PREMIER MINISTRE

Secretariat General for National Defence

French Network and Information Security Agency

Certification Report ANSSI-CC-2009/42

SafeAccess TV Card (smart card)
SAFEACCESS Version 2.0 Release 67 application software embedded in ST19NA18F

Paris, October 26th 2009

Courtesy Translation

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 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-2009/42

Product name

SafeAccess TV Card

SAFEACCESS Version 2.0 Release 67 application software embedded in ST19NA18F

Product reference

Version 2.0 Release 67

Protection profile conformity

[PP/9911]

Protection Profile Smart Card Integrated Circuit With Embedded Software , version 2.0, June 1999 certified by ANSSI under reference PP/9911

Evaluation criteria and version

Common Criteria version 3.1

Evaluation level

EAL 4

augmented with ALC_DVS.2, AVA_VAN.5

Developer(s)

LogiWays
Paris R&D site, 24-26 rue Louis Armand,
75015 Paris, France

ST Microelectronics
190 Avenue Célestin COQ,
13106 Rousset Cedex, France

Sponsor

LogiWays
Paris R&D site, 24-26 rue Louis ARMAND, 75015 Paris, France

Evaluation facility

Serma Technologies
30 avenue Gustave Eiffel, 33608 Pessac, France
Tel: +33 (0)5 57 26 08 75, email: e.francois@serma.com

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 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

Figures

1. The product

1.1. Presentation of the product

The evaluated product is the “SafeAccess TV Card” (smart card), fitted with version 2.0 release 67 of the SAFEACCESS application software developed by LogiWays and embedded in the ST19NA18F microcontroller developed by STMicroelectronics. Release C of the ST19NA18 microcontroller has been certified by ANSSI under reference DCSSI-2007/07 and release F was subject to a maintenance update under reference DCSSI-2007/07-M01, cf. [CERT].

The “SafeAccess TV Card” is designed to manage access rights to pay TV systems.

1.2. Evaluated product description

The Security Target [ST] defines the evaluated product, its evaluated security functionalities and its operating environment. This Security Target is derived from Protection Profile [PP/9911] adapted to Common Criteria v3.1 (need of additional components ADV_IMP.1 and ATE_DPT.2).

1.2.1. Product identification

The configuration list contained in the manual [CONF] identifies the product’s constituent elements.
The certified version of the product can be identified by the following:

- Information engraved on the component:
  - Microcontroller reference number: K7L0A;
  - Dedicated microcontroller software reference number: ZSD;
  - SAFEACCESS application generic reference number: NVB;
- Information displayed on start-up (Answer to Reset or ATR):

Type	Size	Value	Description
<Version>	1	0x91	ROMCODE Version 2
<Copyright>	11	0x28 0x43 0x29 0x4C 0x6F 0x67 0x69 0x77 0x61 0x79 0x73	ASCII character string ‘(C)Logiways’
<Lock>	2	0x33 0x33	

The value 0x91 that identifies version 2.0 of the SAFEACCESS application is the seventh byte of the ATR.
To determine the release number of a smart card (release 67 for the evaluated version), this smart card needs to be given to LogiWays.

1.2.2. Security services

The product provides the following main security services:

- Use of a secure channel to ensure confidentiality and integrity of data exchanged with the pay TV system descrambler;
- Protection of confidentiality and integrity of descrambled data (control words) used by decoder to provide different services (Live, Recorded, Pay-Per-View);
- Protection of confidentiality and integrity of stored sensitive data (eg, keys);
- Secure updating of different protection codes.

1.2.3. Architecture

The evaluated composite product comprises the following:

- The microcontroller and its dedicated software, as described in the microcontroller report [ETR].
  The microcontroller provides elementary cryptographic calculation services (AES, TDES, RSA, SHA, CRC) via APIs (Application Programming Interfaces).
- The "embedded software", which comprises a pay TV application module (hereafter referred to as the "application") and a services module (hereafter referred to as "services"). The applications and services are shown in the figure below.

