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-2012/42

Secure Microcontrollers ST23ZR08A/ST23ZR04A/ST23ZR02A, ST23ZC08A/ST23ZC04A/ST23ZC02A

Paris, July 19th 2012

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-2012/42

Product name

Secure Microcontrollers ST23ZR08A/ST23ZR04A/ST23ZR02A, ST23ZC08A/ST23ZC04A/ST23ZC02A

Product reference

External revision A, internal revision H (dedicated test firmware OST YBC version 61, maskset K340)

Protection profile conformity

[BSI-PP-0035-2007] 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

ZI de Rousset BP 2, 13106 Rousset Cedex, France

Sponsor

STMicroelectronics

ZI de Rousset BP 2, 13106 Rousset Cedex, France

Evaluation facility

THALES (TCS – CNES)

18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

Recognition arrangements

CCRA **SOG-IS**

The product is recognized 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, 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

1.1. Presentation of the product

The evaluated product is the product family « Secure Microcontrollers ST23ZR08A/ST23ZR04A/ST23ZR02A, ST23ZC08A/ST23ZC04A/ST23ZC02A », in external revision A, internal revision H, with dedicated test software OST (« Operating System for Test ») YBC version 61, and maskset K340, developed by STMicroelectronics ZI de Rousset BP 2, 13106 Rousset Cedex, France.

For commercial reasons, this product can be sold under various references, detailed in chapter « 2.1 TOE Overview » of [ST], the differences between references seat in the size of the non volatile memory, and the type of available interface (dual mode or « contactless » only), proposed as summarized in following table :

Product Name	NVM EEPROM Size	I/O Modes
ST23ZR08A	8 Kbytes	Dual
ST23ZR04A	4 Kbytes	Dual
ST23ZR02A	2 Kbytes	Dual
ST23ZC08A	8 Kbytes	Contactless
ST23ZC04A	4 Kbytes	Contactless
ST23ZC02A	2 Kbytes	Contactless

The microcontroller is not a usable product as such. It 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 operating environment.

This security target is strictly compliant to the protection profile [BSI-PP-0035-2007].

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 (refer to [ST], chapter "2.1 TOE overview", and [GUIDES] for more details):

- marked on the Die:
  - K340A : STMicroelectronics internal name of the product (Maskset), the letter A is the external revision, it identifies the major revision of silicon;
  - YBC: trigram identifier of the dedicated test software OST;
  - UZI: trigram identifier of the user software embedded in User ROM; in the case of this evaluation, it identifies the demonstration operating system from STMicroelectronics, called "Card Manager" (or "Reference Implementation"). The Card Manager is not included within the scope of evaluation;
  - ST 4: Identification of the manufacturing site (here, 4 corresponds to the site STMicroelectronics/Rousset);
- information present in the OTP area ("One Time Programmable") of the EEPROM memory, user accessible at the following addresses:
  - C007-C008h = "0015h": these two bytes identify the product variant, (here, 15h is for ST23ZR08A); for other variants ST23ZR04A, ST23ZR02A, ST23ZC08A, ST23ZC04A, ST23ZC02A of the product, the value is "0020h", "0021h" , "0022h", "0023h", "0024h" respectively;
  - C00Eh = "61h": this byte identifies the version of dedicated test software OST, the value is written in hexadecimal;
  - C011h = "48h": this byte identifies the internal revision letter of the product (H), this value is written to an ASCII character encoded in hexadecimal format.

