Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/23

Passport Morpho-ePass V3 with BAC, AA and EAC RSA or EAC ECC, on STMicroelectronics microcontroller

Paris, 28th of July 2008

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 DCSSI (Central Directorate for Information Systems Security), 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 Nationale
Direction Centrale de la Sécurité des Systèmes d'Information
Centre de certification
51, boulevard de la Tour Maubourg
75700 PARIS cedex 07 SP
France

certification.dcssi@sgdn.gouv.fr

Certification report reference

DCSSI-2008/23

Product name

Passport Morpho-ePass V3 with BAC, AA and EAC RSA or EAC ECC, on STMicroelectronics microcontroller

Product reference

MORPHOEPASSCC/ST19NR66-A/1.0.2

Protection profile conformity

BSI-PP-0026 version 1.2

Common Criteria Protection Profile - Machine Readable Travel Document with "ICAO Application", Extended Access Control

Evaluation criteria and version

Common Criteria version 2.3

compliant with ISO 15408:2005

Evaluation level

EAL 4 augmented

ADV_IMP.2, ALC_DVS.2, AVA_MSU.3, AVA_VLA.4

Developers

Sagem Sécurité

Etablissement d'Osny, 18 Chaussée Jules César, 95520 Osny, France

STMicroelectronics

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

Sponsor

Sagem Sécurité

Etablissement d'Osny, 18 Chaussée Jules César, 95520 Osny, France

Evaluation facility

CEA - LETI

17 rue des martyrs, 38054 Grenoble Cedex 9, France

Phone: +33 (0)4 38 78 40 87, email : cesti.leti@cea.fr

Recognition arrangements

CCRA

The product is recognised at EAL4 level.

SOG-IS

Introduction

The Certification

Security certification for information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, and published in the "Journal Officiel de la République Française". This decree stipulates that:

- The central information system security department 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 principals 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.

Content

1. The product

1.1. Presentation of the product

The evaluated product is the software “Passport Morpho-ePass V3 with BAC, AA and EAC RSA or EAC ECC**”** developed by Sagem Sécurité and embedded on the ST19NR66-A revision C secure microcontroller developed and manufactured by STMicroelectronics.

The evaluated product is a contactless smartcard with its antenna. It implements the travel document features according to the specifications from the International Civil Aviation Organization (cf. [ICAO]). The contactless microcontroller with embedded software allows to check the authenticity of the travel document and to identify its holder during a border control, with the support of an inspection system. It enables:

- Protection in integrity of the holder’s data: issuing state or organization, travel document number, expire date, holder’s name, nationality, birth date, sex, holder’s face portrait, other optional data, additional holder’s biometric data and several other pieces of data for managing the document security;
- Authentication between the travel document holder and the inspection system prior to any border control by means of the Basic Access Control mechanism;
- Protection in integrity and confidentiality of data read by means of the secure messaging mechanism;
- Authentication of the genuine chip by means of the Active Authentication mechanism (if activated as an alternative for the Chip Authentication mechanism);
- Strong authentication of the chip and the inspection system prior to any biometric data retrieval by means of the Extended Access Control mechanism.

The product additionally implements e-administration services related to Identification, Authentication and Signature as required by the specification for e-Administration common platform, but these functionalities are not part of the evaluation scope.

The microcontroller also provides a contact interface, thus enabling the contact mode for the final product.

The chip and its embedded software are intended to be inserted into the cover page of traditional passport booklets. They can be integrated into modules or inlay. The final product can be a passport, a plastic card etc…

1.2. Evaluated product description

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

This security target is compliant to [PP EAC] protection profile.

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:

- Brand name: Morpho-ePass V3 / Morpho-Citiz64;
- Name and version of the product: MorphoEpassCC version 1.0.2;
- Name and version of the microcontroller: ST19NR66-A revision C;

- Full reference of the final product: MORPHOEPASSCC/ST19NR66-A/1.0.2.

These elements can be identified with the help of the CPLC data as specified in the configuration management plan (cf. [CONF]).

