Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secretariat General for National Defence

Central Directorate for Information Systems Security

Certification Report DCSSI-2007/14

Sony FeliCa Contactless Smart Card IC Chip RC-S960/1

Paris, 28th of June 2007

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 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.pm.gouv.fr

Certification report reference

DCSSI-2007/14

Product name

Sony FeliCa Contactless Smart Card IC Chip RC-S960/1

Product reference

RC-S960/1

Evaluation criteria and version

Common Criteria version 2.3

compliant with ISO 15408:2005

Evaluation level

EAL 4

Developer(s)

Sony Corporation

4-7-35 Kitashinagawa Shinagawa-ku, Tokyo, 140-0001, Japan

Fujitsu

1-1 Kamikodanaka 4_Chome, Nakahara-Ku, Kawasaki 211-8588 Japan

Sponsor

Sony Corporation

4-7-35 Kitashinagawa Shinagawa-ku, Tokyo, 140-0001, Japan

Evaluation facility

CEACI (Thales Security Systems – CNES)

18 avenue Edouard Belin, 31401 Toulouse Cedex 9, France

Phone: +33 (0)5 62 88 28 01, email : ceaci@cnes.fr

Recognition arrangements

CCRA **SOG-IS**

IT Security Certified

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 « Sony FeliCa Contactless Smart Card IC Chip RC-S960/1 » is a contactless smartcard IC-chip developed by Sony Corporation. This product is designed to be used in several fields, in the field of finance for instance.

1.2. Evaluated product description

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

1.2.1. Product identification

The configuration list [CONF] identifies the product's constituting elements.
The certified version of the product can be identified by the following elements:

- Commercial name: IC Chip RC-S960/1
- Software reference : FeliCa OS version 3.31
- Product ROM reference: 0F (with no patch).
- Microcontroller reference : CXD9861/MB94RS402, FR00 001
- Microcontroller dedicated software references:
  - HAL-API version 22.0
  - DRNG Library version 22.0

This information can be verified with the commands described in the guidance (see [GUIDES]).

