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-2015/25

Plateforme jTOP INFv#46P31 masquée sur les composants M7820 A11 et M11 avec fonctionnalités MRTD, version 46.31

Paris, le 04 août 2015

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

Contre-amiral Dominique RIBAN

[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-2015/25

Nom du produit

Plateforme jTOP INFv#46P31 masquée sur les composants M7820 A11 et M11 avec fonctionnalités MRTD

Référence/version du produit

Version 46.31

Conformité à un profil de protection

[PP_JCS], version 3.0, Java Card™ System Open Configuration Protection Profile

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

TRUSTED LOGIC
6 rue de la verrerie,
92197 Meudon Cedex, France

INFINEON TECHNOLOGIES
AIM CC SM PS - Am Campeon 1-12 -
85579 Neubiberg, Allemagne

Commanditaire

TRUSTED LOGIC
6 rue de la verrerie, 92197 Meudon Cedex, France

Centre d'évaluation

Serma Technologies

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

Accords de reconnaissance applicables

CCRA

SOG-IS

Le produit est reconnu au niveau EAL2.

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 jTOP INFv#46P31 masquée sur les composants M7820 A11 et M11 avec fonctionnalités MRTD, version 46.31 » développé par TRUSTED LOGIC et INFINEON TECHNOLOGIES.

Il s'agit d'une plateforme *Java Card* ouverte conçue de façon à ce que des applications sensibles (passeport électronique, permis de conduire électronique, carte d'identité électronique, …) puissent être chargées et exécutées de façon sécurisée.

Le produit est conforme aux spécifications *GlobalPlatform Card Specification* [GPCS], version 2.2.1 et plus particulièrement avec les spécifications *GlobalPlatform Card ID Configuration* [GPCS-ID], version 1.0.

1.2. Description du produit

1.2.1. Introduction

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

Cette cible de sécurité est conforme au profil de protection [PP-JCS]. Étant donné que cette version du profil de protection rend optionnelle l'utilisation du mécanisme RMI (*Remote Method Invocation* – méthode d'invocation à distance), non présent dans le produit, la conformité au profil de protection est de type démontrable.

1.2.2. Identification du produit

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

La version certifiée du produit est identifiable par les éléments suivants (voir [ST] et [GUIDES]) :

Nom de la TOE	jTOP INFv#46P31 for MRTD
Version de la TOE	46.31
Intitulé dans le système de gestion des versions	TREL_INF_SLE78_GP22ID_V46_P31R
Fabricant du composant	INFINEON TECHNOLOGIES
Identifications du composant	SLE78CLX1600PM-m7820-A11 and M11 SLE78CLX800P-A11 and M11 SLE78CLX360PM-A11 and M11
Version du masque	v#46P3.1

Ces éléments sont obtenus après un ATR[1] ou en utilisant la commande Get Data, tel que décrit dans les [GUIDES].

[1] *Answer to reset.*

Dans le cas présent et conformément aux dispositions de [OPEN], il est à noter qu'aucune application chargée pré-émission n'est présente dans le produit certifié.

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- les services de sécurité au niveau du système d'exploitation :
  - la gestion de l'exécution des applications ;
  - le contrôle du flux d'exécution ;
  - la gestion des états de la carte ;
  - la gestion des accès mémoire ;
  - la gestion de la confidentialité des mémoires ;
  - le chargement de code sécurisé ;
  - l'authentification du porteur de la carte ;
- les services de sécurité au niveau *Java Card* :
  - la machine virtuelle défensive (JCVM – *Java Card Virtual Machine*) ;
  - le pare-feu *Java Card* ;
  - l'effacement sécurisé ;
- les services de sécurité au niveau *GlobalPlatform* :
  - le gestionnaire de commandes ;
  - le gestionnaire de cartes ;
  - les canaux sécurisés :
- les services cryptographiques :
  - la génération de nombres aléatoires ;
  - la génération de clés ;
  - la gestion des clés ;
  - la fourniture de mécanismes de chiffrement et de déchiffrement ;
  - la fourniture de mécanismes de création et de vérification de signatures ;
- la protection du chargement d'applications *post-issuance* ;
- l'isolation des applications entre contextes différents et la protection de la confidentialité et de l'intégrité des données applicatives entre les applications.

