PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/32

SA23YL18A Secure Microcontroller including the cryptographic library NesLib SA revision 1.0

Paris, 16th of September 2008

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 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-2008/32

Product name

SA23YL18A Secure Microcontroller including the cryptographic library NesLib SA revision 1.0

Product reference

SA23YL18 revision A (dedicated software AKA, maskset K2L0A, cryptographic library NesLib SA révision 1.0)

Protection profile conformity

BSI-PP-0035-2007 version 1.0

Evaluation criteria and version

Common Criteria version 3.1

Evaluation level

EAL 5 augmented

ALC_DVS.2, AVA_VAN.5

Developer

STMicroelectronics

Smartcard IC division, 190 Avenue Célestin Coq, 13106 Rousset Cedex, France

Sponsor

STMicroelectronics

Smartcard IC division, 190 Avenue Célestin Coq, 13106 Rousset Cedex, France

Evaluation facility

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France

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

Recognition arrangements

CCRA

SOG-IS

The product is recognised at EAL4 level.

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 SA23YL18 microcontroller revision A (dedicated software AKA, maskset major cut K2L0A) including the cryptographic library NesLib SA revision 1.0, developed by STMicroelectronics.

The hardware part and the dedicated software are identical to the ST23YL18 secure microcontroller certified under the reference DCSSI-2008/31. This version includes in addition the cryptographic library NesLib SA revision 1.0.

The microcontroller aims to host one or several software applications and can be embedded in a plastic support to create a Smartcard with multiple possible usages (secure identity documents, banking, health card, pay-TV or transport applications…) depending on the Embedded Software applications. However, only the microcontroller is evaluated. The software applications are not in the scope of this evaluation.

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 [PP035] protection profile (strict conformance).

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:

- Die identification (maskset major cut): K2L0A;
- Cyptographic library identification: NesLib SA revision 1.0;
- Dedicated software identification: AKA;
- Embedded software identification: this reference depends on the application embedded in ROM memory;
- Manufacturing site identification: ST 4 (Rousset).

These elements can be checked on the die with a microscope. In addition, two bytes in OTP allow identifying the product from a logical point of view, as described in the "Datasheet" (cf. [GUIDES]. The NesLib SA library includes an API that allows retrieving its version, as described in the "User Manual" (cf. [GUIDES]).

1.2.2. Security services

The product provides mainly the following security services:

- Hardware initialisation & TOE attribute initialisation;
- TOE configuration switching and control;
- TOE logical integrity;
- Test of the TOE;
- Memory Firewall;

- Physical tampering protection;
- Security violation administrator;
- Unobservability;
- Symmetric Key Cryptography Support;
- Asymmetric Key Cryptography Support;
- Unpredictable number generation support.

1.2.3. Architecture

The SA23YL18 microcontroller is made up of:

- A Hardware part:
  - An 8/16-bit processing unit;
  - Memories: EEPROM (18KB with integrity control, for program and data storage), ROM (196KB for user, 20KB for dedicated software : autotest and cryptographic libraries) and RAM (4KB);
  - Security Modules: Memory protection unit (MPU), clock generator, security monitoring and control, power management, memories integrity control, fault detection;
  - Functional Modules: 3 8-bits timers, I/O management in contact mode (IART ISO 7816-3), True Random Number Generators, EDES and asymmetric key cryptography (NESCRYPT) co-processing units.
- A dedicated software is embedded in ROM which comprises:
  - Microcontroller test capabilities (“Auto test”);
  - System and Hardware/Software interface management capabilities.
- A cryptographic library (NesLib SA) providing the cryptographic services RSA and SHA, included in the evaluation scope. This library is delivered to the embedded software developer as a linkable object, meaning that it is embedded in user ROM.