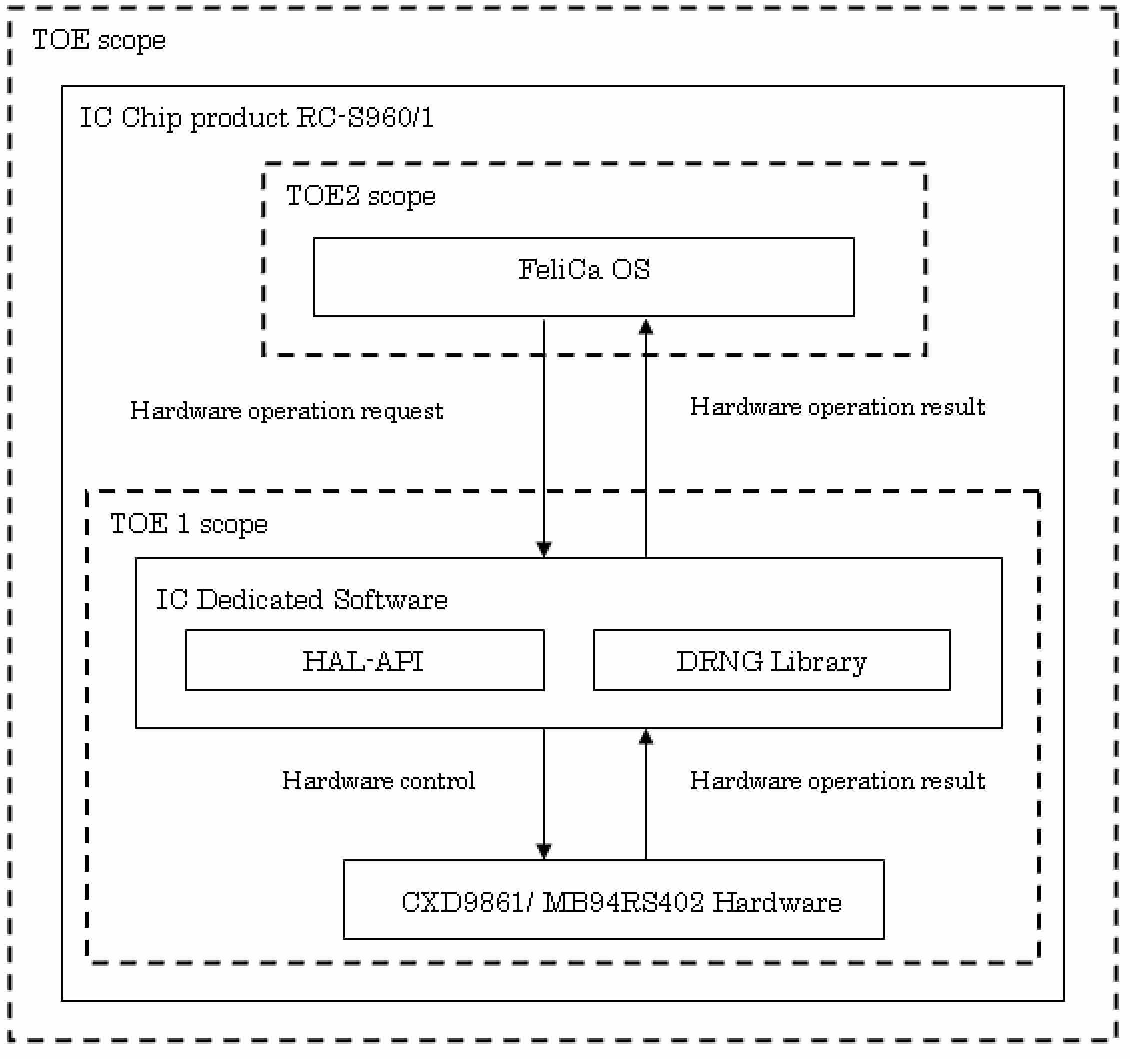
1.2.2. Security services

The product provides mainly the following security services:

- Protection of customer's data from disclosure and modification,
- Communication data flow control between the product and the reader/ writer,
- Creation and management of the file system in FRAM memory,
- File access control for storage, reading, writing and deletion of file in FRAM memory.

