Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2008/37

Carte Linqus USIM 128K : Composant SLE88CFX4002P/m8834b17 masqué par la plateforme GemXplore Generations G152B-EP3B et embarquant l'application de signature ESIGN

Paris, le 3 novembre 2008,

Le Directeur central 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 la direction centrale de la sécurité des systèmes d'information (DCSSI), 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 nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.gouv.fr

Référence du rapport de certification

DCSSI-2008/37

Nom du produit

Carte Linqus USIM 128K : Composant SLE88CFX4002P/m8834b17 masqué par la plateforme GemXplore Generations G152B-EP3B et embarquant l'application de signature ESIGN

Référence/version du produit

T1004530 A3 / Version 1.0

Conformité à un profil de protection

néant

Critères d'évaluation et version

Critères Communs version 2.3
conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 4 augmenté
AVA_MSU.3, AVA_VLA.4

Développeurs

GEMALTO
6 rue de la verrerie, 92197 Meudon, France

Infineon Technologies AG
Automotive, Industrial & Multimarket, Chipcard & Security IC´s, Am Campeon 1-12, 85579 Neubiberg, Allemagne

Commanditaire

GEMALTO
6 rue de la verrerie, 92197 Meudon, France

Centre d'évaluation

CEACI (Thales Security Systems – CNES)
18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France
Tél : +33 (0)5 61 28 16 51, mél : ceaci@cnes.fr

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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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 « Carte Linqus USIM 128K : Composant SLE88CFX4002P/m8834b17 masqué par la plateforme GemXplore Generations G152B-EP3B et embarquant l'application de signature ESIGN**,** version 1.0 » développée par GEMALTO et Infineon Technologies AG.
Ce produit correspond à une carte à puce insérée dans un téléphone portable (i.e. carte SIM). Il est destiné à être utilisé en tant que dispositif sécurisé de création de signature électronique (SSCD) de type 3.

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.
La cible de sécurité s'inspire du profil de protection [PP0006].

Par rapport au document [PP0006] :

- l'application de génération de certificats (CGA : Certification Generation Application) est mise en œuvre par l'opérateur du téléphone portable qui gère la plateforme WPKI[1] ; cette application est chargée de vérifier l'identité du signataire, ainsi que l'authenticité des SVD (Signature Verification Data) générées et émises par le produit ;
- l'application de création de signature (SCA : Signature Creation Application) est mise en œuvre par un ensemble de sites marchands, chargés de présenter les données à signer (DTBS : Data To Be Signed) au signataire sous la forme d'un SMS ;
- l'administrateur correspond à l'opérateur chargé de gérer la plateforme WPKI (à noter que c'est à partir de cette plateforme centralisée que les fonctionnalistes d'IGC du produit évalué sont activées) ;
- le signataire correspond à l'utilisateur du téléphone portable qui s'est enregistré auprès du service de signature offert par l'opérateur.

1.2.1. Identification du produit

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

La procédure permettant d'identifier la TOE est décrite dans le document [TOE_ID].

[1] Wireless Public Key Infrastructure: infrastructure de gestion de clés (IGC) sans fil

Cette procédure consiste en deux étapes :

- tout d'abord, identifier, à l'aide de la commande GetData, le label de la TOE, composé des champs « identifiant client » et « programme de personnalisation » de la table d'identité
- ensuite, contacter les équipes support de GEMALTO afin d'obtenir la référence de la TOE à partir du label identifié précédemment.

1.2.2. Services de sécurité

Le produit évalué comprend les éléments suivants :

- une plate-forme JavaCard, GemXplore Generations, qui fournit les principaux services de sécurité suivants :
  - initialisation du gestionnaire de carte GP[1] et gestion du cycle de vie de la carte ;
  - installation sécurisée d'applications sous le contrôle du gestionnaire de carte en phase d'initialisation ;
  - service de messagerie sécurisée pendant la personnalisation de l'applet ;
  - services de sécurité basiques de la carte :
    - vérification des conditions environnementales d'exécution à l'aide des informations fournies par le microcontrôleur ;
    - vérification de la cohérence du cycle de vie de la carte ;
    - intégrité et confidentialité des clés et des PINS stockés pour le compte de l'applet ;
    - manipulation sécurisée de données et des mécanismes de sauvegarde ;
    - gestion du contenu des mémoires ;
    - mécanismes pour empêcher d'autres applets d'interférer avec l'applet E-SIGN ;

