PREMIER MINISTRE

General Secretariat for Defence and National Security

French Network and Information Security Agency

Certification Report ANSSI-CC-2010/07

ST23ZL48/34/18A Secure Microcontrollers

Paris, March 8th 2010

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 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
France

certification.anssi@ssi.gouv.fr

Certification report reference

ANSSI-CC-2010/07

Product name

ST23ZL48/34/18A Secure Microcontrollers

Product reference

ST23ZL48/34/18A external revision A (dedicated software ASD, K320ACA mask set)

Protection profile conformity

BSI-PP-0035-2007 version 1.0

Security IC Platform Protection Profile v1.0, 15 June 2007

Evaluation criteria and version

Common Criteria version 3.1

Evaluation level

EAL 5 augmented

AVA 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 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.

Content

1. The product

1.1. Presentation of the product

The evaluated products are the ST23ZL48, ST23ZL34, ST23ZL18 secure microcontrollers revision A[1] (dedicated software ASD, K320ACA mask set) developed by STMicroelectronics.

The ST23ZL48A, ST23ZL34A, ST23ZL18A only differ by the logical size of the non volatile EEPROM memory (48Kb or 34Kb or 18Kb), the physical size of the memory being 48Kb in the 3 configurations but only 34Kb or 18Kb are accessible on ST23ZL34A or ST23ZL18A products.

The microcontrollers aim 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 with [PP035] protection profile (strict compliance).

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:

- Marked on the Die:
  - Die identification: K320 (Die name) and all masks revision letters corresponding to K320ACA mask set;
  - Dedicated software identification: ASD (Boot sequence, embedded test software);
  - Embedded software identification: UBX[2] this is the *Card Manager*, a reference Operating System, embedded in the *User* ROM of the samples which have been tested, for the evaluation needs only. The *Card Manager* is not part of the evaluation perimeter, cf §1.2.5;
  - Manufacturing site identification: ST 4 (Rousset).

[1] This is the product external revision.

[2] This trigram features embedded software and is unique to each user code in order to identify the embedded software which is provided by the customer to the silicon provider to be placed in ROM. This trigram present on the chip provided to a customer will be necessarily different from that appearing on the evaluated microcontroller.

-

- Present in the EEPROM OTP (*One Time Programmable*) memory area (cf. [GUIDES]):
    - In C007h and C008h addresses, the User can read the product identification number which is 0001h for ST23ZL48[1].

1.2.2. Security services

The product provides the following main security services:

- Initialisation of the hardware platform and its attributes;
- Secure handling of the life cycle;
- Logical integrity of the product;
- Test of the product;
- Memory management (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 ST23ZL48/34/18A microcontrollers are made up of:

- A Hardware part:
    - An 8/16-bit central processing unit ;
    - Memories :
        - 48 Kbytes of EEPROM (including 128 bytes of OTP) with integrity control, for program and data storage ;
        - 300 Kbytes of ROM for user software ;
        - 6 Kbytes of RAM ;
        - 20 Kbytes of ROM for dedicated software.
    - Security Modules: memory protection unit (MPU), clock generator, security monitoring and control, power management, memory integrity control and fault detection;
    - Functional Modules: three 8-bit timers, I/O management in contact mode (IART ISO 7816-3), True Random Number Generator, EDES co-processor supporting DES algorithms and the NESCRYPT co-processor with a dedicated 2-Kbyte RAM supporting public key cryptographic algorithms.
- A dedicated software is embedded in ROM which comprises:
    - Microcontroller test software ;
    - System and Hardware/Software interface management capabilities.

[1] This is 000Ch for ST23ZL34 and 000Bh for ST23ZL18.