1.2.4. Architecture

Le produit est une carte à puce constitué des éléments suivants :

- du microcontrôleur offrant les fonctionnalités matérielles (gestion de la mémoire et gestion des entrées/sorties) et de sa bibliothèque cryptographique ;
- du système *Java Card* composé de :
  - la machine virtuelle *Java Card* (JCVM) ;
  - l'environnement d'exécution *Java Card* (JCRE) ;
  - l'API *Java Card* (JCAPI) ;
- de diverses API :
  - *GlobalPlatform* ;
  - LDS[1] (API d'accès au système de fichier) ;
  - PACE ;
  - API propriétaires TRUSTED LOGIC ;
- de plusieurs domaines de sécurité (développeur de la carte (ISD[1]) ou autre (SSD[2])).

[1] *Logical Data Structure.*

Aucune application n'est chargée dans le produit.

La figure suivante présente l'architecture du produit :

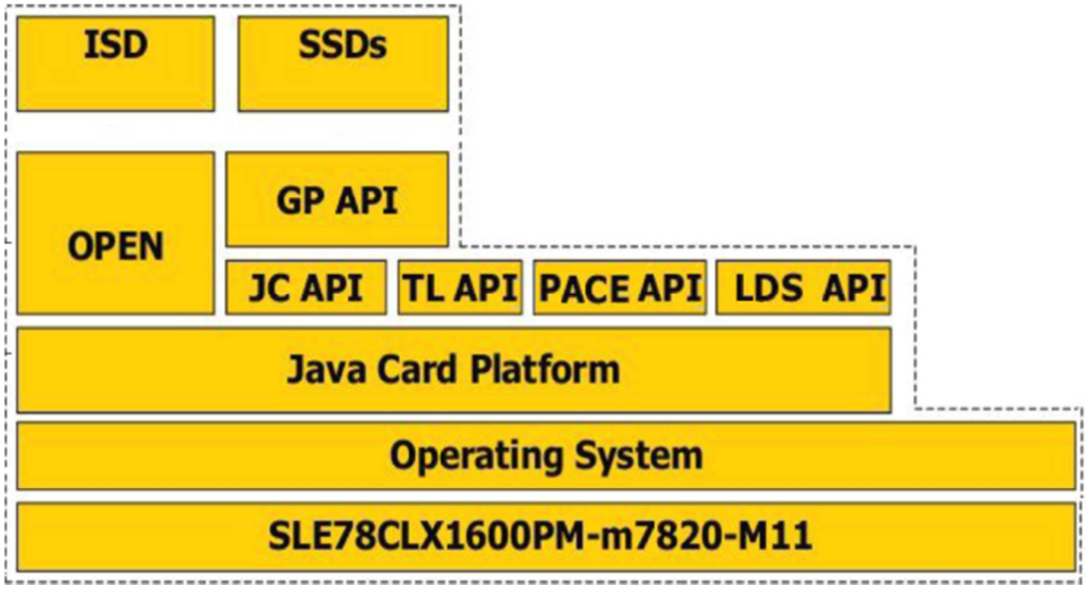

Figure 1 : Architecture du produit

1.2.5. Cycle de vie

Le cycle de vie du produit est composé de quatre principales phases :

- phase 1 : développement ;
- phase 2 : stockage, pré-personnalisation et test ;
- phase 3 : personnalisation et test ;
- phase 4 : utilisation finale.

La figure 2 explicite plus en détail le cycle de vie du produit.