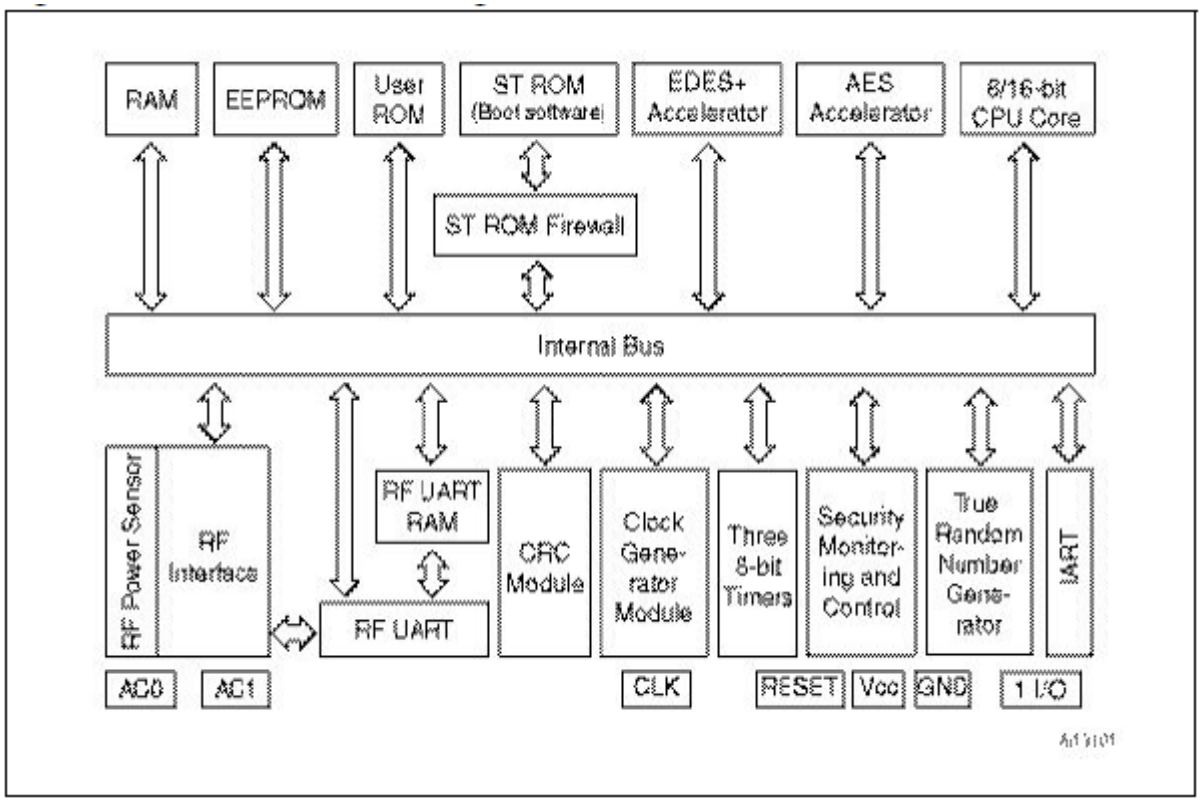
1.2.2. Security services

The product provides the following security services, detailed in chapter "2.1 TOE overview" of the [ST]:

- initialization of the hardware platform and attributes;
- secure management of the lifecycle;
- logical integrity of the product;
- test of the product;
- memory management;
- physical protection;
- management of security violations;
- non-observability;
- support for symmetric-key cryptography;
- support for non-predictable number generation.

1.2.3. Architecture

The TOE architecture is illustrated in the following figure :



In addition to these hardware components, the TOE also embeds in the ROM, a software component OST that:

- starts the product ("Boot");
- provides commands for test and maintenance of the TOE;
- also provides access control to these features when the TOE configuration is "Test" or "User" configuration.

This software is no longer accessible once the TOE is configured for "end user" (see next chapter "Life Cycle 1.2.4).

1.2.4. Life cycle

The life cycle of the product conforms to that described in [BSI-PP-0035-2007]. It is detailed in chapters "2.3 TOE life cycle" and "2.4 TOE environment" of the [ST]. The various steps are summarized in the following table:

Phase	**Name**	**Description**	**Entity**
1	Development of the embedded application	Development of the user application	Developer of the user application
2	Development of the IC	- IC design - Development of the OST dedicated software	Circuit designer and developer : STM (Rousset/France and Ang Mo Kio/Singapore)
3	IC manufacturing	- Manufacturing and integration of the photomask - IC manufacturing - IC test - Preparation - Pre-personalization	- Mask manufacturing: DNP/Japan & DPE/Italy - IC manufacturing: STM (Rousset/France) - IC Test : STM (Rousset/France and Toa Payoh/Singapore)
4	IC packaging	- IC packaging (and test)	IC packaging: STM (Bouskoura/Morocco), SMARTFLEX (Singapore), and NEDCARD (Netherlands), using DISCO (Germany) for wafer sawing
5	Composite product integration	- Finalization process of the composite product - Preparation of composite product - Shipment of composite product	Composite product integrator
6	Personalization	- Composite product personalization - Test of composite du product	Personalizer
7	Usage	Use of composite product by issuers and final users	Final users

Other entities that may intervene during production of the TOE are:

- STM (Loyang / Singapore) for logistics;
- - STM (Shenzhen / China) and DISCO (Germany) for thinning wafers.

This evaluation covered the phases 2, 3 and 4 of the life cycle described above. The evaluation also covered the procedures for delivery and verification of the application

developed in Phase 1, and the procedures for delivery of the TOE to the entity responsible for packaging the component involved in phase 4. The procedures for the other phases are outside the scope of this assessment.

