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-2011/17

Plateforme LinqUs USIM 128k sur composant SC33F640E

Paris, le 17 juin 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 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-2011/17

Nom du produit

Plateforme LinqUs USIM 128k sur composant SC33F640E

Référence/version du produit

T1017287 / Release A

Référence/version de la TOE

S1092122/ Release A

Conformité à un profil de protection

[PP JCS-O], version 2.6

Java Card System Protection Profile - Open Configuration

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

Gemalto

La Vigie, Av du Jujubier, ZI Athelia IV, 13705 La Ciotat Cedex, France

STMicroelectronics

190 avenue Celestin Coq, ZI de Rousset, B.P. 2, 13106 Rousset, France

Commanditaire

Gemalto

La Vigie, Av du Jujubier, ZI Athelia IV, 13705 La Ciotat Cedex, France

Centre d'évaluation

THALES - CEACI (T3S – CNES)

18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Tél : +33 (0)5 62 88 28 01 ou 18, mél : nathalie.feyt@thalesgroup.com

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

1.1. Présentation du produit

Le produit évalué est la « Plateforme LinqUs USIM 128k sur composant SC33F640E, référence T1017287, Release A » développée par Gemalto et STMicroelectronics.

Ce produit correspond à une plateforme (U)SIM[1] Java Card ouverte embarquée dans une carte (U)SIM destinée à être insérée dans un téléphone portable ou tout autre équipement téléphonique.
Ce produit permet d'accueillir des applications qui peuvent être chargées et instanciées soit avant diffusion de la carte à l'utilisateur final (chargement *pré-issuance*) soit à travers le réseau de l'opérateur mobile, dans un environnement connecté et sans manipulation physique du produit (chargement *post-issuance*, *over-the-air* –OTA-).

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 JCS-O]. Cette conformité est de type démontrable. Des objectifs de sécurité ont été ajoutés à la ciblé de sécurité [ST] pour traiter les particularités Telecom de ce produit.

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 plusieurs moyens décrits dans la *Data Sheet* du produit [DS] :

- La réponse à la commande *GetData* (0x00 0xCA 0x9F 0x7F)correspond aux informations CPLC[2] suivantes:

Fabricant du microcontrôleur	0x47 0x50 (ST)
Type du microcontrôleur	0x00 0x25 (SC33F640)
Identifiant de l'OS	0x00 0x27 (STM027)
Date de l'OS	0x03 0x40 (YDDD)
Version de l'OS	0x01 0x0C

[1] Universal Subscriber Identity Module
[2] Card manager Production Life Cycle

- La réponse à la commande *GlobalPlatform GetData* du *Card Manager* fournit le *Card Recognition Data* :

	TOE: S1092122
Label complet du produit (incluant les outils de développement)	1.23.1.18
Label du logiciel	1.23.1.12
Card Recognition Data	0070666664736206072A864886FC6B01600B06092A864886FC6B020202 630906072A864886FC6B03640B06092A864886FC6B048000640B06092 A864886FC6B04**0255**650A06082A864886FC6B05046619060A2B060104 012A026E0102060B47544F4636343**0117010C** SCP[1] :0x02, 0x55 Label du logiciel: 0x01, 0x17, 0x01, 0x0C

La principale différence entre la référence du produit et celle de la plateforme (la TOE) correspond à l'identification de la liste des applications chargées *pré-issuance*[2] sur cette carte à puce.
Toutes les applications qui étaient présentes dans la configuration du produit à la disposition de l'évaluateur sont identifiées dans le document [App_list]. Ce dernier document liste les *packages* et les applications inclus dans le produit, associés à leurs noms et AIDs[3].
La Commande *GetStatus* permet à l'utilisateur du produit de vérifier quels packages et applications sont installés dans le produit à leur disposition.

1.2.2. Services de sécurité

Les services de sécurité évalués fournis par le produit sont :
- la protection de la confidentialité et de l'intégrité des clés cryptographiques et des données applicatives pendant l'exécution des opérations cryptographiques ;
- la protection de la confidentialité et de l'intégrité des données d'authentification et des données applicatives pendant l'exécution des opérations d'authentification ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications ;
- l'intégrité de l'exécution du code applicatif.

