PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2008/37

LINQUS USIM 128K Smartcard: ESIGN PKI signature application loaded on GemXplore Generations G152B-EP3B platform embedded on SLE88CFX4002P/m8834b17

Paris, 3 October 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

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

Certification report reference

DCSSI-2008/37

Product name

LINQUS USIM 128K Smartcard: ESIGN PKI signature application loaded on GemXplore Generations G152B-EP3B platform embedded on SLE88CFX4002P/m8834b17

Product reference

T1004530 A3 / Version 1.0

Protection profile conformity

none

Evaluation criteria and version

Common Criteria version 2.3
compliant with ISO 15408:2005

Evaluation level

EAL 4 augmented

AVA_MSU.3, AVA_VLA.4

Developers

GEMALTO

6 rue de la verrerie, 92197 Meudon, France

Infineon Technologies AG

Automotive, Industrial & Multimarket, Chipcard & Security IC´s, Am Campeon 1-12, 85579 Neubiberg, Germany

Sponsor

GEMALTO

6 rue de la verrerie, 92197 Meudon, France

Evaluation facility

CEACI (Thales Security Systems – CNES)

18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France

Phone: +33 (0)5 61 28 16 51, email : ceaci@cnes.fr

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 « LINQUS USIM 128K Smartcard: ESIGN PKI signature application loaded on GemXplore Generations G152B-EP3B platform embedded on SLE88CFX4002P/m8834b17**,** version 1.0 » developed by GEMALTO and Infineon Technologies AG.
The product is a smart card inserted in a mobile phone (e.g. SIM card), it is designed to be used as a secure signature-creation device (SSCD) of type 3.

1.2. Evaluated product description

The security target [ST] defines the evaluated product, its evaluated security functionalities and its operational environment.
The security target is based on [PP0006].

Regarding [PP0006] document:

- The Certification Generation Application (CGA) is implemented by the operator who manages the Wireless Public Key Infrastructure (WPKI) platform. This application is in charge of final verification of Signatory identity and of authenticity of Signature Verification Data (SVD) generated and sent by the product;
- The Signature Creation Application (SCA) is implemented by a set merchant site-operator in charge of performing the presentation of the DTBS to the signatory using a SMS;
- The administrator is the operator in charge of the WPKI platform (note that the activation of the PKI functionalities of the evaluated product is triggered by WPKI platform centrally;
- The signatory is the user of the Mobile who records to the signature service offered by the operator.

1.2.1. Product identification

The configuration list [CONF] identifies the product's constituent elements.

The procedure to obtain the reference of the TOE is described in [TOE_ID]. It consists in two stages:

- Firstly, the label has to be retrieved by reading the customer ID and personalisation program fields of the identity table, using the GetData command with tag 0046;
- Secondly, GEMALTO support team has to be called so that it can provide the TOE reference corresponding to the TOE label specified.

1.2.2. Security services

The product mainly includes the following components:

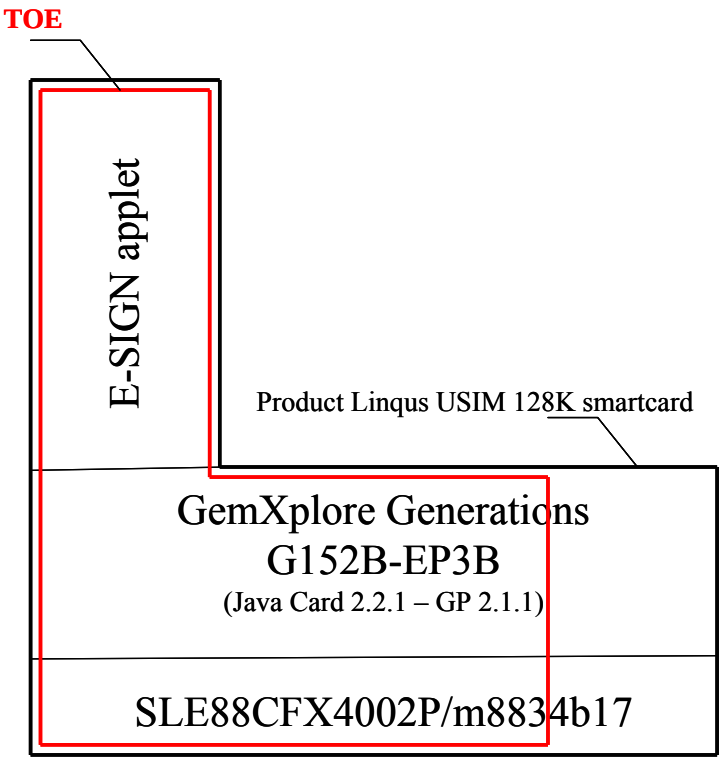
- The GemXplore Generations JavaCard Platform which provides mainly the following security services :
  - Initialization of the GP card Manager and management of the GP Card Life Cycle;
  - Secure installation of the application under Card Manager control during initialization phase;
  - Secure Messaging services during Applet personalization;
  - Card basic security services as:
    - Environmental operating conditions check through information provided by the IC;
    - Life Cycle consistency check;
    - Integrity and confidentiality of Keys and PIN stored for the applet;
    - Secure data object handling and backup mechanisms;
    - Memory content management;
    - Mechanisms to prohibit other applets to interfere with E-SIGN applet;