The TOE is always delivered in "End User" mode:
- either in the form of wafer, optionally sawn, at the end of phase 3;
- or in a packaged form, at the end of phase 4.

The product is designed, developed, integrated (preparation of the product database), manufactured and tested by:

STMicroelectronics SAS (Rousset/France),

SMD division, 190 Avenue Célestin Coq, ZI de Rousset, BP2,
13106 Rousset Cedex,
France.

Part of product development is carried out by:

STMicroelectronics Pte ltd (Ang Mo Kio/Singapore),

5A Serangoon North Avenue 5,
554574, Singapore,
Singapore.

The product can also be tested by:

STMicrolectronics (Toa Payoh/Singapore),

7, Loyang Drive, Loyang Industrial Park,
508938, Singapore,
Singapore.

The photo masks of the product are manufactured by:

DAI NIPPON PRINTING CO., LTD (DNP/Japan),

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

DAI NIPPON PRINTING EUROPE (DPE/Italy),

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

The product can be packaged (micromodule or other case) :

STMicroelectronics SA (Bouskoura/Morocco),

101, boulevard des Muriers BP 97,
20180, Bouskoura – Casablanca,
Morocco.

SMARTFLEX TECHNOLOGIES (Singapore),

No 27, UBI rd 4, MSL building #04-04,
408618 Singapore,
Singapore.

NEDCARD BV (Pays-bas),

Bijsterhuizen 25-29,
6604 LM Wijchen,
Netherlands.

NEDCARD uses **DISCO** for wafer sawing:

DISCO HI-Tec Europe GmbH (Germany),
Liebigstasse 8,
D-85551Kirchheim bei Munchen,
Germany.

For the evaluation, the evaluator considered the user application (embedded in the microcontroller) developer as product user (there is no "administrator" role as defined in the product).

The product itself has a life cycle management, taking the form of two configurations:

- "Test" configuration: at the end of its manufacturing, the microcontroller is tested using the test software in this ROM; the pre-personalization data can be loaded in the EEPROM; this configuration is then blocked irreversibly at switchover to the "User" configuration;
- "User" Configuration: this mode, activated at the end of phase 3, has three sub-modes:
  - mode "Reduced test": enables STMicroelectronics to perform some tests;
  - mode "Diagnosis": subset of "Reduced test", STMicroelectronics reserved;
  - mode "End user": the microcontroller operates under the control of the embedded software of the smart card, the test software is no longer accessible, end users can use the microcontroller in this configuration.

1.2.5. Evaluated configuration

The certificate covers the TOE defined above in section "1.2.3 Architecture" and configured for "User". The characteristics of this TOE are:

Product Name	NVM EEPROM size	I/O Modes	Maskset	Maskset version External/Internal	OST name	OST version
ST23ZR08A	8 Kbytes	Dual	K340	A/H	YBC	61h
ST23ZR04A	4 Kbytes	Dual	K340	A/H	YBC	61h
ST23ZR02A	2 Kbytes	Dual	K340	A/H	YBC	61h
ST23ZC08A	8 Kbytes	Contactless	K340	A/H	YBC	61h
ST23ZC04A	4 Kbytes	Contactless	K340	A/H	YBC	61h
ST23ZC02A	2 Kbytes	Contactless	K340	A/H	YBC	61h

For evaluation purposes, the TOE samples delivered to the evaluator embedded the ROM operating system called "Card Manager", identified by the trigram UZI, and whose purpose was to enable:

- interaction with the TOE through orders passed through the I/O;
- loading test applications in EEPROM or RAM.

This "Card Manager" is not included within the scope of the evaluation.

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1 revision 3** [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. Thus, the AVA_VAN level was determined by respecting the rating scale guide [CC AP]. For the record, this rating scale is more demanding than the default one in the standard method [CC], used for other categories of products (e.g. software).

2.2. Evaluation work

This evaluation is partially based on previous evaluation results of « Microcontroller ST23YS01A » previously certified by ANSSI (see [ANSSI-CC-2011_69]).

The evaluation technical report [ETR], delivered to ANSSI on the 6th of June 2012, describes the work performed by the evaluation facility, and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis

The assessment of cryptographic mechanisms according to ANSSI technical reference frame [REF-CRY] has not been done. Nevertheless, the evaluation did not reveal any vulnerability in design nor implementation for the targeted AVA_VAN level.

