PREMIER MINISTRE

Secrétariat général de la défense nationale

Direction centrale de la sécurité des systèmes d'information

Rapport de certification DCSSI-2007/24

Configuration e-Passport (MRTD) de la plate-forme Xaica-Alpha64K embarquée sur le composant sécurisé ST19WR66I

Paris, le 14 décembre 2007

Le Directeur central de la sécurité des systèmes d'information

Patrick Pailloux
[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 la Direction centrale de la sécurité des systèmes d'information (DCSSI), 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 nationale
Direction centrale de la sécurité des systèmes d'information
Centre de certification
51, boulevard de la Tour Maubourg
75700 Paris cedex 07 SP

certification.dcssi@sgdn.pm.gouv.fr

Référence du rapport de certification

DCSSI-2007/24

Nom du produit

Configuration e-Passport (MRTD) de la plate-forme Xaica-Alpha64K embarquée sur le composant sécurisé ST19WR66I

Référence/version du produit

Référence développeur du logiciel embarqué : SPEC5 V014
Référence complète du microcontrôleur : ST19WR66I PQH

Conformité à un profil de protection

Néant

Critères d'évaluation et version

Critères Communs version 2.3

conforme à la norme ISO 15408:2005

Niveau d'évaluation

EAL 4 augmenté

ACM_SCP.3, ADV_IMP.2, ADV_SPM.3, ALC_DVS.2, ALC_LCD.2, ALC_TAT.2, AVA_VLA.3

Développeurs

NTTDATA Corporation

Toyosu Center Bldg Annex, 3-3-9 Toyosu, Koto-ku, Tokyo 135-8671, Japon

STMicroelectronics

Smartcard IC division, ZI de Rousset, BP2, 13106 Rousset Cedex, France

Commanditaire

NTTDATA Corporation

Toyosu Center Bldg Annex, 3-3-9 Toyosu, Koto-ku, Tokyo 135-8671, Japon

Centre d'évaluation

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

Tél : +33 (0)5 57 26 08 75, mél : e.francois@serma.com

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, publié au Journal officiel de la République française. Ce décret indique que :

- La direction centrale 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 configuration e-Passport (MRTD) de la plate-forme Xaica-Alpha64K développée par la société NTTDATA Corporation, et embarquée sur le microcontrôleur sécurisé ST19WR66I développé et fabriqué par la société STMicroelectronics.

Le produit évalué est de type carte à puce sans contact avec antenne. Il implémente les fonctionnalités de passeport électronique conformément aux spécifications de l'Organisation de l'Aviation Civile Internationale (cf. [OACI]). Il s'agit d'un microcontrôleur à interface sans contact avec un logiciel embarqué permettant :

- de stocker les données signées du futur porteur du passeport (nation ou organisation émettrice, n° de passeport, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, données d'informations optionnelles), une donnée biométrique du porteur (photo du visage), des données d'authentification optionnelles et diverses données permettant de gérer la sécurité du document ;
- de vérifier l'authenticité du passeport et d'identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

Ce micro-circuit et son logiciel embarqué ont vocation à être insérés dans la couverture des passeports traditionnels.

1.2. Description du produit évalué

La cible de sécurité [ST] définit le produit évalué, ses fonctionnalités de sécurité évaluées et son environnement d'exploitation.
La cible de sécurité s'inspire du profil de protection « Machine Readable Travel Document with ICAO Application, Basic Access Control » (cf. [PP MRTD]).

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 suivants :

- Référence de la plateforme : SPEC5 V014 ;
- Référence fondeur du produit : PQH ;
- Référence du microcontrôleur : ST19WR66I.

Ces données peuvent être vérifiées à l'aide des commandes :

- GET TRACEABILITY INF ;
- REQUEST LABEL ;
- GET DATA.

Pour plus de détails, se référer au guide « Xaica-alpha64K - Platform Specification » (cf. [GUIDES]).