- The ESIGN Applet which mainly provides the following security services:
  - The generation of SCD/SVD pairs on-board;
  - The generation of electronic signatures.

1.2.3. Architecture

The product is composed of:

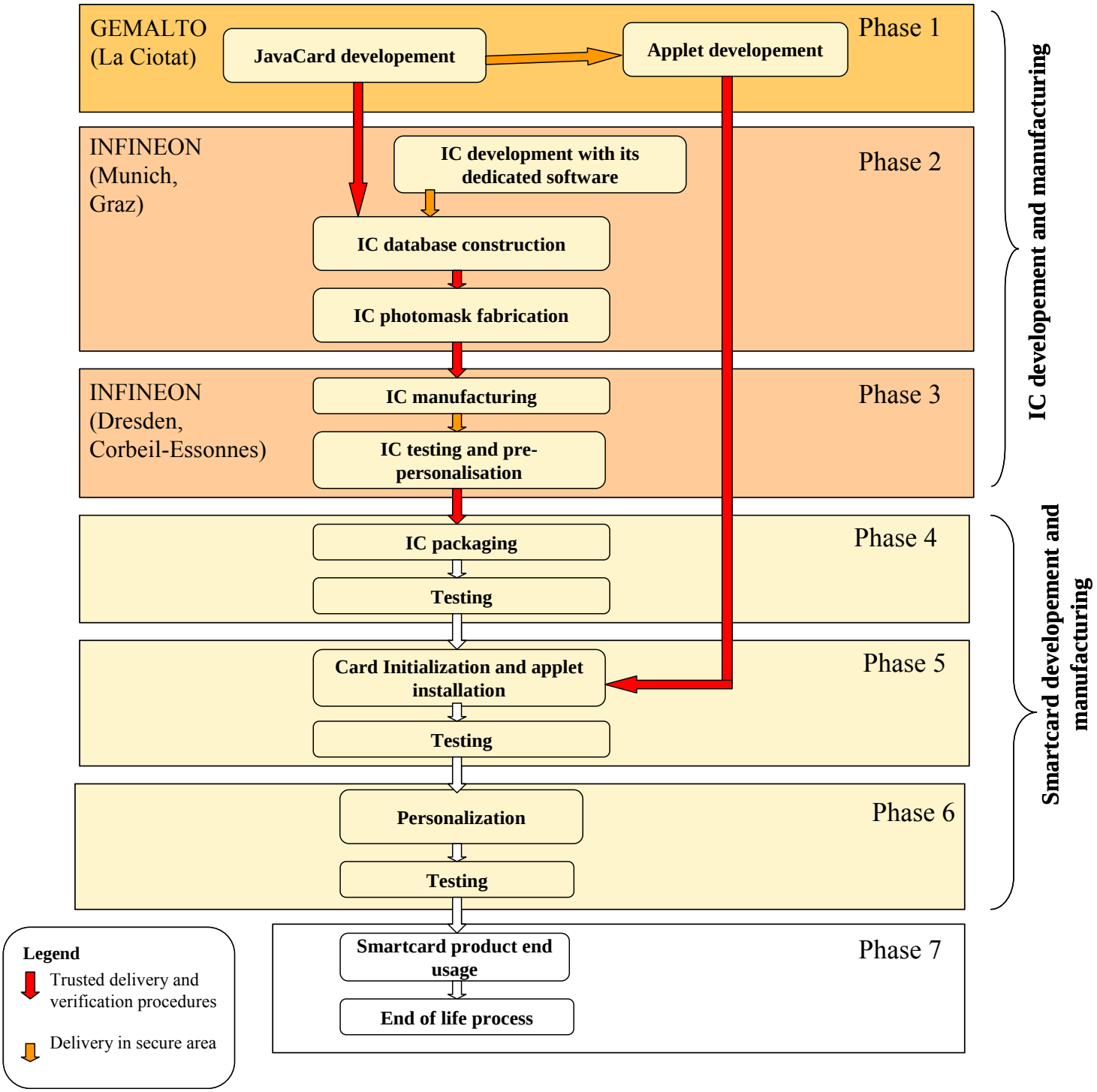
- the microcontroller SLE88CFX4002P/m8834b17 developed and produced by Infineon Technologies AG;
- the JavaCard Operating System, GemXplore Generations G152B-EP3B (label GXG_1_2_2_1_EP3B_ICT_01_G152), developed by GEMALTO, embedded on the ROM's microcontroller;
- the SSCD Application ESIGN (label pki_plugins_dev_09), developed by GEMALTO which is loaded on the card initialization phase.