De plus, des services de sécurité relatifs à la gestion des applications sont également fournis par le produit et ont été évalués :
- la délégation de privilèges : le MNO[4], en tant qu'émetteur de la carte[5], correspond initialement à l'unique entité autorisée à gérer les applications de la carte (chargement, instanciation, suppression) au travers d'un canal de communication sécurisé avec la carte en phase 7 (phase d'utilisation de la carte, voir chapitre 1.2.4). Cependant le

[1] Secure Channel Protocol
[2] Chargement réalisé avant la phase 7 du cycle de vie de la carte
[3] Application Identifier
[4] *Mobile Network Operator,* opérateur mobile
[5] *Card Issuer*

MNO peut céder ce privilège à un fournisseur d'applications[1] à l'aide de la fonctionnalité *Global Platform* de délégation de cette gestion d'applications ;

- la vérification de la signature des applications à charger : chaque application à charger est diffusée à la carte associée à sa signature par une autorité de vérification[2] (*Mandated DAP)* ; cette signature est vérifiée par la carte (par le représentant du VA sur la carte) avant la finalisation du processus de chargement de cette application et de son instanciation ;
- la gestion de *Security Domain* (SD) : les fournisseurs d'applications disposent de jeux de clés spécifiques et connus d'eux seuls associés à leurs SD, leur permettant de s'authentifier auprès de ces SD, ainsi que d'établir un canal de confiance entre la TOE et un autre équipement externe.

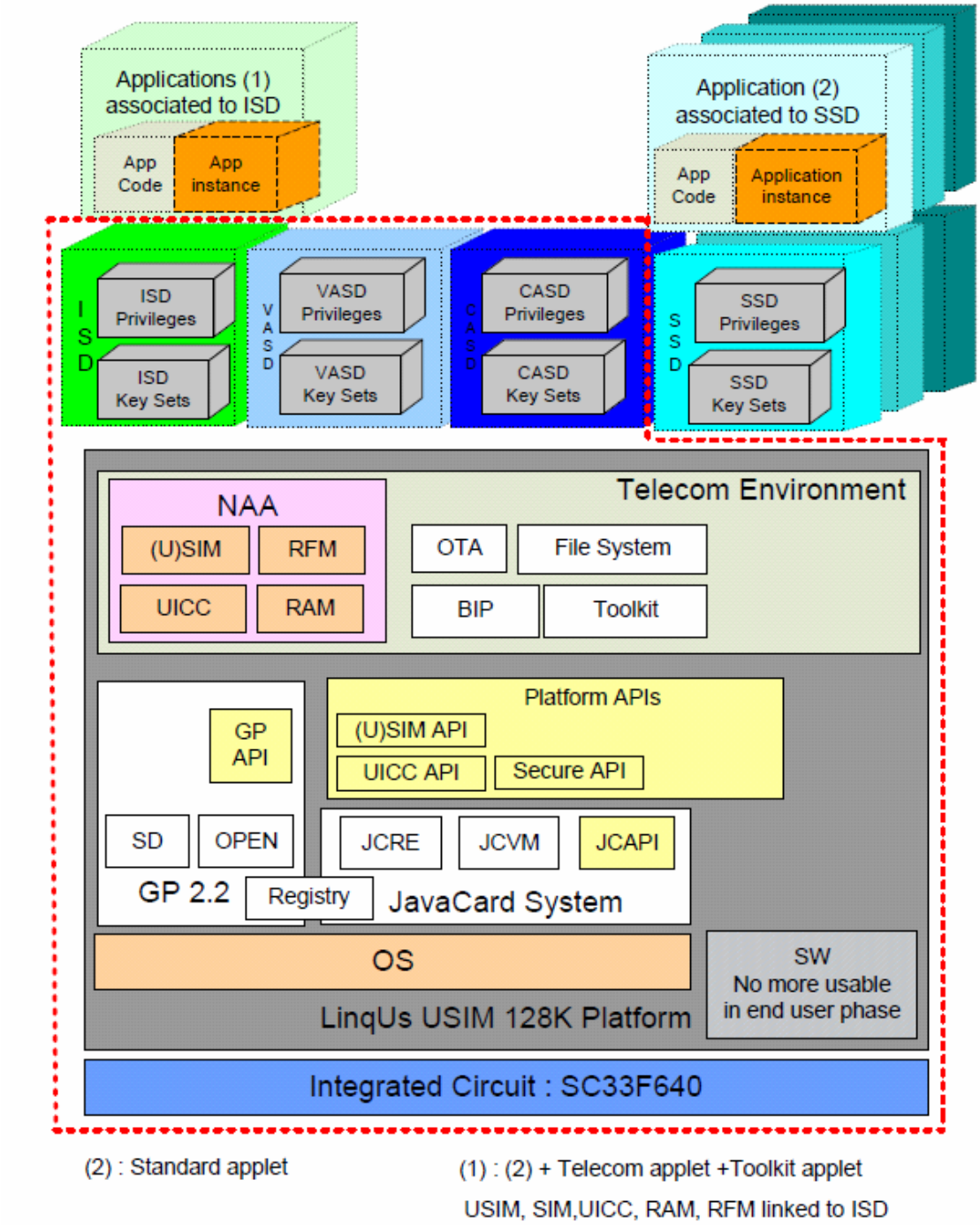
1.2.3. Architecture

Le produit est composé des éléments suivants :

