



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-2012/09
eTravel EAC v1.2 masquée sur le composant
S3CC9LC

Paris, le 16 mars 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 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.

<i>Référence du rapport de certification</i> ANSSI-CC-2012/09	
<i>Nom du produit</i> eTravel EAC v1.2 masquée sur le composant S3CC9LC	
<i>Référence/version du produit</i> T1004548 avec softmask S1081425 révision 01 02	
<i>Conformité à un profil de protection</i> BSI-PP-0026, [PP EAC], version 1.2 Protection Profile – Machine Readable Travel Document with ICAO application, Extended Access Control	
<i>Critères d'évaluation et version</i> Critères Communs version 2.3 conforme à la norme ISO 15408:2005	
<i>Niveau d'évaluation</i> EAL 4 augmenté ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4	
<i>Développeur(s)</i> Gemalto 6 rue de la Verrerie, 92197 Meudon cedex, France	Samsung Electronics La Boursidière, RN 186, Bâtiment Jura, BP 202, 92357 Le Plessis-Robinson, France
<i>Commanditaire</i> Gemalto 6 rue de la Verrerie, 92197 Meudon cedex, France	
<i>Centre d'évaluation</i> Serma Technologies 30 avenue Gustave Eiffel, 33608 Pessac, France	
<i>Accords de reconnaissance applicables</i>   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>	7
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Cycle de vie</i>	8
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 « eTravel EAC v1.2 masquée sur le composant S3CC9LC » développée par la société Gemalto. Le microcontrôleur est développé et fabriqué par la société Samsung Electronics.

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

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

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

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité est conforme au profil de protection [PP EAC].

1.2.1. Identification du produit

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

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

Eléments de configuration		Origine
Nom commercial	eTravel v1.2	Gemalto
Référence de la TOE (label interne)	T1004548 avec softmask S1081425 révision 01 02	Gemalto
Référence de la TOE (label de l'IC)	S3CC9LC	Samsung Electronics
Référence du système d'exploitation	1.2	Gemalto
Référence du softmask	01 02	Gemalto
Identification de l'IC	S3CC9LC revision 11	Samsung Electronics

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 = **42 50** (Samsung Electronics)
- IC TYPE = **33 72** (S3CC9LC)
- OPERATING SYSTEM IDENTIFIER = **D0 00 AC**
- OPERATING SYSTEM RELEASE LEVEL = **01 02**

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par ce produit sont :

- contrôle d'accès ;
- mécanisme d'authentification mutuelle ;
- mécanisme de « *secure messaging* » ;
- authentification du microcontrôleur ;
- validité de la chaîne de certificats ;
- mécanisme d'authentification asymétrique.

Les principaux services de sécurité fournis par le microcontrôleur sont :

- SF.1 : détection, enregistrement et réaction aux attaques environnementales ;
- SF.2 : contrôle d'accès ;
- SF.3 : non-réversibilité des modes « TEST » et « NORMAL » ;
- SF.4 : contre-mesures matérielles pour la non-observabilité ;
- SF.5 : cryptographie.

1.2.3. Architecture

Le produit est constitué du microcontrôleur S3CC9LC, du logiciel embarqué, comprenant les tests et la gestion des commandes et des données, et de la structure logique des données.

La figure suivante résume l'architecture du produit évalué :

