PREMIER MINISTRE

General Secretariat for Defence and National Security

French Network and Information Security Agency

Certification Report ANSSI-CC-2009/56

Multiapp ID IAS ECC Smart card

Paris, 17 February 2010

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-2009/56

Product name

Multiapp ID IAS ECC smart card :

electronic signature application v4.2.7.A loaded on
Multiapp v1.0 Java Card platform with v1.2 soft mask
embedded on NXP P5CD144 VOB

Product reference

Applet version: v4.2.7.A
Multiapp Java Card platform version : v1.0
soft mask version: v1.2
Microcontroller version : V0B

Protection profile conformity

[BSI-PP-0005-2002] : SSCD Type 2, version 1.04
[BSI-PP-0006-2002] : SSCD Type 3, version 1.05

Evaluation criteria and version

Common Criteria version 3.1

Evaluation level

EAL 4 augmented

ALC_DVS.2, AVA_VAN.5

Developer(s)

Gemalto SA[1]
6 rue de la Verrerie
92197 Meudon, France

NXP Semiconductors GmbH[1]
Stresemannallee 101
D-22502 Hamburg, Germany

Sponsor

Gemalto SA
6 rue de la Verrerie, 92197 Meudon, France

Evaluation facility

Serma Technologies

30 avenue Gustave Eiffel, 33608 Pessac, France
Phone: +33 (0)5 57 26 08 75, email : e.francois@serma.com

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 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 Gemalto Multiapp ID IAS ECC smart card product: electronic signature application v4.2.7.A loaded on Multiapp v1.0 Java card platform with v1.2 soft mask embedded on NXP P5CD144 VOB.

The TOE (Target of Evaluation) is dedicated to electronic administration. The TOE is the Secure Signature Creation Device (SSCD) functionalities provided by the IAS ECC (Identification Authentication Signature / European Citizen Card) application, and supported by the Multiapp Java Card platform.

The Gemalto **IAS ECC** application is compliant with E-sign specifications (cf. [E-sign]).

It provides the two main SSCD type 2 and type 3 product services:
- SCD / SVD generation (Signature Creation Data / Signature Verification Data) ;
- Signature creation.

1.2. Evaluated product description

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

This security target is strictly conformed[1] to [BSI-PP-0005-2002] protection profile - SSCD Type 2 - and [BSI-PP-0006-2002] - SSCD Type 3.

[1] Although the [BSI-PP-0005-2002] - SSCD Type 2 - and [BSI-PP-0006-2002] - SSCD Type 3 Protection profiles were written with CCv2.1, so did not (yet) specify strict conformance (or demonstrable), it is accepted for the [ST], written with CCv3.1, to claim strict conformance as that [ST] integrates all protection profiles requirements, with some CC adaptation explained in the [ST] §2.4 PP REFINEMENTS.

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:

Subject	*reference*	*supplier*
Commercial name	MultiApp ID IAS ECC	Gemalto
TOE internal reference	T1009875	Gemalto
Micro-controller reference	P5CD144 VOB	NXP
Platform reference	- Hard mask V1.0 (ref. MPH076) - soft mask V1.2	Gemalto
Applet reference	Applet IAS ECC V4.2.7.A	Gemalto

The TOE is uniquely referenced by the answers to the following Get Data commands:

- For the platform, one gets: **B0 85 14 21 01 12 40 70 51 44 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00**,
  These data have the following meaning:
  - « BO » Gemalto Family Name: Java Card;
  - « 85 » Gemalto OS Name: Multiapp ID v1.0;
  - « 14 » Gemalto Mask Number: MPH076;
  - « 21 » Gemalto Product Name: IAS ECC configuration;
  - « 01 » Gemalto Flow version;
  - « 12 » Gemalto filter set: version 1.2;
  - « 40 70 » Chip Manufacturer: NXP;
  - « 51 44 » Chip version: P5CD144;
  - « 00 00 » RFU;
  - the remaining « 00…00 » will be completed by specific teams during manufacturing and personalization process;
- For IAS ECC applet, one gets : A0 0C **49 41 53 20 45 43 43 20 31 2E 30 31** A1 07 **34 2E 32 2E 37 2E 41**, where:
  - « **49 41 53 20 45 43 43 20 31 2E 30 31** » indicates the applet label (IAS ECC 1.01) in ASCII (American standard Code for Information Interchange);
  - « **34 2E 32 2E 37 2E 41** » applet version (4.2.7.A) in ASCII.

