



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information

Certification Report ANSSI-CC-2012/65

Secure microcontroller ST23YS64C

Dedicated software AIC, *maskset* K2K0CIA

Paris, October 1 , 2012

Courtesy Translation



Warning

The purpose of this report is to provide sponsors with a document enabling them to assess the security level of the product under the conditions of use and operation defined in this report for the evaluated version. This report also aims at providing 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 describes the 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 of the product by the ANSSI (French Network and Information Security Agency), and does not guarantee that the certified product is totally free of all exploitable vulnerabilities.

All 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

Reproduction of this document without any change or cut is authorised.

Certification report reference	ANSSI-CC-2012/65
Product name	Secure microcontroller ST23YS64C
Product reference	ST23YS64 external revision C, dedicated software AIC, maskset K2K0CIA
Protection profile conformity	[PP0035]: Security IC Platform Protection Profile, Version 1.0
Evaluation criteria and version	Common Criteria version 3.1 revision 3
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
Mutual Recognition Agreements	<div style="display: flex; justify-content: space-around;"><div style="text-align: center;">CCRA </div><div style="text-align: center;">SOG-IS </div></div> <p>The product is recognized at level EAL4.</p>

Introduction

The Certification

Certification for the security provided by information technology products and systems is governed by decree number 2002-535 dated April, 18th 2002, modified. 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

1. THE PRODUCT	6
1.1. PRESENTATION OF THE PRODUCT.....	6
1.2. EVALUATED PRODUCT DESCRIPTION	6
1.2.1. <i>Product identification</i>	6
1.2.2. <i>Security services</i>	7
1.2.3. <i>Architecture</i>	7
1.2.4. <i>Life cycle</i>	9
1.2.5. <i>Evaluated configuration</i>	11
2. THE EVALUATION.....	12
2.1. EVALUATION REFERENTIAL	12
2.2. EVALUATION WORK	12
2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS.....	12
2.4. RANDOM NUMBER GENERATOR ANALYSIS	12
3. CERTIFICATION.....	13
3.1. CONCLUSION	13
3.2. RESTRICTIONS	13
3.3. RECOGNITION OF THE CERTIFICATE	14
3.3.1. <i>European recognition agreement (SOG-IS)</i>	14
3.3.2. <i>International common criteria recognition (CCRA)</i>	14
ANNEX 1. EVALUATION LEVEL OF THE PRODUCT.....	15
ANNEX 2. EVALUATED PRODUCT'S REFERENCES.....	16
ANNEX 3. CERTIFICATION REFERENCES	18

1. The product

1.1. Presentation of the product

The evaluated product is «Secure microcontroller ST23YS64C, ST23YS64 external revision C, dedicated software AIC, maskset K2K0CIA» developed by STMicroelectronics.

The hardware part and the dedicated software are identical to those of the ST23YL80C product, certified under the reference ANSSI-CC-2009/37, and maintained under references ANSSI-CC-2009/37-M01 and ANSSI-CC-2009/37-M02.

This microcontroller alone is not a product that can be used as such. It is designed to host one or more applications. It can be embedded in a plastic support to create a smartcard with multiple possible uses. This card has many possible uses (secure identity documents as well as bank, pay TV, transport and health applications, etc.) depending on the embedded software applications. These 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 strictly complies with protection profile [PP0035].

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:

- Etched on the microcontroller:
 - o Chip identification (*major cut* HW reference): "K2K0";
 - o *Maskset*: "K2K0CIA";
 - o Dedicated software reference (*OST name*): "AIC" (*boot & reset* sequence, autotest);
 - o Reference of the (*Card Manager*) embedded software: "UZB" (demonstration operating system embedded in *User ROM* in the samples submitted to the tests for evaluation needs. It is not part of the scope of this evaluation, cf. §1.2.5);
 - o Identification of the manufacturing site: "ST 4" (Rousset);
- Presents in EEPROM memory, as indicated in the document "*Datasheet*" (cf. [GUIDES]):
 - o ST23YS64C identification number: "AC14h" at address C007h-C008h;
 - o Internal revision of the ST23YS64C: "49h" (internal revision I¹) at address C011h.