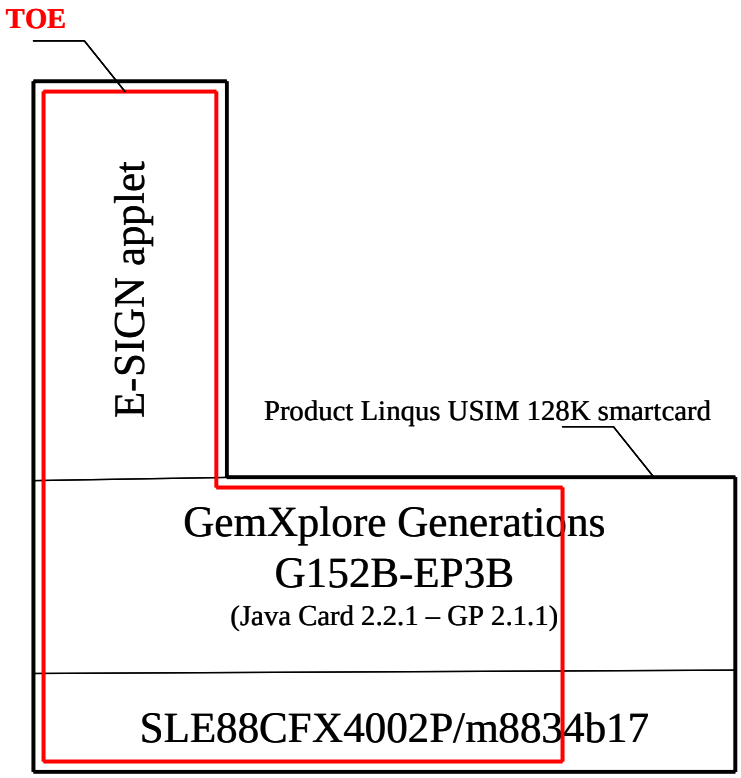
- l'application ESIGN qui fournit les principaux services de sécurité suivants :
  - génération de SCD/SVD (signature creation date/ signature verification data) ;
  - génération de signatures électroniques.

1.2.3. Architecture

Le produit est constitué :

- du microcontrôleur SLE88CFX4002P/m8834b17, développé et fabriqué par Infineon Technologies AG ;
- de l'OS JavaCard, GemXplore Generations G152B-EP3B (label GXG_1_2_2_1_EP3B_ICT_01_G152), développé par GEMALTO masqué dans la ROM du microcontrôleur ;
- de l'application SSCD ESIGN (label pki_plugins_dev_09), développée par GEMALTO, chargée au moment de l'initialisation de la carte.