- le microcontrôleur SC33F640, revision E ;
- un système JavaCard, qui gère et exécute des applications, dénommées applets. Il fournit également des interfaces de programmation (APIs) pour développer des applets chargées sur ce produit, conformes aux spécifications Java Card ;
- un package *Global Platform* (partiellement évalué), qui fournit une interface de communication avec la carte à puce et permet de gérer, de façon sécurisée, des applications ;
- des APIs plateforme, qui fournissent plusieurs moyens pour interagir avec des applications (U)SIM ;
- un environnement Télécom comprenant l'authentification réseau des applications (non évalué) et des protocoles de communication Télécom.

[1] *Application Provide*r (AP)
[2] *Verification Authority* (VA)

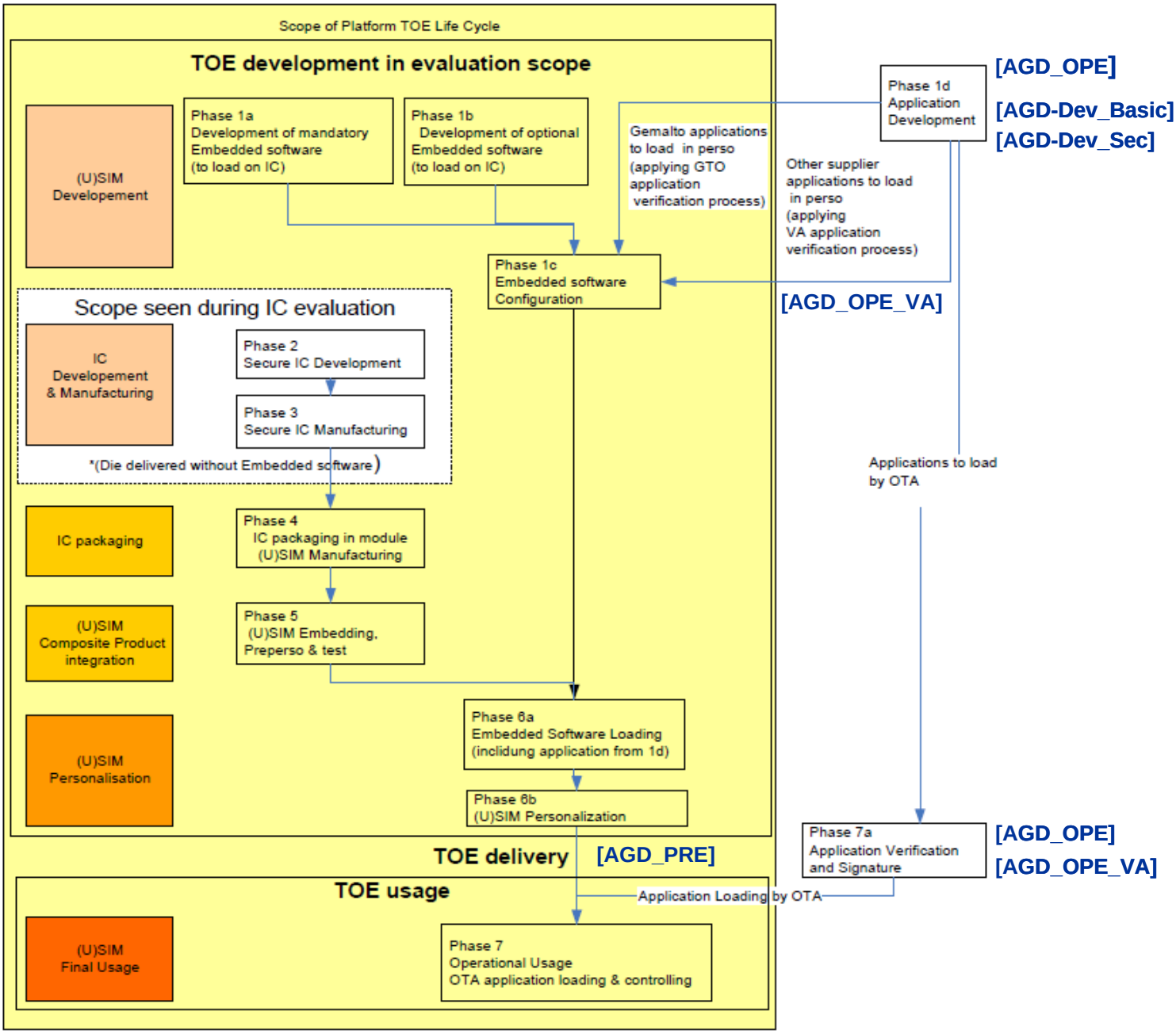
La figure suivante décrit les principaux éléments de la TOE :



