



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-2011/05

**Gemalto ECC CPU card
CPU e-purse application
on GCX5.1 (MPH098) platform
on NXP P5CD081V1A
Version 1.0**

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

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

<i>Certification report reference</i> ANSSI-CC-2011/05	
<i>Product name</i> Gemalto ECC CPU card on GCX5.1 (MPH098) platform on NXP P5CD081V1A	
<i>Product reference</i> CPU e-purse on GCX5.1 MPH098 Version 1.0	
<i>Protection profile conformity</i> None	
<i>Evaluation criteria and version</i> Common Criteria version 3.1 revision 3	
<i>Evaluation level</i> EAL 4 augmented ALC_DVS.2, AVA_VAN.5	
<i>Developer(s)</i> Gemalto SA 6 rue de la Verrerie, 92197 Meudon, France	NXP Semiconductors GmbH Stresemannallee 101, D-22502 Hamburg, Germany
<i>Sponsor</i> Gemalto SA 6 rue de la Verrerie, 92197 Meudon, France	
<i>Evaluation facility</i> CEA - LETI 17 rue des martyrs, 38054 Grenoble Cedex 9, France Phone: +33 (0)4 38 78 37 78, email : elisabeth.crochon@cea.fr	
<i>Recognition arrangements</i>   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	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>	8
1.2.5. <i>Evaluated configuration</i>	10
2. THE EVALUATION.....	11
2.1. EVALUATION REFERENTIAL	11
2.2. EVALUATION WORK	11
2.3. CRYPTOGRAPHIC MECHANISMS ROBUSTNESS ANALYSIS.....	11
2.4. RANDOM NUMBER GENERATOR ANALYSIS	11
3. CERTIFICATION.....	12
3.1. CONCLUSION	12
3.2. RESTRICTIONS	12
3.3. RECOGNITION OF THE CERTIFICATE.....	12
3.3.1. <i>European recognition (SOG-IS)</i>	12
3.3.2. <i>International common criteria recognition (CCRA)</i>	13
ANNEX 1. EVALUATION LEVEL OF THE PRODUCT.....	14
ANNEX 2. EVALUATED PRODUCT REFERENCES	15
ANNEX 3. CERTIFICATION REFERENCES	17

1. The product

1.1. Presentation of the product

The evaluated product is the ECC CPU card, CPU e-purse application on GCX5.1 (MPH098) platform, developed by Gemalto SA. The ECC CPU card is the electronic purse (*EP*) device.

The TOE (*Target Of Evaluation*) is a contactless or dual (contact/contactless) smartcard with electronic purse (CPU e-purse) application, on the closed javacard platform (GCX5.1).

The e-purse application is intended for low value off-line payment transactions. Its functionalities are similar to traditional purse functionalities with the distinction that it uses electronic money (*EM*) instead of cash money. The EP objective is to facilitate to Purseholder the payments of low value, in a simple, fast and secure way.

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 elements of the product are identified in the configuration list [CONF].

The certified version of the product is identified by the following:

- Product name: ECC CPU card;
- TOE reference: CPU e-purse on GCX5.1 ;
- TOE version: 1.0 on MPH098 ;
- IC reference: NXP P5CD081 V1A

These informations can be verified by the ATR¹ reading, Traceability data (CPLC²) reading and CPU e-purse Applet identification reading during phase 7.

ATR reading:

3B 6E 00 00	80 31 80 66 B0 84 0C 01 6E 01 83 00 90 00 (T=0 protocol)
3B EE 00 00 81 31 80 42	80 31 80 66 B0 84 0C 01 6E 01 83 00 90 00 xx ³ (T=1 protocol)

Traceability data reading:

ROM CPLC

via GET DATA command with tag 9F7Fh (80 CA 9F 7F)

In response, the card sends 45 bytes.

The 13 first values must be **9F 7F 2A 40 70 51 44 19 81 01 04 01 00** with:

- Requested tag: **9F 7F**,

¹ Answer To Reset

² Card manager Production Life Cycle

³ xx: checksum byte calculated

- Information size: **2A**,
- IC Fabricator: **40 70** (NXP),
- IC Type: **51 44** (P5CD081),
- OS Identifier: **19 81** GEMALTO OS),
- OS Release date: **01 04** (14/04/2010),
- OS Release level: **01 00** (1.00)

Gemalto CPLC

via GET DATA command with tag 0103h (80 CA 01 03)

CPU e-purse Applet identification reading:

Applet version

via GET DATA command with tag DF13h (80 CA DF 13) after applet selection.

In response, the card sends bytes.

