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-2015/07

Xaica-AlphaPLUS
Version 0116 (PQV) / 0100 (SPI-001 03)

Paris, le 31 mars 2015

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

Guillaume POUPARD
[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-2015/07

Nom du produit

Xaica-AlphaPLUS

Référence/version du produit

Version 0116 (PQV) / 0100 (SPI-001 03)

Conformité à un profil de protection

[PP-PNC], version 1

Personal Number Cards Protection Profile

Critères d'évaluation et version

Critères Communs version 3.1 révision 4

Niveau d'évaluation

EAL 4 augmenté

ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, AVA_VAN.5

Développeurs

NTT DATA Corporation

Toyosu Center Bldg. Annex,
3-9 Toyosu 3-chome, Koto-ku,
TOKYO 135-8671, Japon

STMicroelectronics

190 Avenue Célestin Coq,
ZI de Rousset,
13106 Rousset Cedex, France

Commanditaire

NTT DATA Corporation

Toyosu Center Bldg. Annex, 3-9 Toyosu 3-chome, Koto-ku, TOKYO 135-8671, Japon

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 EAL4.

Préface

La certification

La certification de la sécurité offerte par les produits et les systèmes des technologies de l'information est régie par le décret 2002-535 du 18 avril 2002 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 « Xaica-AlphaPLUS**,** Version 0116 (PQV) / 0100 (SPI-001 03) » développé par NTT DATA Corporation et STMicroelectronics.

Le produit évalué est de type carte à puce avec et sans contact. Il implémente une carte d'identité et des applications gouvernementales japonaises.

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-PNC]. La conformité est 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 du tableau ci-après, qui sont renvoyés par le produit suite à la commande GET DATA avec le tag **'46h'** (voir [GUIDES]) :

Champ	**Valeur**	**Signification**
IC Manufacturer	'0000000002'	STMicroelectronics
Card Manufacturer	'4A50303342'	Outsource
Issue identification	'14140A05'	PQV BANGO card
TOE Version	'0116'	PQV code sur microcontrôleur ST23R160 en révision interne F, incluant NesLib V3.1
« *Softmask revision* »	'0100'	SPI-001-03

1.2.3. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- la protection de l'intégrité des données du porteur stockées dans la carte : pays ou organisation de délivrance, numéro du document, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait du porteur, autres données optionnelles ;
- la protection de l'intégrité et de la confidentialité des données lues à l'aide du mécanisme *secure messaging* ;
- l'authentification du microcontrôleur pour l'exécution des applications BANGO-AP, JUKI-AP, JPKI-AP et KENMAN-AP (voir [ST] pour la description des applications).

1.2.4. Architecture

L'architecture du produit est résumée par la figure 1.

