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-2012/18

Java Card Virtual Machine of LinqUs USIM 128k platform on SC33F640E

Paris, 30th April 2012

Courtesy Translation

SÉCURITÉ CERTIFICATION

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

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

Certification report reference

ANSSI-CC-2012/18

TOE name

Java Card Virtual Machine of LinqUs USIM 128k platform on SC33F640E

Product's reference/ version

T1017287 / Release A

TOE's reference/ version

S1092122/ Release A

Conformité à un profil de protection

none

Evaluation criteria and version

Common Criteria version 3.1 revision 3

Evaluation level

EAL 4 augmented

ADV_FSP.6, ADV_IMP.2, ADV_INT.3, ADV_SPM.1, ADV_TDS.6, ALC_DVS.2, AVA_VAN.5

Developer

Gemalto

La Vigie, Av du Jujubier, ZI Athelia IV, 13705 La Ciotat Cedex, France

Sponsor

Gemalto

La Vigie, Av du Jujubier, ZI Athelia IV, 13705 La Ciotat Cedex, France

Evaluation facility

THALES - CEACI (T3S – CNES)

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

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, 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 “LinqUs USIM 128k platform on SC33F640E, reference T1017287, release A” developed by Gemalto and STMicroelectronics. This product has been already certified under the reference ANSSI-CC_2011/17 [2011/17].

This time, the evaluation scope corresponds to the “Java Card Virtual Machine of LinqUs USIM 128k platform on SC33F640E, reference S1092122, Release A” developed by Gemalto.

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operational environment.

1.2.1. Product identification

The configuration list [CONF] identifies the LinqUs USIM) 128k platform constituent elements, including its Java Card System.

The certified version of the product can be identified by several means describe in the delivery sheet [DS].

- the response to the GetData command (0x00 0xCA 0x9F 0x7F) corresponds to the following CPLC[1] information:

IC Fabricator	0x47 0x50 (ST)
ICType	0x00 0x25 (SC33F640)
osId	0x00 0x27 (STM027)
osDate	0x03 0x40 (YDDD)
osVersion	0x01 0x0C

[1] Card manager Production Life Cycle.

- the response to the GlobalPlatform GetData command (0x00 0xCA 0x00 0x66) of the card manager gives the Card Recognition Data:

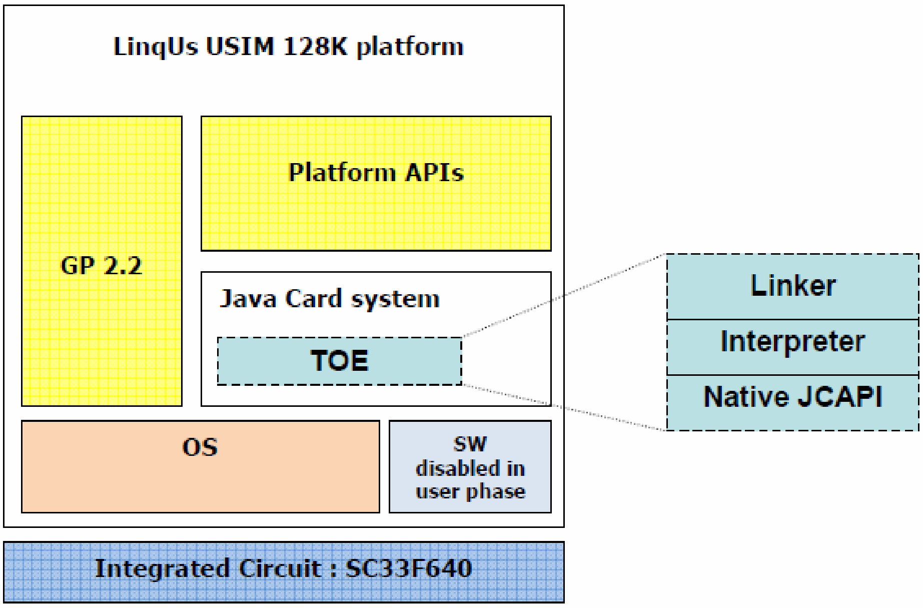
Complete label of the product	1.23.1.18
Software label	1.23.1.12
Card Recognition Data	007066666473620607 2A864886FC6B01600B06092A864886FC6B02 0202630906072A864886FC6B03640B06092A864886FC6B04800064 0B06092A864886FC6B04**0255**650A06082A864886FC6B050466190 60A2B060104012A026E0102060B47544F46363430**0117010C** SCP[1] : 0x02, 0x 55 Software label: 0x01, 0x17, 0x01, 0x0C

