résultats de l'évaluation du produit « Plateforme Java Card en configuration ouverte de la carte à puce MultiApp V3 masquée sur le composant M7820 A11 » (version du patch : 1.3) certifié le 10 mai 2013 sous la référence [ANSSI-CC-2013/32].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 3 septembre 2013, 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 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.5 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 (voir [BSI-DSZ-CC-0829-2012]).



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 la « Plateforme Java Card en configuration ouverte de la carte à puce MultiApp V3 masquée sur le composant M7820 A11 » (version du patch : 1.5) soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

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].

Plus particulièrement, toutes les applications qui seront chargées sur la carte (qu'elles soient certifiées ou non) devront satisfaire l'ensemble des contraintes et exigences relatives aux propriétés de cloisonnement d'applications, imposées par la plateforme, avant leur installation effective (voir [GUIDES_APP]).

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 :



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 signataires², 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 5+	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	5	Complete semi-formal functional specification with additional error information
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3	2	Well-structured internals
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	4	Semiformal 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	5	Development tools 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	2	Compliance with implementation standards
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	3	Testing: modular design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - MultiApp V3 Cyllene3 JCS Security Target, Référence : ST_D1184308, Version 1.2 du 24 janvier 2013, 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 V3 JCS Security Target, Référence : ST_D1184308, Version 1.2p du 6 mai 2013, Gemalto.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation Technical Report – CYLLENE3 Project, Référence : CYLLENE3_ETR_JCS_v2.1, Version 2.1 du 3 septembre 2013, Serma Technologies.
[CONF]	<p>Listes de configuration :</p> <ul style="list-style-type: none"> - LIS: Configuration List for platform, Référence : D1288947, version 1.0 du 12/02/2013, Gemalto. - D1288947-LIS-PLF-DOCUMENT, version 1.3 du 28/08/2013, Gemalto. - LIS_filter-dev.txt, build/project.pj (1.35), Gemalto. - LIS_MASK_LABEL-dev.txt, build/project.pj (1.51), Gemalto.
[GUIDES]	<ul style="list-style-type: none"> - MultiApp ID V3 Software – AGD_PRE document – JavaCard Platform, Référence : D1283210, version 1.1 du 25/06/2013, Gemalto. - MultiApp ID V3 Software – AGD_OPE document – JavaCard Platform, Référence : D1283373, version 1.2 du 25/06/2013, Gemalto. - MultiApp ID Operating System – Reference Manual, Référence : D1203727, version du 19 mars 2013, Gemalto.



[GUIDES_APP]	<ul style="list-style-type: none"> - Rules for applications on Multiapp certified product, Référence : D1280572, version A00 de décembre 2012, Gemalto. - Guidance for secure application development on Multiapp platforms, Référence : D1280580, version A00 de décembre 2012, Gemalto. - Verification process of Third Party non sensitive applet loaded in pre-issuance, Référence : D1283120, version A00 de janvier 2012, Gemalto. - Verification process of Gemalto non sensitive applet loaded in pre-issuance, Référence : D1283121, version A01 de juin 2013, Gemalto.
[PP JCS]	<p>“Java Card Protection Profile – Open Configuration”, version 3.0, 18 mai 2012. <i>Maintenu par l’ANSSI sous la référence ANSSI-CC-PP-2010/03-M01.</i></p>
[BSI-PP-0035-2007]	<p>Security IC Platform Protection Profile, version 1.0, août 2007. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.</i></p>
[BSI-DSZ-CC-0829-2012]	<p>Infineon smart card IC (Security Controller) M7820 A11 and M11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software. <i>Certifié par le BSI le 5 septembre 2012 sous la référence BSI-DSZ-CC- 0829-2012.</i></p>
[ANSSI-CC-2013/32]	<p>Plateforme Java Card en configuration ouverte de la carte à puce MultiApp V3 masquée sur le composant M7820 A11. <i>Certifié par l’ANSSI le 10 mai 2013 sous la référence ANSSI-CC- 2013/32.</i></p>

Annexe 3. Références liées à la certification

<p>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.</p>	
[CER/P/01]	<p>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.</p>
[CC]	<p>Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, révision 4, ref CCMB-2012-09-004.</p>
[CC IC]	<p>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.</p>
[JIWG AP]*	<p>Joint Interpretation Library – Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, January 2013.</p>
[COMP]*	<p>Joint Interpretation Library – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.</p>
[OPEN]*	<p>Joint Interpretation Library – Certification of « open » smart card products, version 1.1 (for trial use), 4 February 2013.</p>
[CC RA]	<p>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.</p>
[SOG-IS]	<p>« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.</p>
[REF]	<p>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.</p>

* Document du SOG-IS ; dans le cadre de l'accord de reconnaissance du CCRA, le document support du CCRA équivalent s'applique.