[1] *Issuer security domain.*
[2] *Supplementary security domains.*

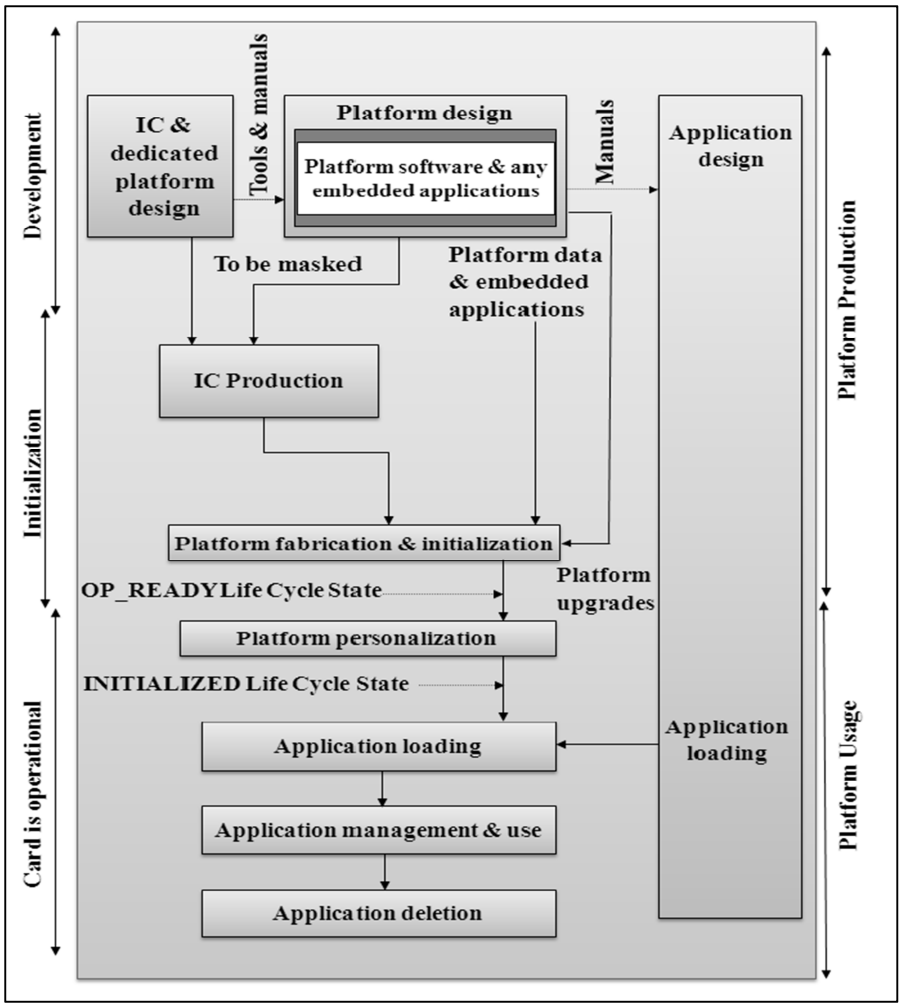

Figure 2 : Cycle de vie de la plateforme

Les phases de conception (bloc *IC & dedicated platform design*) et de fabrication (bloc *IC Production*) du composant sont couvertes par l'évaluation du composant (voir [CER-IC]).

Le périmètre d´évaluation comprend les phases de conception et de développement du logiciel masqué. Cette phase est représentée dans la figure 2 par le bloc *Platform design*.

Les phases couvertes par l'évaluation correspondent à l'ensemble des phases jusqu'à ce que le produit atteigne l'état *INITIALIZIED Life Cycle State* (voir figure 2). Les phases d'initialisation et de personnalisation de la plateforme ont été évaluées dans le cadre de l'évaluation du composant (voir [CER-IC]) et sont couvertes par les guides (voir [GUIDES]).

Les phases suivantes liées au chargement, à la gestion, à l'utilisation et à la suppression l'applications sont couvertes par les guides (voir [GUIDES]).

Les fonctions de sécurité de la TOE sont évaluées dans la phase d'utilisation.

Le produit a été développé et fabriqué sur les sites suivants :

- site de développement de la plateforme :

  TRUSTED LOGIC
  6 rue de la Verrerie
  92190 Meudon
  France

- site de développement et fabrication du microcontrôleur :

  INFINEON TECHNOLOGIES AG

  AIM CC SM PS
  Am Campeon 1-12
  85579 Neubiberg
  Allemagne

Pour l'évaluation, l'évaluateur a considéré comme administrateur du produit le *Card Administrator* (administrateur de la carte) dont le rôle est défini dans [ST].

En particulier, le *Card Administrator* est le représentant du *Card Issuer* (émetteur de la carte). Il a le contrôle du contenu de la carte, ainsi que de la gestion du cycle de vie de cette dernière. Durant la phase d'initialisation de la plateforme, ce rôle est endossé par le *Card Enabler* (chargé d'habilitations de la carte). Durant la phase d'utilisation de la plateforme, le *Card Administrator* peut verrouiller, déverrouiller, ou bloquer la carte, télécharger de nouvelles applets sur la carte, modifier les clés statiques de l'ISD ou récupérer des informations d'administration de la carte.

Par ailleurs, l'évaluateur a considéré comme utilisateurs du produit les *Application Developers* (développeurs d'applications) dont les responsabilités sont détaillées dans le guide d'utilisation du produit (voir [GUIDES]).