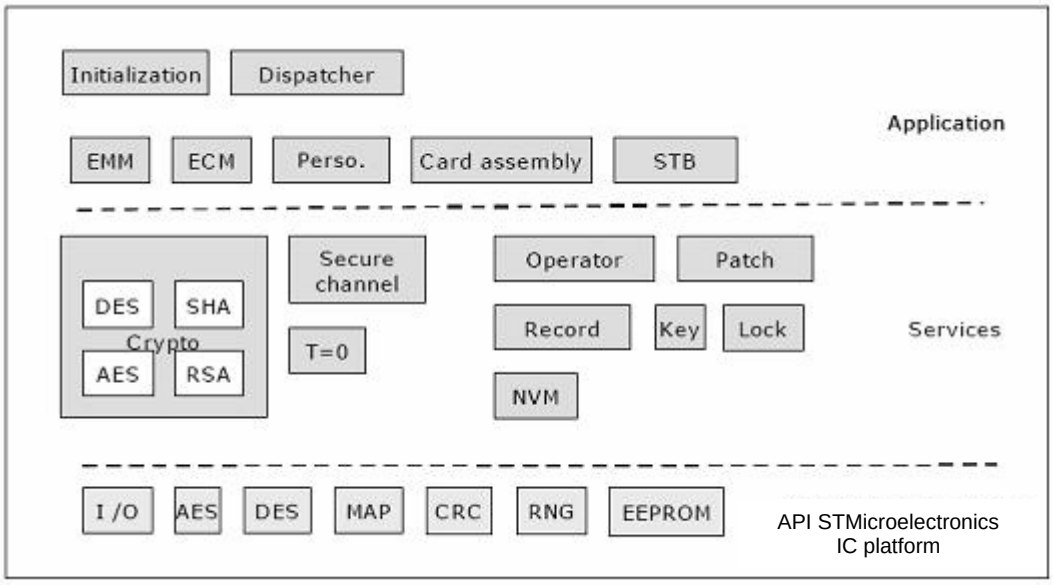
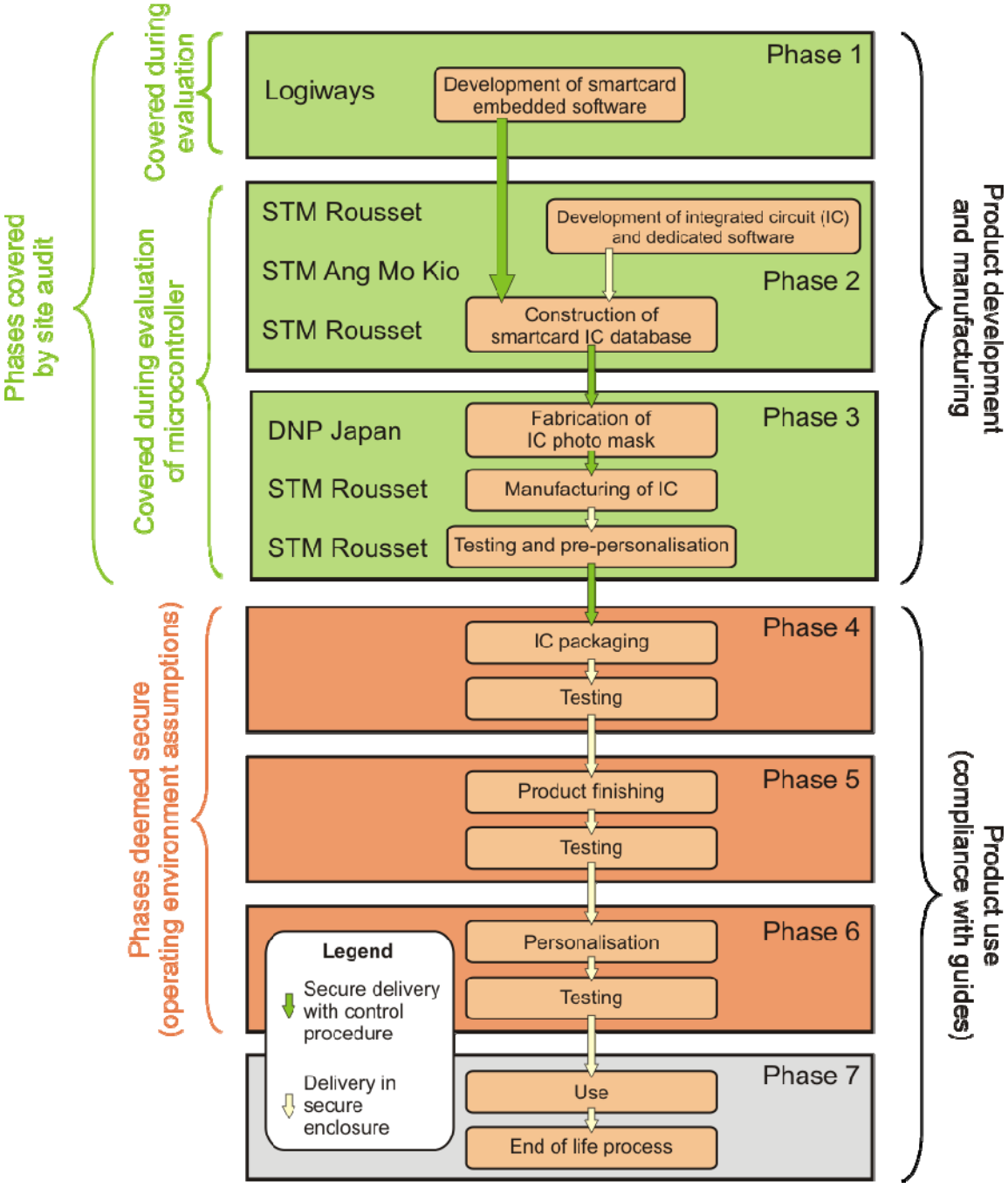