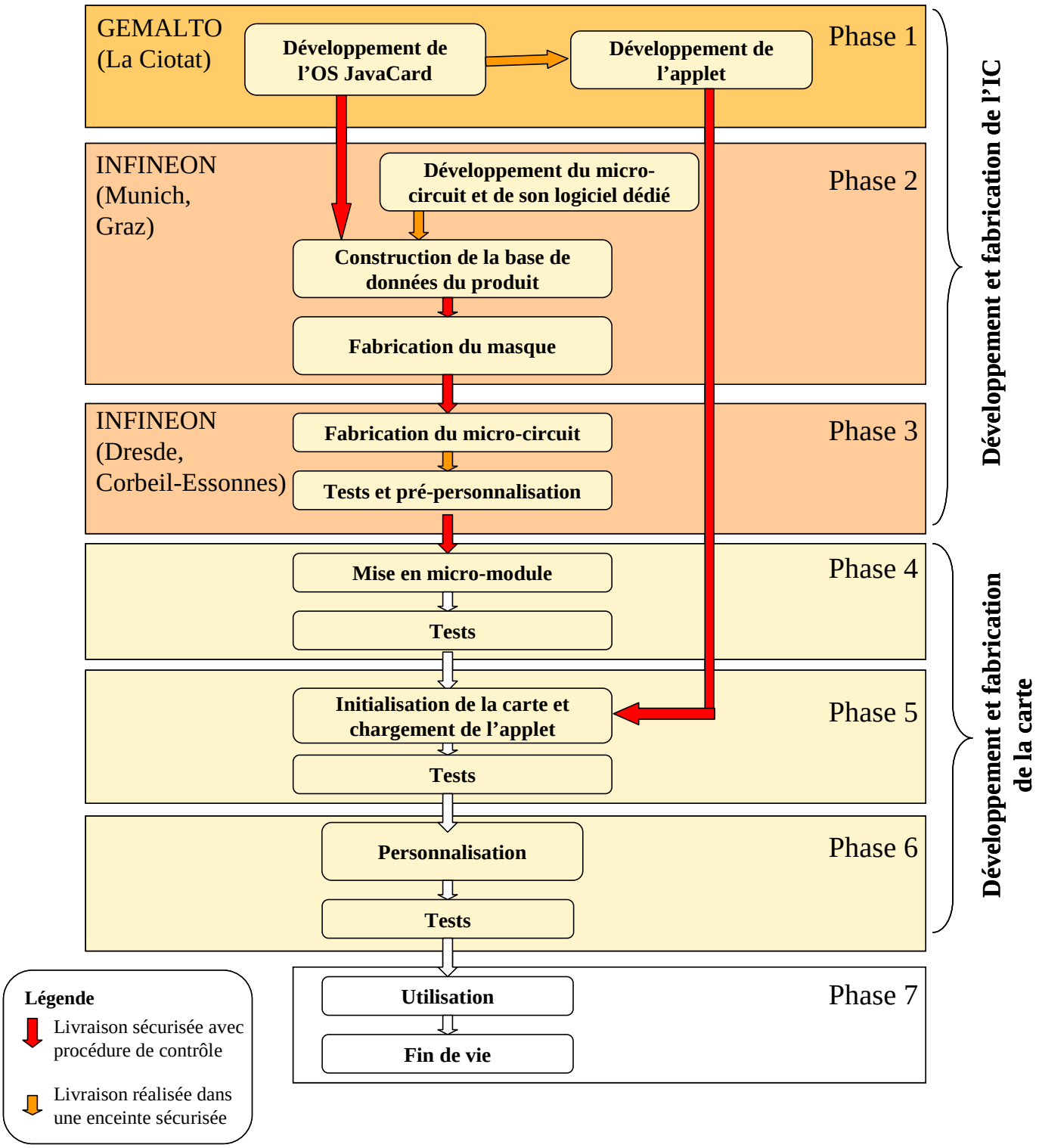
[1] Global Platform



La TOE correspond à l'application de signature numérique E-SIGN, associée aux fonctionnalités et services de l'OS JavaCard GXG et du microcontrôleur requis pour mettre en œuvre les fonctionnalités de l'applet.
Le CESTI a vérifié que les fonctionnalités du produit ne participant pas à la réalisation des services de sécurité de la TOE n'interfèrent pas avec ceux-ci.

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :



La plateforme JavaCard et l'application ont été développées sur le site suivant :

Gemalto - La Vigie,

Avenue du Jujubier, Z.I. Athélia IV,
BP 90,
13702 La Ciotat Cedex,
France

Le microcontrôleur, certifié par le BSI, a été développé et produit par Infineon Technologies AG.

Pour l'évaluation, l'évaluateur a considéré comme « administrateurs du produit » les personnalisateurs des cartes (émetteurs de la carte) et comme « utilisateurs du produit » les personnalisateurs des cartes ainsi que les utilisateurs finaux du produit.

1.2.5. Configuration évaluée

A la fin de la phase 6, la carte personnalisée est verrouillée : le chargement et la suppression d'application ne sont plus disponibles après cette phase.

Le produit testé par le CESTI correspond au produit en phase 7 (produit destiné à l'utilisateur final).