1.2.4. Life cycle

The product's life cycle is organised as follow:

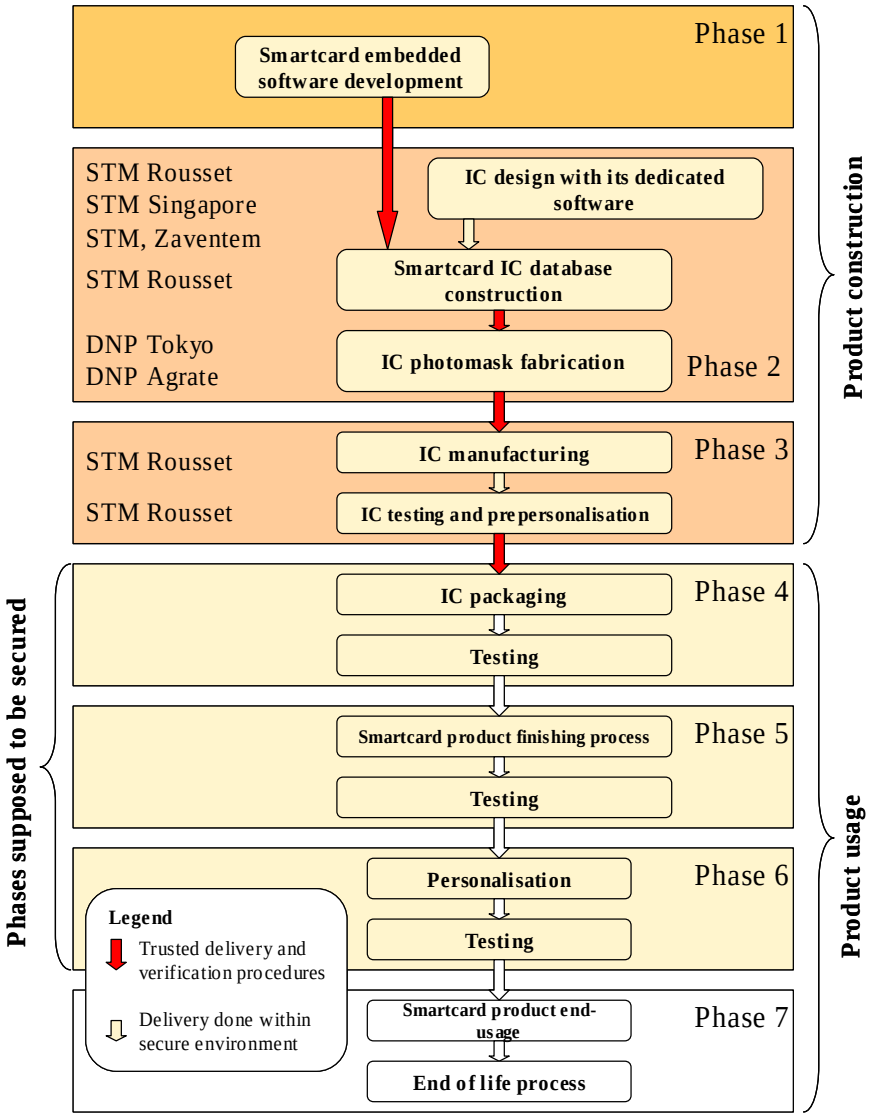

Figure 1 – Life cycle of a smart card

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: at the end of IC manufacturing, the microcontroller is tested using the test software stored in ROM. Pre-personalization data can be loaded in the EEPROM. The product configuration is changed to "User" before delivery to the next user, and the device cannot be reversed to the "test" configuration.
- "User" configuration : including 3 modes :
  - "reduced test", 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 identified in §1.2.1. Any other embedded application, embedded for evaluation purpose only, 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, only the products SB23ZL48A, SB23ZL34A, SB23ZL18A (with internal revision C), including the cryptographic library Neslib v3.0, were provided to the ITSEF with a dedicated evaluation software in a mode known as "open[1]".

The Evaluator clearly mentions in Chapter 5.3 of the ETR *lite* [RTE] that the evaluation results are also applicable to ST23ZL48/34/18A[1] products.

[1] mode that enables to load and execute a native code in EEPROM and also to disable the configurable security mechanisms.