1.2.2. Security services

The product provides mainly the following security services:

- Authentications: Personalization agent authentication, BAC authentication, Active Authentication, Chip Authentication, Terminal Authentication;
- Cryptography: ECDSA, RSA, ECDH, DH, TDES, Retail MAC, SHA;
- Implementation of the BAC, EAC and secure messaging mechanisms;
- Access control to data stored in the product;
- Secure management of the cryptographic keys;
- Life cycle management;
- Embedded application separation;
- Management of the secure state of the TOE;
- Protection against attacks.

The security services offered by the microcontroller are detailed in its certification report (cf. [2007/23]).

1.2.3. Architecture

The product consists in the microcontroller, the embedded operating system and three applications:

- The AIP application performs the personalization operations of the product and is deactivated in operational use phase;
- The ICAO application performs all the electronic passport operations during the operational use phase;
- The IAS application performs electronic administration operations during the operational use phase. There might be none, one or several instances of the IAS application. This application is outside the scope of the evaluation

The following picture sums up the product architecture:

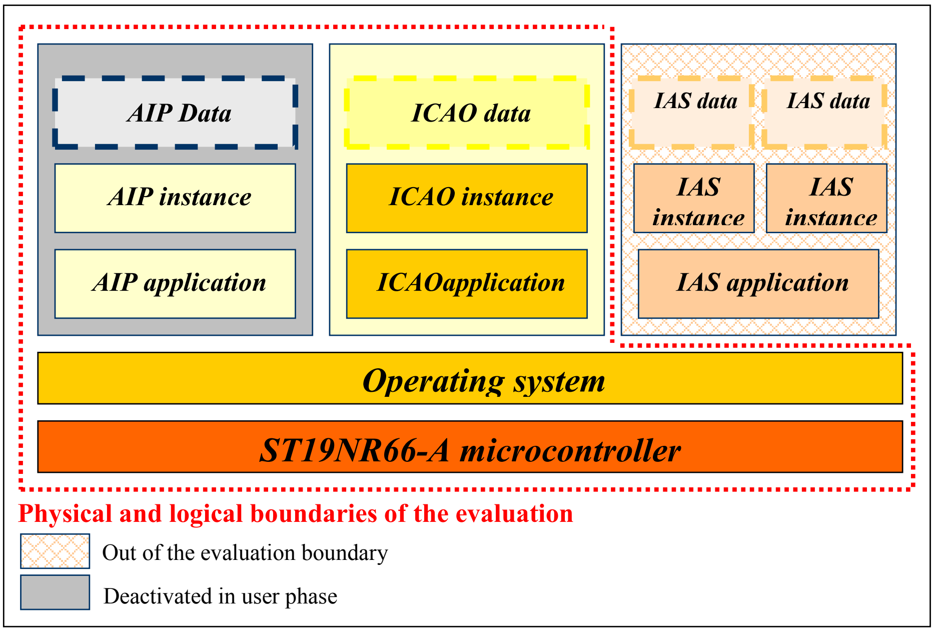

Figure 1 – Product architecture

1.2.4. Life cycle

The product's life cycle is organised as follow:

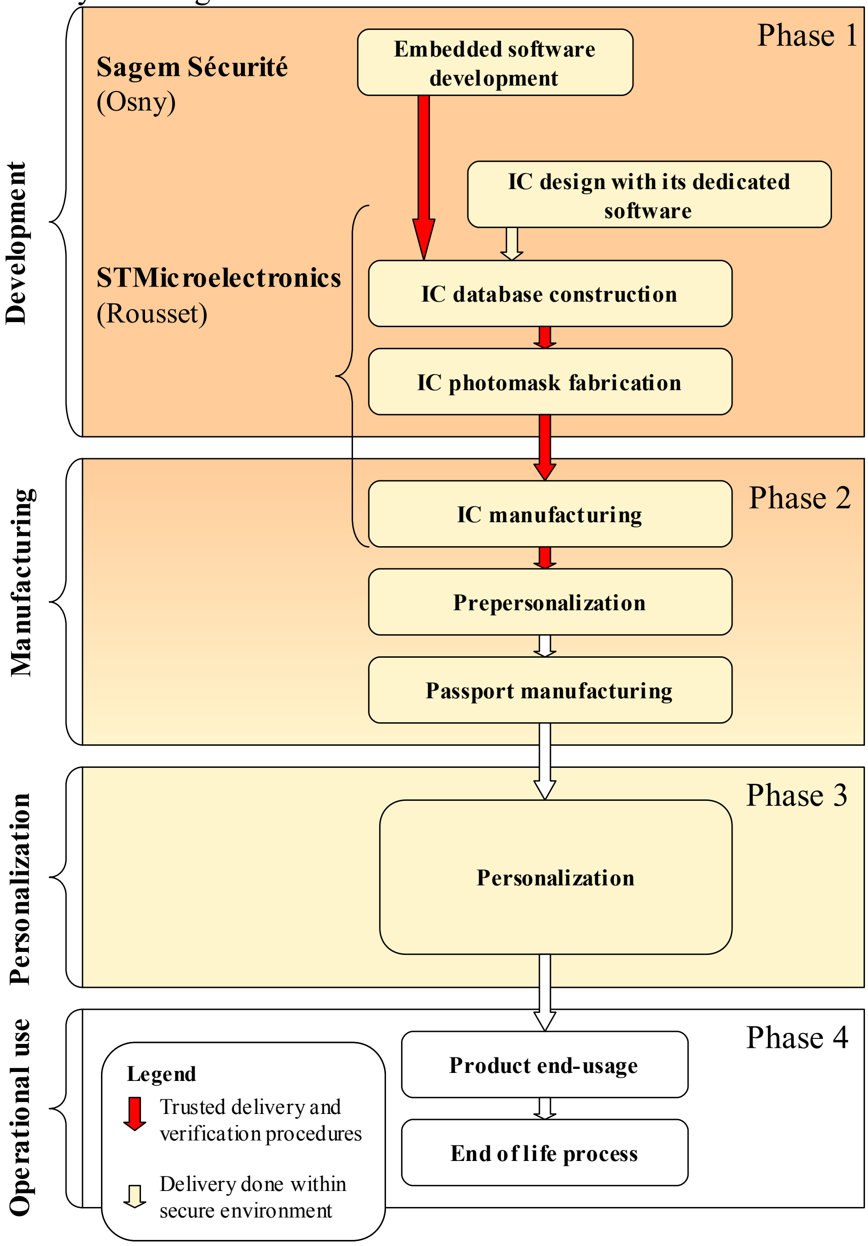

Figure 2 – Product Life-cycle

The product has been developed on the following sites:

Sagem Sécurité

Etablissement d'Osny, 18 Chaussée Jules César,
95520 Osny,
France

The microcontroller is developed and manufactured by:

STMicroelectronics

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

The manufacturing phase of the travel document (prepersonalization) can be performed either by STMicroelectronics or by a subcontractor. This phase is not in the evaluation scope and is covered by guidance (cf. [GUIDES]).

The phases of inlay and booklet manufacturing are not covered by the evaluation: it is considered that these phases have no impact on security, the product being self protected during these stages.

1.2.5. Evaluated configuration

The evaluated product is a generic e-Passport platform that can be personalized under different configurations. This certification report covers the configuration including the following mechanisms:

- Basic Access Control;
- Extended Access Control with RSA or ECC algorithm;
- Active Authentication.

The IAS application is out of the evaluation scope as no associated sensitive data is considered to be protected by the product in the security target. The existence of this application has nevertheless been considered during the evaluation, particularly for the vulnerability analysis.

The antenna and the travel document manufacturing phase (booklet) are not in the scope of the evaluation.

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC] and with the Common Evaluation Methodology [CEM].
For assurance components above EAL4 level, the evaluation facility own evaluation methods consistent with [AIS 34], validated by DCSSI have been used.

In order to meet the specificities of smart cards, the [CC IC] and [CC AP] guides have been applied.

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 is introduced from the integration of the software in the microcontroller already certified.
Therefore, the results of the evaluation of the microcontroller "ST19NR66-A revision C " at EAL5 level augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with [PP/9806] and [PP0002] protection profiles, have been used. This microcontroller has been certified the 13th of December 2007 under the reference 2007/23 (cf. [2007/23]).