1.2.2. Architecture

The product is composed of the following components:

- the microcontroller SC33F640 revision E;
- an operating system;
- a Java Card System which manages and executes applications called applets. It also provides APIs to develop applets on top of it, in accordance with the Java Card specifications;
- GlobalPlatform (GP) packages (partially evaluated), which provides an interface to communicate with the smart card and manage applications in a secure way;
- platform APIs, which provides ways to specifically interact with (U)SIM applications;
- telecom environment including network authentication applications (not evaluated) and Telecom communication protocol.

The following figure describes the product and identifies the TOE:


LinqUs USIM 128K platform
GP 2.2
Platform APIs
Java Card system
TOE
OS
SW disabled in user phase
Integrated Circuit : SC33F640
Linker
Interpreter
Native JCAPI

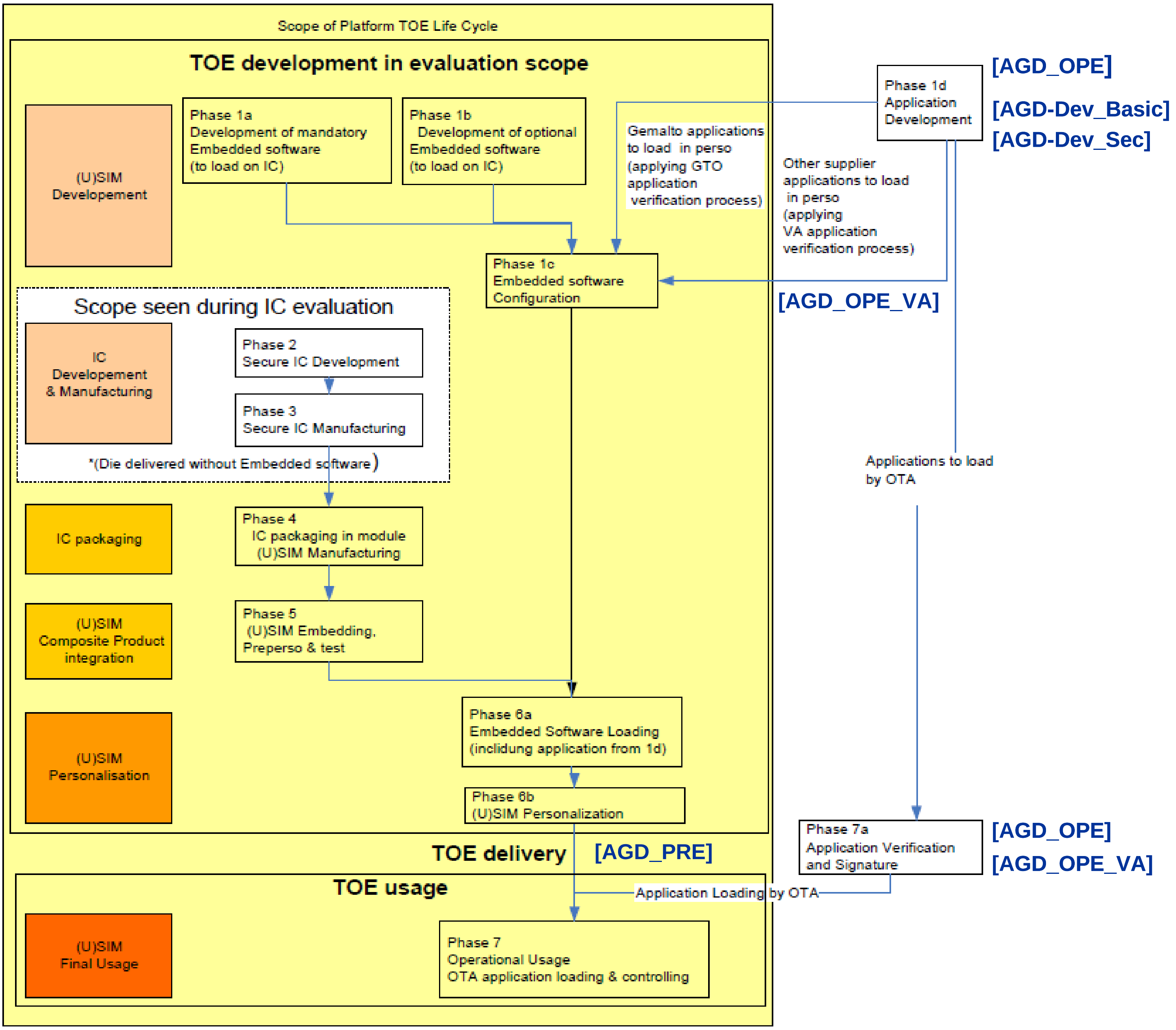
[1] Secure Channel Protocol.