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1** [CC] and the Common Evaluation Methodology [CEM].
For assurance components above EAL4 level, the evaluation facility own evaluation methods, validated by ANSSI, 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 ANSSI on the 4th of March 2010, describes the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis according to ANSSI technical reference frame

The evaluated product provides the following cryptographic support services:

- support for symmetric key cryptography (EDES) ;
- support for asymmetric key cryptography (NESCRYPT) ;
- support for random numbers generation (TRNG).
-

These services, however, cannot be analyzed in relation to the ANSSI technical reference frame [REF-CRY], [REF-CLE] and [REF-AUT] as they do not contribute to the inherent security of the product; their strength will depend on their use by the application embedded in the microcircuit.

2.4. Random number generator analysis

The evaluated product provides a hardware random number generator that has been evaluated according to the [AIS31] methodology by the evaluation facility: the generator reaches the class "P2 – *SOF-high*" according to [AIS31].

[1] Products without Neslib v3.0 cryptographic library in ROM

3. Certification

3.1. Conclusion

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

This certificate testifies that the secure microcontrollers ST23ZL48/34/18A submitted for evaluation fulfil the security features specified in its security target [ST] for the evaluation level EAL augmented.

3.2. Restrictions of use

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

This certificate provides a resistance assessment of the ST23ZL48/34/18A products 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 microcontrollers would only be assessed through the final product evaluation, which could be performed using the results of current evaluation listed in Chapter 2.

The user of the certified product shall respect the operational environmental security objectives 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 such scope are released with the following marking:

1 The signatory countries of the SOG-IS agreement are: Finland, France, Germany, 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, Pakistan, 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									
	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**	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 the evaluation: - Sx23ZLxxA Security Target, Reference: SMD_Sx23ZLxx_ST_09_001, v01.00, STMicroelectronics - For the needs of publication, the following security target has been provided and validated in the evaluation: - ST23ZLxxA Security Target - Public Version, Reference: SMD_ST23ZLxx_ST_09_001, v01.00, STMicroelectronics
[ETR]	Evaluation technical report : - Evaluation Technical Report - LAFITE Project, Reference: LAFITE_SB23ZL48A_ETR_v1.2 / 1.2, 4 March 2010, Serma Technologies For the needs of composite evaluation with this microcontroller a technical report for composition has been validated: - ETR Lite for Composition – LAFITE Project, Reference: LAFITE_SB23ZL48A_ETRLiteComp_v1.2/ 1.2, 4 March 2010, Serma Technologies
[CONF]	Products configuration list: - Configuration list SA/SB23ZL48/34/18 (internal version C), Reference : SMD_STSB23ZL48_CFGL_09_001 rev 2.0, STMicroelectronics List of the delivered materials: - documentation report, Reference: SMD_STSB23ZL48_DR_09_001_v1.0, STMicroelectronics.
[GUIDES]	The product user guidance documentation is the following: - ST23ZL48 Datasheet, Référence : DS_23ZL48 Rev 0.4, STMicroelectronics - ST23ZL34 Datasheet, Reference : DS_23ZL34 Rev 0.2, STMicroelectronics - ST23ZL18 Datasheet, Reference : DS_23ZL18 Rev 0.2, STMicroelectronics - ST23Z Platform - Security Guidance, Reference : AN_SECU_23Z Rev 2, STMicroelectronics - ST23 Reference Implementation User Manual, Reference : UM_23_RefImp Rev 18,

	STMicroelectronics - ST21/23 programming manual Reference : PM_21_23/0709 Rev 1, STMicroelectronics - Porting code from ST23Y to ST23Z devices, Reference : AN_23_Porting Rev 3, STMicroelectronics
[PP0035]	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-2009-03-001 version 2.7 revision 1, March 2009.
[REF-CRY]	Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms, version 1.11, 24th of October 2008, see www.ssi.gouv.fr
[REF-CLE]	Cryptographic keys management - Rules and recommendations about management of keys used in cryptographic mechanisms, version 1.10, 24th of October 2008, see www.ssi.gouv.fr
[REF-AUT]	Authentication - Rules and recommendations about authentication mechanisms with standard level robustness, v0.13 12th of April 2007, No. 729/SGDN/DCSSI/SDS
[AIS31]	Functionality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25/09/2001, Bundesamt für Sicherheit in der Informationstechnik (BSI)