Comme identifié au chapitre 1.2.4 ci-dessous, le produit évalué est personnalisé. Ainsi la création des *Security Domain* identifiés dans la figure précédente a été étudiée pendant cette évaluation. Le produit fourni au CESTI contenait effectivement ces *Security Domain.*
Ici, ISD correspond à l'*Issuer Security Domain*, le VASD au *Verification Authority Security Domain,* le CASD au *Controlling Authority Security Domain*, et le SSD au *Supplementary Security Domain*.
Les applications, déjà chargées dans le SSD, sont toutes identifiées dans le document [App_list].

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



Le produit a été développé sur les sites suivants :

Sites de développement

La Vigie
Avenue du Jujubier
ZI Athelia IV
13705 La Ciotat Cedex
France

8, rue de la Verrerie
92197 Meudon Cedex
France

12 Ayar Rajah Crescent
Singapour 139941
Singapour

Sites de configuration du logiciel embarqué

525, Avenue du Pic de Bretagne
13420 Gemenos
France

Ul. Skarszewska 2
83-110 Tczew
Pologne

Sites de *packaging*

Rue de Saint Ulfrant
27500 Pont-Audemer
France

Ul. Skarszewska 2
83-110 Tczew
Pologne

Sites de pré-personnalisation

Rue de Saint Ulfrant
27500 Pont-Audemer
France

Ul. Skarszewska 2
83-110 Tczew
Pologne

Sites de personnalisation

Rue de Saint Ulfrant
27500 Pont-Audemer
France

Ul. Skarszewska 2
83-110 Tczew
Pologne

Les sites de développement et de fabrication du microcontrôleur sont identifiés dans le rapport de certification [ANSSI-CC-2011/07].

Le développement des applications chargées *pré-issuance*, identifiées dans [App_list], a été réalisé sur le site de La Ciotat. Leur livraison et leur vérification ont également été réalisées sur le site de La Ciotat, mais par des équipes distinctes de celles les ayant développées. Conformément à [NOTE.10], ces procédures ont été analysées et auditées pendant cette évaluation.

Les procédures mises en œuvre pour les applications développées par d'autres équipes que celles de Gemalto n'ont pas été analysées au cours de cette évaluation, toutes les applications chargées *pré-issuance* considérées ici ayant été développées par Gemalto.

1.2.5. Guides du produit

Le cycle de vie du produit évalué correspondant aux phases 1 à 6, le guide de préparation du produit personnalisé [AGD-PRE] est essentiellement dédié à la description des recommandations relatives à la gestion de clés associée aux *Security Domain* VASD, CASD, ISD et APSD.

Le guide opérationnel [AGD-OPE] fournit des recommandations pour chacun des utilisateurs suivants du produit :

- le MNO (opérateur télécom) en sa qualité d'émetteur de la carte ;
- les fournisseurs d'application (*Application Provider*, AP), entité ou institution responsable des applications et de leurs services associés ;
- l'autorité de contrôle (*Controlling Authorit*y, CA), entité indépendante du MNO représentée sur la carte, responsable de la protection de la gestion des clés de la carte ainsi que de la personnalisation des *Security Domain* des fournisseurs d'applications (*Application Provider Security Domain*, APSD) ;
- l'autorité de vérification (*Verification Authorit*y, VA), tierce partie représentée sur la carte, agissant pour le compte du MNO et responsable de la vérification de la signature des applications à chargées.

[AGD-OPE] identifie également des recommandations relatives à la livraison des futures applications à charger sur cette carte.

Par ailleurs, les guides [AGD-Dev_Basic] et [AGD-Dev_Sec] décrivent les règles de développement des applications destinées à être chargées sur cette carte ; le guide [AGD-OPE-VA] décrit les règles de vérification qui doivent être appliquées par l'autorité de vérification.