2.4. Random number generator analysis

The hardware random number generator has been evaluated according to the [AIS31] methodology by the evaluation facility: it reaches the level “P2 – SOF-high”.

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 Microcontrollers ST23ZR08A/ST23ZR04A/ST23ZR02A, ST23ZC08A/ST23ZC04A/ST23ZC02A", external rev A, internal rev H, with OST dedicated test software YBC version 61, and maskset K340, submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL5 augmented with ALC_DVS.2 and AVA_VAN.5 components.

3.2. Restrictions

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

This certificate provides a resistance assessment of the "Secure Microcontrollers ST23ZR08A/ST23ZR04A/ST23ZR02A, ST23ZC08A/ST23ZC04A/ST23ZC02A" 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 listed in Chapter 2.

The user of the certified product shall respect the security objectives for the operational environment, as specified in the security target [ST], 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 released in accordance with the provisions of the SOG-IS agreement [SOG-IS].

The European Recognition Agreement made by SOG-IS in 2010 allows recognition from Signatory States of the agreement[1], of ITSEC and Common Criteria certificates. The European recognition is applicable, for smart cards and similar devices, up to ITSEC E6 High and CC EAL7 levels. The certificates that are 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 countries[2], 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 SOG-IS agreement are: Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and United Kingdom.

2 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 semi-formal 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 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	1	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
	ALC_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 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	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: - ST23ZR08A, ST23ZR04A, ST23ZR02A, ST23ZC08A, ST23ZC04A, ST23ZC02A, Security Target, reference SMD_ST23Zxxx_ST_10_001_V02.02, version 02.02, STMicroelectronics. For the needs of publication, the following security target has been provided and validated in the evaluation: - ST23ZR08A, ST23ZR04A, ST23ZR02A, ST23ZC08A, ST23ZC04A, ST23ZC02A, Security Target – Public Version, reference SMD_ST23ZRCxxx_ST_11_001_V01.01, version 01.01, STMicroelectronics.
[ETR]	Evaluation technical report : - Evaluation technical report - Project: COGNAC_R, reference CGR_ETR, version: 1.0, THALES-CEACI. For the needs of composite evaluation with this microcontroller a technical report for composition has been validated: - Evaluation technical report lite - Project: COGNAC_R, reference CGR_ETR Lite, version: 1.0, THALES (TCS-CNES).
[CONF]	Products configuration list: - ST23ZR08 Configuration List, reference SMD_ST23ZRxx_CFGL_12_001, version 2.0, STMicroelectronics. Product documentation list for the evaluation: - Cognac-R - ST23ZR08 - CC Evaluation Documentation Report, reference SMD_ST23Zxxx_DR_11_001, version 1.00, STMicroelectronics.
[GUIDES]	The product user guidance documentation is the following: - ST23ZRxx/ST23ZCxx Secure microcontroller with enhanced security with up to 8 Kbyte EEPROM and dual or contactless-only interface - Preliminary Datasheet, reference DS_23ZR08, version 2.0, STMicroelectronics. - Programming Manual ST21/23 Smartcard MCU, reference PM_21_23, version 3.0, STMicroelectronics. Application Note - ST23ZRxx/ST23ZCxx Recommendations for Contactless Operations, reference AN_23Zx_RF_RCMD, version 1.0, STMicroelectronics.

	- How to identify certified hardware devices using additional ST traceability information. reference AN_TRACE, version 1.0, STMicroelectronics. - ST23 AIS 31: Compliant Random Number – User Manual, reference UM_23_AIS31, v2.0 STMicroelectronics. - ST23 AIS 31: Reference Implementation - StartUp, Online and Total Failure Tests, reference AN_23_AIS31, v2.0 STMicroelectronics. - Application Note ST23ZRxx/ST23ZCxx Security guidance, reference AN_23ZRxx_SECU, v2.0 STMicroelectronics.
[ANSSI-CC-2011_69]	ANSSI certificate issued on 31th January2012 for « Microcontroller ST23YS01A ».
[BSI-PP-0035-2007]	Protection Profile, Security IC Platform Protection Profile Version 1.0 June 2007. *Certified by the BSI (Bundesamt für Sicherheit in der Informationstechnik), reference BSI-PP-0035-2007.*

Annex 3. Certification references

Decree number 2002-535, 18th 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 January 2010, Management Committee.
[AIS 31]	Functionnality classes and evaluation methodology for physical random number generator, AIS31 version 1, 25 September 2001, BSI (Bundesamt für Sicherheit in der Informationstechnik).