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-2019/32

IDeal Citiz v2.3-n embedding ID.me 1.6-n application (ID.me 1.6-n / 2.1.6.0.0)

Paris, le 21 août 2019

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

Emmanuel GERMAIN
[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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2019/32

Nom du produit

IDeal Citiz v2.3-n embedding ID.me 1.6-n application

Référence/version du produit

ID.me 1.6-n / 2.1.6.0.0

Conformité à un profil de protection

Protection profiles for secure signature creation device :

Part 2: Device with key generation, v2.0.1, certifié BSI-CC-PP-0059-2009-MA-01 le 21 février 2012;
Part 3: Device with key import, v1.0.2, certifié BSI-CC-PP-0075-2012 le 27 septembre 2012 ;
Part 4: Extension for device with key generation and trusted communication with certificate generation application, v1.0.1, certifié BSI-CC-PP-0071-2012 le 12 décembre 2012 ;
Part 5: Extension for device with key generation and trusted communication with signature creation application, v1.0.1, certifié BSI-CC-PP-0072-2012 le 12 décembre 2012 ;
Part 6: Extension for device with key import and trusted communication with signature creation application, v1.0.4, certifié BSI-CC-PP-0076-2013 le 16 avril 2013.

Critères d'évaluation et version

Critères Communs version 3.1 révision 5

Niveau d'évaluation

EAL 5 augmenté

ALC_DVS.2, AVA_VAN.5

Développeurs

IDEMIA
2 place Samuel Champlain
92400 Courbevoie, France

NXP Semiconductors
Troplowitzstrasse 20,
22529 Hamburg, Allemagne

Commanditaire

IDEMIA
2 place Samuel Champlain
92400 Courbevoie, France

Centre d'évaluation

CEA - LETI
17 avenue des martyrs, 38054 Grenoble Cedex 9, France

Accords de reconnaissance applicables

CCRA

SOG-IS

Ce certificat 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 l'*applet* Java Card « IDeal Citiz v2.3-n embedding ID.me 1.6-n application, version ID.me 1.6-n / 2.1.6.0.0 », développée par *IDEMIA* et *NXP SEMICONDUCTORS*.

Ce produit offre des services d'authentification et de signature électronique (SSCD[1]) conformes aux spécifications IAS ECC v1.0.1. Il est embarqué sur la plateforme *Java Card* ouverte [CER_PTF] préalablement certifiée, et peut être utilisé dans différents types de documents (carte d'identité, permis de conduire, carte d'entreprise, passeport, etc.) disposant d'interfaces avec et/ou sans contact.

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 aux profils de protection [PP-SSCD-Part2], [PP-SSCD-Part3], [PP-SSCD-Part4], [PP-SSCD-Part5] et [PP-SSCD-Part6].

Elle se base également sur le profil de protection [PP-EAC2] pour les fonctions additionnelles du protocole EAC V2.

1.2.2. Services de sécurité

Les services de sécurité fournis par le produit sont décrits dans [ST]. Les principaux services sont :

- la génération de la donnée de création de signature (*Signature Creation Data* ou SCD) et de la donnée de vérification de signature (*Signature Verification Data* ou SVD) associée ;
- l'import de la donnée de création de signature (SCD) et, optionnellement, de la donnée de vérification de signature (SVD) associée ;
- l'export de la donnée de vérification de signature (SVD) pour une création de certificat électronique ;
- la création de signature électronique via un canal de confiance.

Les principaux services de sécurité de la plateforme sont décrits dans [CER-PTF].

1.2.3. Architecture

Le produit est constitué :

[1] *Secure Signature Creation Device.*

- du microcontrôleur P6022y VB et de ses bibliothèques logicielles, certifiés sous la référence [CER-IC] ;
- de la plateforme *Java Card* ouverte cloisonnante « NXP JCOP 3 P60 », certifié sous la référence [CER-PTF] ;
- de l'application « ID.me v1.6-n » découpée en trois modules. Le premier module fournit les services SSCD et les deux autres, qui sont optionnels, fournissent les services PKI[1] IAS ECC et EAC2.

Tous ces éléments font partie de la cible d'évaluation (TOE).