These elements have been verified by the evaluator.

¹ The internal revision I is associated with the external (commercial) revision C as indicated in [CONF].

1.2.2. Security services

The product provides the following main security services:

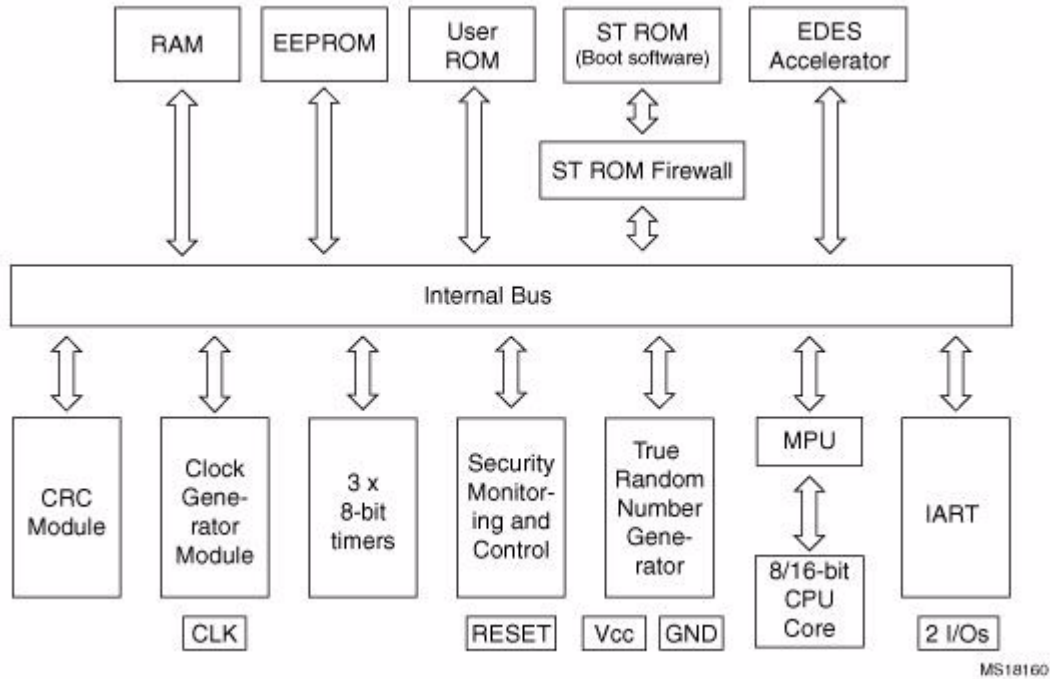
- Initialization of the hardware platform and attributes;
- Secure management of the life cycle;
- Logical integrity of the product;
- Product test;
- Memory management (*firewall*);
- Physical tampering protection;
- Management of security violations;
- Unobservability;
- Support for symmetric key cryptography;
- Support for random number generation.

1.2.3. Architecture

The ST23YS64C microcontroller consists of the following components:

