



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-2014/26
SOMA801STM - application EAC, version 1.0

Paris, le 04 avril 2014

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

[Original signé]

Guillaume Poupard



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 présumées 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

La reproduction de ce document sans altération ni coupure est autorisée.

Référence du rapport de certification

ANSSI-CC-2014/26

Nom du produit

SOMA801STM – application EAC

Référence/version du produit

Version 1.0

Conformité à un profil de protection

**BSI-CC-PP-0056-2009, [BSI-PP-0056], version 1.10
Machine Readable Travel Document with "ICAO
Application", Extended Access Control**

Critères d'évaluation et version

CC version 3.1 révision 4

Niveau d'évaluation

**EAL4 Augmenté
ALC_DVS.2 et AVA_VAN.5**

Développeurs

**Arjowiggins Security SAS -
Gep S.p.A.**
Viale Remo De Feo 1,
80022 Arzano (NA),
Italy

STMicroelectronics
190 avenue Celestin Coq, ZI de Rousset,
B.P. 2, 13106 ROUSSET,
France

Commanditaire

Arjowiggins Security SAS - Gep S.p.A.
Viale Remo De Feo 1, 80022 Arzano (NA),
Italy

Centre d'évaluation

SERMA TECHNOLOGIES
14 rue Galilee, CS 10055, 33615 Pessac,
France

Accords de reconnaissance applicables



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	6
1.1. PRESENTATION DU PRODUIT	6
1.2. DESCRIPTION DU PRODUIT	6
1.2.1. <i>Introduction</i>	6
1.2.2. <i>Identification du produit</i>	6
1.2.3. <i>Services de sécurité</i>	7
1.2.4. <i>Architecture</i>	7
1.2.5. <i>Cycle de vie</i>	8
1.2.6. <i>Configuration évaluée</i>	9
2. L’EVALUATION	10
2.1. REFERENTIELS D’EVALUATION	10
2.2. TRAVAUX D’EVALUATION	10
2.3. COTATION DES MECANISMES CRYPTOGRAPHIQUES SELON LES REFERENTIELS TECHNIQUES DE L’ANSSI	10
2.4. ANALYSE DU GENERATEUR D’ALEAS	10
3. LA CERTIFICATION	11
3.1. CONCLUSION	11
3.2. RESTRICTIONS D’USAGE	11
3.3. RECONNAISSANCE DU CERTIFICAT	11
3.3.1. <i>Reconnaissance européenne (SOG-IS)</i>	11
3.3.2. <i>Reconnaissance internationale critères communs (CCRA)</i>	12
ANNEXE 1. NIVEAU D’EVALUATION DU PRODUIT	13
ANNEXE 2. REFERENCES DOCUMENTAIRES DU PRODUIT EVALUE	14
ANNEXE 3. REFERENCES LIEES A LA CERTIFICATION	16

1. Le produit

1.1. Présentation du produit

Le produit évalué est la carte à puce « SOMA801STM – application EAC, version 1.0 », développée par Arjowiggins security SAS - Gep S.p.A. sur microcontrôleur SB23YR80B fabriquée par la société STMicroelectronics.

Le produit évalué est de type carte à puce sans contact. Il implémente les fonctionnalités de document de voyage électronique conformément aux spécifications de l'organisation de l'aviation civile internationale. Ce produit est destiné à permettre de vérifier l'authenticité du document de voyage et d'identifier son porteur lors d'un contrôle frontalier, à l'aide d'un système d'inspection.

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.

La cible de sécurité est strictement conforme au profil de protection [BSI-PP-0056].

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 présents dans la réponse que donne le produit suite à la commande GET DATA (voir [GUIDES]).

La version certifiée du produit est également identifiable par les éléments suivants :

Configuration		Source
Nom commercial de la TOE	SOMA Electronic Passport with EAC	Arjowiggins security SAS - Gep S.p.A.
Référence du produit (label interne)	SOMA801STM_1_0	Arjowiggins security SAS - Gep S.p.A.
Référence du produit (label IC)	SB23YR80B	Arjowiggins security SAS - Gep S.p.A.
Référence du système d'exploitation	SOMA	Arjowiggins security SAS - Gep S.p.A.
Référence fichier HEX	SOMA801STM_1_0.dlv	Arjowiggins security SAS - Gep S.p.A.
Identification du circuit intégré	SB23YR80B	STMicroelectronics

Référence du circuit intégré	SB23YR80B QLF	STMicroelectronics
Version du code ROM	1.0	Arjowiggins security SAS - Gep S.p.A.