1.2.3. Architecture

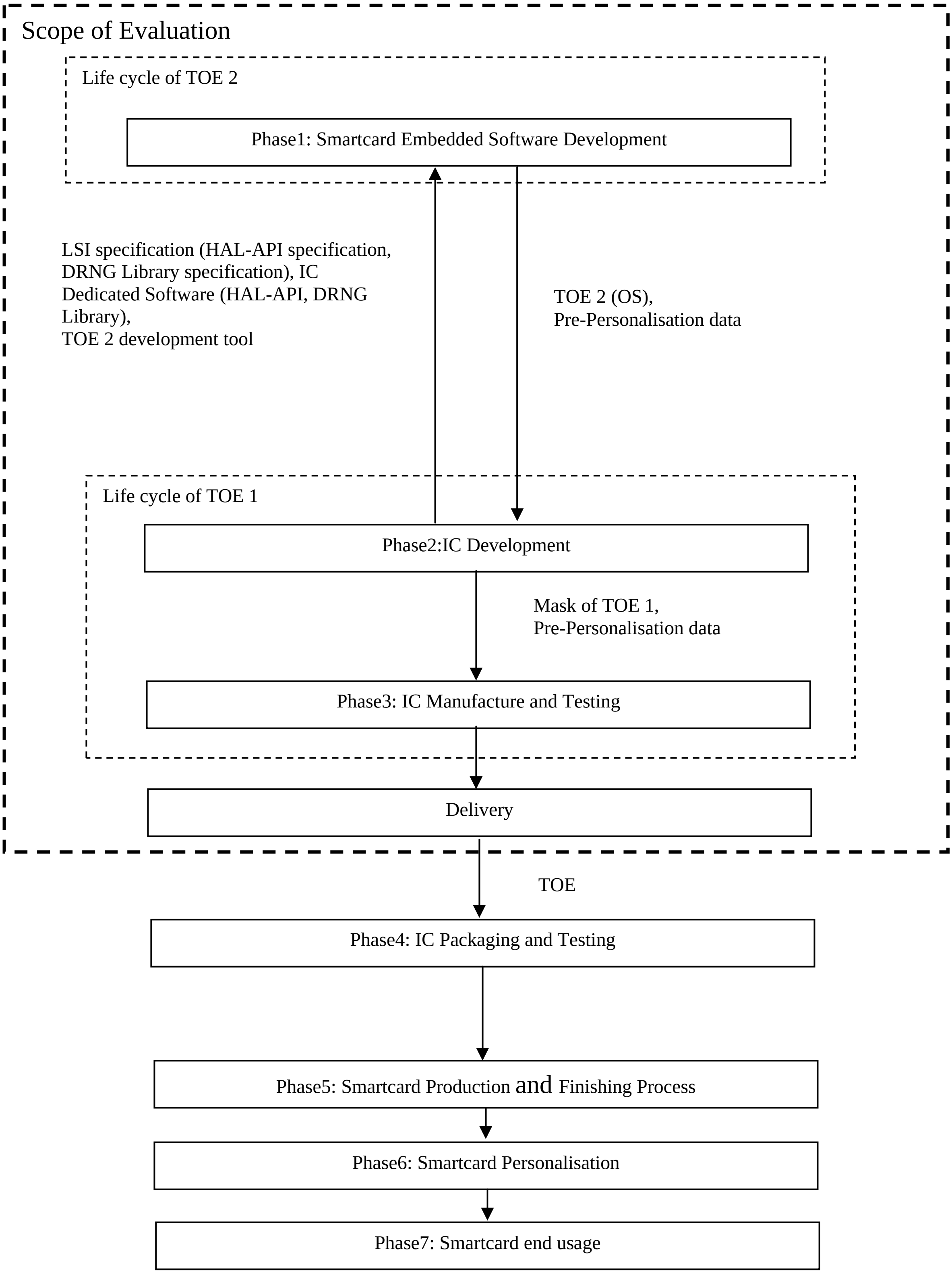
The product consists of a microcontroller and dedicated software on which the operating system FeliCa OS is embedded.
In the charts below the microcontroller and its dedicated software are identified as TOE1 and the operating system as TOE2. The target of the evaluation corresponds to the elements identified as TOE1 and TOE2.


TOE scope
IC Chip product RC-S960/1
TOE2 scope
FeliCa OS
Hardware operation request
Hardware operation result
TOE 1 scope
IC Dedicated Software
HAL-API
DRNG Library
Hardware control
Hardware operation result
CXD9861/ MB94RS402 Hardware

HAL: Hardware Abstraction Layer
DRNG: Deterministic Random Number Generator

1.2.4. Life cycle

The product's life cycle is organised as follow:


Scope of Evaluation
Life cycle of TOE 2
Phase1: Smartcard Embedded Software Development
LSI specification (HAL-API specification, DRNG Library specification), IC Dedicated Software (HAL-API, DRNG Library), TOE 2 development tool
TOE 2 (OS), Pre-Personalisation data
Life cycle of TOE 1
Phase2:IC Development
Mask of TOE 1, Pre-Personalisation data
Phase3: IC Manufacture and Testing
Delivery
TOE
Phase4: IC Packaging and Testing
Phase5: Smartcard Production and Finishing Process
Phase6: Smartcard Personalisation
Phase7: Smartcard end usage

The product has been developed on the following sites:

Sony Gotenyama Garden office

4-7-35 Kitashinagawa Shinagawa-ku,
Tokyo, 140-0001
Japan

Sony Toyosato Plant

130 Koguchimae, Toyosato-cho, Tome-shi,
Miyagi-ken. 987-0362
Japan

In the evaluation context, the IC manufacturer, mask developer and the card manufacturer have been considered as "product administrator" and the card issuer, area administrator and service user have been considered as "product user" as described in [ST].

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 2.3** [CC] and with the Common Evaluation Methodology [CEM].

In order to meet the specificities of smart cards, the [CCAP] guide has 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 Fujitsu microcontroller "CXD9861/ MB94RS402 with HAL-API & DRNG Library" at EAL4 level augmented with ADV_IMP.2, ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with the « Smart card IC Platform Protection Profile » [PP0002]. This microcontroller has been certified the 14th of December, 2006 under the reference 2006/29.