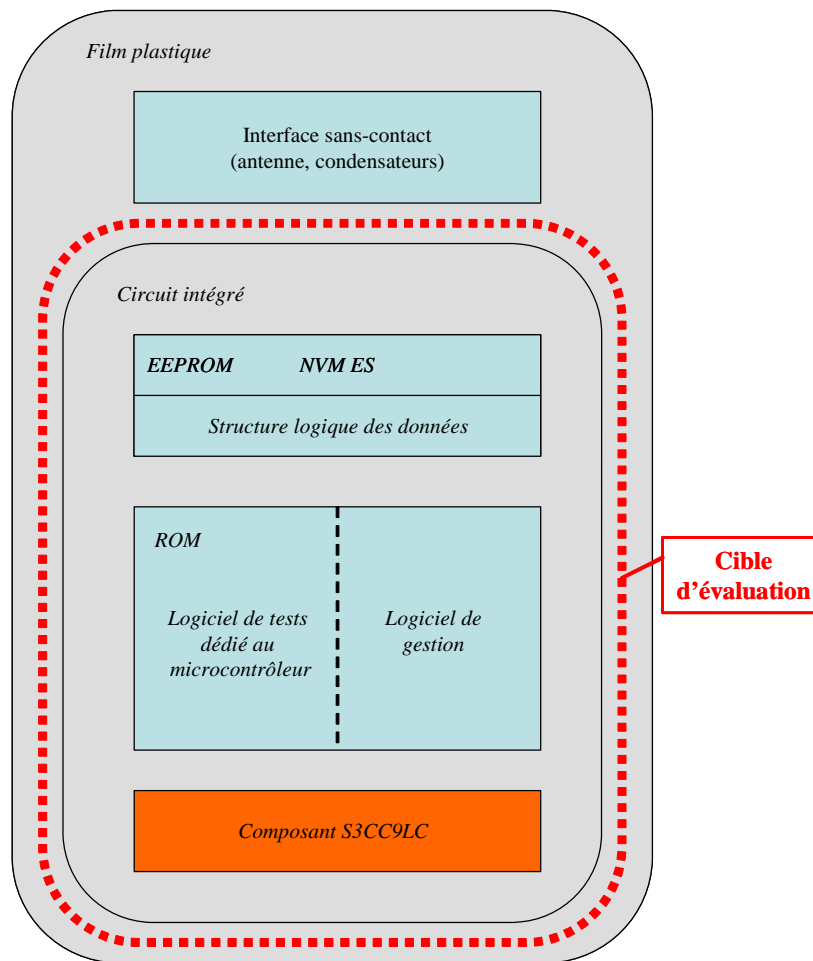


Figure 1 - Architecture du produit

1.2.4. Cycle de vie

Le produit a trois cycles de vie possibles, qui sont explicités ci-dessous.

Pour chacun des cycles de vie, l'évaluation se limite aux étapes allant jusqu'à la fabrication de l'inlay, fabrication non incluse.