1.2.4. Life cycle

The product's life cycle is organised as follow:

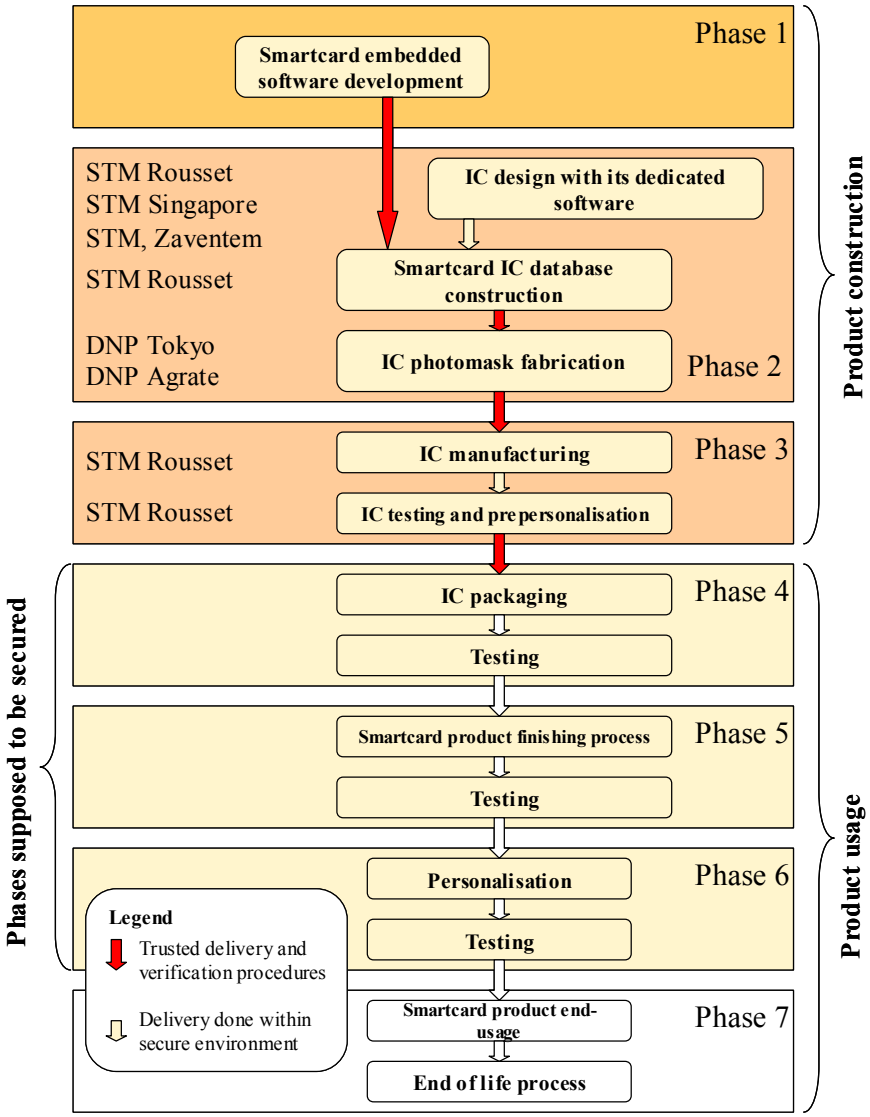

Figure 1 – Life cycle

The product is designed, prepared, manufactured and tested by:

STMicroelectronics SAS

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

A part of the design is realised by:

STMicroelectronics Pte Ltd

5A Serangoon North Avenue 5
554574 Singapore
Singapore

and by:

STMicroelectronics

Excelsiorlaan 44-46,
B-1930 Zaventem,
Belgium.

The photo masks of the product are manufactured by:

DAI NIPPON PRINTING CO., LTD

2-2-1, Fukuoka, kamifukuoka-shi,
Saitama-Ken, 356-8507
Japan

and by:

DAI NIPPON PRINTING EUROPE

Via C. Olivetti, 2/A,
I-20041 Agrate Brianza,
Italy

The product manages itself the logical phases of its life cycle and can be in one of its two following configurations:

- "Test" configuration: product configuration at the end of developer IC manufacturing. The product is tested with a part of the Dedicated Software (called "Autotest") within the secure developer premises. Pre-personalization data can be loaded in the EEPROM. The product configuration is changed to "User" before delivery to the next user, and the part cannot be reversed to the "test" configuration.
- "User" configuration: final configuration of the product, including 3 modes:
  - "reduced test" mode, allowing STMicroelectronics to perform some reduced sets of test;
  - "diagnosis", allowing even more limited operations restricted to STMicroelectronics;
  - "end user", final usage mode of the product, whose functionalities are driven exclusively by the Embedded Software. The developer test functionalities are unavailable. The end-users of the product can use it only under this mode.

