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-2013/04

Xaica-Alpha PLUS ePassport Configuration BAC and Active Authentication

Xaica-Alpha PLUS ePassport Configuration BAC and Active Authentication on STMicroelectronics SB23YR80 Microcontroller

Paris, le 15 février 2013

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

Patrick Pailloux
[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-2013/04

Nom du produit

Xaica-Alpha PLUS ePassport Configuration BAC and Active Authentication

Référence/version du produit

- Xaica-Alpha PLUS with eTransport application: version 0111, softmask revision 1A00

- STMicroelectronics SB23YR80B: revision interne G

- STMicroelectronics NesLib: version 3.0

Conformité à un profil de protection

Critères d'évaluation et version

Critères Communs version 3.1 révision 3

Niveau d'évaluation

EAL 4 augmenté

ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3

Développeurs

NTT DATA Corporation
3-3-9 Toyosu Center Building ANNEX, Koto-ku,
Tokyo, Japan

STMicroelectronics
190 Avenue Célestin Coq, ZI de Rousset, BP2,
13106 Rousset Cedex, France

Commanditaire

NTT DATA Corporation
3-3-9 Toyosu Center Building ANNEX, Koto-ku, Tokyo, Japan

Centre d'évaluation

Serma Technologies
30 avenue Gustave Eiffel, 33608 Pessac, 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 la carte à puce « Xaica-Alpha PLUS ePassport Configuration BAC and Active Authentication », développée par NTT DATA Corporation et STMicroelectronics.

Le produit évalué est de type « carte à puce » avec et sans contact. Il implémente les fonctions de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale (ICAO). Ce produit permet la vérification de l'authenticité du document de voyage et l'identification de son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.
Ce microcontrôleur et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels. Ils peuvent être intégrés sous forme de module ou d'inlay. Le produit final peut être un passeport, une carte plastique, etc.

1.2. Description du produit

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.

Cette cible de sécurité respecte le profil de protection [PP JPN] à l'exception du composant initial AVA_VAN.5 remplacé par le composant AVA_VAN3 du fait du mécanisme BAC.

1.2.1. 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]) :

Valeur	Champ	Signification
'0000000002'	« *IC Manufacturer* »	STMicroelectronics
'4A50303542'	« *Card Manufacturer* »	NTT DATA Corporation
'0F0C4803'	« *Issue Identification* »	PQQ e-Passport
'0111'	« *TOE Version* »	PQQ code sur microcontrôleur SB23YR80B en révision interne G
'1A00'	« *Softmask revision* »	SPI-001-01

1.2.2. Services de sécurité

Les principaux services de sécurité évalués fournis par la TOE sont :

- la protection de l'intégrité des données du porteur stockées dans la carte : pays ou organisation de délivrance, numéro du document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait du porteur, autres données

optionnelles, données biométriques additionnelles et autres données permettant de gérer la sécurité du document de voyage ;
- l'authentification entre le document de voyage et le système d'inspection lors du contrôle aux frontières par le mécanisme BAC (« *Basic Access Control* ») ;
- la protection de l'intégrité et de la confidentialité des données lues à l'aide du mécanisme « *secure messaging* » ;
- l'authentification du microcontrôleur par le mécanisme AA (« *Active Authentication* »).

1.2.3. Architecture

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

Le produit est une carte à puce constituée :
- du microcontrôleur SB23YR80B en révision interne G avec librairie cryptographique NesLib v3.0, développé et fabriqué par STMicroelectronics ;
- du système d'exploitation Xaica-Alpha PLUS développé par NTT DATA Corporation et masqué dans la ROM du microcontrôleur ;
- de l'application ePassport développée par NTT DATA Corporation et masquée dans la ROM du microcontrôleur ;
- du code correctif (« *softmask* »), développé par NTT DATA Corporation et chargé en EEPROM en pré-personnalisation ;
- des données de l'application ePassport chargées en EEPROM lors de la personnalisation et temporairement en RAM lors de l'utilisation.