1.2.2. Services de sécurité

Les principaux services de sécurité fournis par le produit sont :

- Identification et authentification ;

- Contrôle d'accès ;
- Fonctions cryptographiques ;
- Gestion du cycle de vie ;
- Canal sécurisé ;
- Gestion des clés de session ;
- Gestion du stockage des clés ;
- Gestion de la politique de sécurité ;
- Auto-tests ;

Ces services s'ajoutent à ceux fournis par le microcontrôleur :

- initialisation de la plate-forme matérielle et des attributs ;
- gestion sécurisée du cycle de vie ;
- intégrité logique du produit ;
- tests des fonctions de sécurité ;
- authentification de l'administrateur ;
- stockage et firewall de contrôle d'accès ;
- détection des attaques ;
- gestions des violations sécuritaires ;
- non-observabilité ;
- support au chiffrement cryptographique à clés symétriques ;
- support au chiffrement cryptographique à clés asymétriques ;
- support à la génération de nombres non prédictibles.

1.2.3. Architecture

Le produit est constitué du microcontrôleur ST19WR66I embarquant la plate-forme Xaica-Alpha64K configurée en mode e-Passport et comprenant les données du porteur. Le microcontrôleur est inséré dans un film papier avec une antenne (inlay) et la feuille est insérée dans la couverture d'un passeport. La figure suivante résume cette description :

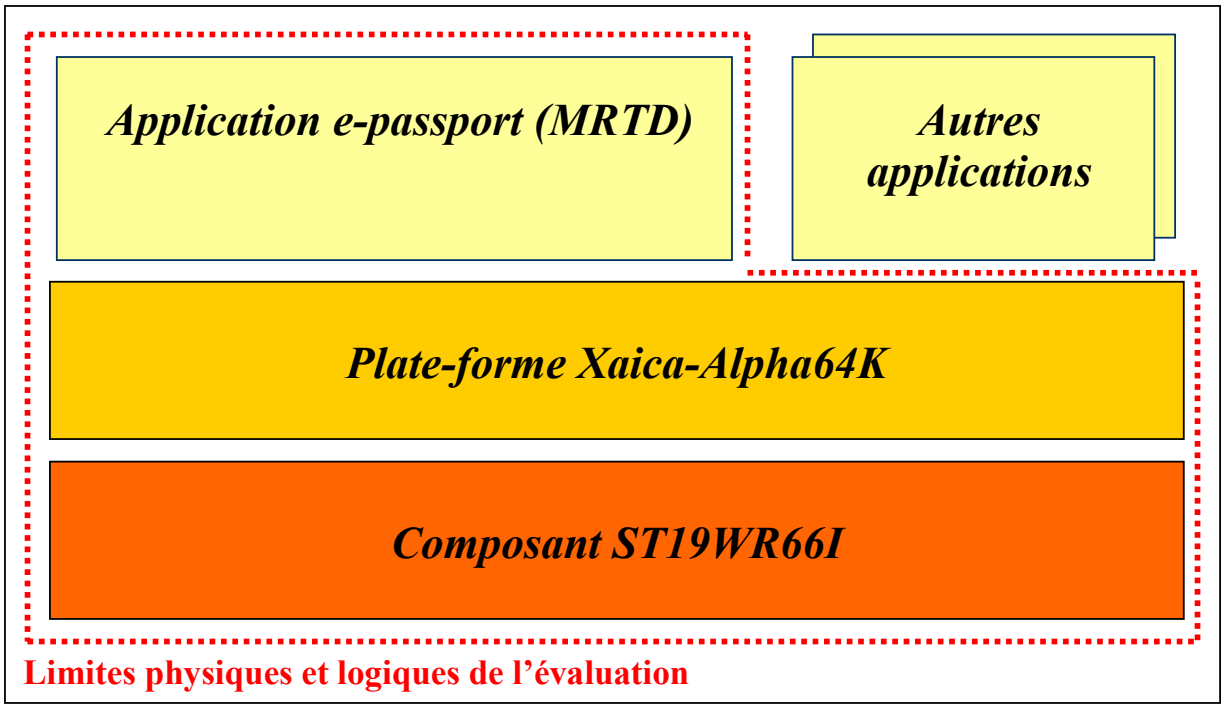

Figure 1 – Architecture du produit

Le produit offre les fonctionnalités suivantes durant sa phase de personnalisation et d'usage :