1.2.5. Evaluated configuration

This certification report presents the evaluation work related to the product and the dedicated software library identified in §1.2.1. Any other embedded application, such as embedded applications intended specifically for the sake of the evaluation is not part of the evaluation perimeter.
Referring to the life-cycle, the evaluated product is the product that comes out the manufacturing, test and pre-personalization phase (phase 3).
For the evaluation needs, the product SA23YL18A was provided to the ITSEF with a dedicated test software in a mode known as "open[1]".

[1] mode that enables to load and execute a native code in EEPROM and also to disable the configurable security mechanisms (see [CC AP], chapter 3.8).

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1** [CC] and with the Common Evaluation Methodology [CEM].
For assurance components above EAL4 level, the evaluation facility own evaluation methods 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 technical report [ETR], delivered to DCSSI the 1st of September 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.

2.4. Random number generator analysis

The evaluated product provides a hardware random number generator that can be used by the embedded software.
The evaluation facility has evaluated the random number generator with the [AIS31] methodology.
The generator reaches the class "P2 – *SOF-high*" according to [AIS31].

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 secure microcontroller SA23YL18A submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 5 augmented.

3.2. Restrictions

This certificate only applies on the product specified in chapter 1.2 of this certification report.

This certificate provides a resistance assessment of the SA23YL18A product to a set of attacks which remains generic due to the missing of any specific embedded application. Therefore, the security of a final product based on the evaluated microcontroller would only be assessed through the final product evaluation, which could be performed on the basis of the current evaluation results.

The user of the certified product shall respect the operational environmental security objectives summarized specified in the security target [ST] chapter 5.2 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:

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

3.3.2. International common criteria recognition (CCRA)

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 5+	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**	**5**	Complete semiformal functional specification with additional error information
	ADV_IMP				**1**	1	**2**	**2**	**1**	Implementation representation of the 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 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 procedure
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	**5**	Development tools CM coverage
	ADO_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 Security target evaluation	ASE_CCL	**1**	1	1	1	1	1	1	**1**	Conformance claim
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended component 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 specifications
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	2	**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**	Independant 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 the evaluation: - ST23YL80 / ST23YL18 Security Target, Reference: SMD_ST23YL_ST_08_001 V01.01, STMicroelectronics. For the needs of publication, the following security target has been provided and validated in the evaluation: - SA23YL18A Security Target - Public Version, Reference: SMD_SA23YL18_ST_08_001 Rev 01.01, STMicroelectronics
[ETR]	Evaluation technical report : - Evaluation Technical Report - LAFITE Project, Reference: LAFITE_YL18A_YL80B_ETR_v2.0, Serma Technologies For the needs of composite evaluation with this microcontroller a technical report for composition has been validated: - ETR Lite for Composition - SA23YL18A, Référence : LAFITE_SA23YL18A_ETRLiteComp_v1.0, Serma Technologies
[CONF]	Product configuration list: - ST23YL18 and SA23YL18 products - Configuration list, Référence : SCP_ST23YL18_CFGL_08_001 V01.02, STMicroelectronics, List of the delivered materials by STMicroelectronics: - LAFITE - ST/SA23YL80B and ST23/SA23YL18A documentation report, Référence : SMD_ST23YL_DR_08_001 V1.0 STMicroelectronics.
[GUIDES]	The product user guidance documentation is the following: - ST23YL18 Smartcard MCU with enhanced security, crypto-processor and 18 Kbytes EEPROM – Datasheet, Référence : DS_23YL18 Rev 0.3, STMicroelectronics - Neslib Cryptographic Library SA – User Manual, Reference: UM_NesLib_SA Rev 2, STMicroelectronics - ST23 Platform - Security Guidance, Reference: AN_SECU_23 Rev 4, STMicroelectronics - ST23 Reference Implementation User Manual, Reference: UM_23_RefImp/0802 Rev 9, STMicroelectronics - ST21/23 programming manual Reference: PM_21_23/0709 Rev1, STMicroelectronics

	- ST23 AIS31 Compliant Random Number User Manual, Reference: UM_23_AIS31 Rev 1, STMicroelectronics - ST23 AIS31 Tests reference implementation user manual, Reference: AN_23_AIS31 Rev1, STMicroelectronics
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007.*

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.
[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
[AIS31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25/09/2001, Bundesamt für Sicherheit in der Informationstechnik