1.2.6. Configuration évaluée

Le certificat porte sur la plateforme avec l'ensemble des API indiquées dans la figure 1 et décrite au paragraphe 1.2.4 et configuré conformément aux guides (voir [GUIDES]).

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Ainsi tout chargement de nouvelles applications conformes aux contraintes exposées au chapitre 3.2 du présent rapport de certification et réalisé selon les processus audités ne remet pas en cause 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 les composants d'assurance qui ne sont pas couverts par le manuel [CEM], des méthodes propres au centre d'évaluation et validées par l'ANSSI ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [JIWG IC] et [JIWG AP] ont été appliqués. Ainsi, le niveau AVA_VAN a été déterminé en suivant l'échelle de cotation du guide [JIWG AP]. Pour mémoire, cette échelle de cotation est plus exigeante que celle définie par défaut dans la méthode standard [CC], utilisée pour les autres catégories de produits (produits logiciels par exemple).

2.2. Travaux d'évaluation

L'évaluation en composition a été réalisée en application du guide [COMP] permettant de vérifier qu'aucune faiblesse n'est introduite par l'intégration du logiciel dans le microcontrôleur déjà certifié par ailleurs.
Cette évaluation a ainsi pris en compte les résultats de l'évaluation du microcontrôleur de la famille « *M7820 A11 et M11* » au niveau EAL5 augmenté des composants ALC_DVS.2 et AVA_VAN.5, conforme au profil de protection [PP-0035]. Ce microcontrôleur a été certifié le 05 septembre 2012 sous la référence [CER-IC] et maintenu le 24 juin 2013 sous la référence [CER-IC_M01]. Le niveau de résistance du microcontrôleur a été confirmé le 02 mai 2014 dans le cadre du processus de surveillance.

L'évaluation s'appuie sur les résultats des évaluations des plateformes jTOP INFv#46 masquée sur composants Infineon SLE78CLX1600PM, SLE78CLX800P, SLE78CLX360PM avec et sans les fonctionnalités MRTD certifié le 27 juin 2013 (pour la plateforme avec fonctionnalités MRTD) et le 07 août 2013 (pour la plateforme sans les fonctionnalités MRTD), respectivement sous les références ANSSI-CC-2013/42 et ANSSI-CC-2013/55.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 20 juillet 2015 détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Cotation des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF], n'a pas été réalisée. Néanmoins, l'évaluation n'a pas mis en évidence de vulnérabilités de conception et de construction pour le niveau AVA_VAN visé.

2.4. Analyse du générateur d'aléas

Le générateur de nombres aléatoires, de nature physique, utilisé par le produit final a été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER-IC]). Par ailleurs, la sortie du générateur physique d'aléas subit un retraitement de nature cryptographique suivant l'implémentation du standard [X931]. Les 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_VAN.5 visé.

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 jTOP INFv#46P31 masquée sur les composants M7820 A11 et M11 avec fonctionnalités MRTD, version 46.31 » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 5 augmenté des composants ALC_DVS.2 et AVA_VAN.5.

3.2. Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 1.2 du présent rapport de certification.

L'utilisateur du produit certifié devra s'assurer du respect des objectifs de sécurité sur l'environnement d'exploitation, tels que spécifiés dans la cible de sécurité [ST], et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doivent respecter les contraintes de développement de la plateforme (guides [AGD-PRE]) selon la sensibilité de l'application considérées ;
- les autorités de vérification doivent appliquer le guide [AGD-PRE] ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement *post-issuance*) doit être activée conformément aux indications de [AGD_OPE] ;
- les développeurs d'applications doivent appliquer [AGD_OPE].

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 EAL2 ainsi qu'à la famille ALC_FLR.
Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'Autriche, l'Espagne, la Finlande, la France, l'Italie, la Norvège, les Pays-Bas, le Royaume-Uni et la Suède.
[2] Les pays signataires de l'accord CCRA sont : l'Allemagne, l'Australie, l'Autriche, le Canada, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Inde, Israël, l'Italie, le Japon, la Malaisie, la Norvège, la Nouvelle-Zélande, le Pakistan, les Pays-Bas, la République de Corée, la République Tchèque, le Royaume-Uni, Singapour, la Suède et la Turquie.