The values must be **DF 13 00 10 00 02 81** with:

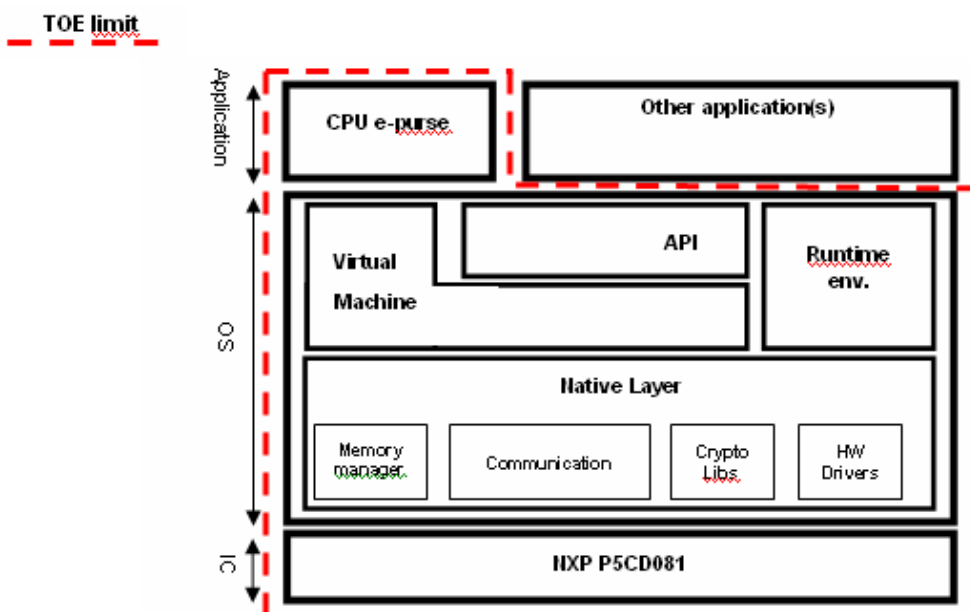
- Requested tag: **DF 13**
- Internal meaning: **00**
- Applet version: **10 00** (1.0.00),
- Applet version day: **02 81** (07/10/2010)

1.2.2. Security services

The product provides mainly the following security services:

- Electronic money (*EM*) protection in term of integrity during **Credit**, **Auto-Load** and **Debit** operations;
- Security assets protection in term of integrity and confidentiality when used or stored;
- Mutual authentication between the TOE and the ECC SAM (*Secure Access Module*) card during **Auto-Load** and **Debit** operations;
- Mutual authentication between the TOE and the Host device during **Credit** operations;
- Invalidation (i.e. de-activation) of the card via **Write Lock** command.

1.2.3. Architecture



The product is composed of:

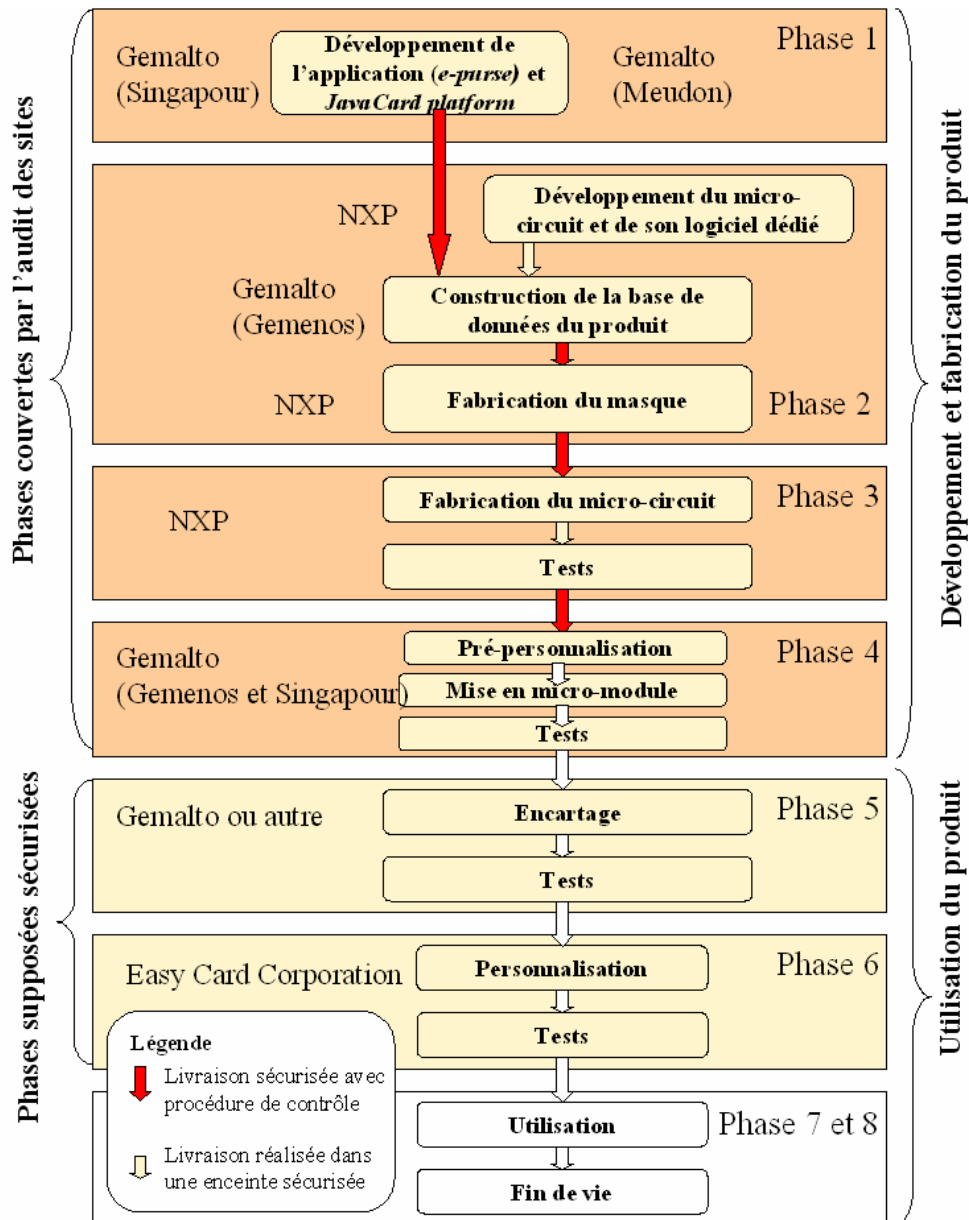
- The CPU e-purse application;
- The GCX5.1 OS composed of:
 - o Javacard platform part composed of:
 - **Runtime environment,**
 - **Virtual machine,**
 - **APIs.**
 - o Native part composed of:
 - Memory management (**Memory manager**),
 - Communication management (**Communication**),
 - Cryptographic libraries management (and the cryptographic libraries itself) (**Crypto libs**),
- The NXP P5CD081 IC

The Other applications¹ on the card are written in java language and are out of scope of the TOE.

1.2.4. Life cycle

The product's life cycle is organised as follow:

¹ Applications: VSDC271, MChipPaypass, DualPSE



Gemalto(La Ciotat) : hébergement des serveurs IT

The product has been developed on the following sites:

GEMALTO Site de Meudon

6 rue de la Verrerie
91197 Meudon Cedex
France

GEMALTO Site de Singapour

12 Ayar Rajah Crescent
139941 Singapore
Singapore

GEMALTO Site de Gemenos

Avenue Pic de Bertagne
13881 Gémenos Cedex
France

NXP Semiconductors GmbH

Stresemannallee 101
D-22502 Hamburg
Germany

The transitions between these development phases lead to the transfer of sensitive data, logical (specification data, source code) or physical (samples during development).

During this evaluation, the security of the delivering process has been evaluated (ALC component) :

- Dedicated software and guide to the Developer (up to the phase 1);
- Embedded software code to the IC manufacturer (between phases 1 and 2);
- Data required to the IC manufacturer (during phase 2);
- Developed masks to the IC manufacturer (between phases 2 and 3);
- Manufactured masks to the Card manufacturer (between phases 3 and 4);

The security of the delivering process are out of the evaluation and hasn't been evaluated:

- Modules to the Card manufacturer (between phases 4 and 5);
- Pre-personalized cards to the Personalizer (between phases 5 and 6);

The security of the delivering process is covered by guides [GUIDES].

1.2.5. Evaluated configuration

The certificate applies to the following configurations given in §1.2.1.

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].

For assurance components which are not covered by [CEM] manual, the evaluation facility own evaluation methods, validated by ANSSI have been used.

In order to meet the specificities of smart cards, the [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 comes from the integration of the software in the microcontroller already certified.

Therefore, the results of the evaluation of the microcontroller “*P5CD081 VIA*” at EAL5 level augmented with ALC_DVS.2, AVA_VAN.5 and ASE_TSS.2, compliant with the [PP] protection profile, have been used. This microcontroller has been certified the 10th November of 2009 under the reference BSI-DSZ-CC-0555-2009.