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

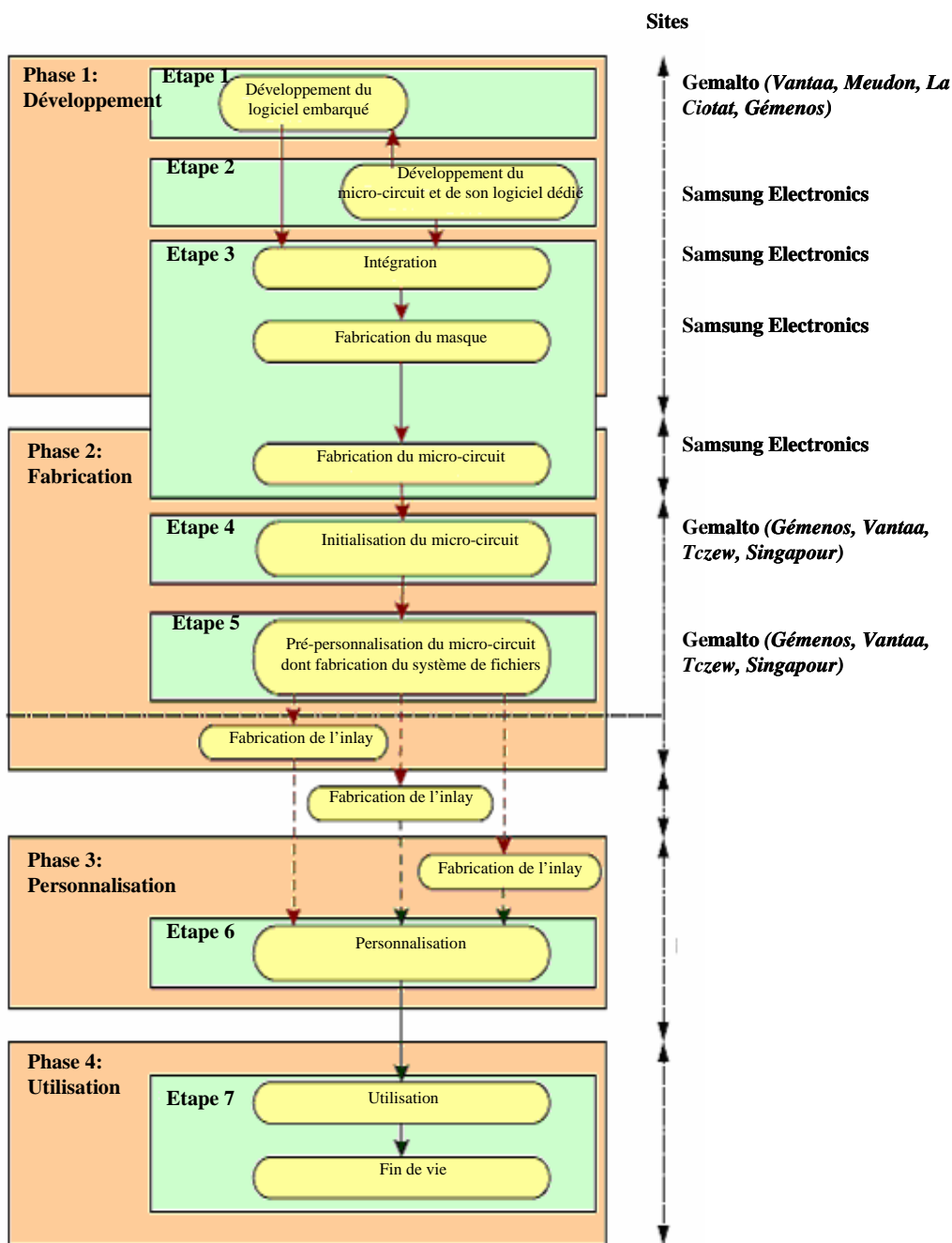


Figure 2 - Cycle de vie n° 1 : Initialisation du module sur le site de Gemalto

Le cycle de vie n° 1 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.

