Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2012/18

Machine virtuelle Java Card de la plateforme LinqUs USIM 128k sur composant SC33F640E

Paris, le 30 avril 2012

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

Patrick Pailloux
[ORIGINAL SIGNE]

SÉCURITÉ CERTIFICATION

Avertissement

Ce rapport est destiné à fournir aux commanditaires un document leur permettant d'attester du niveau de sécurité offert par le produit dans les conditions d'utilisation ou d'exploitation définies dans ce rapport pour la version qui a été évaluée. Il est destiné également à fournir à l'acquéreur potentiel du produit les conditions dans lesquelles il pourra exploiter ou utiliser le produit de manière à se trouver dans les conditions d'utilisation pour lesquelles le produit a été évalué et certifié ; c'est pourquoi ce rapport de certification doit être lu conjointement aux guides d'utilisation et d'administration évalués ainsi qu'à la cible de sécurité du produit qui décrit les menaces, les hypothèses sur l'environnement et les conditions d'emploi présupposées afin que l'utilisateur puisse juger de l'adéquation du produit à son besoin en termes d'objectifs de sécurité.

La certification ne constitue pas en soi une recommandation du produit par l'agence nationale de la sécurité des systèmes d'information (ANSSI), et ne garantit pas que le produit certifié soit totalement exempt de vulnérabilités exploitables.

Toute correspondance relative à ce rapport doit être adressée au :

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.anssi@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2012/18

Nom de la TOE

Machine virtuelle Java Card de la 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

néant

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ADV_FSP.6, ADV_IMP.2, ADV_INT.3, ADV_SPM.1, ADV_TDS.6, ALC_DVS.2, AVA_VAN.5

Développeur

Gemalto

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

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 a déjà été certifié sous la référence ANSSI-CC_2011/17 [2011/17].

L'évaluation a ici portée sur la « Machine virtuelle Java Card de la plateforme LinqUs USIM 128k sur composant SC33F640E , référence S1092122, Release A » développée par Gemalto.

1.2. Description du produit

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

1.2.1. Identification du produit

Les éléments constitutifs de la plateforme LinqUs USIM 128k, dont son système Java Card, 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[1] 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] Card manager Production Life Cycle.

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

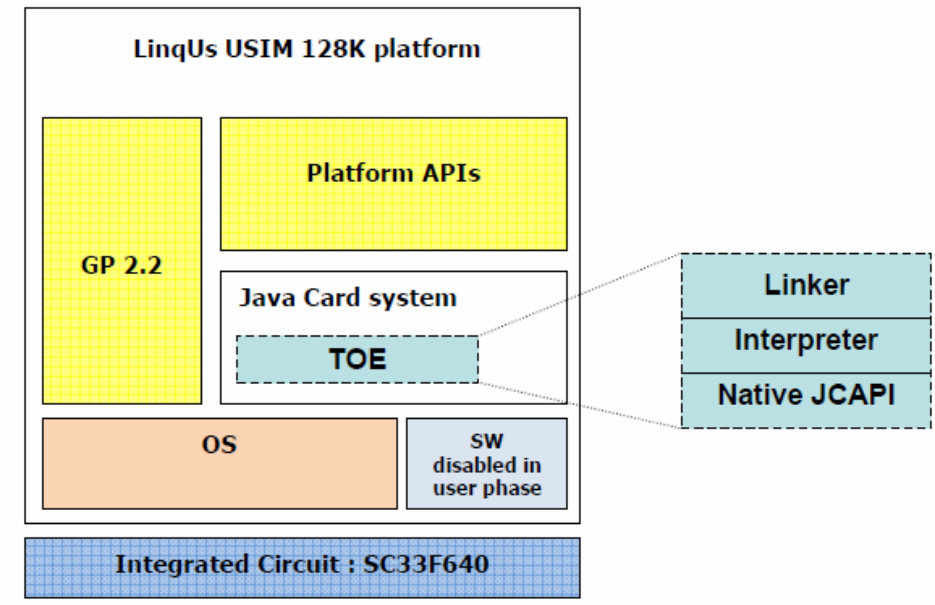
Label complet du produit	1.23.1.18
Label du logiciel	1.23.1.12
Card Recognition Data	0070666664736206072A864886FC6B01600B06092A864886FC6B020202630906072A864886FC6B03640B06092A864886FC6B048000640B06092A864886FC6B04**0255**650A06082A864886FC6B05046619060A2B060104012A026E0102060B47544F46363430**0117010C** SCP[1] :0x02, 0x55 Label du logiciel: 0x01, 0x17, 0x01, 0x0C

1.2.2. Architecture

Le produit est composé des éléments suivants :

- le microcontrôleur SC33F640, revision E ;
- un système d'exploitation ;
- un système Java Card, qui gère et exécute des applications. 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*, 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.

La figure suivante décrit les principaux éléments de la TOE :