- authentification conformément aux spécifications [OACI] (« Basic Access Control » et « Active Authentication ») ;
- stockage et contrôles d'accès des données porteurs et système ;
- mécanismes d'authentification dédiés conforme aux spécifications gouvernementales japonaises permettant la personnalisation et l'administration sécurisée du produit ;
- interface sans contact (ISO14443 Type B) ;
- commandes APDU de la carte à puces conforme aux spécifications JICSAPV1.1 (équivalent des normes ISO7816-3 et ISO7816-4).

1.2.4. Cycle de vie

Le cycle de vie du produit est le suivant :

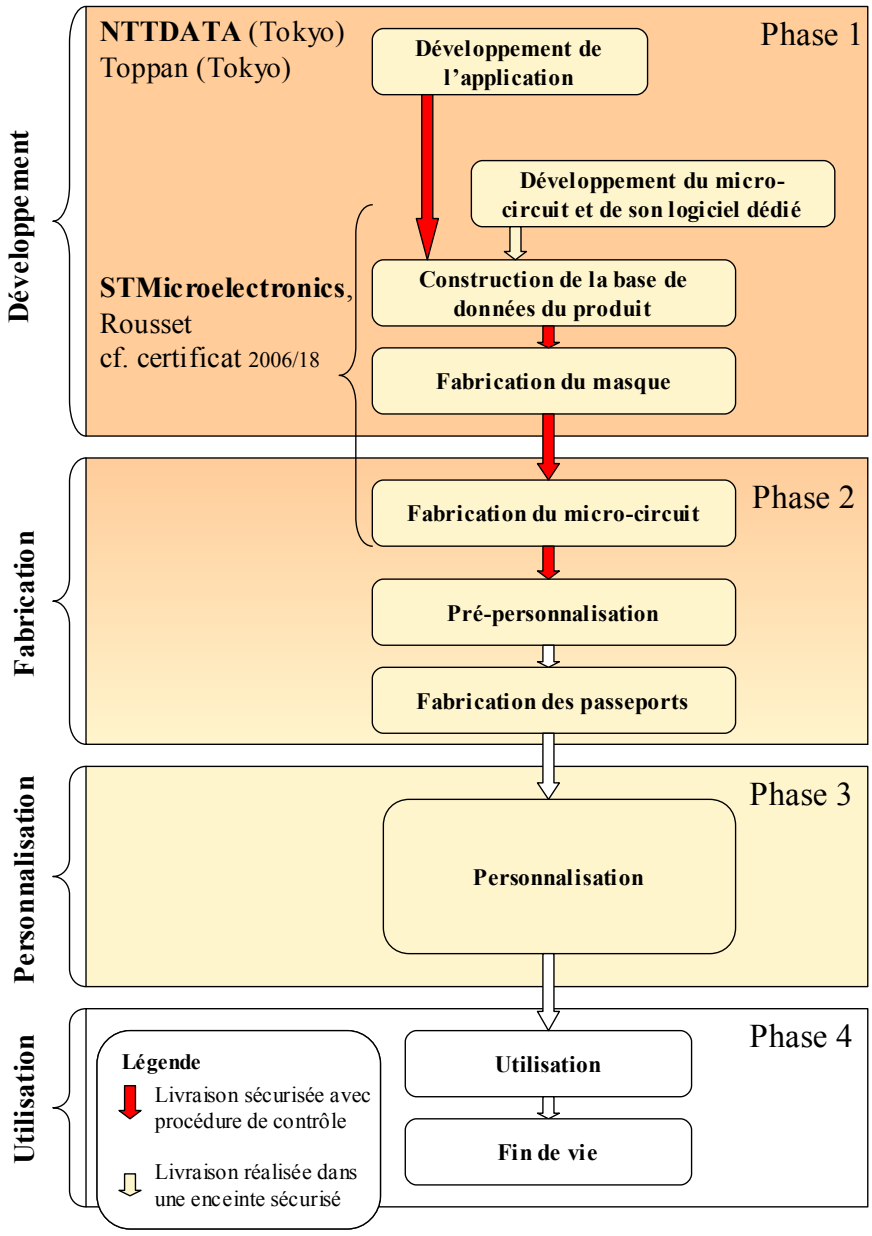

Figure 2 - Cycle de vie du produit

La plate-forme a été développée par NTTDATA sur le site suivant :