1.2.3. Services de sécurité

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

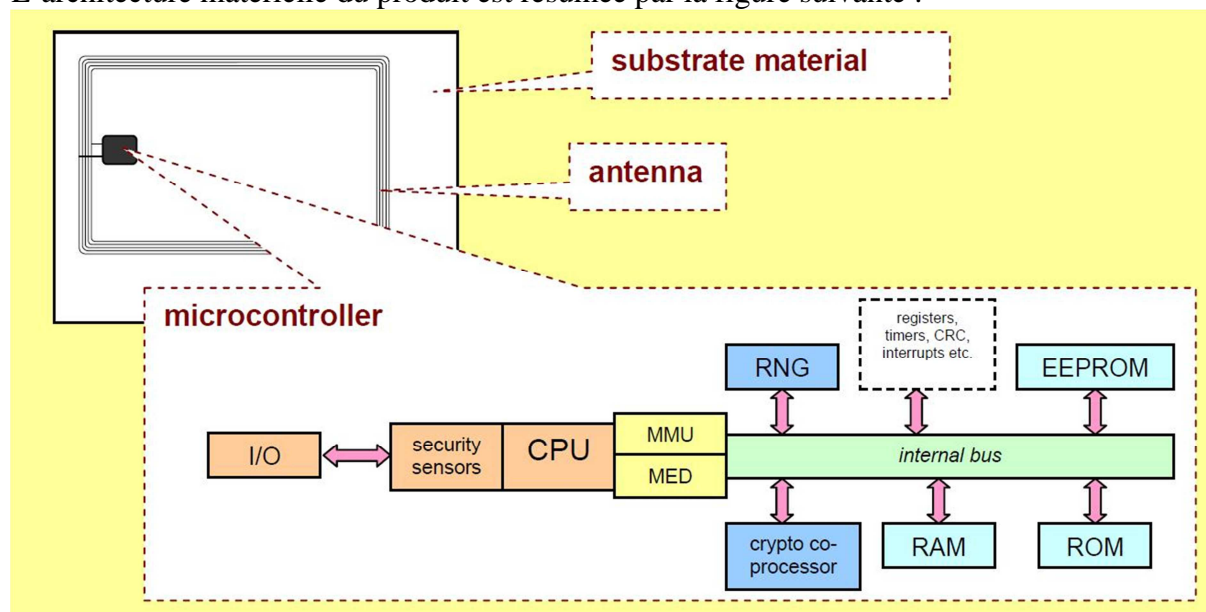
- la protection de l'intégrité des données du porteur stockées dans la carte : pays ou organisation de délivrance, numéro du document de voyage, date d'expiration, nom du porteur, nationalité, date de naissance, sexe, portrait du porteur, données biométriques additionnelles, données permettant de gérer la sécurité du document de voyage et autres données optionnelles ;
- l'intégrité et la confidentialité des données lues à l'aide du mécanisme *Secure Messaging* ;
- l'authentification forte entre le microcontrôleur et le système d'inspection par le mécanisme EAC (*Extended Access Control*) préalablement à tout accès aux données biométriques.

1.2.4. Architecture

Le produit est une carte à puce constituée :

- du microcontrôleur SB23YR80 révision B, développé et fabriqué par STMicroelectronics ;
- du système d'exploitation SOMA développé par Arjowiggins security SAS - Gep S.p.A. ;
- de l'application MRTD développée par Arjowiggins security SAS - Gep S.p.A..

L'architecture matérielle du produit est résumée par la figure suivante :



Les composants logiciels sont divisés en un ensemble de sous-systèmes :

- gestion de la couche d'abstraction du matériel HAL (*Hardware Abstract Layer*) ;

