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

Certification Report ANSSI-CC-2015/07

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

Paris, March 31, 2015

Courtesy Translation

SÉCURITÉ CERTIFICATION

Warning

This report is designed to provide sponsors with a document enabling them to assess the security level of a product under the conditions of use and operation defined in this report for the evaluated version. It is also designed to provide the potential purchaser of the product with the conditions under which he may operate or use the product so as to meet the conditions of use for which the product has been evaluated and certified; that is why this certification report must be read alongside the evaluated user and administration guidance, as well as with the product security target, which presents threats, environmental assumptions and the supposed conditions of use so that the user can judge for himself whether the product meets his needs in terms of security objectives.
Certification does not, however, constitute a recommendation product from ANSSI (French Network and Information Security Agency), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

Any correspondence about this report has to be addressed to:

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
France

certification.anssi@ssi.gouv.fr

Certification report reference

ANSSI-CC-2015/07

Product name

Xaica-AlphaPLUS

Product reference

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

Protection profile conformity

[PP-PNC], version 1
Personal Number Cards Protection Profile

Evaluation criteria and version

Critères Communs version 3.1 révision 4

Evaluation level

EAL 4 augmenté

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

Developer(s)

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

Sponsor

NTT DATA Corporation

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

Evaluation facility

Serma Technologies

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

Recognition arrangements

CCRA

SOG-IS

The product is recognised at EAL4 level.

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, modified. This decree stipulates that:

- The French Network and Information Security Agency draws up **certification reports**. These reports indicate the features of the proposed security targets. They may include any warnings that the authors feel the need to mention for security reasons. They may or may not be transmitted to third parties or made public, as the sponsors desire (article 7).
- The **certificates** issued by the Prime Minister certify that the copies of the products or systems submitted for evaluation fulfil the specified security features. They also certify that the evaluations have been carried out in compliance with applicable rules and standards, with the required degrees of skill and impartiality (article 8).

The procedures are available on the Internet site www.ssi.gouv.fr.

Contents

1. The product

1.1. Presentation of the product

The evaluated product is "Xaica-AlphaPLUS**,** Version 0116 (PQV) / 0100 (SPI-001 03)" developed by NTT DATA Corporation and STMicroelectronics.

The evaluated product is a smart card with contact and contactless. It implements an identity card and governmental Japanese applications.

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operational environment.

The security target is based on [PP-PNC]. Its compliance can be proven.

1.2.1. Product identification

The configuration list [CONF] identifies the product's constituent elements.

The certified version of the product can be identified by the following elements, which have sent by the product after the command GET DATA with the tag **'46h'** (see [GUIDES]):

Field	**Value**	**Signification**
IC Manufacturer	'0000000002'	STMicroelectronics
Card Manufacturer	'4A50303342'	Outsource
Issue identification	'14140A05'	PQV BANGO card
TOE Version	'0116'	PQV code on microcontroller ST23R160 in internal revision F, with NesLib V3.1
Softmask revision	'0100'	SPI-001-03

1.2.2. Security services

The product provides mainly the following security services:

- Integrity protection of user data stored in the card: country or delivery organization, document number, user name, expiry date, nationality, date of birth, gender, user's picture, other optionally data;
- Confidentiality and/or integrity protection of communication data read using the "secure messaging" mechanism;
- Authentication of the microcontroller to execute the applications BANGO-AP, JUKI-AP, JPKI-AP and KENMAN-AP (see [ST] for description of these applications).

1.2.3. Architecture

The architecture of the product is described by the figure 1.