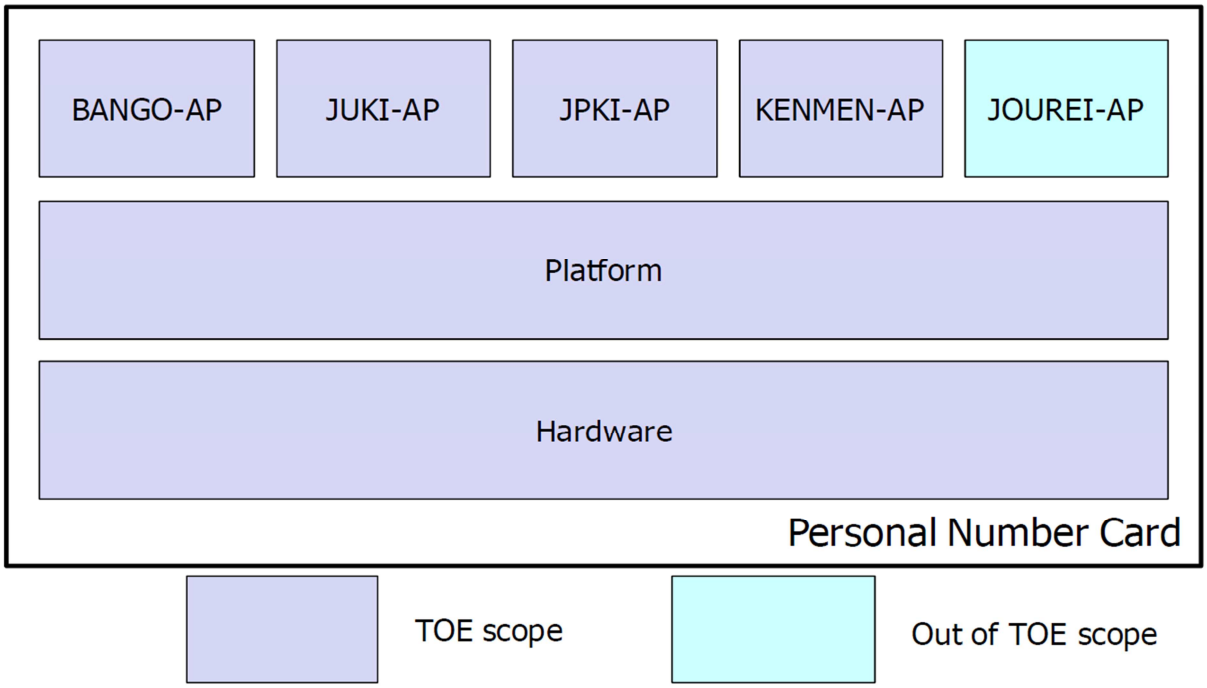

Figure 1 – Architecture du produit

Le produit est une carte à puce constitué :

- du microcontrôleur ST23R160 en révision interne F avec librairie cryptographique NesLib v3.1, développé et fabriqué par STMicroelectronics ;
- d'un système d'exploitation ;
- de l'application IAP (application d'initialisation) permettant de personnaliser les cartes vierges ;
- des applications requises par le profil de protection [PP-PNC], identifiées dans [ST] et dans [GUIDES] : BANGO-AP, JUKI-AP, JPKI-AP et KENMAN-AP ;
- d'un *Card Manager* se comportant comme une application *Global Platform*. Il permet notamment de créer les fichiers requis par les applications susmentionnées.

Note : Le profil de protection [PP-PNC] mentionne que d'autres applications gouvernementales peuvent être installées sur la plateforme (application JOUREI-AP en dehors du périmètre de la TOE décrit ci-dessus figure 1).

1.2.5. Cycle de vie

Le cycle de vie du produit est basé sur celui du profil de protection [PP-PNC] :

- phase 1 : développement du composant et du logiciel ;
- phase 2 : développement du logiciel (développement de la plateforme, des applications susmentionnées et du script de pré-personnalisation appelé *OUT SOURCE*) ;
- phase 3 : fabrication ;
- phase 4 : personnalisation ;
- phase 5 : installation des applications additionnelles ;
- phase 6 : utilisation de la carte.

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

- sites de développement du logiciel :

  - **NTT DATA Corporation Toyosu Center Building**
    3-3-9 Toyosu
    Koto-ku Tokyo
    Japan 135-8671
  - **TOPPAN Printing Koishikawa Building**
    1-3-3, Suido
    Bunkyo-ku Tokyo
    Japan

- site de développement et fabrication du microcontrôleur :
  - **STMicroelectronics**
    190 Avenue Célestin Coq
    ZI de Rousset
    13106 Rousset Cedex
    France

Les composants sont développés et fabriqués par STMicroelectronics. Les sites de développement et de fabrication des puces STMicroelectronics sont détaillés dans le rapport de certification [CER-IC], ainsi que dans les rapports de maintenance [CER-IC_M02] et [CER-IC_M03].

1.2.6. Configuration évaluée

Le certificat porte sur la configuration de la TOE décrite au paragraphe 1.2.4 et configuré conformément aux [GUIDES]. La TOE est considérée comme étant une plateforme fermée sans l'application JOUREI-AP (les interfaces de la TOE avec cette application ne sont pas évaluées).

