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-2019/31

BELPIC V1.8 applet on MultiApp V4.1 Platform Révision 1.0

Paris, le 7 août 2019

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

Emmanuel GERMAIN
[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@ssi.gouv.fr

Référence du rapport de certification

ANSSI-CC-2019/31

Nom du produit

BELPIC V1.8 applet on MultiApp V4.1 Platform

Référence/version du produit

Version de l'application Belpic : 1.8 revision 1.0

Version de la plateforme JavaCard MultiApp : 4.1

Conformité à un profil de protection

Protection profiles for secure signature creation device:

Part 2: Device with key generation, v2.0.1, BSI-CC-PP-0059-2009-MA-01 ;

Part 5: Extension for device with key generation and trusted communication with signature creation application, v1.0.1, BSI-CC-PP-0072-2012.

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

Gemalto

6, rue de la Verrerie,

92197 Meudon cedex, France

Samsung Electronics Co.

17 Floor, B-Tower, DSR building,

Samsungjeonja-ro 1-1, Hwaseong-si, Gyeonggi-do

445-330 Corée du Sud

Commanditaire

Gemalto

6, rue de la Verrerie, 92197 Meudon cedex, France

Centre d'évaluation

Serma Safety & Security

14 rue Galilée, CS 10071, 33608 Pessac Cedex, 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 la carte à puce « BELPIC V1.8 applet on MultiApp V4.1 Platform » développée par la société *GEMALTO* et embarquée sur le microcontrôleur S3FT9MH, fabriqué par la société *SAMSUNG ELECTRONICS CO.*

Cette carte à puce dispose d'une interface contact. Elle est destinée à être utilisé comme dispositif sécurisé de création de signature électronique (SSCD) pour le marché de carte d'identité belge.

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 strictement conforme aux profils de protection [PP-SSCD-Part2] et [PP-SSCD-Part5].

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la génération des clés de signature (c'est-à-dire la génération de la donnée de création de signature (SCD[1]) et de la donnée de vérification de signature (SVD[2]) associée) ;
- la protection en confidentialité et en intégrité de la clé privée (la SCD) ;
- l'export de clé publique (c'est-à-dire la SVD) vers le CGA[3] ;
- l'initialisation de la RAD[4] ;
- l'identification et l'authentification d'utilisateurs de confiance ou d'applications à travers un code PIN ;
- la création de signature électronique ;
- la création d'un canal de communication de confiance.

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

1.2.3. Architecture

Le périmètre d'évaluation (TOE[5]) est illustré par la figure ci-après, il est constitué :

- du microcontrôleur « S3FT9MH » développé par *SAMSUNG ELECTRONICS CO.* et certifié sous la référence [CER-IC] ;

[1] *Signature Creation Data*.
[2] *Signature Verification Data*.
[3] *Certification Generation Application*.
[4] *Reference Authentication Data*.
[5] *Target Of Evaluation* – cible d'évaluation

- de la plateforme *Java Card* ouverte « MultiApp V4.1», développée par *GEMALTO* et certifiée sous la référence [CER-PTF] ;
- de l'application « BELPIC V1.8 » développée par *GEMALTO*.

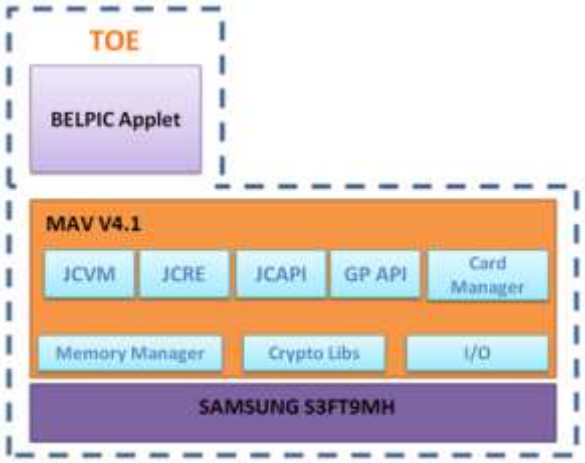

Figure 1 : Architecture de la TOE

Des applications peuvent être chargées sur la plateforme Java Card ouverte, au côté de l'application « BelPIC v1.8 ». La conformité aux prescriptions du document [OPEN] pour le chargement d'applications a été prise en compte pour les seules applications identifiées dans le certificat de la plateforme [CER-PTF].

En complément, les guides de la plateforme [PTF-AGD] identifient les recommandations relatives à la livraison des applications à charger sur cette carte. Par ailleurs, les guides [PTF-AGD-DevBasic] et [PTF-AGD-DevSec] décrivent les règles de développement des applications destinées à être chargées sur cette carte, et les règles de vérification qui doivent être appliquées par l'autorité de vérification sont décrites dans le guide [AGD-OPE-VA].

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 du tableau ci-après, détaillés dans la cible de sécurité [ST] au chapitre 3.2 « TOE identification ».

Eléments de configuration		Origine
Nom de la TOE	BelPIC V1.8 on MultiApp V4.1	*GEMALTO*
Référence de l'application Révision de l'application	« 18 » (*applet version* : v1.8) « 00 01 » (révision 1.0)	
Référence de la plateforme Révision de la plateforme	« 5B » (*OS number* : MultiApp v4.1) « 01 » (*OS version* : v1)	
Référence du circuit intégré	« 20 » (Samsung S3FT9MH)	*SAMSUNG ELECTRONICS CO.*

Ces éléments peuvent être vérifiés par l'utilisation de la commande GET CARD DATA (voir [GUIDES]).

1.2.5. Cycle de vie

Le cycle de vie est décrit au chapitre 4.5 de la cible de sécurité [ST] et illustré par la figure ci-dessous. Il suit les sept phases du profil de protection [PP0084] :

- phase 1 : développement du logiciel embarqué, c'est-à-dire de la plateforme et de l'application ;
- phase 2 : développement du microcontrôleur ;
- phase 3 : fabrication et test du microcontrôleur ;
- phase 4 : *packaging* (fabrication et test du module carte à puce) ;
- phase 5 :
  - 5a : pré-personnalisation ;
  - 5b : fabrication *supply chain* (intégration du module carte à puce dans le corps plastique),
- phase 6 : personnalisation ;
- phase 7 : utilisation opérationnelle.

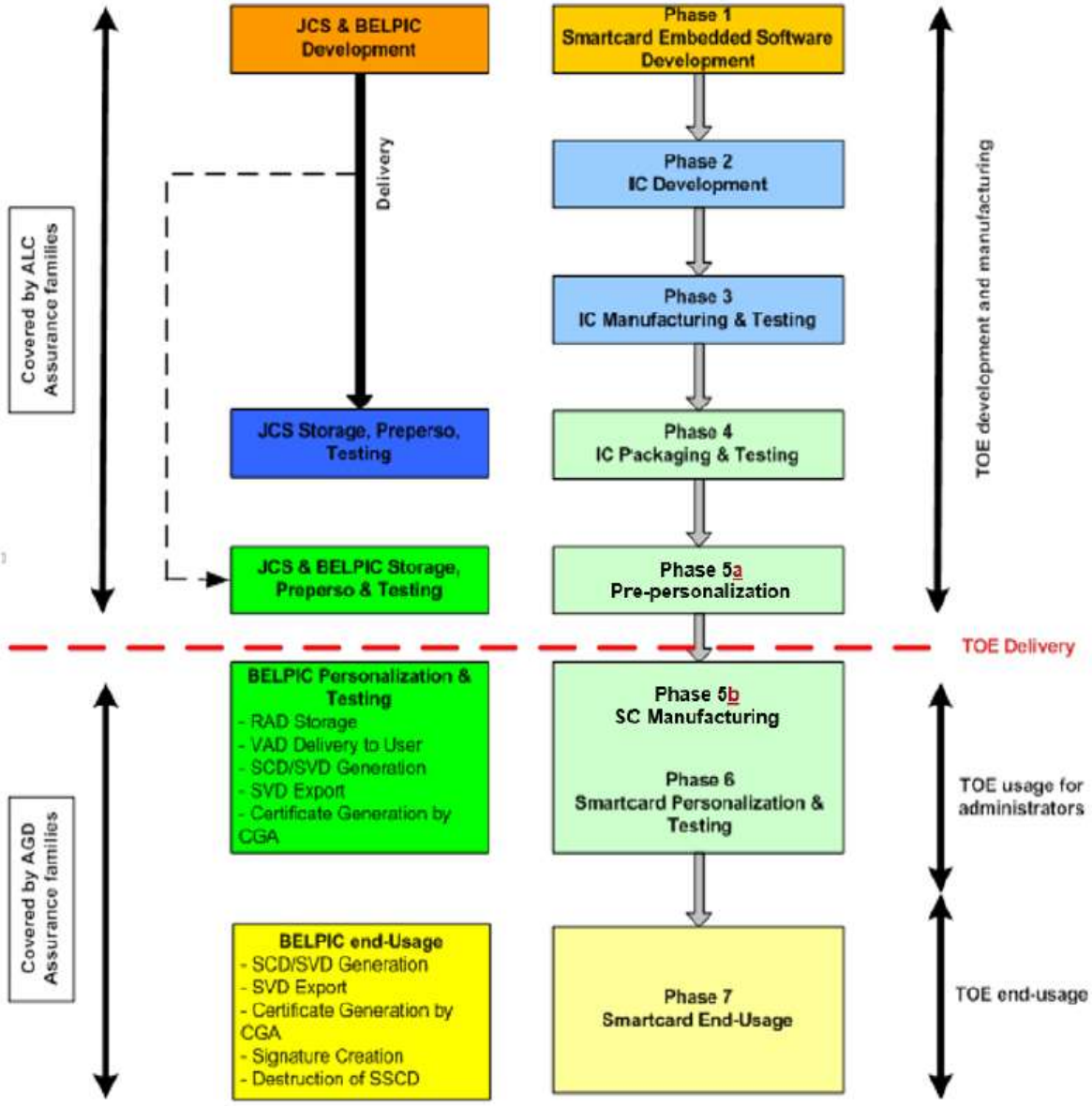

Figure 2 : Cycle de vie

Le point de livraison, ou d'émission de la carte, est en sortie de phase 5a. Jusqu'à cette phase, le produit est considéré comme étant en construction. Ainsi :

- les phases 1, 4 et 5 sont réalisées par *GEMALTO* et couvertes par les audits des sites suivants (voir [SITES]) :

***GEMALTO* Meudon [GEN17], [MDN]** 6 rue de la Verrerie, 92197 Meudon, France	***GEMALTO* Singapore [GEN18], [SGP]** 12Ayer Rajah Crescent. 139941, Singapore, Singapore
***GEMALTO* Barcelona [GEN18], [BAR]** Poligono Industrial Llevant, CL Llevant 12, 08150 Parets del Valles, Barcelona, Spain	***GEMALTO* Gemenos [GEN18], [GEM]** 251 avenue du Pic de Bertagne, 13881 Gemenos, France
***ATOS* Aubervilliers [GEN18], [PAR]** 153 avenue Jean Jaurès, 93307 Aubervilliers Cedex, France	***ATOS* Croissy [GEN18], [PAR]** 4 rue des vieilles vignes, 77183 Croissy Beaubourg, France
***ATOS* Pune [GEN19], [PUN]** Embassy Tech Zone, Phase II, Rajiv Gandhi Infotech Park, MIDC, Hinjewadi, Pune – 411057, India	

- les phases 2 et 3 sont assurées par le développeur du microcontrôleur, à savoir *SAMSUNG ELECTRONICS CO.* Les sites de développement et de fabrication de ce microcontrôleur sont détaillés dans le rapport de certification [CER-IC].

1.2.6. Configuration évaluée

Le certificat porte sur l'application « BelPIC v1.8 » en composition sur la plateforme ouverte Java Card « MultiApp V4.1 » masquée sur le microcontrôleur S3FT9MH, telles que présentées au chapitre « 1.2.3 Architecture ».

La configuration ouverte du produit a été évaluée conformément à [OPEN] : ce produit correspond à une plateforme ouverte cloisonnante. Tout chargement de nouvelles applications doit être effectué conformément aux processus audités et doit répondre aux contraintes exposées au chapitre 3.2 de ce présent rapport de certification et du rapport de certification de la plateforme [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 26 juin 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 conformément au référentiel technique de l'ANSSI [REF]. Les résultats obtenus ont fait l'objet d'un rapport d'analyse inclus dans le [RTE]. Afin que les mécanismes analysés soient conformes aux exigences du référentiel cryptographique de l'ANSSI ([REF]), les recommandations données dans le document [AGD-CPS] doivent être respectées.

Dans le cadre du processus de certification eIDAS, une expertise de l'implémentation de la cryptographie a été réalisée par le CESTI, voir [RTE].

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 pseudo-aléatoires utilisé par le produit final a été évalué dans le cadre de l'évaluation de la plateforme (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 « BELPIC V1.8 applet on MultiApp V4.1 Platform, révision 1.0 » 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], notamment :

- toutes les applications chargées en *post-issuance* sur ce produit doivent respecter les contraintes de développement de la plateforme (voir [PTF-AGD-DevBasic] et [PTF-AGD-DevSec]) selon la sensibilité de l'application considérées, notamment toutes les applications y compris celles chargées en pre-issuance doivent être vérifiée avec la dernière version disponible du *bytecode verifier* ;
- les autorités de vérification doivent appliquer le guide [AGD-OPE-VA] ;
- la protection du chargement de toutes les applications sur ce produit doit être activée conformément aux indications des guides [PTF-AGD].

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 : - BelPIC V1.8 applet on MultiApp v4.1 Platform – Security Target, référence D1459901, version 1.12 du 26/02/2019, *GEMALTO*. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - BelPIC V1.8 applet on MultiApp v4.1 Platform – Security Target, référence D1459901_P, version 1.1 du 26/02/2019, *GEMALTO*.
[RTE]	Rapport technique d'évaluation : - Evaluation Technical Report – HORTA project, référence HORTA_ETR_v1.1, version 1.1 du 26/06/2019, *SERMA SAFETY & SECURITY*.
[CONF]	Listes de configuration du produit : - D1479077-LIS-DOC-BELPICv18.xlsx, référence D1479077, version 1.11du 07/06/2019, *GEMALTO* ; - Configuration list: BELPIC v1.8 code, référence LIS_CODE.belpic.releasecandidate.0010_v1.0.txt, version 1.0 du 31/01/2019, *GEMALTO* ; - Configuration list: BELPIC v1.8 doc, référence LIS_DOC.belpic.prjdocs.releasecandidate.0010_v1.6.txt, version 1.6 du 07/06/2019, *GEMALTO*.
[GUIDES]	Guide d'installation et d'administration du produit [AGD-PRE-OPE] : - BELPIC V1.8 Applet on MultiApp ID V4.1 Platform AGD Top-level Document, référence D1468995, version 1.7 du 29/01/2019, *GEMALTO* ; - Annexe.08.General.Technical .Specification.Belpic.Applet.v1.8, référence D1459928, version 1.8h, *GEMALTO*. Guide de personnalisation d'applications sécurisées [AGD-CPS] : - Personalization Manual Applet For Belpic v1.8, référence D1446778, version 1.12 du 29/01/2019, *GEMALTO*. Guides d'installation et d'administration de la plateforme [PTF-AGD] : - MultiApp V4.1 AGD_PRE document - Javacard Platform, version 1.0, 5 juin 2017, référence D1431347, *GEMALTO* ; - MultiApp V4.1 : AGD_OPE document – Javacard Platform, version 1.5, 16 mars 2018, référence D1424308, *GEMALTO*. Guide de développement d'applications basiques [PTF-AGD-DevBasic] : - Rules for applications on Multiapp certified product, version 1.2, novembre 2017, référence D1390963, *GEMALTO* ; - GlobalPlatform Card Composition Model, Security Guidelines for Basic Applications, version 2.0, public release, novembre 2014, reference GPC_GUI_050.