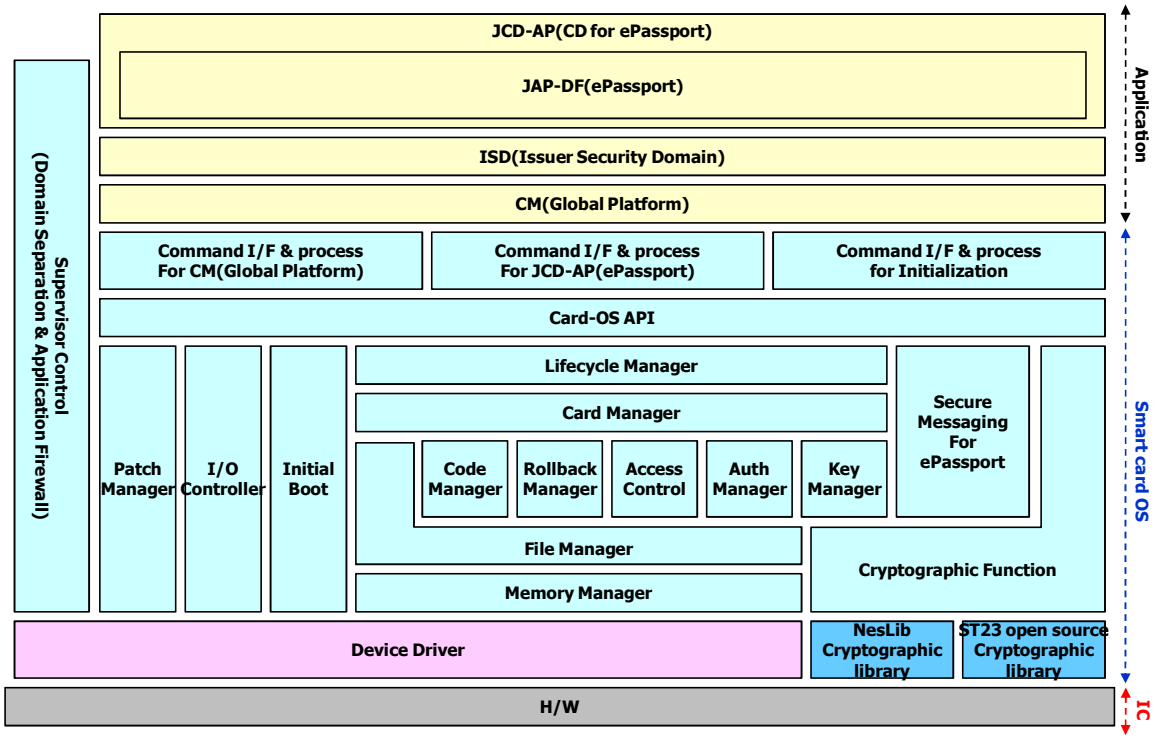

Figure 1 – Architecture du produit

1.2.4. Cycle de vie

Le cycle de vie du produit (figure 2) est basé sur celui du Profile de Protection référencé [PP JPN].