This evaluation has also taken into account the maintenance of the microcontroller in date of the 23rd of April, 2007 under the reference M-2007/03.

The evaluation technical report [ETR], delivered to DCSSI on the 15th of June 2007, 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 identified in chapter 2 and described in the evaluation technical report [ETR], was carried out according to the current rules and standards, with the required competency and impartiality by 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 "Sony FeliCa Contactless Smart Card IC Chip RC-S960/1" submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 4 .

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 ensure the operational environmental security objectives specified in the security target [ST] are met and shall fulfil the recommendations in the guidance [GUIDES], in particular:

- the Remote Trusted IT Product shall provide a trusted channel for secure communication with the TOE ;

- security procedures shall be used after TOE delivery up to delivery to the end-user to maintain confidentiality and integrity of the TOE and of its manufacturing and test data (to prevent any possible copy, modification, retention, theft or unauthorised use of the TOE) (see1.2.4).

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:

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: Finland, France, Germany, Greece, Italy, The Netherlands, Norway, Portugal, Spain, Sweden, Switzerland 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 Netherlands, New-Zealand, Norway, Singapore, Spain, Sweden, Turkey, United Kingdom and United States.

Annex 1. Evaluation level of the product

Classe	Famille	Composants par niveau d'assurance							Niveau d'assurance retenu pour le produit	
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7	EAL 4	Intitulé du composant
ACM Gestion de configuration	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 Livraison et opération	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 Développement	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 Guides d'utilisation	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 Support au cycle de vie	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 Estimation des vulnérabilités	AVA_CCA					1	2	2		
	AVA_MSU			1	2	2	3	3	2	Validation of analysis
	AVA_SOF		1	1	1	1	1	1	1	Strength of TOE security function evaluation
	AVA_VLA		1	1	2	3	4	4	2	Independent vulnerability analysis

Annex 2. Evaluated product references

[ST]	Reference security target for the evaluation: - RC-S960/1 Composite Security Target v1.43 ref. : 960-ST-E01-43 For the needs of publication, the following security target has been provided and validated in the evaluation: - RC-S960/1 Composite Security Target - Public Version ref. :960-STL-E01-43
[ETR]	Evaluation technical report : - Evaluation Technical Report - Project: TYPHON23 ref. : TYP_ETR v5.0 dated 15th June 2007 - Addendum of Evaluation Technical Report Project: TYPHON23 ref. : TYP_ADD_ETR Revision :1.0 dated 26th June 2007
[CONF]	RC-S960 Configuration Management List 1 00 réf. : 960-CML-E01-00 /1.00
[GUIDES]	Delivery guidance: - IC Delivery Rules v1.2 ref. : 960-DEL_IC-E01-20 - Document Delivery Rules v1.0 ref.: 960-DEL_DOC-E01-00 Administration and user guidance: - FeliCa Card IC Security Operation Guidelines v1.0 ref. : M292-E0.1-00 - RC-S960 Series FeliCa OS Command Reference Manual v1.0 ref. : M247-E01-00 - Security Reference Manual Group Service Key & User Service Key Generation v1.0 ref. : SR-030-001E - Security Reference Manual Mutual Authentication & Packet Cryptography v1.0 ref. : SR-030-002E - Security Reference Manual Issuing Package Generation v1.0 ref. : SR-030-003E - Security Reference Manual Changing Key Package Generation v1.0 ref. : SR-030-004E Administration guidance: - RC-S960 Series Manufacture ID Writing Procedure v1.0 ref. : M248-E01-00 - RC-S960 Series Inspection/Verification Procedure v1.0 ref. : M252-E01-00 - FeliCa Card Rewriting Transport key v1.1 ref. : Tec01-E01-10 - RC-S960 Series FeliCa OS Status Flag Reference v 1.0

	réf. : M294-E01-00
[PP0002]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified by BSI 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, version 2.1, April 2006.
[COMP]	Common Criteria Supporting Document - Mandatory Technical Document - ETR-lite for composition, Version 1.3, April 2006.
[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.