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

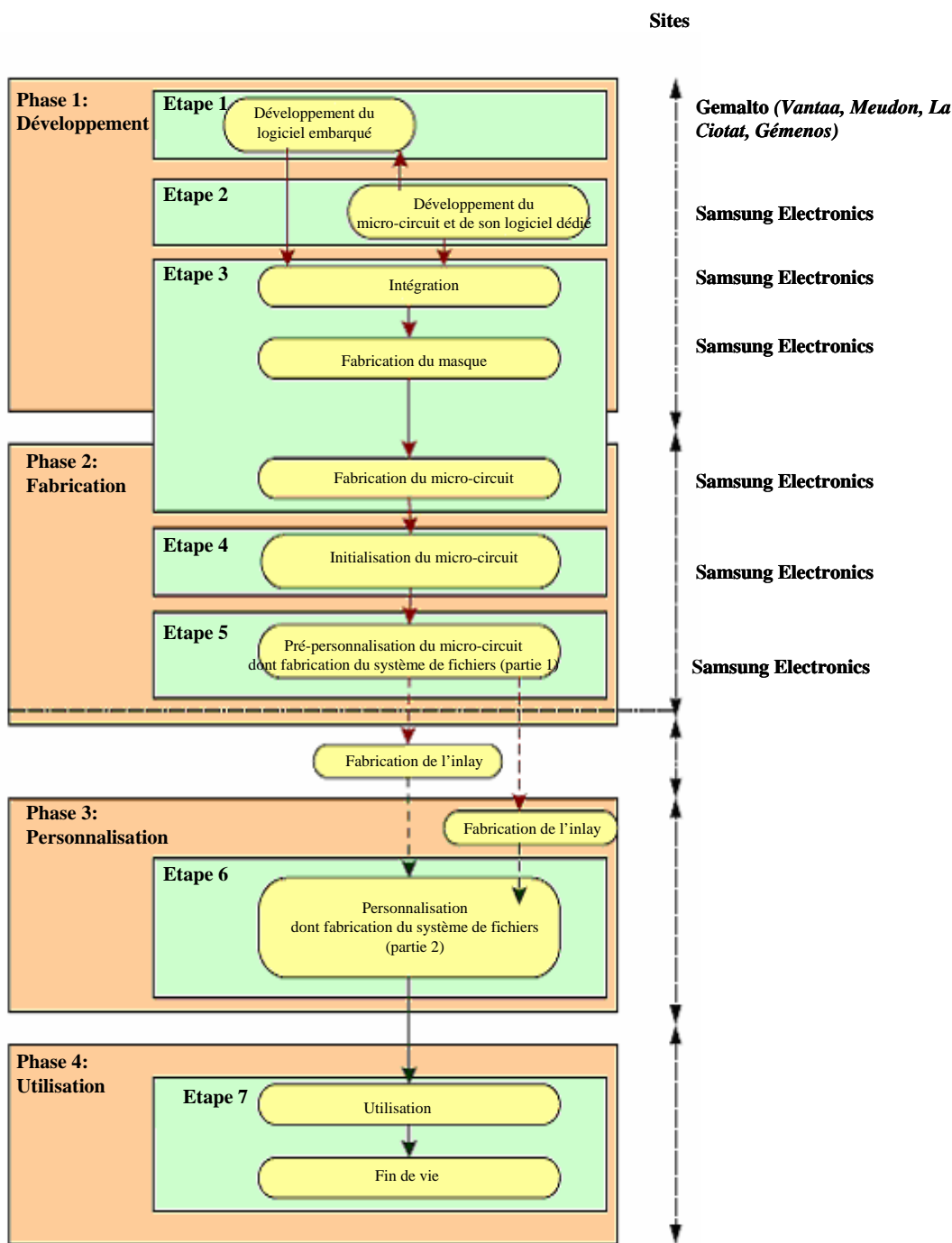


Figure 3 - Cycle de vie n° 2 : Initialisation du module sur le site du fondeur

Le cycle de vie n° 2 est une alternative au cycle de vie n° 1. Il 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. 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 :

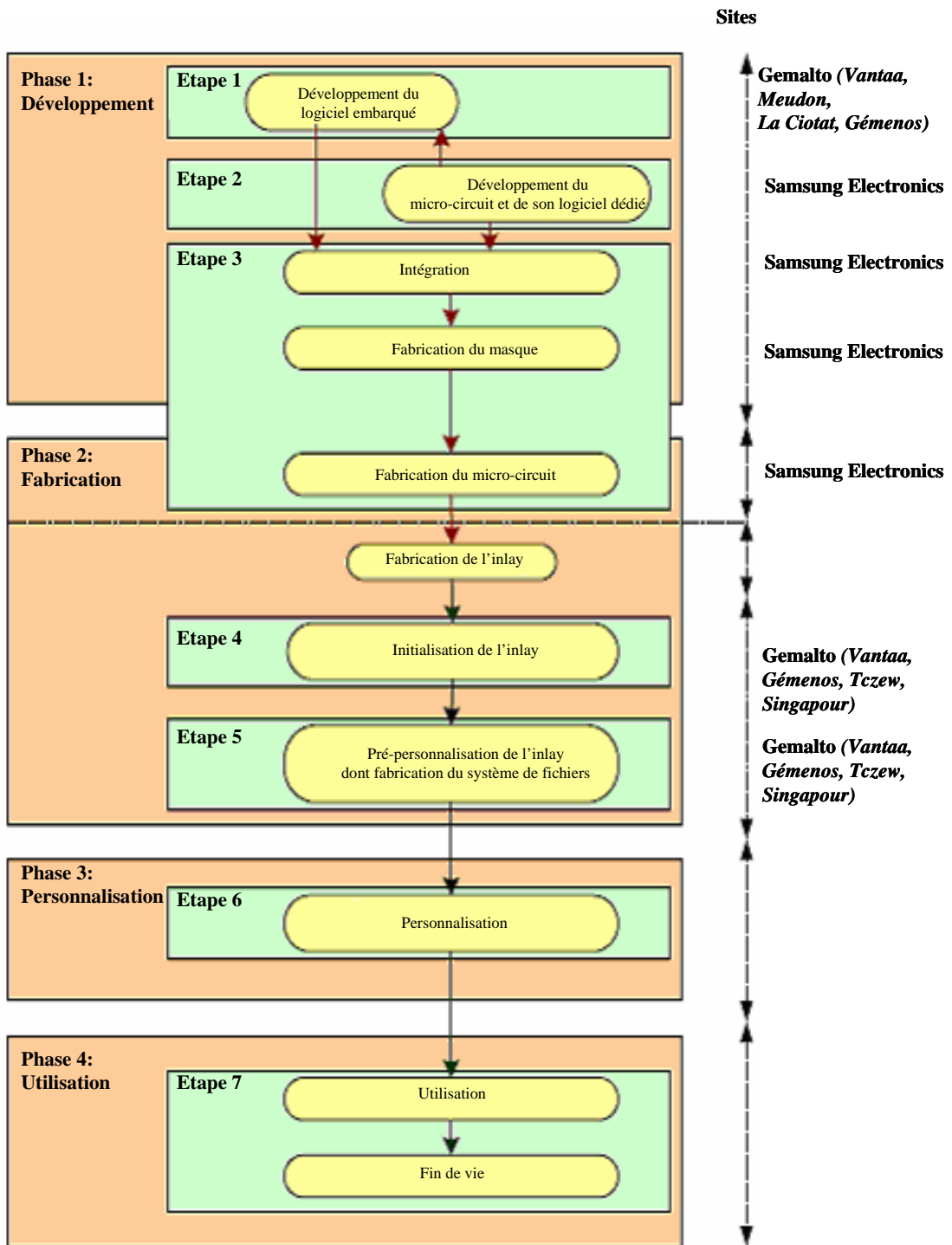


Figure 4 - Cycle de vie n° 3 : Initialisation sur inlay sur le site de Gemalto

Le cycle de vie n° 3 est une autre alternative au cycle de vie n° 1. Il correspond 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
283-110 Tczew
Pologne