Figure 1 : General structure of the Target of Evaluation (TOE)

1.2.4. Life cycle

The product's life cycle is broken down into 7 phases as detailed in [ST], chapter 1.4.2.

The pay TV application is masked by the microcontroller manufacturer. The microcontroller is supplied to companies that manufacture and personalise cards in the "user" configuration.
Phase 2 (microcontroller development) and phase 3 (microcontroller manufacturing and testing) evaluations were carried out during the evaluation of the microcontroller.
Phase 1 (development of software embedded in microcontroller) and phase 7 (end use of product) evaluations are covered by this evaluation of the SafeAccess TV Card. The remaining phases (4 to 6) are not covered by the present evaluation but are required to comply with the operating environment assumptions in order to guarantee end use as evaluated in phase 7.



The product was developed on the following sites:

Development and testing site for all software components embedded in TOE

LogiWays
Paris R&D site
24-26 rue Louis ARMAND
75015 Paris
France

Microcontroller manufacturing and design site
STMicroelectronics SAS (see details in [DCSSI-2007/07])
Smartcard IC division
190 Avenue Célestin Coq, ZI de Rousset, BP2
13106 Rousset Cedex
France

Three roles can be distinguished:

- The manager (LogiWays) manages the cards by creating/deleting operators; he manages the updating of codes (EEPROM patches) and the personalisation of cards (LogiWays' role) ;

- The operator manages the subscriber rights and grants access to the various pay TV services ;

- The set-top box ensures communication via the trusted channel and provides information on the operator rights. The set-top box is usually associated with a subscriber.

1.2.5. Evaluated configuration

This certification report describes the evaluation work carried out in relation to the microcontroller, the dedicated software and embedded application software identified in §1.1 and §1.2.1.

Any other embedded application software, notably routines developed and embedded for the purposes of the evaluation, do not fall within the scope of this evaluation.

The evaluation was carried out using the composition principle described in [COMP]. The evaluation target is therefore the composition of the microcontroller, which is evaluated elsewhere (ST19NA18F, certificate [DCSSI-2007/07]), and the pay TV application.

2. The evaluation

2.1. Evaluation referential

The evaluation was performed in conformance with **Common Criteria version 3.1** [CC] on the basis of the evaluation methodology defined in the Common Evaluation Methodology manual [CEM].