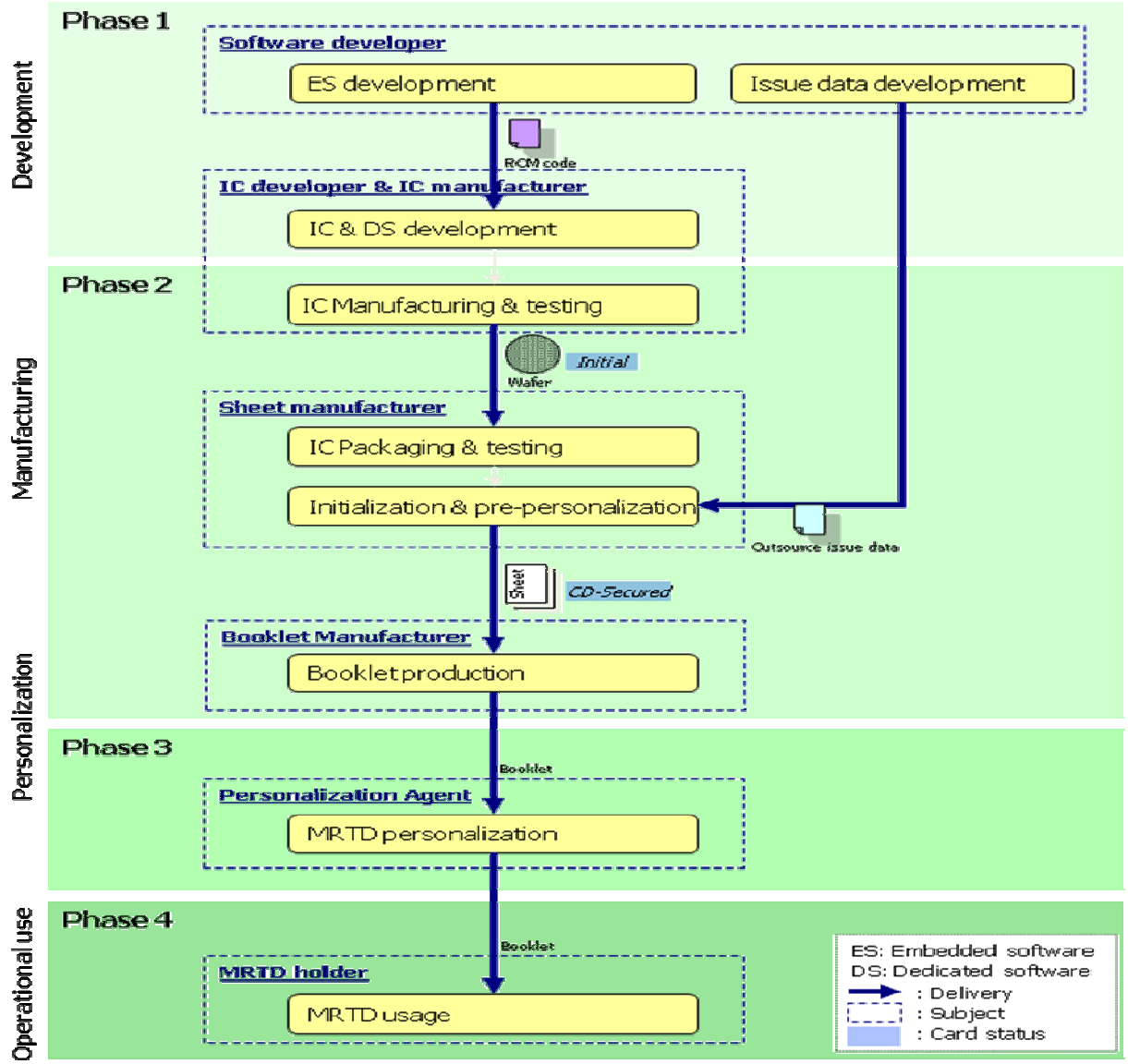

Figure 2 – Cycle de vie du produit

Le point de livraison est situé dans la phase 2 à la sortie de l'étape « *Initialization & Pre-personalization* ». Toutes les étapes qui précèdent ce point de livraison ont été couvertes par la présente évaluation (au titre d'ALC), le cas échéant en réutilisant les résultats obtenus lors de l'évaluation du composant sous-jacent.

Le code correctif du produit est chargé pendant la phase 2 lors de l'étape « *Initialization & Pre-personalization* ».

Les tests, réalisés au titre des activités ATE et AVA, ont porté sur les fonctionnalités du produit disponibles :

- en phase 2, lors des étapes « *IC Packaging and Testing* » , « *Initialization & Pre-personalization* » et « *Booklet production* » ;
- en phase 3, lors de l'étape « *MRTD Personalization* » ;
- en phase 4, lors de l'étape « *MRTD Usage* ».

Les étapes « *IC Packaging and Testing* » , « Initialization & Pre-personalization », « *Booklet production* », « *MRTD Personalization* » et « *MRTD Usage* » ont été prises en compte durant l'évaluation au travers des guides (au titre d'AGD).

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

Site de développement du logiciel

NTTDATA Corporation

Toyosu Center Building,
3-3-9 Toyosu, Koutou-ku Tokyo,
Japan, 135-8671

Site de développement et fabrication du microcontrôleur

STMicroelectronics.

190 Avenue Célestin Coq
ZI de Rousset, BP2
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 référencé [2010/02].

Les « administrateurs du produit » sont les nations ou organisations émettrices du document de voyage.
Les « utilisateurs du produit » sont les voyageurs et les systèmes d'inspection pendant la phase d'utilisation.