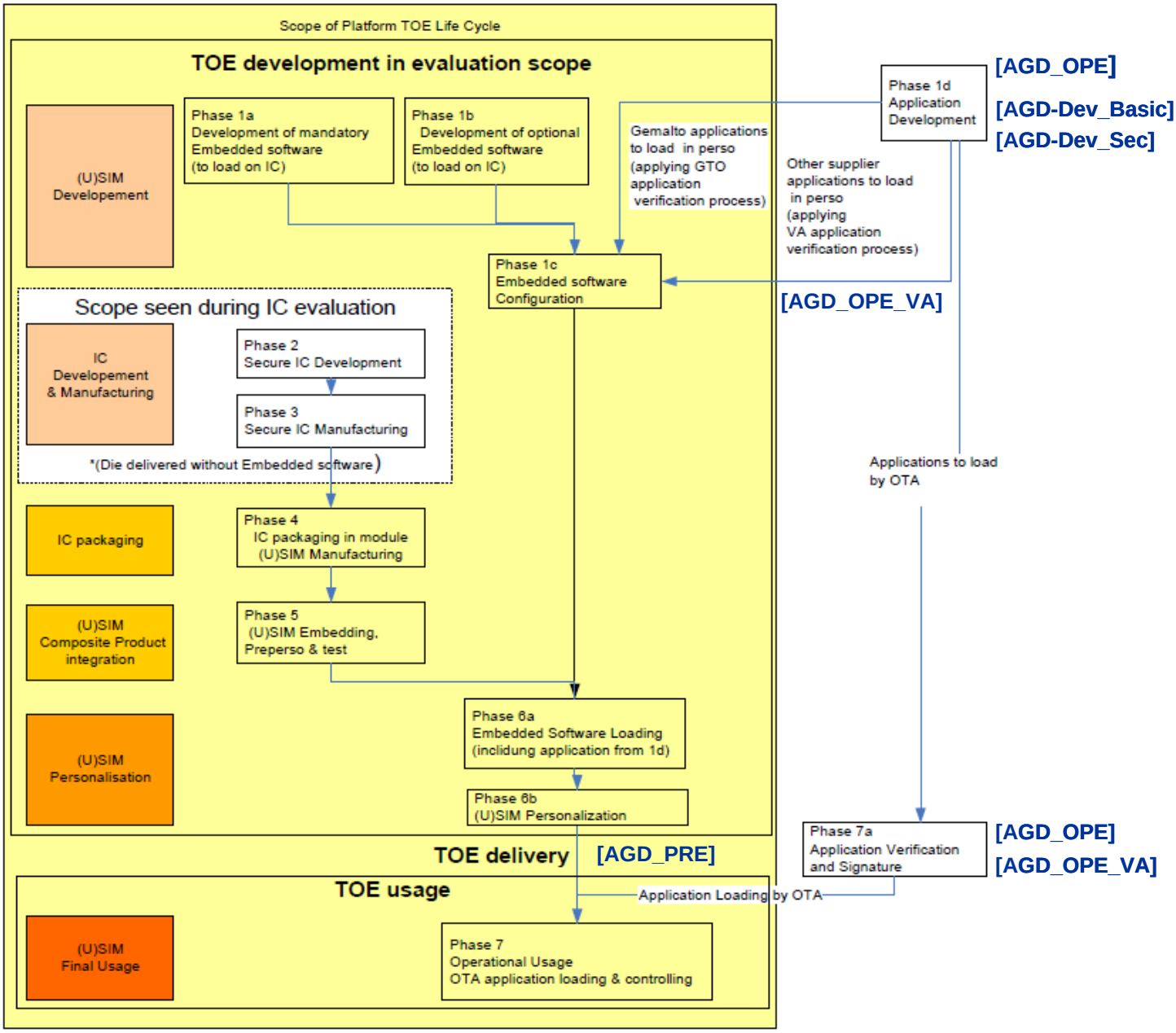
[1] Secure Channel Protocol.

1.2.3. Services de sécurité

Le principal service de sécurité évalué ici correspond à l'exécution correcte et sûre des applications embarquées sur le produit si celles-ci ont été préalablement vérifiées à l'aide d'un outil de type *byte code verifier*.
L'ensemble des services évalués est détaillé au chapitre 6.1 de la cible de sécurité [ST] publique.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



Le développement du modèle formel de la cible d'évaluation a été réalisé sur le site suivant :

Trusted Labs

5, rue du Baillage
78000 Versailles
France

Les autres sites de développement du produit, ainsi que la description des différents guides évalués, sont identifiés dans le rapport de certification [2011/17].

1.2.5. 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.

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 s'appuie sur les résultats d'évaluation de la « Plateforme LinqUs USIM 128k sur composant SC33F640E, release A » certifiée le 17 juin 2011 sous la référence ANSSI-CC-2011/17 [2011_17].

Cette évaluation a consisté à réévaluer le système Java Card du produit selon les plus hautes exigences des Critères Communs relatives au développement : les composants ADV retenus ici correspondent à ceux du niveau EAL7, qui nécessitent la mise en œuvre de méthodes formelles. La plupart des résultats relatifs aux autres composants d'assurance ont été obtenus lors de l'évaluation précédente.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 2 avril 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 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 la « Machine virtuelle Java Card de la plateforme LinqUs USIM 128k sur composant SC33F640E, référence S1092122, 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'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.
[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**6**	Complete semi-formal functional specification with additional formal specification
	ADV_IMP				**1**	1	**2**	2	**2**	Complete mapping of the implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**3**	Minimally complex internals
	ADV_SPM						**1**	1	**1**	Formal TOE security policy model
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**6**	Complete semiformal modular design with formal high-level design presentatio
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 - Formal assurances on the Java Card Virtual Machine of LinqUs USIM 128k PK certified using SC33F640 », référence D1185035, release 1.5. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - « Security Target - Formal assurances on the Java Card Virtual Machine of LinqUs USIM 128k PK certified using SC33F640 », référence D1185035, release 1.5p.
[RTE]	Rapport technique d'évaluation : - « Evaluation technical report - Project: LIOUQUET2 extended», référence LIE_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 opérationnels 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.
[2011/17]	Plateforme LinqUs USIM 128k sur composant SC33F640E. *Certifiée par l'ANSSI sous la référence* ANSSI-CC- 2011/17.

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.
[NOTE.10]	« Note d'application - Certification d'applications sur "plateformes ouvertes cloisonnantes" », référence ANSSI-CC-NOTE/10.0, voir www.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.