2.2. Evaluation work

The evaluation was performed according to the composition scheme defined in the guide [COMP] in order to assess that no weakness is introduced by the integration of the software in the previously certified microcontroller.
Use has therefore been made of the evaluation results for microcontroller "**ST19NA18 release C**" at EAL5 level augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4 in CC 2.3, compliant with the [PP/9806] and [PP0002] protection profiles.
This microcontroller was certified on March 28th 2007 under reference DCSSI-2007/07 and a maintenance update was performed on this microcontroller in its current release "**ST19NA18 release F" or ST19NA18F** under reference DCSSI-2007/07-M01, cf. [CERT].

The Evaluation Technical Report [ETR] delivered to ANSSI on June 17th 2009, together with its supplements, provides details on the work carried out by the evaluation facility and certifies that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis

At the request of the sponsor, ANSSI did not carry out an analysis of the robustness of the cryptographic mechanisms on the basis of the technical reference framework [REF-CRY]. Nevertheless, the evaluation did not uncover any design or manufacturing flaws linked to cryptography for the targeted AVA_VAN level.

2.4. Random number generator analysis

The product does not offer a service to generate random numbers.

However, for internal purposes, the product makes direct use of the physical random number generator offered by the underlying component (see DCSSI-2007/07 certification report, [CERT]).

3. Certification

3.1. Conclusion

The evaluation was carried out in accordance with current rules and standards, with the required competency and impartiality of a licensed evaluation facility. A certificate has been issued on the basis of the work performed in conformance with the decree 2002-535.

This certificate attests that the “SAFEACCESS” pay TV application software (version 2.0, release 67), embedded in the microcontroller ST19NA18F developed by STMicroelectronics, fulfils the security characteristics specified in its Security Target [ST] for the augmented EAL4 evaluation level.

3.2. Restrictions

This certificate relates to the product specified in chapter 1.2 of this certification report.

The user of the certified product must comply with the operating environment security objectives defined in the Security Target [ST] and follow the recommendations given in the guides provided [GUIDES].

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
ADV Development	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	3	Basic 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		2	3	4	4	5	5	4	Production support, acceptance procedures and automation
	ALC_CMS	1	2	3	4	5	5	5	4	Problem Tracking CM overage
	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	1	Well-defined development tools
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	2	3	3	4	2	Testing: security enforcing modules
	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 evaluation: - LOGIWAYS TV CARD Security Target Reference: TWSTVC-002-ST, v1.3, dated 25/09/2008 For publication purposes, the following security target was provided and validated as part of this evaluation: - LOGIWAYS TV CARD Security Target Reference: LWSTVC-004-ST, v1.5, dated 15/10/2009
[ETR]	Evaluation technical report: - SAFEACCESS v2.0 embedded in ST19NA18 v1.0 Supplement to RTE: - Answers to questions of ANSSI certifiers, dated 15/07/2009 For the purposes of the composition evaluations with this microcontroller, a technical report for the composition was used: - ST19NA18C (Evaluation EAL5+) v1.1 Reference: YQUEM_ETRLite_ST19NA18C_v1.1
[CERT]	Certification and maintenance reports - DCSSI-2007/07 certification report “Secure microcontroller ST19NA18C”, dated 28/03/2007 - 2007/07-M01 maintenance report “Secure microcontroller ST19NA18F”, dated 04/05/2009
[CONF]	Software manufacturing manual for smart card v1.2, dated 30/04/2009
[GUIDES]	Daughterboard personalisation guide: (destined exclusively for “personalisers” of smart cards) - PERS-FILLE V5.1R3 of 22/10/2008 Card-Terminal Interface Guide: (destined exclusively for “set-top box” manufacturers) - MSD-STBV2.6 of 22/10/2008 “EMM generator specifications” guide: (destined exclusively for manufacturer of EMM Generator) - V1.0 of 11/01/2009 “ECM generator specifications” guide: (destined exclusively for manufacturer of ECM Generator) - V2.1 of 19/12/2008
[PP/9911]	Protection Profile Smart Card Integrated Circuit With Embedded Software, version 2.0, June 1999. *Certified by ANSSI under reference PP/9911.*
[PP/9806]	Protection Profile Smart Card Integrated Circuit Version 2.0, September 1998. Certified by ANSSI 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.

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, revision 2, ref CCMB-2007-09-004.
[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-2009-03-001 version 2.7 revision 1, March 2009.
[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.
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.11 du 24 octobre 2008, voir www.ssi.gouv.fr