1.2.4. Identification du produit

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

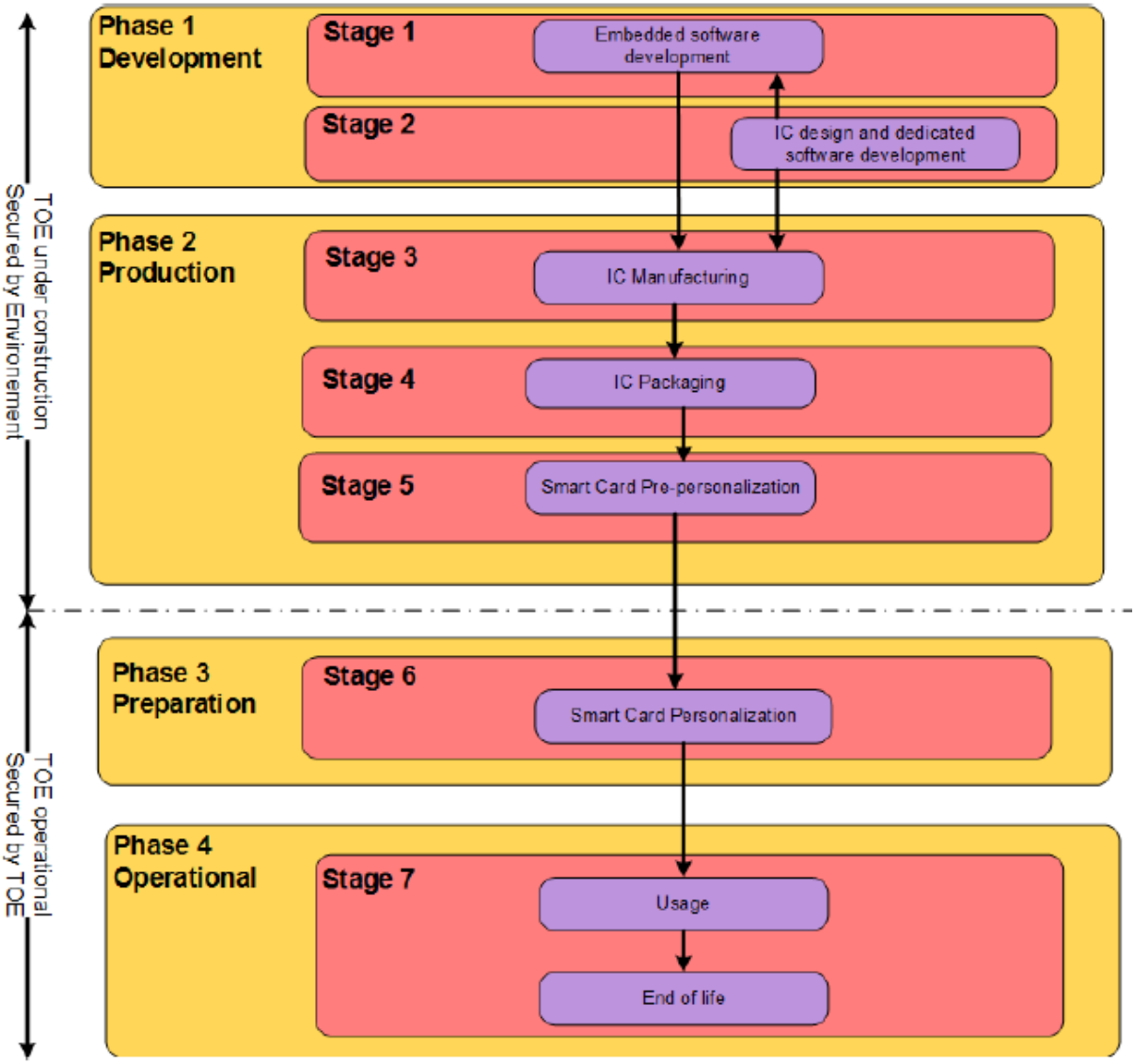
La version certifiée du produit est identifiable par les éléments suivants :

- La méthode d'identification de la plateforme est présentée dans [PTF_UM] :
  - Platform ID = JxHyyy0019790400 ;
  - Patch ID = 0x0000000000000000 (pour JCOP 3 OSB.2 RC9) ;
  - Ou Patch ID = 0x4000000000000000 (pour JCOP 3 OSB.2 RC9 PL4).
- La méthode d'identification de l'applet ID.me est présentée dans le guide [APP_PRE]:
  - §3.2.2.2 pour l'identification et la version du produit : '49 44 2E 6D 65 20 31 2E 36 2D 6E 20 2F 20 32 2E 31 2E 36 2E 30 2E 30' réprésentant en ASCII 'ID.me 1.6-n / 2.1.6.0.0' ;
  - §3.2.2.1 pour les différentes valeurs des *Executable Load Files*.