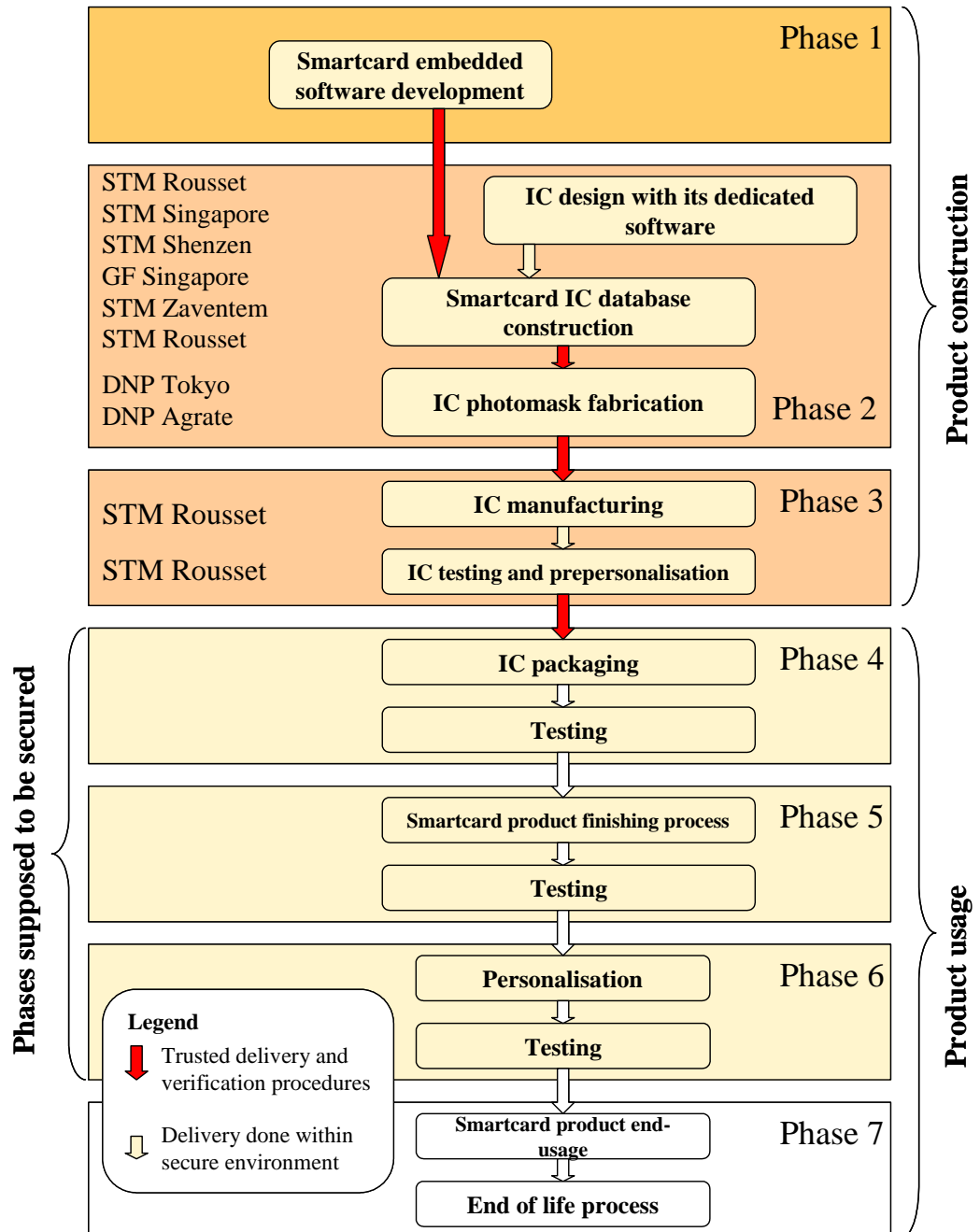
- A hardware part with:
 - o An 8/16-bit processor;
 - o Memories: 64 KB of EEPROM (with integrity check) for storing programs and data, 396 KB of ROM memory for storing user programs, 6 KB of RAM and 20 KB of ROM for storing dedicated software (OST);
 - o Security modules: Memory Protection Unit (MPU), clock generator, security control and monitoring, power management, memory integrity control, fault detection;
 - o Functional modules: three 8-bit timers, input/output management in contact mode (IART ISO 7816-3), random number generators (TRNG), EDES coprocessors¹;
- a "dedicated software" part in ROM including:
 - o Test software for the microcontroller (autotest);
 - o Utility software for system and hardware/software interface management.