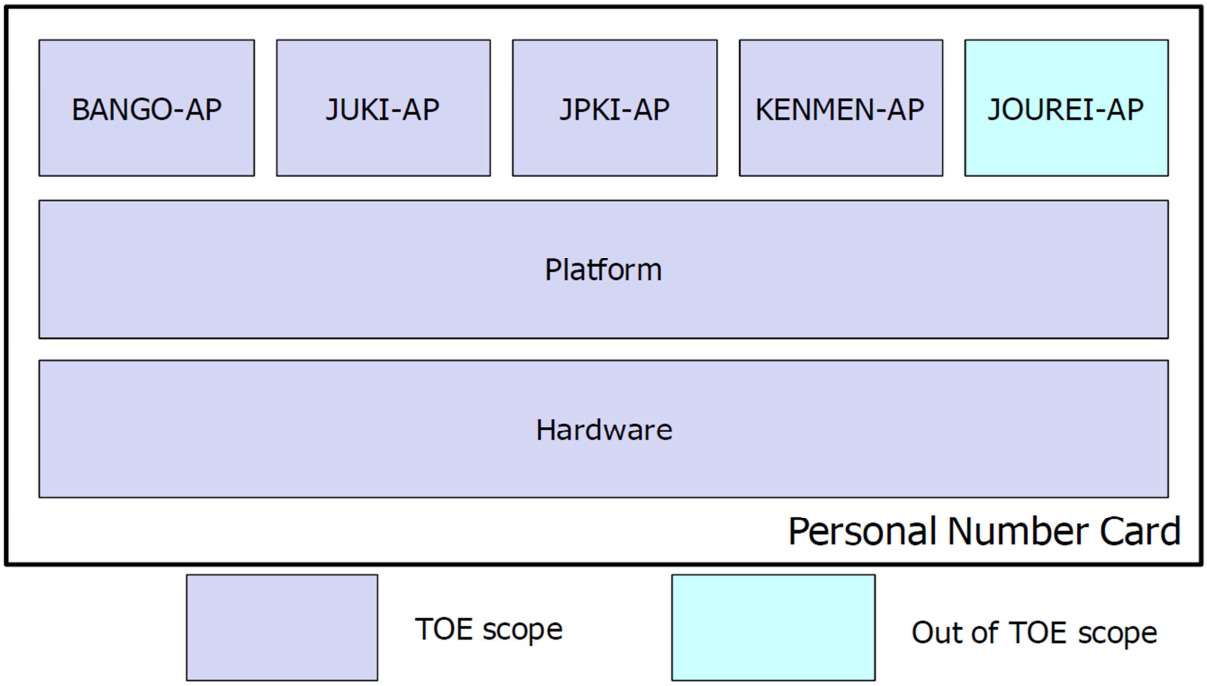

Figure 1 – Product architecture

The product is a smart card composed on:

- The microcontroller ST23R160 in internal revision F with cryptographic library NesLib v3.1 developed and manufactured by STMicroelectronics;
- The operating system (OS);
- The Initialization Application (IAP). It enables to personalize a virgin card;
- The applications required by the protection profile [PP-PNC] identified in [ST] and [GUIDES]: BANGO-AP, JUKI-AP, JPKI-AP et KENMAN-AP;
- The Card Manager behaving as a Global Platform application. It enables to create files required by the above applications.

Note: the protection profile [PP-PNC] specifies that other governmental applications can be installed on the platform (JOUREI-AP application is out of the TOE scope described by figure 1).

1.2.4. Life cycle

The product's life cycle is based on the life cycle of the protection profile [PP-PNC]:

- Phase 1: IC chip (hardware) development;
- Phase 2: Development of the platform, the applications: BANGO-AP, JUKI-AP, JPKI-AP et KENMAN-AP and OUT SOURCE script;
- Phase 3: Personal number Card production;
- Phase 4: Personal number Card issuance;
- Phase 5: Additional application installation;
- Phase 6: Use by Personal number Card holder.

The product has been developed and made on the following sites:

- Software development site:

- **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

- Production and development site of the microcontroller:
  - **STMicroelectronics**
    190 Avenue Célestin Coq
    ZI de Rousset
    13106 Rousset Cedex
    France

The microcontrollers are developed and produced by STMicroelectronics. The development and production sites of the STMicroelectronics' microcontrollers are detailed in the certification report [CER-IC] and in the maintenance reports [CER-IC_M02] and [CER-IC_M03].

1.2.5. Evaluated configuration

The certificate applies to the TOE configuration described in section 1.2.4 and configured in accordance with [GUIDES]. The TOE is considered as a closed platform without JOUREI-AP application (the TOE interfaces with this application are not evaluated).

2. The evaluation

2.1. Evaluation referential

The evaluation was carried out in compliance with **Common Criteria version 3.1 revision 4** [CC], with the Common Evaluation Methodology [CEM].

For assurance components which are not covered by [CEM] manual, the evaluation facility own evaluation methods, validated by ANSSI have been used.

In order to meet the specificities of smart cards, the [JIWG IC] and [JIWG AP] guides have been applied. Thus the reached AVA_VAN level has been determined according to the rating table of the [JIWG AP] guides that is more demanding than the default one defined in [CC] used for other types of products (software products for example).

2.2. Evaluation work

The evaluation has been performed according to the composition scheme as defined in the guide [COMP] in order to assess that no weakness comes from the integration of the software in the microcontroller already certified.
Therefore, the results of the evaluation of the microcontroller "*ST23R160*" (revision F) at EAL6 level augmented with [ALC_FLR.1], compliant with the [PP-0035] protection profile, have been used. This microcontroller has been certified the 8th November 2012 under the reference [CER-IC] and maintained under the references [CER-IC_M01], [CER-IC_M02] and [CER-IC_M03]. The microcontroller robustness level has been confirmed the 22th December 2014 in a surveillance process, see [SUR_IC].

The evaluation technical report [ETR], delivered to ANSSI March, 18, 2015 provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis

The rating of cryptographic mechanisms according to the ANSSI technical reference framework [REF-CRY] has not been carried out. Nonetheless, the evaluation has not detected any design or manufacturing vulnerabilities for the targeted AVA_VAN level.

2.4. Random number generator analysis

The hardware generator is out of the TOE scope evaluation and has not been analysed. However the hardware generator used by the final product has been evaluated in the microcontroller evaluation (see [CER-IC]).

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality of a licensed evaluation facility. All the evaluation work performed permits the release of a certificate in conformance with the decree 2002-535.