Gemalto

12 Ayer Rajah Crescent
Singapor 139941
Singapour

Le microcontrôleur est développé et fabriqué par Samsung Electronics. Les sites de développement et de fabrication du microcontrôleur sont détaillés dans le rapport de certification dont la référence est [BSI-DSZ-CC-0624-2010].

Les « administrateurs du produit » sont les nations ou organisations émettrices du document de voyage.

Les « utilisateurs du produit » sont les voyageurs et les systèmes d'inspection pendant la phase d'utilisation.

1.2.5. Configuration évaluée

Le certificat porte sur l'application eTravel EAC v1.2, masquée sur le composant S3CC9LC révision 11, telle que présentée plus haut au paragraphe 1.2.1.

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

- « *Basic Access Control* » ;
- « *Extended Access Control* » avec algorithmes RSA ou ECDSA.

L'antenne et la phase de fabrication du document de voyage lui-même ne sont pas incluses dans le périmètre de l'évaluation.

2. L'évaluation

2.1. Référentiels d'évaluation

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

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

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [CC AP] ont été appliqués.

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.

Le microcontrôleur S3CC9LC révision 9 a été certifié au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 at AVA_VLA.4, conformément au profil de protection [BSI-PP-0002-2001], le 29 janvier 2010, sous la référence [BSI-DSZ-CC-0624-2010].

Le microcontrôleur S3CC9LC révision 11 utilisé dans le cadre de cette évaluation, et dont les différences avec le microcontrôleur certifié sous la référence [BSI-DSZ-CC-0624-2010] n'ont pas d'impact sur la sécurité, a fait l'objet d'un rapport de maintenance daté du 16 mars 2010 référencé [BSI-DSZ-CC-0624-2010-MA-01].

Le niveau de résistance du microcontrôleur S3CC9LC révision 11 a été confirmé par le BSI le 7 novembre 2011 dans le cadre du processus de surveillance.

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].

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

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 15 février 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 aux référentiels techniques de l'ANSSI [REF-CRY], [REF-KEY] et [REF-AUT]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Il en ressort que pour assurer la conformité aux référentiels techniques de l'ANSSI cités ci-dessus, les recommandations suivantes devront être suivies :

- la taille des clés RSA devront être d'au moins 2048 bits ;
- la taille des clés ECDSA devront être d'au moins 224 bits ;
- la taille du corps DH doit être d'au moins 2048 bits ;
- la taille du corps ECDH doit être d'au moins 224 bits ;
- le nombre d'authentifications BAC réalisées avec la même clé doit être inférieur à 2^{27} et les clés utilisées doivent être de taille au moins égale à 8 octets ;
- le nombre de messages échangés dans le cadre du « *Secure Messaging* » avec la même clé doit être inférieur à 2^{27} ;
- la fonction de hachage SHA-1 ne doit pas être utilisée pour les applications de signature.

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_VLA 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-0624-2010]).

3. La certification

3.1. Conclusion

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

Ce certificat atteste que l'application « eTravel EAC v1.2 masquée sur le composant S3CC9LC » 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
ACM Gestion de configuration	ACM_AUT				1	1	2	2	1	Partial CM automation
	ACM_CAP	1	2	3	4	4	5	5	4	Configuration support and acceptance procedures
	ACM_SCP			1	2	3	3	3	2	Problem tracking CM coverage
ADO Livraison et opération	ADO_DEL		1	1	2	2	2	3	2	Detection of modification
	ADO_IGS	1	1	1	1	1	1	1	1	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	1	1	1	2	3	3	4	2	Fully defined external interfaces
	ADV_HLD		1	2	2	3	4	5	2	Security enforcing high-level design
	ADV_IMP				1	2	3	3	2	Implementation of the TSF
	ADV_INT					1	2	3		
	ADV_LLD				1	1	2	2	1	Descriptive low-level design
	ADV_RCR	1	1	1	1	2	2	3	1	Informal correspondence demonstration
	ADV_SPM				1	3	3	3	1	Informal TOE security policy model
AGD Guides d'utilisation	AGD_ADM	1	1	1	1	1	1	1	1	Administrator guidance
	AGD_USR	1	1	1	1	1	1	1	1	User guidance
ALC Support au cycle de vie	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				1	2	2	3	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	Well-defined development tools
ATE Tests	ATE_COV		1	2	2	2	3	3	2	Analysis of coverage
	ATE_DPT			1	1	2	2	3	1	Testing: high-level design
	ATE_FUN		1	1	1	1	2	2	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	Independent testing – sample
AVA Estimation des vulnérabilités	AVA_CCA					1	2	2		
	AVA_MSU			1	2	2	3	3	3	Analysis and testing for insecure states
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evaluation
	AVA_VLA		1	1	2	3	4	4	4	Highly resistant