¹ *Enhanced DES.*



1.2.4. Life cycle

The product's life cycle is organised as follow:



The product is developed, integrated (reparation of the product database), manufactured and tested on the following site:

STMicroelectronics SAS

Secure MCU Division
 190 Avenue Célestin Coq, ZI de Rousset, BP2
 13106 Rousset Cedex
 France

GlobalFoundries

60 Woodlands industrial park
D street 2
Singapore 738406

STMicroelectronics

629 Lorong 4/6 Toa Payoh
Singapore 319521

STMicroelectronics

16 Tao hua Rd
Futian free trade zone
Shenzen
P.R. China 518048

STMicroelectronics

7 Loyang drive
Singapore 508938

The product is partly developed by:

STMicroelectronics Pte ltd

5A Serangoon North Avenue 5,
554574 Singapore.
Singapore

and by:

STMicroelectronics

Excelsiorlaan 44-46,
B-1930 Zaventem,
Belgium

The reticles 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 provides its own life cycle management system in the form of two user configurations:

- "test" configuration: at the end of the manufacturing phase, the microcontroller is tested using the test software included in ROM. The pre-personalization data can be loaded in EEPROM. This configuration is then irreversibly blocked when it switches to "user" configuration;
- "user" configuration: this mode consists in three submodes:
 - o "Reduced test" mode that enables STMicroelectronics to perform several restricted tests;
 - o "Diagnosis" mode: a part of the "*Reduced test*" mode reserved for STMicroelectronics;
 - o "End user" mode: final user mode of the microcontroller that then operates under the control of the smartcard's embedded software. The test software is no longer accessible. The end users can only use the microcontroller in this configuration.

1.2.5. *Evaluated configuration*

This certification report presents the evaluation work related to the microcontroller and dedicated software described in paragraph 1.2.1. Any other potentially embedded application, in particular routines embedded for evaluation needs, is therefore not in the scope of the evaluation.

With respect to the life cycle, the evaluated product is the product at the end of the manufacturing, test and pre-personalization phase (phase 3).

For the evaluation needs, the ST23YS64C microcontroller has been provided to the evaluation center with a software operating system called *Card Manager*, in a so-called "open mode"¹.

¹ Mode used to load native code into EEPROM and execute it; also used to disconnect parameterizable security mechanisms.

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1 revision 3** [CC] and with the Common Evaluation Methodology [CEM].

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 relies on the evaluation results of the the ST23YL80 product revision C, certified EAL5 augmented for ALC_DVS.2 and AVA_VAN.5 in October 2009 under the reference [2009/37]

The evaluation technical report [ETR], delivered to ANSSI the 24th July 2012, 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 rating of cryptographic mechanisms according to the ANSSI technical reference framework [REF] has not been carried out. Nonetheless, the evaluation has not detected any design or manufacturing vulnerabilities for the targeted AVA_VAN level.

2.4. Random number generator analysis

The evaluation facility evaluated the random number generator using the [AIS 31] methodology in the frame of the work on the ST23YL80: it reached the "P2 - *SOF High*" level in accordance with [AIS 31].

3. Certification

3.1. Conclusion

The evaluation was carried out according to the current rules and standards, with the required competency and impartiality of 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 “Secure microcontroller ST23YS64C, external revision C, dedicated software AIC, maskset K2K0CIA” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 5 augmented for ALC_DVS.2 and AVA_VAN.5 components.

3.2. Restrictions

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

This certificate provides a resistance assessment of the “ST23YS64C Secure microcontroller” product to a set of attacks which remains highly generic due to the absence of a specific embedded application. Therefore, the security of a final product based on the evaluated microcontroller can only be assessed through the final product evaluation, which may be performed on the basis of the current evaluation results.

The user of the certified product must ensure compliance with the security objectives for the operational environment, as specified in the security target [ST], and shall comply with the recommendations in the guidance [GUIDES].

3.3. Recognition of the certificate

3.3.1. *European recognition agreement (SOG-IS)*

This certificate is released in accordance with the provisions of the SOG-IS [SOG-IS].

The 2010 SOG-IS Recognition Agreement allows recognition of ITSEC and Common Criteria certificates by Signatory States of the agreement¹. The European recognition agreement is applicable, for smart cards and similar devices, up to ITSEC E6 High and CC EAL7 levels. The certificates recognized in the agreement scope are released with the following marking:



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 countries², 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 following countries have signed the SOG-IS recognition agreement: Germany, Austria, Spain, Finland, France, Italy, Norway, the Netherlands, the United Kingdom and Sweden.