The evaluation relies on the evaluation results related to Sagem Sécurité development environment, evaluated under the control of BSI[1] with satisfactory results at the certification date (last control performed by BSI for the certificate BSI-DSZ-CC-0449).

The evaluation technical report [ETR], delivered to DCSSI the 11th of July 2008, 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 robustness of cryptographic mechanisms has not been analysed by DCSSI at the certification date.

[1] Bundesamt für Sicherheit in der Informationstechnik

3. Certification

3.1. Conclusion

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

This certificate testifies that the product “Passport Morpho-ePass V3 with BAC, AA and EAC RSA or EAC ECC, on STMicroelectronics microcontroller” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 4 augmented.

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 operational environmental security objectives summarized specified in the security target [ST] chapter 4.3 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 issued in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 1999 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable up to ITSEC E6 and CC EAL7 levels. The certificates that are recognized in the agreement scope are released with the following marking:

IT
Security
Certified

3.3.2. International common criteria recognition (CCRA)

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

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[1], 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 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, 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+	Name of the component
ACM Configuration management	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	2	Problem tracking CM coverage
ADO Delivery and operation	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 Development	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	1	Informal TOE security policy model
AGD Guidance	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 Life-cycle support	ALC_DVS			1	1	1	2	2	2	Sufficiency of security measures
	ALC_FLR									
	ALC_LCD				1	2	2	3	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	1	Well-defined development tools
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 Vulnerability assessment	AVA_CCA					1	2	2		
	AVA_MSU			1	2	2	3	3	3	Analysis and testing of insecure states
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evaluation
	AVA_VLA		1	1	2	3	4	4	4	Highly resistant

Annex 2. Evaluated product references

[2007/23]	Certification Report DCSSI-2007/23 - ST19NR66-A Secure Microcontroller, 13th of December 2007, SGDN/DCSSI.
[ST]	Reference security target for the evaluation: - Security Target: Morpho-ePass V3, Reference: SK 00000 63506 version 1.5, Sagem Sécurité For the needs of publication, the following security target has been provided and validated in the evaluation: - Security Target: Morpho-ePass V3, Public version Reference: SSE-00000 70468 version 1.1, Sagem Sécurité
[ETR]	HELIOS - Rapport Technique d'Evaluation, Reference : LETI.CESTI.HEL.RTE.001 - v1.1 - 10/07/08, CESTI LETI
[CONF]	- Plan de gestion de configuration logiciel, Reference: SK 0000066065 version 1.1, Sagem Sécurité - Fiche de version du logiciel MorphoEpassCC 1.0.2, Reference: SSE-0000067783 version 1.1, Sagem Sécurité
[GUIDES]	Installation guidance: - Documentation d'installation, de génération et de démarrage, Reference: SSE-0000068096 version 1.1, Sagem Sécurité - ICAO Application Prepersonalisation manual, Reference: SSE-0000070088 version 1.2, Sagem Sécurité Administration guidance: - ICAO Application Personalisation manual, Reference: SSE-0000067414 version 1.2, Sagem Sécurité User guidance: - ICAO Application User manual, Reference: SSE-0000067415 version 1.2, Sagem Sécurité
[ICAO]	ICAO Doc 9303, Sixth Edition, 2007
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. *Certified by DCSSI under the reference PP/9806.*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0002-2001.*

[PP EAC]	Protection Profile - Machine Readable Travel Document with ICAO Application, Extended Access Control, version 1.2, 19 November 2007. *Certifier by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0026*

Annex 3. Certification references

Decree number 2002-535 dated 18th April 2002 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 2006, version 3.1, revision 1, ref CCMB-2006-09-001, Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002, Part 3: Security assurance components, September 2007, version 3.1, revision 2,ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, ref CCMB-2007-09-004, revision 2.
[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-2008-04-001 version 2.5 revision 1, April 2008.
[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 2.0, April 1999, Management Committee of Agreement Group.
[REF-CRY]	Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms with standard robustness level version 1.10, 14th of September 2007, No. 1904/SGDN/DCSSI/SDS/LCR
[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