Annexe 1. Niveau d'évaluation du produit

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 5+	Intitulé du composant
ADV Développement	ADV_ARC		**1**	1	1	1	1	1	**1**	Security architecture description
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**	**5**	Complete semi-formal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	2	**1**	Implementation representation of the TSF
	ADV_INT					**2**	**3**	3	**2**	Well-structured internals
	ADV_SPM						**1**	1		
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**	**4**	Semiformal modular design
AGD Guides d'utilisation	AGD_OPE	**1**	1	1	1	1	1	1	**1**	Operational user guidance
	AGD_PRE	**1**	1	1	1	1	1	1	**1**	Preparative procedures
ALC Support au cycle de vie	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Production support, acceptance procedures and automation
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5	**5**	Development tools CM coverage
	ALC_DEL		**1**	1	1	1	1	1	**1**	Delivery procedures
	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD			**1**	1	1	1	**2**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ASE Evaluation de la cible de sécurité	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claims
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended components definition
	ASE_INT	**1**	1	1	1	1	1	1	**1**	ST introduction
	ASE_OBJ	**1**	**2**	2	2	2	2	2	**2**	Security objectives
	ASE_REQ	**1**	**2**	2	2	2	2	2	**2**	Derived security requirements
	ASE_SPD		**1**	1	1	1	1	1	**1**	Security problem definition
	ASE_TSS	**1**	1	1	1	1	1	1	**1**	TOE summary specification
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**3**	3	**4**	**3**	Testing: modular design
	ATE_FUN		**1**	1	1	1	**2**	2	**1**	Functional testing
	ATE_IND	**1**	**2**	2	2	2	2	**3**	**2**	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5	**5**	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - jTOP INFv#46P31 Security Target for MRTD, 15 juillet 2015, référence CP-2011-RT-484-46P31, version 1.2. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Java Card Open Platform for MRTD Security Target LITE, 15 juillet 2015, référence PU-2011-RT-484-46P31, version 1.2.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report - Kottos Project, 20 juillet 2015, référence KOTTOS_ETR_v1.4, version 1.4. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - ETR-Lite for Composition - Kottos Project, 20 juillet 2015, référence KOTTOS_ETR-lite_v1.2, version 1.2.
[CONF]	Liste de configuration du produit : KOTTOS_CONFIGURATION_ITEMS_20150715.
[GUIDES]	- [AGD_PRE] jTOP INFv#46 - Operational User Guidance, 15 juillet 2015, référence CP-2011-RT-732-46P31, version 1.5 ; - [AGD_OPE] jTOP INFv#46 – Preparative Procedures, 15 juillet 2015, référence CP-2011-RT-731-46P31, version 1.2 ; - jTOP® Card Initialization Phase Specification for V#46.0x, 09 février 2015, référence CP-2003-RT-52-46P31, version 1.3.
[PP0035]	Protection Profile, Security IC Platform Protection Profile, version 1.0, juin 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*
[PP-JCS]	Protection Profile, Java Card™ System Open Configuration Protection Profile, version 3.0, 18 mai 2012. *Certifié par l'ANSSI sous la référence ANSSI-CC-PP-2010/03-M01.*
[CER-IC]	« Infineon smart card IC (Security Controller) M7820 A11 and M11 with optional RSA2048/4096 v1.02.013, EC v1.02.013, SHA-2 v1.01 and Toolbox v1.02.013 libraries and with specific IC dedicated software ». *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 05 septembre 2012 sous la référence BSI-DSZ-CC-0829-2012.*
[CER-IC_M01]	Rapport de maintenance délivré le 24 juin 2013 sous la référence BSI-DSZ-CC-0829-2012-MA-01.

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, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-001 ; - Part 2: Security functional components, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-002 ; - Part 3: Security assurance components, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, juillet 2009, version 3.1, révision 3 Final, référence CCMB-2009-07-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, février 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, janvier 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, janvier 2012.
[OPEN]	Certification of « Open » smart card products, version 1.1 (for trial use), 4 février 2013.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, 2 juillet 2014.
[SOG-IS]	Mutual Recognition Agreement of Information Technology Security Evaluation Certificates, version 3.0, 8 janvier 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 2.03 du 21 février 2014 annexée au Référentiel général de sécurité (RGS_B1), voir www.ssi.gouv.fr.
[X931]	ANSI X9.31 Digital Signatures using Reversible Public Key Cryptography for the Financial Services Industry (rDSA), 1998.
[GPCS]	GlobalPlatform Card Specification, version 2.2.1, janvier 2011.
[GPCS-ID]	GlobalPlatform Card ID Configuration, version 1.0, décembre 2011.

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