1.2.6. Configuration évaluée

La configuration ouverte du produit a été évaluée conformément à [NOTE.10] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 et réalisé selon les processus audités ne remet pas en question le présent rapport de certification.

Toutes les applications identifiées dans [App_list] ont été vérifiées conformément aux contraintes décrites dans [AGD-OPE_VA].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM].

Pour répondre aux spécificités des cartes à puce, les guides [CC IC] et [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 de l'évaluation du microcontrôleur « SC33F640E » au niveau EAL5 augmenté des composants ALC_DVS.2, et AVA_VAN.5, conforme au profil de protection [PP0035]. Ce microcontrôleur a été certifié le 5 avril 2011 sous la référence ANSSI-CC-2011/07 [ANSSI-CC-2011/07].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 31 mai 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 le référentiel technique de l'ANSSI [REF-CRY], 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 retraitement de la sortie du générateur matériel du microcontrôleur sous-jacent a été étudié dans le cadre de cette évaluation.
L'évaluation n'a pas mis en évidence de vulnérabilités exploitables pour le niveau AVA_VAN visé si le guide [AGD-Dev_Sec] est appliqué.

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 « Plateforme LinqUs USIM 128k sur composant SC33F640E, référence T1017287, release A » 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], notamment :

- les développeurs d'applications doivent appliquer le guide de développement d'applications basiques [AGD-Dev_Basic] ou le guide de développement d'applications sécurisées [AGD-Dev_Sec], selon la sensibilité des applications concernées ;
- les autorités de vérification doivent appliquer le guide [AGD-OPE_VA].

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'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: basic design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - « Security Target LinqUs USIM 128k PK certified using SC33F640 », référence D117263, release 1.7. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « Security Target LinqUs USIM 128k PK certified using SC33F640 », référence D117263, release 1.7p.
[RTE]	Rapport technique d'évaluation : - « Evaluation technical report - Project: LIOUQUET2 », référence LI2_ETR, révision 2.0.
[CONF]	- Delivery Sheet [DS], référence D1189308 ; - TOE software configuration list: « TOE file configuration list », référence listeFichiersPhenix_1_23_1_18 ; - Documentation configuration list: « Documentation configuration list rev 2 », référence Action_List_LIOUQUET2, version 27052011 ; - Product pre-issuance packages [App_list]: « STM027 : Linqus USIM 128k PK Certified », référence Gemalto_STM027_profile description_vA6, release A6.
[GUIDES]	Guide de préparation : - Guide de réception et d'installation [AGD-PRE] : « Preparative Guidance for LinqUs USIM 128K PK certified », référence D1185540, release 1.3 ; Guides opérationnel du produit : - Administration guidance [AGD-OPE] : « Guidance for Administration of LinqUs USIM 128K PK certified », référence D1185542, release 1.3 ; - Guidance for application development • Guidance for basic application development [AGD-Dev_Basic]: « Rules for applications on Upteq mNFC certified product », référence D1186227, release A03 ; • Guidance for secure application development [AGD-Dev_Sec]: « Guidance for secure application development on Upteq mNFC platforms », référence D1188231, release A04 ; - Guidance for Verification Authority [AGD-OPE_VA]: « Guidance for Verification Authority of LinqUs USIM 128K PK », référence D1185542_VA, release 1.3.
[PP JCS-O]	Java Card System Protection Profile - Open Configuration, version 2.6, 19 April 2010. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03.*

[PP0035]	Security IC Platform Protection Profile, version 1.0, 15 juin 2007. *Certifié par le* BSI *(Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI_PP_0035.*
[ANSSI-CC-2011/07]	Microcontrôleurs sécurisés ST33F1ME, ST33F768E, SC33F768E, ST33F640E, SC33F640E, ST33F512E, SC33F512E et SC33F384E avec la bibliothèque cryptographique optionnelle NesLib v3.0. *Certifié par l'ANSSI sous la référence* ANSSI-CC- 2011/07.

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, référence CCDB-2009-03-002 version 3.0, revision 1, mars 2009.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, référence CCDB-2009-03-001 version 2.7 revision 1, mars 2009.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, référence CCDB-2007-09-001 version 1.0, revision 1, septembre 2007.
[NOTE.10]	« Note d'application - Certification d'applications sur "plateformes ouvertes cloisonnantes" », référence ANSSI-CC-NOTE/10.0, voir ssi.gouv.fr
[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
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, mai 2000.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.