The TOE is the Digital Signature Application E-SIGN, together with the functions/services provided by the GXG JavaCard OS and the IC required to support the applet functionalities. The evaluation facility verified that the product functionalities which do not enforce the security services don't interfere on those.

1.2.4. Life cycle

The product's life cycle is organised as follow:



The platform and the application have been developed on the following site:

Gemalto - La Vigie,

Avenue du Jujubier, Z.I. Athélia IV,
BP 90,
13702 La Ciotat Cedex,
France

The microcontroller, certified by BSI, is developed and manufactured by Infineon Technologies AG.

In the evaluation context, the card issuer has been considered as “product administrator” and “product user”, the end user has also been considered as “product user”.

1.2.5. Evaluated configuration

At the end of phase 6, the card is personalized and closed. In other words, the loading or deletion of applet is no longer available after personalization phase.

The product tested by the evaluation facility is typical to the final product (phase 7).

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC], with the Common Evaluation Methodology [CEM].
For assurance components above EAL4 level, the evaluation facility own evaluation methods consistent with [AIS 34], 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 has been performed according to the composition scheme as defined in the guide [COMP] in order to assess that no weakness is introduced from the integration of the software in the microcontroller already certified.
Therefore, the results of the evaluation of the microcontroller "SLE88CFX4002P/m8834b17" at EAL5 level augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with the [PP0002] protection profile, have been used. This microcontroller has been certified the 21th june 2006 under the reference BSI-DSZ-CC-0376-2006.
The microcontroller robustness level has been confirmed the 24th August 2007 in a surveillance process.

The evaluation technical report [ETR], delivered to DCSSI the 16th October 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.

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 product "LINQUS USIM 128K Smartcard: ESIGN PKI signature application loaded on GemXplore Generations G152B-EP3B platform embedded on SLE88CFX4002P/m8834b17, version 1.0" 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 operational environmental security objectives summarized specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular :

- the generation of qualified certificates (OE.CGA_Qcert);
- the authenticity check of the SVD by the CGA (OE.SVD_Auth_CGA);
- the protection of the verification authentication data –VAD- (OE.HI_VAD);
- the management of the data to be signed (OE.SCA_Data_Intend);
- the implementation of the IC management recommendations (OE.IC_Usage_and_Protection).

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 4+	Name of the component
ACM Configuration management	ACM_AUT				**1**	1	**2**	2	**1**	Partial CM automation
	ACM_CAP	**1**	**2**	**3**	**4**	4	**5**	5	**4**	Configuration support and acceptance procedures
	ACM_SCP			**1**	**2**	**3**	3	3	**2**	Problem tracking CM coverage
ADO Delivery and operation	ADO_DEL		**1**	1	**2**	2	2	**3**	**2**	Detection of modification
	ADO_IGS	**1**	1	1	1	1	1	1	**1**	Installation, generation and start-up procedures
ADV Development	ADV_FSP	**1**	1	1	**2**	**3**	3	**4**	**2**	Fully defined external interfaces
	ADV_HLD		**1**	**2**	2	**3**	**4**	**5**	**2**	Security enforcing high-level design
	ADV_IMP				**1**	**2**	**3**	3	**1**	Subset of the implementation of the TSF
	ADV_INT					**1**	**2**	**3**		
	ADV_LLD				**1**	1	**2**	2	**1**	Descriptive low-level design
	ADV_RCR	**1**	1	1	1	**2**	2	**3**	**1**	Informal correspondence demonstration
	ADV_SPM				**1**	**3**	3	3	**1**	Informal TOE security policy model
AGD Guidance	AGD_ADM	**1**	1	1	1	1	1	1	**1**	Administrator guidance
	AGD_USR	**1**	1	1	1	1	1	1	**1**	User guidance
ALC Life-cycle support	ALC_DVS			**1**	1	1	**2**	2	**1**	Identification of security measures
	ALC_FLR									
	ALC_LCD				**1**	**2**	2	**3**	**1**	Developer defined life-cycle model
	ALC_TAT				**1**	**2**	**3**	3	**1**	Well-defined development tools
ATE Tests	ATE_COV		**1**	**2**	2	2	**3**	3	**2**	Analysis of coverage
	ATE_DPT			**1**	1	**2**	2	**3**	**1**	Testing: high-level 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_CCA					**1**	**2**	2		
	AVA_MSU			**1**	**2**	2	**3**	3	**3**	Analysis and testing for insecure states
	AVA_SOF		**1**	1	1	1	1	1	**1**	Strength of TOE security function evaluation
	AVA_VLA		**1**	1	**2**	**3**	**4**	4	**4**	Highly resistant