NTTDATA

Toyosu Center Building Annex,
3-3-9 Toyosu, Koto-ku,
Tokyo 135-8671, Japon

Une partie du développement a été sous-traité à la société Toppan :

TOPPAN

Koishikawa building
1-3-3, Suido,Bunkyo-ku
Tokyo, Japon

Le microcontrôleur est développé et fabriqué par STMicroelectronics sur le site suivant :

STMicroelectronics

Smartcard IC division
ZI de Rousset, BP2
13106 Rousset Cedex
France

La phase de fabrication du passeport (pré-personnalisation) ne fait pas partie du périmètre d'évaluation. Néanmoins, le schéma de pré-personnalisation sécurisée fourni par le développeur a été évalué (cf. [GUIDES]).

1.2.5. Configuration évaluée

Le certificat porte sur la configuration e-passport de la plateforme Xaica-Alpha64K embarquée sur le microcontrôleur ST19WR66I, identifiée au §1.2.1.
La plateforme Xaica-Alpha64K comporte des commandes visant d'autres besoins (e.g. JUKI ou applications Z). Ces commandes ne sont pas utilisables du fait de la personnalisation particulière en configuration e-passeport du produit et sont donc en dehors du périmètre d'évaluation.
L'antenne et la phase de fabrication du passeport lui-même ne sont pas incluse dans le périmètre d'évaluation.

2. L'évaluation

2.1. Référentiels d'évaluation

L'évaluation a été menée conformément aux **Critères Communs version 2.3** [CC] et à la méthodologie d'évaluation définie dans le manuel CEM [CEM]. Pour les composants d'assurance supérieurs au niveau EAL4, des méthodes propres au centre d'évaluation, validées par la DCSSI et compatibles avec le document [AIS34], ont été utilisées.

Pour répondre aux spécificités des cartes à puce, les guides [CCIC] et [CCAP] ont été appliqués.

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 « **ST19WR66I** » au niveau EAL5 augmenté des composants ALC_DVS.2, AVA_MSU.3 et AVA_VLA.4, conforme aux profils de protection [PP0002] et [PP9806]. Ce microcontrôleur a été certifié le 7 novembre 2006 sous la référence 2006/18 (cf. [2006/18]).

Le rapport technique d'évaluation [RTE], remis à la DCSSI le 11 décembre 2007, détaille les travaux menés par le centre d'évaluation et atteste que toutes les tâches d'évaluation sont à « **réussite** ».

2.3. Analyse de la résistance des mécanismes cryptographiques

La résistance des mécanismes cryptographiques a été analysée par la DCSSI. Les résultats obtenus ont fait l'objet d'un rapport d'analyse [ANA-CRY]. Ils 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 VLA 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 « Configuration e-Passport (MRTD) de la plate-forme Xaica-Alpha64K embarquée sur le composant sécurisé ST19WR66I » soumis à l'évaluation répond aux caractéristiques de sécurité spécifiées dans sa cible de sécurité [ST] pour le niveau d'évaluation EAL 4 augmenté.