1.2.5. Cycle de vie

Le cycle de vie du produit, qui suit celui défini dans le profil de protection [PP0084] est présenté au chapitre 4 de la cible de sécurité [ST]. Il.est composé des étapes illustrées par la figure ci-dessous, pouvant être regroupées en quatre phases :

[1] *Public Key Intrastructure.*



Le point de livraison de la TOE est en sortie de la phase 2, étape 5. Jusqu'à cette phase, le produit est considéré comme étant en construction. Ainsi :

- les étapes 1 (pour ce qui concerne le développement de l'application), 4 et 5 sont réalisées par *IDEMIA* et couvertes par les audits des sites suivants (voir [SITES]) :

***IDEMIA* – Courbevoie** [CRB] 2, place Samuel de Champlain 92400 Courbevoie, France	***IDEMIA* – Vitré** [VTR] Avenue d'Helmstedt BP 90308 35503 Vitré Cedex France
***IDEMIA* – Noida** [NOI] Syscom India Private Limited PLOT-1A, sector 73, Noida Uttar Pradesh 201307, India	***IDEMIA* – Shenzhen** [SZN] 4F, Great wall technology building No 2, Kefa Rd Science and technology park, Nanshan district Shenzhen, 518057 PR of China

***IDEMIA* – Haarlem** [HAA] Oudeweg 32, 2031 CC Haarlem, The Netherlands	

- l'étape 1 (pour ce qui concerne le développement de la plateforme) est réalisée par *NXP SEMICONDUCTORS*. Les sites de développement de la plateforme sont couverts par le certificat [CER-PTF] ;
- l'étape 2 est assurée par le développeur du microcontrôleur, à savoir *NXP SEMICONDUCTORS*. Les sites de développement et de fabrication de ce microcontrôleur sont détaillés dans le rapport de certification [CER-IC] ;
- l'étape 3 est assurée soit par *NXP SEMICONDUCTORS*, soit par *IDEMIA*. Les sites sont couverts par le certificat [CER-IC] pour *NXP SEMICONDUCTORS*, et les audits des sites cités plus haut pour *IDEMIA*.

1.2.6. Configuration évaluée

Selon sa configuration, le produit peut offrir jusqu'à trois services pour répondre aux différentes infrastructures à clés publiques (PKI) possibles :

- pas de PKI ;
- PKI IAS ;
- PKI EAC : nouveau *package* qui supporte le protocole EAC version 2 [PP-EAC2].

La TOE a été vérifiée conformément aux contraintes décrites dans les guides de la plateforme, référencées dans [CER-PTF].

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 5** [CC] et à la méthodologie d'évaluation définie dans le manuel [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 sur la plateforme déjà certifiée par ailleurs (voir [CER-PTF]).

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 7 août 2019, 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. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations données aux chapitres 4.2, 5.2 et 6.3 du guide [APP_OPE] doivent être respectées.
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.

Dans le cadre du processus de qualification renforcée, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI (voir [ANA-CRY]). 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_VAN.5 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-PTF]).

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 « IDeal Citiz v2.3-n embedding ID.me 1.6-n application, version ID.me 1.6-n / 2.1.6.0.0 » 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].

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].

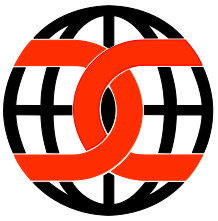
L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] La liste des pays signataires de l'accord SOG-IS est disponible sur le site web de l'accord : www.sogis.org.

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[1], 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] La liste des pays signataires de l'accord CCRA est disponible sur le site web de l'accord : www.commoncriteriaportal.org.

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 : - Security Target IDeal Citiz v2.3-n embedding ID.me 1.6-n application, version 4.0, référence 2018_2000034214, 20/06/2019, *IDEMIA*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Security Target Lite IDeal Citiz v2.3-n embedding ID.me 1.6-n application, version 1.0, référence 2019_2000043199, 20/06/2019, *IDEMIA*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report (full ETR) – TULIP, référence LETI.CESTI.TUL.RTE.002, version 1.1, 7/08/2019, *CEA-LETI*.
[ANA-CRY]	Cotation des mécanismes cryptographiques TULIP, référence LETI.CESTI.TUL.RT.008, version 1.2, 6/08/2019, *CEA-LETI*.
[CONF]	Liste de configuration du produit : - Software Release Sheet for IDealCitiz v2.3-n, version 4.0, reference 2018_2000033008, 10/07/19, *IDEMIA*.
[GUIDES] [APP_PRE]	Guide d'installation du produit : - Preparative procedures for IDealCitiz V2.3-n, version 2.3, référence 2018_2000033006, 20/06/2019, *IDEMIA* ; - Personalization Specification for IDealCitiz V2.3-n , version 2.2, référence 2018_2000033005, 20/06/2019, *IDEMIA*. Guide opérationnel du produit : - Operational Guidance for IDealCitiz V2.3-n, version 2.2, référence 2018_2000033003, 20/06/2019, *IDEMIA*. Guide utilisateur du produit : - User Manual for IDealCitiz V2.3-n, version 2.2, référence 2018_2000033004, 18/06/2019, *IDEMIA*.
[PTF_UM]	Guides de la plateforme : - JCOP 3 SECID P60 CS - User Guidance and Administration - Manual, version 3.1, référence 367531, 23/10/2018, *NXP SEMICONDUCTORS*.