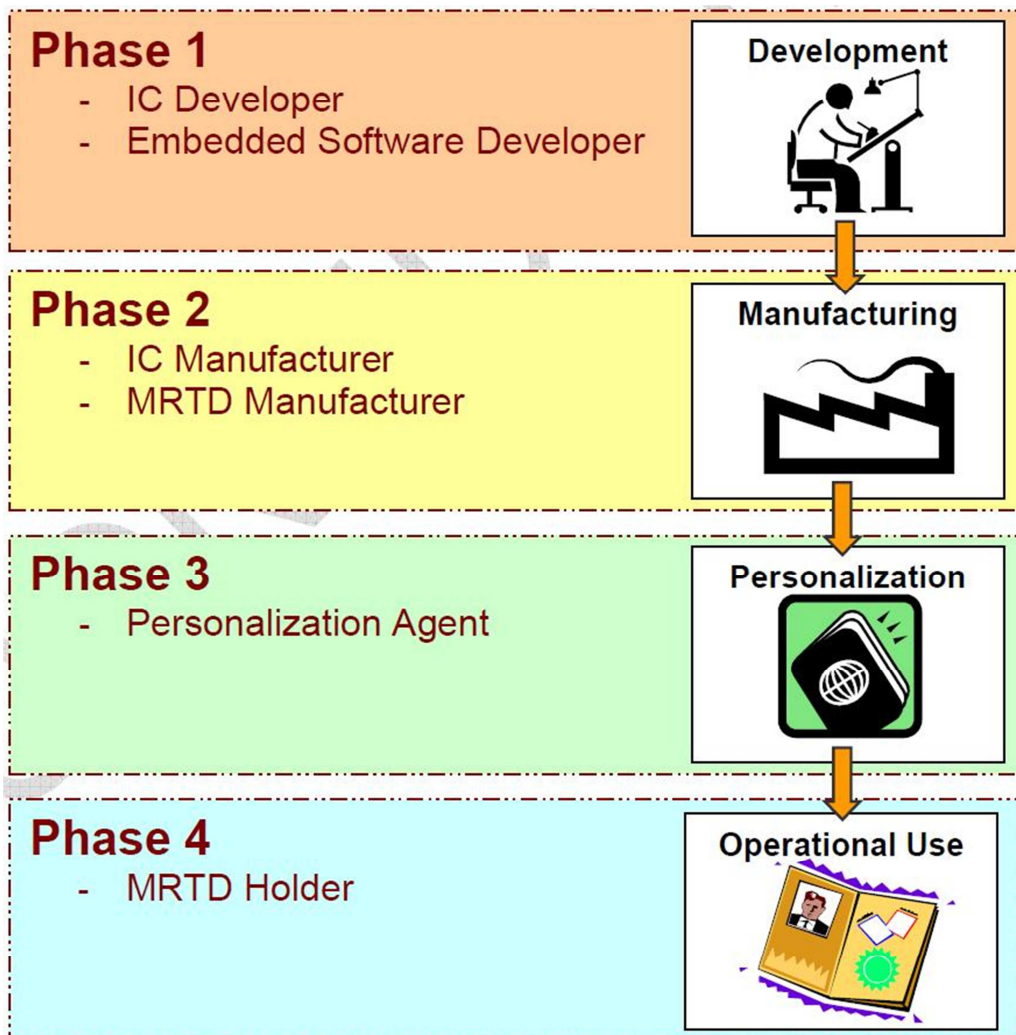
- gestion des commandes (*Commands Management*) ;
- gestion de la sécurité (*Security Management*) ;
- gestion des données et NVM (*Data object and Non Volatile Memory Management*) ;
- gestion de la communication (*Communication Management*) ;
- gestion de l'initialisation et de la carte (*Initialization and Card Management*) ;
- gestion de correctif (*Patch Management*).

Ils sont embarqués sur le circuit SB23YR80B, compris dans la TOE.

1.2.5. Cycle de vie

Le cycle de vie du produit est le suivant :

- phase de développement (phase 1) ;
- phase de fabrication (phase 2) ;
- phase de personnalisation (phase 3) ;
- phase d'utilisation (phase 4).



Les composants logiciels du produit ont été développés sur le site suivant :

Arjowiggins security SAS - Gep S.p.A.

Corso Salvatore D'Amato, 90

80022 Arzano (NA),

Italie

Le microcontrôleur a été développé et fabriqué par STMicroelectronics sur ses sites (voir [ANSSI-CC-2012/68]).

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.

1.2.6. Configuration évaluée

Le certificat porte sur le produit présenté au chapitre 1.2.1. L'évaluation n'a porté que sur l'application EAC.

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 [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 du microcontrôleur « *SB23YR80B* » au niveau EAL6 augmenté du composant ALC_FLR.1, conforme au profil de protection [BSI-PP-0035]. Ce microcontrôleur a été certifié le 4 janvier 2013 sous la référence [ANSSI-CC-2012/68].

Le niveau de résistance du microcontrôleur a été confirmé le 4 décembre 2013 dans le cadre du processus de surveillance, voir [SUR_IC].

Le rapport technique d'évaluation [RTE], remis à l'ANSSI le 25 mars 2014, 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 [ANSSI-CC-2012/68]).

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 « SOMA801STM – application EAC, version 1.0 » 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 ALC_DVS.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 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'accord¹, 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 signataires¹, 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