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 la DCSSI 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.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur «SLE88CFX4002P/m8834b17» au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme au profil de protection [PP0002]. Ce microcontrôleur a été certifié le 21 juin 2006 sous la référence BSI-DSZ-CC-0376-2006.
Le niveau de résistance du microcontrôleur a été confirmé le 24 août 2007 dans le cadre du processus de surveillance.

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 16 octobre 2008, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques n'a pas été analysée par la DCSSI.

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 « Carte Linqus USIM 128K : Composant SLE88CFX4002P/m8834b17 masqué par la plateforme GemXplore Generations G152B-EP3B et embarquant l'application de signature ESIGN, version 1.0» 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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- la génération de certificats qualifiés (OE.CGA_Qcert) ;
- la vérification de l'authenticité de la clé publique de vérification de signature électronique –SVD– par l'application de génération de certificats –CGA– (OE.SVD_Auth_CGA) ;
- la protection des données de vérification de l'authentification –VAD– (OE.HI_VAD) ;
- la gestion des données devant être signées (OE.SCA_Data_Intend) ;
- la mise en œuvre des recommandations de gestion du microcontrôleur (OE.IC_Usage_and_Protection).

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 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 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, la Grèce, 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, la République de Corée, les Pays-Bas, 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	**1**	Subset of the 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	**1**	Identification 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]	Cible de sécurité de référence pour l'évaluation : - "ASE – Security Target ; TOE: ESIGN PKI signature application on GemXplore Generations G152B-EP3B OS platform, running on Infineon SLE88CFX4002P/m8834b17 chip; Ref T1004530 A3 / Version 1.0; Product: Linqus USIM 128K smartcard ; Based on SSCD Type 3", référence ASE10448, version 1.4 Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - "LINQUS USIM 128K Smartcard; ESIGN PKI Signature Application On GemXplore Generations G152B-EP3B OS platform, Running on Infineon SLE88CFX4002P/m8834b17 chip Security Target" – Public version, référence ASE10448_Public, version 1.0
[RTE]	Rapport technique d'évaluation : - « Evaluation Technical Report- Project: BOSPHORE », référence BOS_ETR, version 2.0
[CONF]	"Bosphore project - List of evaluation documentation", référence BOS_DOC_10448, version 1.5
[TOE_ID]	« Bosphore Project -TOE identification », référence TOE_ID_10448, version 0.6
[GUIDES]	Guides d'installation du produit : - "Dev Configuration Check - GXGenerations platforms-TURKCELL porting on GXG1.2", référence E6K009_001_CFG, version A03 - "Delivery & Operation ; TOE - GXG-ESIGN; Product - G152-ESIGN", référence ADO10448, version 0.3 - "Card Initialization Specification For Garlaban V1.2 on Infineon SLE88 chip family", référence CIS02R10527A, version A04 - "Card Personalization Specification - Master Part For Garlaban V1.2 - Core volume", référence CPS01R10527A, version A12 - "Memory Replication Specification For Garlaban V1.2 on Infineon SLE88 chip family", référence MRS02R10527A, version A01 - "Card Personalization Specification - Daughter Part For Flexible V1.2 - Core volume", référence CPS02R10527A, version A16 Guides d'administration et d'utilisation du produit : - "GemXplore Generations Java Card and GlobalPlatform Environment", référence DOC113342B, version2.0 - "GemXplore Generation CAT features", référence DOC113397A, version1.0

	- "GemXplore Generations OTA remote management - Reference Manual", référence DOC113356A, version1.0 - "GemXplore Generations 3G and GSM Operation Modes-Reference Manual", référence DOC113364C, version3 .0 - "Card Issuer and End-User Guidance; TOE – GXG-ESIGN; Product – G152-ESIGN; Based on SSCD Type 3", référence SEC_REC_10448, version 0.3
[PP0006]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. *Certifié par le BSI sous la référence BSI-PP-0006-2002T.*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 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, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2008-04-001 version 2.5, revision 1, April 2008.
[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 2.0, April 1999, Management Committee of Agreement Group.
[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 (Bundesamt für Sicherheit in der Informationstechnik)