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - eTravel v1.2 MAIA2 EAC Security Target <p>Référence : D1118008 Version 0.8 du 11 mars 2011 Gemalto</p> <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"> - eTravel EAC v1.2 – MRTD EAC – Common Criteria / ISO 15408 – Security Target - Public version – EAL4+ <p>Référence : D1104527 Version 1.0 du 5 mars 2012 Gemalto</p>
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation Technical Report – MAIA2 Project <p>Référence : MAIA2_ETR_v1.1 Version 1.1 du 15 février 2012 Serma Technologies</p>
[ANA-CRY]	<p>Cotation des mécanismes cryptographiques – Projet MAIA2</p> <p>Référence : 1688/ANSSI/ACE/LCR Version du 30 juin 2011 ANSSI</p>
[CONF]	<p>Liste de configuration :</p> <ul style="list-style-type: none"> - eTravel v1.2 MAIA2 : ACM Configuration List <p>Référence : D1128599 Version 0.6 du 23 février 2011 Gemalto</p>
[GUIDES]	<p>Guide d'administration du produit :</p> <ul style="list-style-type: none"> - eTravel v1.2 MAIA2 : Administrator Guide <p>Référence : D1128608 Version 0.7 du 25 novembre 2009 Gemalto</p> <p>Guide d'utilisation du produit :</p> <ul style="list-style-type: none"> - eTravel v1.2 MAIA2 : User Guide <p>Référence : D1128610 Version 0.7 du 25 novembre 2009 Gemalto</p> <p>Guide de personnalisation du produit :</p> <ul style="list-style-type: none"> - Card Personalization Specification eTravel v1.2 <p>Référence : D1129544 Version 0.01 du 14 mai 2009 Gemalto</p>

[BSI-PP-0002-2001]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.</i>
[PP EAC]	Protection Profile - Machine Readable Travel Document with “ICAO Application”, Extended Access Control, référence BSI-PP-0026, version 1.2 du 19 Novembre 2007. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0026-2006-MA-01.</i>
[BSI-DSZ-CC-0624-2010]	Samsung S3CC9LC 16-bit RISC Microcontroller for Smart Card, Revision 9 with optional secure RSA 3.7S and ECC 2.4S Libraries including specific IC Dedicated Software. <i>Certifié par le BSI le 29 janvier 2010 sous la référence BSI-DSZ-CC-0624-2010.</i>
[BSI-DSZ-CC-0624-2010-MA-01]	Samsung S3CC9LC 16-bit RISC Microcontroller for Smart Card, Revision 11 with optional secure RSA 3.7S and ECC 2.4S Libraries including specific IC Dedicated Software. <i>Maintenu par le BSI le 16 mars 2010 sous la référence BSI-DSZ-CC-0624-2010-MA-01.</i>
[DCSSI-2008/45]	eTravel EAC version 1.1 (version 01 02) sur composants P5CD080 et P5CD144. <i>Certifié par l'ANSSI le 18 décembre 2008 sous la référence DCSSI-2008/45.</i>
[ANSSI-2009/17]	eTravel EAC version 1.0 (version 01 03) sur composant SLECLX800PE m1581 e13/a14. <i>Certifié par l'ANSSI le 27 janvier 2009 sous la référence ANSSI-2009/17.</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]	<p>Common Criteria for Information Technology Security Evaluation :</p> <p>Part 1: Introduction and general model, August 2005, version 2.3, ref CCMB-2005-08-001;</p> <p>Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002;</p> <p>Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003.</p> <p>Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation :</p> <p>Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004.</p> <p>Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.</p>
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-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.
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, BSI (<i>Bundesamt für Sicherheit in der Informationstechnik</i>)

[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
[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 annexée au Référentiel général de sécurité, 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 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr