PREMIER MINISTRE

Liberté
Égalité
Fraternité

Secrétariat général de la défense et de la sécurité nationale

Agence nationale de la sécurité des systèmes d'information

Rapport de certification ANSSI-CC-2025/56

BELPIC V1.8 applet On MultiApp V4.1 Platform (Révision 1.0 version 2)

Paris, le 2/2/2026 | 18:35 CET

Vincent Strubel

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

PREFACE

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 directeur général de l'Agence nationale de la sécurité des systèmes d'information attestent que l'exemplaire des produits 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.cyber.gouv.fr.

TABLE DES MATIERES

1 Résumé

Référence du rapport de certification **ANSSI-CC-2025/56**
Nom du produit **BELPIC V1.8 applet On MultiApp V4.1 Platform**
Référence/version du produit **Révision 1.0 version 2**
Type de produit **Cartes à puce et dispositifs similaires**
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.
Critère d'évaluation et version **Critères Communs version 3.1 révision 5**
Niveau d'évaluation **EAL5 augmenté** ALC_DVS.2, AVA_VAN.5
Référence du rapport d'évaluation *Evaluation Technical Report HORTA-R02 Project* référence HORTA-R02_ETR_v1.0 version 1.0 14 aout 2025.
Fonctionnalité de sécurité du produit voir 2.2.2 Services de sécurité
Exigences de configuration du produit voir 4.2 Restrictions d'usage
Hypothèses liées à l'environnement d'exploitation voir 4.2 Restrictions d'usage
Développeur **THALES DIS FRANCE SAS** 6, rue de la Verrerie, 92197 Meudon cedex, France
Commanditaire **THALES DIS FRANCE SAS** 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

2 Le produit

2.1 Présentation du produit

Le produit évalué est l'application « BELPIC V1.8 applet On MultiApp V4.1 Platform, Révision 1.0 version 2 » développée par THALES DIS FRANCE SAS. et embarquée sur le microcontrôleur S3FT9MH, fabriqué par la société SAMSUNG ELECTRONICS CO. LTD.

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.

2.2 Description du produit

2.2.1 *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] et [PP-SSCD-Part5].

2.2.2 *Services de sécurité*

Les principaux services de sécurité fournis par le produit sont détaillés dans la cible de sécurité [ST] au chapitre 10.1.2 « *TOE security functionalities provided by Belpic applet* ». Ils sont résumés ci-après :

- 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].

2.2.3 *Architecture*

Le périmètre d'évaluation (TOE) est décrit au chapitre 4.1 « *TOE boundaries* » de la cible de sécurité [ST].

[1] *Signature Creation Data*.

[2] *Signature Verification Data*.

[3] *Certification Generation Application*.

[4] *Reference Authentication Data*.

Il est constitué :

- du microcontrôleur « S3FT9MH », développé par SAMSUNG ELECTRONICS CO. LTD et certifié sous la référence [CER-IC] ;
- de la plateforme *JavaCard* ouverte « MultiApp V4.1 », développée par THALES DIS FRANCE SAS et certifiée sous la référence [CER-PTF] ;
- de l'application « BELPIC V1.8 » développée par THALES DIS FRANCE SAS.

Des applications peuvent être chargées sur la plateforme *JavaCard* 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].

Bien que ces applications ne soient pas incluses dans le périmètre de l'évaluation, elles ont été prises en compte dans le processus d'évaluation conformément aux prescriptions de [OPEN]. En effet, ces applications ont été vérifiées conformément aux contraintes de développements d'applications décrites dans le rapport de certification [CER-PTF].

2.2.4 *Identification du produit*

La version certifiée du produit est identifiable par les éléments détaillés dans la cible de sécurité [ST] au chapitre 3.2 « *TOE Identification* ».

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

2.2.5 *Cycle de vie*

Le cycle de vie est décrit au chapitre 4.5 *« Life-cycles »* de la cible de sécurité [ST].

Les rapports des audits de sites effectués dans le schéma français et pouvant être réutilisés, hors certification de site, sont mentionnés dans [SITES].

Les guides [PTF_AGD] identifient des recommandations relatives à la livraison des futures applications à charger sur cette carte.

Par ailleurs, les guides [AGD-Dev_Basic] et [AGD-Dev_Sec] décrivent les règles de développement des applications destinées à être chargées sur cette carte ; le guide [AGD-OPE-VA] décrit les règles de vérification qui doivent être appliquées par l'autorité de vérification

2.2.6 *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 « 2.2.3 Architecture ».

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 4.2 du présent rapport de certification ne remet pas en cause le présent rapport de certification lorsqu'il est réalisé selon les processus audités.

3 L'évaluation

3.1 Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs [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 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).

3.2 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.

Cette évaluation a ainsi pris en compte les résultats de l'évaluation de la « Plateforme Java Card MultiApp V4.1 », voir [CER- PTF].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le jour de sa finalisation par le CESTI (voir date en bibliographie), détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

3.3 Analyse des mécanismes cryptographiques selon les référentiels techniques de l'ANSSI

Les mécanismes cryptographiques mis en œuvre par les fonctions de sécurité du produit (voir [ST]) ont fait l'objet d'une analyse conformément à la procédure [CRY-P-01] et les résultats ont été consignés dans le rapport [RTE].

Cette analyse a identifié des non-conformités par rapport au référentiel [ANSSI Crypto]. Elles ont été prises 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 d'attaquant visé.

L'utilisateur doit se référer aux [GUIDES] afin de configurer le produit de manière conforme au référentiel [ANSSI Crypto], pour les mécanismes cryptographiques qui le permettent.

4 La certification

4.1 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 soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation visé (voir chapitre 1 Résumé).

Le certificat associé à ce rapport, référencé ANSSI-CC-2025/56 a une date de délivrance identique à la date de signature de ce rapport et a une durée de validité de cinq ans à partir de cette date.

4.2 Restrictions d'usage

Ce certificat porte sur le produit spécifié au chapitre 2.2 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--émission) doivent respecter les contraintes de développement de la plateforme (guides [AGD-Dev_Basic] et [AGD-Dev_Sec]) selon la sensibilité de l'application considérées ;
- les autorités de vérification doivent appliquer le guide [AGD-OPE_VA] ;
- la protection du chargement de toutes les futures applications chargées sur ce produit (chargement post-émission) doit être activée conformément aux indications de [TECH_LOAD] ;
- le chargement des applications pré- émission doit être protégé conformément au guide [ORG_LOAD] ;

4.3 Reconnaissance du certificat

4.3.1 *Reconnaissance européenne (SOG-IS)*

Ce certificat est émis dans les conditions de l'accord du SOG-IS [SOG-IS].

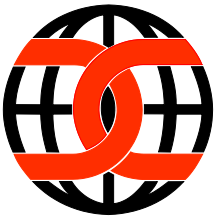
L'accord de reconnaissance européen du SOG-IS de 2010 permet la reconnaissance, par les pays signataires de l'accord[5], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique, pour les cartes à puce et les dispositifs similaires, jusqu'au niveau ITSEC E6 Elevé et CC EAL7 lorsque les dépendances CC sont satisfaites. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

4.3.2 *Reconnaissance internationale critères communs (CCRA)*

Ce certificat est émis dans les conditions de l'accord du CCRA [CCRA].

L'accord « *Common Criteria Recognition Arrangement* » permet la reconnaissance, par les pays signataires[6] , 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 :



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

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

ANNEXE A. 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 1.21, 08/08/2025. 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 – Public Version*, référence D1459901_P, version 1.21p, août 2025.
[RTE]	Rapport technique d'évaluation : *Evaluation Technical Report HORTA-R02 Project*, référence HORTA-R02_ETR_v1.0, version 1.0, 14 août 2025.
[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 1.9, 02 juin 2023. Guide de personnalisation d'applications sécurisées [AGD-CPS] : - *Personalization Manual Applet For Belpic v1.8*, référence D1446778, version 1.14, 01 juin 2023. Guide d'installation et d'administration de la plateforme [PTF_AGD]: - *MultiApp ID Operating System –Reference Manual*, référence D1392687I, 13 avril 2021. Guide de développement d'applications basiques [AGD-Dev_Basic] : - *Rules for applications on Multiapp certified product,* référence D1390963, version 1.2, novembre 2017. Guide de développement d'applications sécurisées [AGD-Dev_Sec] : - *Guidance for secure application development on Multiapp platforms,* référence D1390326, version A05, juillet 2025. Guides pour l'autorité de vérification [AGD_OPE_VA] : - *Verification process of Gemalto non sensitive applet*, référence D1390670, version A01, février 2016 ; - *[ORG_LOAD] Verification process of Third Party non sensitive applet,* référence D1390671, version A01, février 2016.
[SITES]	Rapports d'analyse documentaire et d'audit de site pour la réutilisation : - DISGEN23_ALC_GEN_v1.1 ; - DISGEN24_ALC_GEN_v1.1 ; - DISGEN25_ALC_GEN_v1.2 ;

	- [ELC] DISGEN24_ELC_ STAR_v1.1 ; - [GEM] DISGEN24_GEM_ STAR_v1.0 ; - [LVG] DISGEN24_LVG_ STAR_v1.1 ; - [MDN] DISGEN23_MDN_ STAR_v1.1 ; - [SGP] DISGEN24_SGP_ STAR_v1.0 ; - [SSN_SSC] DISGEN23_SSN_ SSC_STAR_v1.1 ; - [TLH] DISGEN23_TLH_ STAR_v1.0 ; - [VFO-CAL] DISGEN25_VFO-CAL_STAR_v1.0
[CER-IC]	Rapport de *certification S3FT9MH/S3FT9MV/S3FT9MG 16-bit RISC Microcontroller for Smart Card with optional CE1 Secure RSA/ECC/SHA Libraries including specific IC Dedicated Software (S3FT9MH_20220713)*. Certifié par l'ANSSI sous la référence ANSSI-CC-2023/20-R02.
[CER-PTF]	Rapport de certification MultiApp v4.1 Javacard Platform (Version 4.1.0.4) Certifié par l'ANSSI sous la référence ANSSI-CC-2025/53
[PP-SSCD-Part2]	*Protection profiles for secure signature creation device – Part 2: Device with key generation*, référence : prEN 419211-2:2013, version 2.0.1 datée du 18 mai 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0059-2009-MA-02.
[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 419211-5:2013, version 1.0.1 datée du 12 octobre 2013. Maintenu par le BSI (*Bundesamt für Sicherheit in der Informationstechnik*) le 30 juin 2016 sous la référence BSI-CC-PP-0072-2012-MA-01.

ANNEXE B. 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]	Certification critères communs de la sécurité offerte par les produits, les systèmes des technologies de l'information, ou les profils de protection, référence ANSSI-CC-CER-P-01, version 5.4.
[CRY-P-01]	Modalités pour la réalisation des analyses cryptographiques et des évaluations des générateurs de nombres aléatoires, référence ANSSI-CC-CRY-P01, version 4.1.
[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 AP] *	*Mandatory Technical Document – Application of attack potential to smartcards and similar devices*, version 3.2.1, février 2024.
[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 2.0, mai 2024.
[CCRA]	*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.
[ANSSI Crypto]	Guide des mécanismes cryptographiques : Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, ANSSI-PG-083, version 2.04, janvier 2020.

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