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 spécifiés dans la cible de sécurité [ST] et suivre les recommandations se trouvant dans les guides fournis [GUIDES], notamment :

- le fabricant du microcontrôleur, le fabricant du passeport et l'agent de personnalisation doivent contrôler tous les éléments constitutifs du passeport, les équipements et les informations pour les fabriquer, les initialiser, les pre-personnaliser et les personnaliser, de façon à prévenir toute contrefaçon ;
- l'Etat émetteur ou l'organisation doit s'assurer que les utilisateurs agissant en tant qu'agents de personnalisation :
    - établissent l'identité correcte du porteur du passeport et identifient ses données biographiques pour le passeport électronique ;
    - enregistrent les données biométriques de référence du porteur, c'est-à-dire son portrait ;
    - personnalisent le passeport pour le porteur avec les mesures sécuritaires physiques et logiques requises (incluant la signature électronique des données du porteur dans le passeport et la clé privée d'authentification active). L'agent de personnalisation active la fonction de contrôle d'accès basique (BAC) et génère la clé de contrôle d'accès basique dans le passeport.
- l'Etat émetteur ou l'organisation doit :
    - générer une bi-clé de signature nationale cryptographiquement sûre ;
    - garantir le secret de la clé privée de cette bi-clé nationale de signature et signer les certificats des signataires de document dans un environnement opérationnel sécurisé ;
    - distribuer un certificat de la clé publique nationale de signature aux Etats et organisations hôtes. Ce certificat assure l'intégrité et l'authenticité de cette clé.

  L'Etat émetteur ou l'organisation doit également :
    - générer une bi-clé de signature des documents cryptographiquement sûre ;

  - garantir le secret de la clé privée de cette bi-clé de signature de document, et signer les données sécuritaires d'un passeport authentique dans un environnement opérationnel sécurisé ;
  - distribuer aux Etats et organisations hôtes le certificat de la clé publique de signature de document signé avec la clé publique nationale, en maintenant son intégrité et son authenticité en utilisant l'infrastructure de clés décrite dans [OACI] ;
- le système d'inspection de l'Etat ou organisation hôte doit vérifier le passeport présenté par le voyageur pour s'assurer son authenticité à l'aide de moyens physiques, afin de détecter toute manipulation physique du passeport ;
- le système d'inspection doit vérifier la signature des données signées du passeport préalablement à leur utilisation pour identifier le porteur. Les Etats et organisations hôtes doivent maintenir l'authenticité et la disponibilité des clés publiques de signature nationales et de signature des documents au sein de tous les systèmes d'inspection ;
- Le système d'inspection étendu doit utiliser le mécanisme « Active Authentication » pour vérifier l'authenticité de la puce du passeport présenté ;
- le système d'inspection des Etats et organisations hôtes doit garantir la confidentialité et l'intégrité des données lues dans le passeport. A cette fin, les Etats et organisations hôtes examinant le passeport doivent utiliser un terminal d'inspection implémentant la partie « terminal » du protocole BAC afin de chiffrer les communications et données transmises entre le passeport et le terminal, et implémentant la partie « terminal » du protocole « Active Authentication ».
- le porteur ne doit pas divulguer les données MRZ de son passeport à des tiers non autorisés afin de protéger les données électronique du passeport.
- L'entropie des données MRZ imprimées sur le passeport doit être maintenue à un minimum de 56 bits pour le niveau VLA visé. Le détail de la méthode de calcul est décrite dans le guide « Operator Manual for Personalization Agent » (cf. [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 1999 permet la reconnaissance, par les pays signataires de l'accord[1], des certificats ITSEC et Critères Communs. La reconnaissance européenne s'applique jusqu'au niveau ITSEC E6 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'Espagne, la Finlande, la France, la Grèce, l'Italie, la Norvège, les Pays-Bas, le Portugal, le Royaume-Uni, la Suède et la Suisse.

3.3.2. Reconnaissance internationale critères communs (CCRA)

Ce certificat est émis dans les conditions de l'accord du CC RA [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, la République de Corée, les Pays-Bas, 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
ACM Gestion de configuration	ACM_AUT				**1**	1	**2**	2	**1**	Partial CM automation
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Configuration support and acceptance procedures
	ACM_SCP			**1**	**2**	**3**	3	3	**3**	Development tools CM coverage
ADO Livraison et opération	ADO_DEL		**1**	1	**2**	2	2	**3**	**2**	Detection of modification
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Développement	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**2**	Fully defined external interfaces
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**2**	Implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**3**	Formal TOE security policy model
AGD Guides d'utilisation	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Support au cycle de vie	ALC_DVS			**1**	1	1	**2**	2	**2**	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				**1**	**2**	2	**3**	**2**	Standardized life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**2**	Compliance with implementation standards
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-level 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_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**2**	Validation of analysis
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**3**	Moderately resistant