This certificate testifies that the product "Xaica-AlphaPLUS, Version 0116 (PQV) / 0100 (SPI-001 03)" submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 4 augmented for ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2 and AVA_VAN.5 components.

3.2. Restrictions

This certificate only applies on the product specified in chapter 1.2 of this certification report.

The user of the certified product shall respect the security objectives for the operational environment, as specified in the security target [ST], and shall respect the recommendations in the guidance [GUIDES].

3.3. Recognition of the certificate

3.3.1. European recognition (SOG-IS)

This certificate is released in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 2010 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable, for smart cards and similar devices, up to ITSEC E6 High and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

3.3.2. International common criteria recognition (CCRA)

This certificate is released in accordance with the provisions of the CCRA [CC RA].

The Common Criteria Recognition Arrangement allows the recognition, by signatory countries[2], of the Common Criteria certificates. The mutual recognition is applicable up to the assurance components of CC EAL4 level and also to ALC_FLR family. The certificates that are recognized in the agreement scope are released with the following marking:

1 The signatory countries of the SOG-IS agreement are: Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.

2 The signatory countries of the CCRA arrangement are: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, the Republic of Korea, Malaysia, Netherlands, New-Zealand, Norway, Pakistan, Singapore, Spain, Sweden, Turkey, the United Kingdom and the United States of America.

Annex 1. Evaluation level of the product

Class	Family	Components by assurance level							Assurance level of the product	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4+	Intitulé du composant
ADV Development	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 Guidance	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 Life-cycle support	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 Security Target Evaluation	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 Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5	5	Advanced methodical vulnerability analysis

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: - Xaica-alphaPLUS Security Target, March 4th 2015, reference Xaica-alphaPLUS-SPC_ST, version 1.1. For the needs of publication, the following security target has been provided and validated in the evaluation: - Xaica-alphaPLUS Security Target Lite, March 4th 2015, reference Xaica-alphaPLUS-SPC_ST_lite, version 1.1.
[ETR]	Evaluation technical report: Evaluation Technical Report – ALPHA-PLUS Project, March 18th 2015, reference ALPHA-PLUS_ETR_V1.2, version 1.2.
[CONF]	Configuration list: Xaica-alphaPLUS-TCL-TOE Configuration List, version 2.2, March 4th 2015, NTT DATA Corporation.
[GUIDES]	Guidance: - Delivery Procedure ICcard, March 26th 2012, version 2.10, NTT DATA Corporation; - Manual for BANGO-AP administrator, March 3rd 2015, version 2.30, NTT DATA Corporation; - Manual for JPKI-AP administrator, March 3rd 2015, version 2.30, NTT DATA Corporation; - Manual for JUKI-AP administrator, March 3rd 2015, version 2.30, NTT DATA Corporation; - Manual for KENMEN-AP, administrator, March 3rd 2015, version 2.30, NTT DATA Corporation; - Manual for Platform administrator, March 3rd 2015, version 2.30, NTT DATA Corporation; - Manual for PrePerso and OUTSOURCE Specifications, version 2.00, January 27th 2014, NTT DATA Corporation; - Manual for Cardholder, January 15th 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 », reference Maskset K2V0A, internal revision B. C*ertified by ANSSI on November 8th 2012 under the reference ANSSI-CC-2012/77.*
[SUR-IC]	« ST23R160 & produits dérivés », *surveillance report on December 22th 2014 under the reference ANSSI-CC-2012/77-S02.*
[CER-IC_M01]	Maintenance report ANSSI-CC-2012/77-M01, delivered on July 11th 2013, relative to the certificate ANSSI-CC-2012/77.

[CER-IC_M02]	Maintenance report ANSSI-CC-2012/77-M02, delivered on March 4th 2014, relative to certificate ANSSI-CC-2012/77.
[CER-IC_M03]	Maintenance report ANSSI-CC-2012/77-M03, delivered on February 19th 2015, relative to certificate ANSSI-CC-2012/77.
[PP-PNC]	Protection Profile, Personal Number Cards Protection Profile, version 1.0, May 2015. *Certified by JISEC (Japan IT Security Evaluation and Certification Scheme) under the reference CRP-C0431-01*.
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007.*

Annex 3. Certification references

Decree number 2002-535, 18th April 2002, modified related to the security evaluations and certifications for information technology products and systems.	
[CER/P/01]	Procedure CER/P/01 - Certification of the security provided by IT products and systems, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, September 2012, version 3.1, revision 4, reference CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, reference CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, reference CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, September 2012, version 3.1, revision 4, reference CCMB-2012-09-004.
[JIWG IC] *	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.
[JIWG AP] *	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, January 2013.
[COMP] *	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.
[CC RA]	Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, the 2nd July2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, the 8th January 2010, Management Committee.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20, the 26th January 2010 annexed by the general security referential, see www.ssi.gouv.fr.

*Document of the SOG-IS; the support equivalent CCRA document applies to the frame of the mutual recognition agreement of the CCRA.