[SITES]	Rapports d'analyse documentaire : - [GEN17] o Oberthur Technologies Development Environment (Generic Documentary activities), référence 17-0232_ALC_GEN_v1.0, 25/08/2017, *SERMA SAFETY & SECURITY*, - [GEN19] o IDEMIA Development Environment ALC Class Evaluation Report (Generic Documentary activities), référence IDEMIA R&D site 2018_GEN_v1.1, 19/06/2019, *SERMA SAFETY & SECURITY ;* o IDEMIA Haarlem Development Environment - ALC Class Evaluation Report (Generic Documentary activities), référence SITE_IDEMIA_HAARLEM_ALC_GEN_v1.0, 24/08/2019, *SERMA SAFETY & SECURITY*. Rapports d'audit de site pour la réutilisation : - [CRB] o Site Technical Audit Report CRB, référence IDEMIA R&D site 2018_CRB_STAR_v1.3, 26/06/2019, *SERMA SAFETY & SECURITY*, - [HAA] o Site Technical Audit Report IDEMIA Haarlem, référence SITE_IDEMIA_HAARLEM_STAR_v1.1, 03/01/2019, *SERMA SAFETY & SECURITY*, - [VTR] o Vitré Site Visit lite report, référence 17-0232_SVR-VTR_M_V1.0, 17/01/18, *SERMA SAFETY & SECURITY*, - [SZN] o Shenzhen Site Visit lite report, référence 17-0232_SZN_SVR-M_v1.0, 08/02/18, *SERMA SAFETY & SECURITY*, - [NOI] o Site technical Audit Report 2019 NOI-D, référence IDEMIA R&D site 2018_NOI-D_STAR_v1.0, 17/04/19, *SERMA SAFETY & SECURITY*.
[PP-SSCD-Part2]	Protection profiles for secure signature creation device – Part 2: Device with key generation, référence : prEN 14169-2:2012, version 2.0.1 datée du 23 janvier 2012. *Maintenu par le BSI (Bundesamt für Sicherheit in der Informationstechnik) le 21 février 2012 sous la référence BSI-CC-PP-0059-2009-MA-01.*

[PP-SSCD-Part3]	Protection profiles for secure signature creation device – Part 3: Device with key import, référence : prEN 14169-3:2012, version 1.0.2 datée du 24 juillet 2012. *Certifié par le BSI le 27 septembre 2012 sous la référence BSI-CC-PP-0075-2012.*
[PP-SSCD-Part4]	Protection profiles for secure signature creation device – Part 4: Extension for device with key generation and trusted communication with certificate generation application, référence : prEN 14169-4:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0071-2012.*
[PP-SSCD-Part5]	Protection profiles for secure signature creation device – Part 5: Extension for device with key generation and trusted communication with signature creation application, référence : prEN 14169-5:2012, version 1.0.1 datée du 14 novembre 2012. *Certifié par le BSI le 12 décembre 2012 sous la référence BSI-CC-PP-0072-2012.*
[PP-SSCD-Part6]	Protection profiles for secure signature creation device – Part 6: Extension for device with key import and trusted communication with signature creation application, référence : prEN 14169-6:2013, version 1.0.4 datée du 3 avril 2013. *Certifié par le BSI le 16 avril 2013 sous la référence BSI-CC-PP-0076-2013.*
[PP-EAC2]	Protection profile for Electronic Document implementing Extended Access Control Version 2 defined in BSI TR-03110, version 1.01, BSI-CC-PP-0086, version 1.01, 20 mai 2015. *Certifié par le BSI le 13 juillet 2015 sous la référence BSI-CC-PP-0086-2015.*
[CER-PTF]	NXP JCOP 3 P60 *Certifiée par le NSCIB le 29 novembre 2018 sous la référence CC-18-98209/2*.
[CER-IC]	NXP Secure Smart Card Controller P6022y VB including IC Dedicated Software *Certifié par le BSI le 18 mai 2018 sous la référence BSI-DSZ-CC-1059-2018.*

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 ANSSI-CC-CER-P-01 Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, les sites ou les profils de protection, ANSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : - Part 1: Introduction and general model, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-001; - Part 2: Security functional components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-002; - Part 3: Security assurance components, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, avril 2017, version 3.1, révision 5, référence CCMB-2017-04-004.
[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 1.5.1, mai 2018.
[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.

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