Annexe 2. Références documentaires du produit évalué

[2006/18]	Rapport de certification 2006/18 – microcontrôleur ST19WR66I, 7 novembre 2006 SGDN/DCSSI
[ST]	Cible de sécurité de référence pour l'évaluation : - Xaica-alpha64K Security Target (ePassport configuration) Référence : NTTD-STep-XAICAALPHA64KST19, version 1.20, December 6, 2007 NTTDATA Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation : - Xaica-alpha64K Security Target Lite, Référence : NTTD-STL-XAICAALPHA64K-ST19, Version 1.00, December 14, 2007 NTTDATA
[RTE]	Evaluation Technical Report - ALPHA64K project, Référence: ALPHA64K_ETR_v1.2 Serma Technologies
[ANA-CRY]	Rapport d'analyse crypto N°902/SGDN/DCSSI/SDS/Crypto du 27 avril 2007 SGDN/DCSSI
[CONF]	Xaica-alpha64K - TOE Configuration List, Référence: NTTD-TCL-XAICAALPHA64K-ST19 v1.40 NTTDATA
[GUIDES]	- Xaica-alpha64K - Platform specification, Référence: NTTD-DD-XAICAALPHA64K-ST19 version 1.40 NTTDATA - Xaica-alpha64K - Procedure for OUTSOURCE issue data creation, Référence: NTTD-POS-XAICAALPHA64K-ST19 version 1.10 NTTDATA - Xaica-alpha64K - Manual for OUTSOURCE issue data creation, Référence: NTTD-MOS-XAICAALPHA64K-ST19 v1.20 NTTDATA - Xaica-alpha64K - Manual for delivery, installation and Issuance of OUTSOURCE, Référence: NTTD-DIO-XAICAALPHA64K -ST19 v1.20 NTTDATA - Operator Manual for MRTD manufacturer (booklet), Référence: NTTD-OMB-XAICAALPHA64K-ST19, version 1.10, NTTDATA

	- Operator Manual for Personalization Agent, Référence: NTTD-OMP-XAICAALPHA64K-ST19, version 1.30, NTTDATA - Operational Manual for User, Référence: NTTD-OMU-XAICAALPHA64K-ST19 version 1.10, NTTDATA
[OACI]	- PKI for Machine Readable Travel Documents offering ICC Read-Only Access, Version 1.1, October 1st 2004 International Civil Aviation Organization, - Machine Readable Travel Documents Technical Report, Development of a Logical Data Structure – LDS, For Optional Capacity Expansion Technologies, Revision –1.7, May 18th 2004, International Civil Aviation Organization, - Machine Readable Travel Documents, supplement 9303, version 3.0, 12nd June 2005
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. *Certifié par la DCSSI sous la référence PP/9806.*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certifié par le BSI sous la référence BSI-PP-0002-2001.*
[PP MRTD]	Protection Profile - Machine Readable Travel Document with ICAO Application, Basic Access Control, version 1.0, 18 August 2005. *Certifié sous la référence BSI-PP-0017*

Annexe 3. Références liées à la certification

Décret 2002-535 du 18 avril 2002 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, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. Le contenu des Critères Communs version 2.3 est identique à celui de la Norme Internationale ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. Le contenu de la CEM version 2.3 est identique à celui de la Norme Internationale ISO/IEC 18045:2005.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006
[CC AP]	Common Criteria Supporting Document - Mandatory Technical Document - Application of attack potential to smart-cards, reference CCDB-2007-04-001 version 2.3, revision 1, April 2007.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.3, April 2006.
[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 2.0, April 1999, Management Committee of Agreement Group.
[REF-CRY]	Mécanismes cryptographiques - Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques de niveau de robustesse standard, 1.10 du 19 décembre 2006, réf: 2741/SGDN/DCSSI/SDS/Crypto.

[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, Bundesamt für Sicherheit in der Informationstechnik