	Guides de développement d'applications sécurisées [PTF-AGD-DevSec] : - Guidance for secure application development on Multiapp platforms, version A01, mars 2018, référence D1390326, *GEMALTO*. Guides pour l'autorité de vérification [AGD-OPE-VA] : - Verification process of Gemalto non sensitive applet, version A01, février 2016, référence D1390670, *GEMALTO* ; - Verification process of Third Party non sensitive applet, version A01, février 2016, référence D1390671, *GEMALTO*.
[SITES]	Rapports d'analyse documentaire : - [GEN17] o GEMALTO Development Environment (Generic activities – Full Report), référence 17-0118_GEN_V1.0, février 2017, *SERMA SAFETY & SECURITY*, - [GEN18] o GEMALTO Development Environment – ALC Class Evaluation Report (Generic Documentary activities), référence 17-0466_ALC-GEN_V1.0, mars 2018, *SERMA SAFETY & SECURITY*, - [GEN19] o GEMALTO Development Environment ALC Class Evaluation Report (Generic Documentary activities), référence GTOGEN19_GEN_v1.0, février 2019, *SERMA SAFETY & SECURITY*. Rapports d'audit de site pour la réutilisation : - [BAR] o GEMALTO Development Environment BARCELONA Site Visit Report (Lite Report), référence 17-0466_BAR_STAR_v1.0, août 2018, *SERMA SAFETY & SECURITY*, - [GEM] o GEMALTO Development Environment GEMENEOS Site Visite Lite Report, 170466_GEM_SVR-M_v1.1, novembre 2018, *SERMA SAFETY & SECURITY*, - [MDN] o GEMALTO Development Environment MEUDON Site Visit Report (Lite Report), référence 17-0118-MDN_SVR-M_v1.0, juillet 2017, *SERMA SAFETY & SECURITY*, - [PAR] o Site Technical Audit Report ATOS_PAR, référénce ATOS_PAR_STAR_v1.0, août 2018, *SERMA SAFETY & SECURITY*, - [SGP] o GEMALTO Development Environment Singapore Site Visit Lite Report, référence 17-0466-SGP_SVR-M_v1.0, mai 2018, *SERMA SAFETY & SECURITY*,

	- [PUN] o Site Technical Audit Report – ATOS Pune (PUN), référénce GTOGEN19_PUN_STAR_v1.0, avril 2019, *SERMA SAFETY & SECURITY*.
[CER-IC]	Rapport de certification ANSSI-CC-2017/24, S3FT9MH / S3FT9MV / S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional Secure RSA and ECC Library including specific IC Dedicated Software. *Certifié par l'ANSSI le 11 mai 2017 sous la référence ANSSI-CC-2017/24.*
[CER-PTF]	Rapport de certification ANSSI-CC-2018/32, Plateforme ouverte Java Card MultiApp V4.1 en configuration ouverte masquée sur le composant S3FT9MH. *Certifiée par l'ANSSI le 3 août 2018 sous la référence ANSSI-CC-2018/32.*
[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-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.*
[PP0084]	Protection Profile, Security IC Platform Protection Profile with Augmentation Packages, version 1.0, 13 janvier 2014. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0084-2014.*

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.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 2.00 du 8 juin 2012 annexée au Référentiel général de sécurité (RGS_B2), voir www.ssi.gouv.fr.

	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010 annexée au Référentiel général de sécurité (RGS_B3), 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.