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: - "ASE – Security Target ; TOE: ESIGN PKI signature application on GemXplore Generations G152B-EP3B OS platform, running on Infineon SLE88CFX4002P/m8834b17 chip; Ref T1004530 A3 / Version 1.0; Product: Linqus USIM 128K smartcard ; Based on SSCD Type 3", reference ASE10448, version 1.4 For the needs of publication, the following security target has been provided and validated in the evaluation: - "LINQUS USIM 128K Smartcard; ESIGN PKI Signature Application On GemXplore Generations G152B-EP3B OS platform, Running on Infineon SLE88CFX4002P/m8834b17 chip Security Target" – Public version, reference ASE10448_Public, version 1.0
[ETR]	Evaluation technical report : - « Evaluation Technical Report- Project: BOSPHORE », reference BOS_ETR, version 2.0
[CONF]	"Bosphore project - List of evaluation documentation", reference BOS_DOC_10448, version 1.5
[TOE_ID]	« Bosphore Project -TOE identification », reference TOE_ID_10448, version 0.6
[GUIDES]	Installation guidance: - "Dev Configuration Check - GXGenerations platforms-TURKCELL porting on GXG1.2", reference E6K009_001_CFG, version A03 - "Delivery & Operation ; TOE - GXG-ESIGN; Product - G152-ESIGN", reference ADO10448, version 0.3 - "Card Initialization Specification For Garlaban V1.2 on Infineon SLE88 chip family", reference CIS02R10527A, version A04 - "Card Personalization Specification - Master Part For Garlaban V1.2 - Core volume", reference CPS01R10527A, version A12 - "Memory Replication Specification For Garlaban V1.2 on Infineon SLE88 chip family", reference MRS02R10527A, version A01 - "Card Personalization Specification - Daughter Part For Flexible V1.2 - Core volume", reference CPS02R10527A, version A16 Administration and user guidance: - "GemXplore Generations Java Card and GlobalPlatform Environment", reference DOC113342B, version2.0 - "GemXplore Generation CAT features", reference DOC113397A, version1.0 - "GemXplore Generations OTA remote management - Reference

	Manual", reference DOC113356A, version1.0 - "GemXplore Generations 3G and GSM Operation Modes-Reference Manual", reference DOC113364C, version3 .0 - "Card Issuer and End-User Guidance; TOE – GXG-ESIGN; Product – G152-ESIGN; Based on SSCD Type 3", reference SEC_REC_10448, version 0.3
[PP0006]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. *Certified by BSI(Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0006-2002T.*
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0002-2001.*

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, August 2005, version 2.3, ref CCMB-2005-08-001; Part 2: Security functional requirements, August 2005, version 2.3, ref CCMB-2005-08-002; Part 3: Security assurance requirements, August 2005, version 2.3, ref CCMB-2005-08-003. The content of Common Criteria version 2.3 is identical to the international ISO/IEC 15408:2005.
[CEM]	Common Methodology for Information Technology Security Evaluation: Evaluation Methodology, August 2005, version 2.3, ref CCMB-2005-08-004. The content of CEM version 2.3 is identical to the international ISO/IEC 18045:2005.
[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.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - Composite product evaluation for smart cards and similar devices, reference CCDB-2007-09-001 version 1.0, revision 1, September 2007.
[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.
[AIS 34]	Application Notes and Interpretation of the Scheme - Evaluation Methodology for CC Assurance Classes for EAL5+, AIS34, Version 1.00, 01 June 2004, Bundesamt für Sicherheit in der Informationstechnik