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux Critères Communs version 3.1 révision 4 [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 « *ST23R160 »* (révision F) au niveau EAL6 augmenté du composant ALC_FLR.1, conforme au profil de protection [PP-0035]. Ce microcontrôleur a été certifié le 08 novembre 2012 sous la référence [CER-IC] et maintenu sous les références [CER-IC_M01], [CER-IC_M02] et [CER-IC_M03]. Le niveau de résistance du microcontrôleur a été confirmé le 22 décembre 2014 dans le cadre du processus de surveillance, voir [SUR_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 18 mars 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 [REF-CRY] de l'ANSSI 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 d'aléas du produit était en dehors du périmètre de l'évaluation et n'a pas été analysé. Le générateur d'aléas utilisé par le produit final a cependant été évalué dans le cadre de l'évaluation du microcontrôleur (voir [CER-IC]).

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 « Xaica-AlphaPLUS, Version 0116 (PQV) / 0100 (SPI-001 03) » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL4 augmenté des composants ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.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 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 EAL4 ainsi qu'à la famille ALC_FLR. Les certificats reconnus dans le cadre de cet accord sont émis avec la marque suivante :

[1] Les pays signataires de l'accord SOG-IS sont : l'Allemagne, l'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 4+	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 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**	**1**	Testing: basic 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 : - Xaica-alphaPLUS Security Target, 04 mars 2015, référence Xaica-alphaPLUS-SPC_ST, version 1.1. Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Xaica-alphaPLUS Security Target Lite, 04 mars 2015, référence Xaica-alphaPLUS-SPC_ST_lite, version 1.1.
[RTE]	Rapport technique d'évaluation : Evaluation Technical Report – ALPHA-PLUS Project, 18 mars 2015, référence ALPHA-PLUS_ETR_V1.2, version 1.2.
[CONF]	Liste de configuration du produit : Xaica-alphaPLUS-TCL-TOE Configuration List, version 2.2, 04 mars 2015, NTT DATA Corporation.
[GUIDES]	Guides de préparation du produit : - Delivery Procedure ICcard, 26 mars 2012, version 2.10, NTT DATA Corporation ; - Manual for BANGO-AP administrator, 03 mars 2015, version 2.30, NTT DATA Corporation ; - Manual for JPKI-AP administrator, 03 mars 2015, version 2.30, NTT DATA Corporation ; - Manual for JUKI-AP administrator, 03 mars 2015, version 2.30, NTT DATA Corporation ; - Manual for KENMEN-AP, administrator, 03 mars 2015, version 2.30, NTT DATA Corporation ; - Manual for Platform administrator, 03 mars 2015, version 2.30, NTT DATA Corporation ; - Manual for PrePerso and OUTSOURCE Specifications, version 2.00, 27 janvier 2014, NTT DATA Corporation; - Manual for Cardholder, 15 janvier 2015, version 2.00, NTT DATA Corporation.
[CER-IC]	« Microcontrôleurs sécurisés ST23R160/80A/48A et ST23L160/80A/48A, incluant optionnellement la bibliothèque cryptographique NesLib v3.1 », référence Maskset K2V0A, révision interne B. C*ertifié par l'ANSSI le 8 novembre 2012 sous la référence ANSSI-CC-2012/77.*
[SUR-IC]	« ST23R160 & produits dérivés », r*apport de surveillance du 22 décembre 2014 sous la référence ANSSI-CC-2012/77-S02.*
[CER-IC_M01]	Rapport de maintenance ANSSI-CC-2012/77-M01, délivré le 11 juillet 2013, relatif au certificat ANSSI-CC-2012/77.
[CER-IC_M02]	Rapport de maintenance ANSSI-CC-2012/77-M02, délivré le 04 mars 2014, relatif au certificat ANSSI-CC-2012/77.

[CER-IC_M03]	Rapport de maintenance ANSSI-CC-2012/77-M03, délivré le 19 février 2015, relatif au certificat ANSSI-CC-2012/77.
[PP-PNC]	Protection Profile, Personal Number Cards Protection Profile, version 1.0, mai 2015. *Certifié par le JISEC (Japan IT Security Evaluation and Certification Scheme) sous la référence CRP-C0431-01.*
[PP-0035]	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.*

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, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-001 ; Part 2: Security functional components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-002 ; Part 3: Security assurance components, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, septembre 2012, version 3.1, révision 4, référence CCMB-2012-09-004.
[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.
[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-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité, 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.