1.2.5. Configuration évaluée

Le certificat porte sur l'application ePassport en configuration BAC avec le mécanisme « *Active Authentication* » associée au système d'exploitation Xaica-Alpha PLUS, masquées sur le microcontrôleur SB23YR80B en révision interne G avec librairie cryptographique NesLib v3.0 et telles que présentées plus haut, au paragraphe 1.2.3.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 3.1 révision 3** [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 [CC 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 des microcontrôleurs « Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB » au niveau EAL6 augmenté du composant ALC_FLR.1, conforme au profil de protection [PP0035]. Ces microcontrôleurs ont été certifiés le 10 février 2010 sous la référence [2010/02]. Le niveau de résistance de ces microcontrôleurs, maintenus le 8 juillet 2010 sous la référence [2010/02-M02], a été confirmé dans le cadre de leur surveillance le 27 septembre 2012.

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 8 février 2013, 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 le référentiel technique de l'ANSSI

La cotation des mécanismes cryptographiques selon le référentiel technique de l'ANSSI [REF] 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.3 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.

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-Alpha PLUS ePassport Configuration BAC and Active Authentication » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté des composants ADV_FSP.5, ADV_INT.2, ADV_TDS.4, ALC_CMS.5, ALC_DVS.2, ALC_TAT.2, ATE_DPT.3.

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 :

[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.

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 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 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

	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**	**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	**3**	Focused vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	Cible de sécurité de référence pour l'évaluation : - Xaica-alphaPLUS ePassport Configuration (BAC + AA) Security Target version 1.4, 10/10/2012, NTT DATA Corporation. Pour les besoins de publication, la cible de sécurité suivante a été fournie dans le cadre de cette évaluation : - Xaica-alphaPLUS ePassport Configuration (BAC+AA) Security Target Lite, version 1.0, 2/10/2012, NTT DATA Corporation.
[RTE]	Rapport technique d'évaluation : - Evaluation technical report - Project: PLUSeP, version: 1.1, 08/02/2013, Serma Technologies.
[CONF]	Liste de configuration du produit : - Xaica-alphaPLUSEP-TCL-TOE Configuration List, version 1.3, 18 September 2012, NTT DATA Corporation.
[GUIDES]	Guides de préparation du produit : - Xaica-alphaPLUSEP-MPO-Manual for PrePerso and OUTSOURCE, version 1.3, 14 Sept. 2012, NTT DATA Corporation. - Xaica-alphaPLUSEP Operator Manual for Booklet manufacturer, version 1.2, 14 Sept. 2012, NTT DATA Corporation. - Xaica-alphaPLUSEP Operator Manual for Personalization Agent, version 1.2, 14 Sept. 2012, NTT DATA Corporation. - Xaica-alphaPLUSEP-DIO-Manual for Delivery, Installation, and Guidance of OUTSOURCE issue data, version 1.0, 21 March 2012, NTT DATA Corporation. Guide d'opération du produit : Xaica-alphaPLUSEP Operator Manual for User, version 1.2, 14 Sept. 2012, NTT DATA Corporation.
[PP JPN]	Protection Profile for ePassport IC with Active Authentication, version

	1.10, 15 Février 2010. Passport Division, Consular Affairs Bureau, Ministry of Foreign Affairs of Japan JBMIA. *Certifié par IPA (Information-technology Promotion Agency, Japan) sous la référence C0247.*
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.*
[2010/02]	« Microcontrôleurs sécurisés SA23YR48/80B et SB23YR48/80B, incluant la bibliothèque cryptographique NesLib v2.0 ou v3.0, en configuration SA ou SB » *Certifié par l'ANSSI le 10 février 2010 sous la référence ANSSI-CC-2010/02*.
[2010/02-M02]	Rapport de maintenance ANSSI-2010/02-M02, délivré le 8 juillet 2010, relatif au certificat ANSSI-CC-2010/02.

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, DCSSI.
[CC]	Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smart-cards, JIWG, version 2.8, January 2012.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.
[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 1.20 du 26 janvier 2010 annexée au Référentiel général de sécurité (RGS_B_1), voir www.ssi.gouv.fr.
	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008 annexée au Référentiel général de sécurité (RGS_B_2), 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_B_3), voir www.ssi.gouv.fr.