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	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	1	Implementation representation of the TSF
	ADV_INT					2	3	3			
	ADV_SPM						1	1			
	ADV_TDS		1	2	3	4	5	6	3	3	Basic modular design
AGD Guides d'utilisation	AGD_OPE	1	1	1	1	1	1	1	1	1	Operational user guidance
	AGD_PRE	1	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	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	4	Problem tracking configuration management coverage
	ALC_DEL		1	1	1	1	1	1	1	1	Delivery procedures
	ALC_DVS			1	1	1	2	2	2	2	Sufficiency of security measures
	ALC_FLR										
	ALC_LCD			1	1	1	1	2	1	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	1	Well-defined development tools
ASE Evaluation de la cible de sécurité	ASE_CCL	1	1	1	1	1	1	1	1	1	Conformance claims
	ASE_ECD	1	1	1	1	1	1	1	1	1	Extended components definition
	ASE_INT	1	1	1	1	1	1	1	1	1	ST introduction
	ASE_OBJ	1	2	2	2	2	2	2	2	2	Security objectives
	ASE_REQ	1	2	2	2	2	2	2	2	2	Derived security requirements
	ASE_SPD		1	1	1	1	1	1	1	1	Security problem definition
	ASE_TSS	1	1	1	1	1	1	1	1	1	TOE summary specification
ATE Tests	ATE_COV		1	2	2	2	3	3	2	2	Analysis of coverage
	ATE_DPT			1	1	3	3	4	1	1	Testing: basic design
	ATE_FUN		1	1	1	1	2	2	1	1	Functional testing
	ATE_IND	1	2	2	2	2	2	3	2	2	Independent testing: sample
AVA Estimation des vulnérabilités	AVA_VAN	1	2	2	3	4	5	5	5	5	Advanced methodical vulnerability analysis

Annexe 2. Références documentaires du produit évalué

[ST]	<p>Cible de sécurité de référence pour l'évaluation :</p> <ul style="list-style-type: none"> - Security Target SOMA801STM electronic passport Extended Access Control référence TCAE110002, version 1.3, 19 août 2013, éditée par Arjowiggins security SAS - Gep S.p.A. <p>Pour les besoins de publication, la cible de sécurité suivante a été fournie et validée dans le cadre de cette évaluation :</p> <ul style="list-style-type: none"> - Security Target SOMA801STM electronic passport Extended Access Control – Public version référence TCLE130007, version 1.2, 19 août 2013, éditée par Arjowiggins security SAS - Gep S.p.A.
[RTE]	<p>Rapport technique d'évaluation :</p> <ul style="list-style-type: none"> - Evaluation Technical Report - SOMA801STM Projet référence SOMA801STM_ETR_V1.1, version 1.1, 25 mars 2014, édité par Serma Technologies.
[CONF]	<p>Liste de configuration :</p> <ul style="list-style-type: none"> - Configuration List for the SOMA801STM electronic passport, référence TCAE130002, version 1.0, 15 septembre 2013, édité par Arjowiggins security SAS - Gep S.p.A.
[GUIDES]	<p>Guide d'administration du produit :</p> <ul style="list-style-type: none"> - Personalization Guidance for the SOMA801STM Electronic Passport, référence TCAE120024, version 1.1, 23 avril 2013, édité par Arjowiggins Security SAS - Gep S.p.A. ; - Pre-Personalization Guidance for the SOMA801STM Electronic Passport, référence TCAE120023, version 1.1, 23 avril 2013, édité par Arjowiggins Security SAS - Gep S.p.A. <p>Guide d'utilisation du produit :</p> <ul style="list-style-type: none"> - User guidance for the SOMA801STM electronic passport référence TCAE120025, version 1.1, 23 avril 2013, édité par Arjowiggins Security SAS - Gep S.p.A.
[ANSSI-CC-2012/68]	<p>« Microcontrôleurs sécurisés SA23YR80/48 et SB23YR80/48, incluant la bibliothèque cryptographique NesLib v2.0, v3.0 ou v3.1, en configuration SA ou SB, référence: maskset K2M0A, révision externe B, révision interne H ou I » <i>Certifié le 04 janvier 2013 sous la référence ANSSI-CC-2012/68.</i></p>
[SUR_IC]	<p>« SA23YR48B / SB23YR48B / SA23YR80B / SB23YR80B » <i>Rapport de surveillance du 04 décembre 2013 sous la référence ANSSI-CC-2012/68-S01.</i></p>

[BSI-PP-0056]	Protection Profile - Machine Readable Travel Document with “ICAO Application”, Extended Access Control, version 1.10, 25 Mars 2009. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0056-2009.</i>
[BSI-PP-0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. <i>Certifié par le BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0035-2007.</i>

Annexe 3. Références liées à la certification

<p>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.</p>	
[CER/P/01]	<p>Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, ANSSI.</p>
[CC]	<p>Common Criteria for Information Technology Security Evaluation : Part 1: Introduction and general model, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.</p>
[CEM]	<p>Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, revision 4, ref CCMB-2012-09-004.</p>
[CC IC]*	<p>Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2009-03-002 version 3.0, revision 1, March 2009.</p>
[JIWG AP]*	<p>Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, January 2013.</p>
[COMP]*	<p>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.</p>
[CC RA]	<p>Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, May 2000.</p>
[SOG-IS]	<p>« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 Janvier 2010, Management Committee.</p>
[REF-CRY]	<p>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.</p>

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