1.2.3. Security services

The TOE ensures mainly the secure execution of an applet that has been byte code verified and loaded on the product.
The others evaluated security services are described in chapter 6.1 of the security target [ST].

1.2.4. Life cycle

The product’s life cycle is organised as follow:


Scope of Platform TOE Life Cycle
TOE development in evaluation scope
(U)SIM Developement
Phase 1a Development of mandatory Embedded software (to load on IC)
Phase 1b Development of optional Embedded software (to load on IC)
Gemalto applications to load in perso (applying GTO application verification process)
Phase 1d Application Development
[AGD_OPE]
[AGD-Dev_Basic]
[AGD-Dev_Sec]
Other supplier applications to load in perso (applying VA application verification process)
Phase 1c Embedded software Configuration
[AGD_OPE_VA]
Scope seen during IC evaluation
IC Developement & Manufacturing
Phase 2 Secure IC Development
Phase 3 Secure IC Manufacturing
*(Die delivered without Embedded software)
Applications to load by OTA
IC packaging
Phase 4 IC packaging in module (U)SIM Manufacturing
(U)SIM Composite Product integration
Phase 5 (U)SIM Embedding, Preperso & test
(U)SIM Personalisation
Phase 6a Embedded Software Loading (inclidung application from 1d)
Phase 6b (U)SIM Personalization
Phase 7a Application Verification and Signature
[AGD_OPE]
[AGD_OPE_VA]
TOE delivery
[AGD_PRE]
TOE usage
Application Loading by OTA
(U)SIM Final Usage
Phase 7 Operational Usage OTA application loading &amp; controlling

The formal model development has been performed on the following site:

Trusted Labs

5, rue du Baillage
78000 Versailles
France

The other development sites of this product, as well as the description of the different evaluated guidance, are identified in the certification report [2011/17].

1.2.5. Evaluated configuration

The open configuration of the product has been evaluated according to [NOTE.10]: this product corresponds to an open and isolating platform. As a consequence new applications that respect the constraints stated in chapter 3.2 and are loaded according to the audited process do not impact the current certification report.

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1 revision 3** [CC], 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 “LinqUs USIM 128k platform on SC33F640E, release A” product certified the 17th June 2011 under the reference ANSSI-CC-2011/17 [2011_17].

This evaluation was a new evaluation of the Java Card System of the already certified product against the higher CC requirements of the ADV class: the ADV components used here are those of the EAL7 level, which require formal methods. Most of the former evaluation results of the others assurance requirements had been reused.