The microcontroller robustness level has been confirmed the 17th December 2010 in a surveillance process.

The evaluation technical report [ETR], delivered to ANSSI the 22th March of 2011, 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 quotation of the cryptographic mechanisms haven't been analyzed in relation to the ANSSI technical reference frame [REF-CRY], [REF-CLE] and [REF-AUT]. Nevertheless, the evaluations didn't show any building or conception weakness related to the considered AVA_VAN.

2.4. Random number generator analysis

The random generator used by the product is the one proposed by the certified IC [CERTIF_IC].

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 “Gemalto ECC CPU card on GCX5.1 (MPH098) platform on NXP P5CD081V1A”, 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 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 agreement¹, 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:



¹ The signatory countries of the SOG-IS agreement are: Finland, France, Germany, 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 countries¹, 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, 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 Développement	ADV_ARC		1	1	1	1	1	1	1	Security architecture description
	ADV_FSP	1	2	3	4	5	5	6	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	Implementation representation of the TSF
	ADV_INT					2	3	3		
	ADV_SPM						1	1		
	ADV_TDS		1	2	3	4	5	6	3	Basic 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	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_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	2	3	3	4	2	Testing: security enforcing modules
	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	Focused vulnerability analysis

Annex 2. Evaluated product references

[ST]	<p>Security Target for evaluation: <i>Security Target for ECC CPU card, version 2.0, reference ROR20512_CCD_ASE_001, 24th january 2011, GEMALTO.</i> <i>Security Target lite for ECC CPU card, version 1.01, reference ROR20512_CCD_ASE_002, 7th april 2011, GEMALTO.</i></p>
[RTE]	<p>Evaluation Technical Report: <i>Evaluation Technical Report (ETR), version 1.2, reference DRT/LETI/DCIS/CESTI/.FOR.4.044.G, 22th march 2011, CEA LETI.</i></p>
[CONF]	<p>Product configuration list : <i>TOE applet elements configuration, reference Items for applet.zip, 21st december 2010 ; GEMALTO.</i> <i>TOE platform elements configuration, reference Items for GCX5.1.zip, 21st december 2010 ; GEMALTO.</i> <i>TOE cryptolib elements configuration, version 1.1, reference LIB/ALC directory, 11th june 2010. GEMALTO.</i></p>
[CERTIF_IC]	<p>Certification report : - <i>NXP Smart Card Controller P5CD081V1A and its major configurations P5CC081V1A, P5CN081V1A, P5CD041V1A, P5CD021V1A and P5CD016V1A each with IC dedicated Software, reference : BSI-DSZ-CC-0555-2009, 10th november 2009, BSI.</i></p>
[GUIDES]	<p>AGD : <i>Guidance Documents, version 1.0, reference ROR20512_CCD_AGD_006, 22nd december 2010 ;</i> - <i>Personalization Specification – CPU Card, version A18, reference CPU_PS_ECC, 18th october 2010 ;</i> - <i>Pre-Personalization Specification, version A01, reference CPU_PPS_ECC, 29th april 2010 ;</i> - <i>Functional Specification, version A18, reference CPU_FS_ECC, 21st october 2010 ;</i> - <i>FSP : complete fonctionnal specification, version 1.0, reference ROR20512_CCD_ADV_FSP_002, 20th december 2010 ;</i> - <i>Software Requirement Specifications – GCX5.1 platform “EasyCard”, version A06, reference ROR20855_005_SRS_GCX5, 17th september 2010 ;</i></p>



	<p>- <i>Key Management Specification – CPU Card, version A18, reference KMS_ECC, 19th october 2010.</i></p> <p>GEMALTO.</p>
[PP]	<p><i>Security IC Protection Profile, version 1.0, 23 August 2007. Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under BSI-CC-0035-2007 reference.</i></p>

Annex 3. Certification references

Décret 2002-535 du 18 avril 2002 modifié relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information.	
[CER/P/01]	Procédure CER/P/01 Certification de la sécurité offerte par les produits et les systèmes des technologies de l'information, 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 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.
[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 3.0, 8 January 2010, Management Committee.
[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
[REF-KEY]	Gestion des clés cryptographiques – Règles et recommandations concernant la gestion des clés utilisées dans des mécanismes cryptographiques, version 1.10 du 24 octobre 2008, voir www.ssi.gouv.fr
[REF-AUT]	Authentification – Règles et recommandations concernant les mécanismes d'authentification de niveau de robustesse standard, version 1.0 du 13 janvier 2010, voir www.ssi.gouv.fr