2 The following countries have signed the CCRA agreement: Germany, Australia, Austria, Canada, Denmark, Spain, the United States of America, Finland, France, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, Norway, New Zealand, Pakistan, the Netherlands, the Republic of Korea, the Czech Republic, the United Kingdom, Singapore, Sweden and Turkey.

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+	Component name
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_TDS		1	2	3	4	5	6	4	Semiformal modular design
AGD User 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 Support to lifecycle	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_LCD			1	1	1	1	2	1	Developer defined life-cycle model
	ALC_TAT				1	2	3	3	2	Compliance with implementation standards
ASE Evaluation of the security target	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's references

[ST]	<p>Reference security target for the evaluation :</p> <ul style="list-style-type: none"> - <i>ST23YS64C Security Target</i>, Reference: SMD_ST23YS64_ST_11_001_V01.00, <i>September 2011</i>, STMicroelectronics. <p>For publication requirements, the following security target was provided and validated in the scope of this evaluation :</p> <ul style="list-style-type: none"> - <i>ST23YS64C Security Target – Public Version</i>, Reference: SMD_ST23YS64_ST_11_002 Rev 01.00, <i>September 2011</i>, STMicroelectronics.
[RTE]	<p>Technical report of the evaluation:</p> <ul style="list-style-type: none"> - <i>Evaluation Technical Report - LAFITE Project</i>, Reference: LAFITE_ST23YS64C_ETR_v2.0/2.0, 24 July 2012, Serma Technologies. <p>For the composition evaluation needs for this microcontroller, a technical report on composition has been validated:</p> <ul style="list-style-type: none"> - <i>ETR Lite for Composition – LAFITE Project</i>, Reference: LAFITE_ST23YS64C_ETRLiteComp_v2.0/2.0, 24 July 2012, Serma Technologies.
[CONF]	<p>Product configuration list:</p> <ul style="list-style-type: none"> - <i>ST23YL80 and SA23YL80 products - Configuration list</i>, Reference: SCP_ST23YL80_CFGL_08_001 V01.02, STMicroelectronics <p>Documentation list:</p> <ul style="list-style-type: none"> - <i>LAFITE - ST/SA23YL80C, ST23/SA23YL18B and ST23YS64C documentation report</i>, Reference: SMD_ST23YL_DR_08_001 V1.03 STMicroelectronics
[GUIDES]	<p>The user manuals of the product consist of the following documents:</p> <ul style="list-style-type: none"> - <i>ST23YS64 – Datasheet</i>, Reference: DS_23YS64 Rev 0.1, <i>January 2011</i> STMicroelectronics - <i>ST23 Platform - Security Guidance</i>, Reference: AN_SECU_23 Rev 9, STMicroelectronics - <i>ST21/23 programming manual</i> Reference: PM_21_23_Rev3, STMicroelectronics - <i>ST23 AIS31 Compliant Random Number User Manual</i>, Reference: UM_23_AIS31 Rev 2, STMicroelectronics - <i>ST23 AIS31 Reference implementation Startup, Online and Total Failure Tests</i>, Reference: AN_23_AIS31 Rev2, STMicroelectronics



[2009/37]	Certification report ANSSI-CC-2009/37, ST23YL80C Secure microcontroller, 22 th October 2009, ANSSI.
[PP0035]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. <i>Certified by the BSI (Bundesamt für Sicherheit in der Informationstechnik) under reference BSI_PP_0035-2007.</i>

Annex 3. Certification references

Decree number 2002-535, 18 th April 2002, modified, 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, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-001; Part 2: Security functional components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-002; Part 3: Security assurance components, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, July 2009, version 3.1, revision 3 Final, ref CCMB-2009-07-004.
[CC IC]	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.
[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.
[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 3.0, 8 th January 2010, Management Committee.
[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 of 26 January 2010 annexed to the "Référentiel général de sécurité", see www.ssi.gouv.fr . Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.20 of the 24 th October 2008 annexed to the "Référentiel général de sécurité", see www.ssi.gouv.fr .
[AIS31]	Functionality classes and evaluation methodology for physical random number generator, AIS31 version 1, the 25 th September 2001, Bundesamt für Sicherheit in der Informationstechnik