The evaluation technical report [ETR], delivered to ANSSI the 2nd April 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 robustness of cryptographic mechanisms hasn’t been analysed. Nevertheless the evaluation hasn’t lead to the identification of design or construction vulnerabilities for the targeted AVA_VAN level.

2.4. Random number generator analysis

The Random number generator has been analysed during the previous evaluation (see [2011/17]). It hasn’t lead to the identification of design or construction vulnerabilities for the targeted AVA_VAN level if the guidance [AGD-Dev_Sec] is correctly applied.

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 “Java Card Virtual Machine of LinqUs USIM 128k platform on SC33F640E E, reference S1092122, release A” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 4 augmented.

3.2. Restrictions

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

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], in particular:

- applications developers must follow the guidance for basic applications development [AGD-Dev_Basic] or the guidance for secure applications development [AGD-Dev_Sec] depending of the sensibility of the targeted application;
- the Verification Authority must follow the guidance for verification authority [AGD-OPE_VA].

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:

INFORMATION TECHNOLOGY SECURITY
SOGIS
IT SECURITY CERTIFIED
MUTUAL RECOGNITION AGREEMENT

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 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	6	Complete semi-formal functional specification with additional formal specification
	ADV_IMP				1	1	2	2	2	Complete mapping of the implementation representation of the TSF
	ADV_INT					2	3	3	3	Minimally complex internals
	ADV_SPM						1	1	1	Formal TOE security policy model
	ADV_TDS		1	2	3	4	5	6	6	Complete semiformal modular design with formal high-level design presentatio
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	4	Problem tracking 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_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	1	3	3	4	1	Testing: basic 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: - "Security Target - Formal assurances on the Java Card Virtual Machine of LinqUs USIM 128k PK certified using SC33F640", reference D1185035, release 1.5. For the needs of publication, the following security target has been provided and validated in the evaluation: - "Security Target - Formal assurances on the Java Card Virtual Machine of LinqUs USIM 128k PK certified using SC33F640", reference D1185035, release 1.5p.
[ETR]	Evaluation technical report : - "Evaluation technical report - Project: LIOUQUET2 extended", reference LIE_ETR, revision 2.0.
[CONF]	- Delivery Sheet [DS], reference D1189308; - TOE software configuration list: "TOE file configuration list", reference listeFichiersPhenix_1_23_1_18 ; - Documentation configuration list: "Documentation configuration list rev 2", reference Action_List_LIOUQUET2, version 27052011; - Product pre-issuance packages [App_list]: "STM027 : Linqus USIM 128k PK Certified" , reference Gemalto_STM027_profile description_vA6, release A6.
[GUIDES]	Preparative guidance : - Acceptance and installation guidance [AGD-PRE] : "Preparative Guidance for LinqUs USIM 128K PK certified", reference D1185540, release 1.3 Operational guidance: - Administration guidance [AGD-OPE] : "Guidance for Administration of LinqUs USIM 128K PK certified", reference D1185542, release 1.3 - Guidance for application development • Guidance for basic application development [AGD-Dev_Basic]: "Rules for applications on Upteq mNFC certified product", reference D1186227, release A03 • Guidance for secure application development [AGD-Dev_Sec]: "Guidance for secure application development on Upteq mNFC platforms", reference D1188231, release A04 - Guidance for Verification Authority [AGD-OPE_VA]: "Guidance for Verification Authority of LinqUs USIM 128K PK" reference D1185542_VA, release 1.3
[2011/17]	LinqUs USIM 128k platform on SC33F640E *Certified by ANSSI under the reference ANSSI-CC- 2011/17*

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.
[NOTE.10]	« Application note - Certification of applications on “open and cloisonning platform” », reference ANSSI-CC-NOTE/10.0EN, see www.ssi.gouv.fr
[REF-CRY]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 du 26 janvier 2010, voir www.ssi.gouv.fr
[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, 8th January 2010, Management Committee.