This information allows tracing back to all items constituting of the TOE (IC, hard mask, soft mask/filter and applet). It allows properly and uniquely identifying the TOE. The above information was checked on the TOE samples provided for evaluation.

1.2.2. Security services

The product provides mainly the following security services:

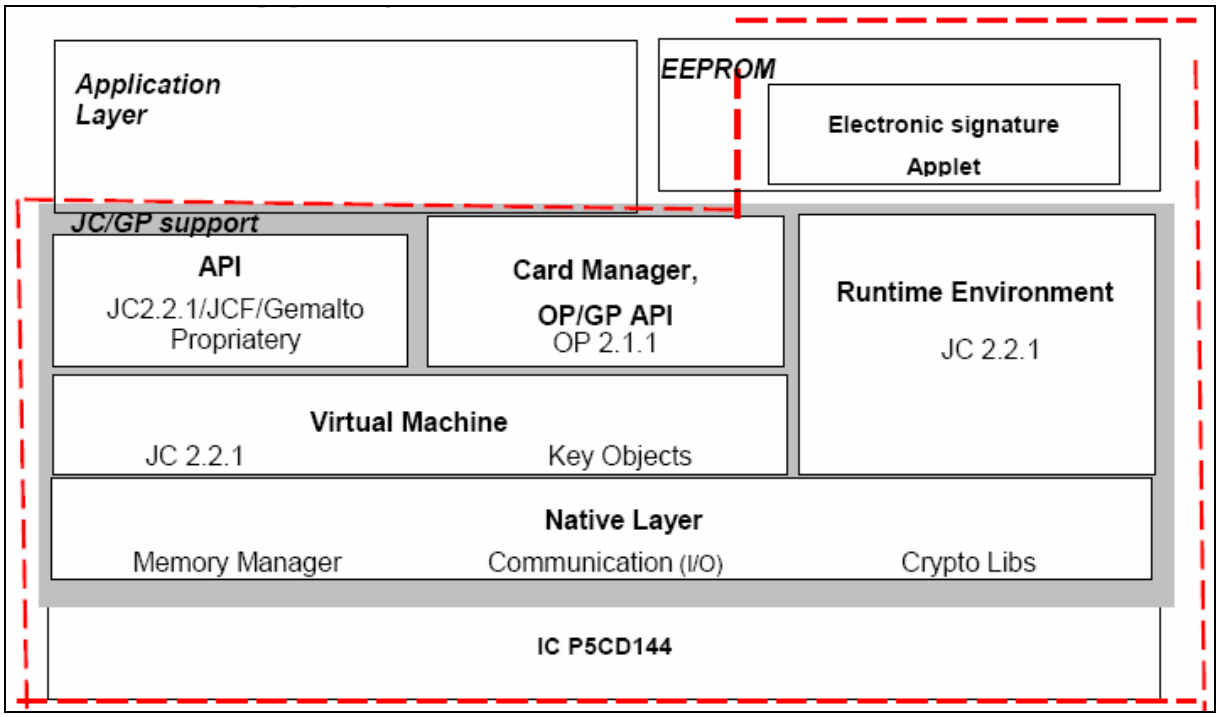
- Security services provided by the platform (see [ST] on chapter §7.1) :
  - Emanation protection in order to protect data, the RAD (Reference Authentication Data) and the SCD ;
  - Card operation protection (in particular, check of operations consistancy depending on the card life-cycle, management of security highlights provided by the underlying IC) ;
- Security services provided by applet IAS ECC (see [ST] on chapter §7.2) :
  - Authentication management (for role management and for secure channel management) ;
  - Cryptography management (Key generation and correspondence verification (for RSA key pairs), Key destruction and cryptographic operations);
  - Integrity monitoring of sensitive user data and of the DTBS (Data To Be Signed) ;
  - Operation management and access control;
  - Secure messaging management.

1.2.3. Architecture

The product consists of:

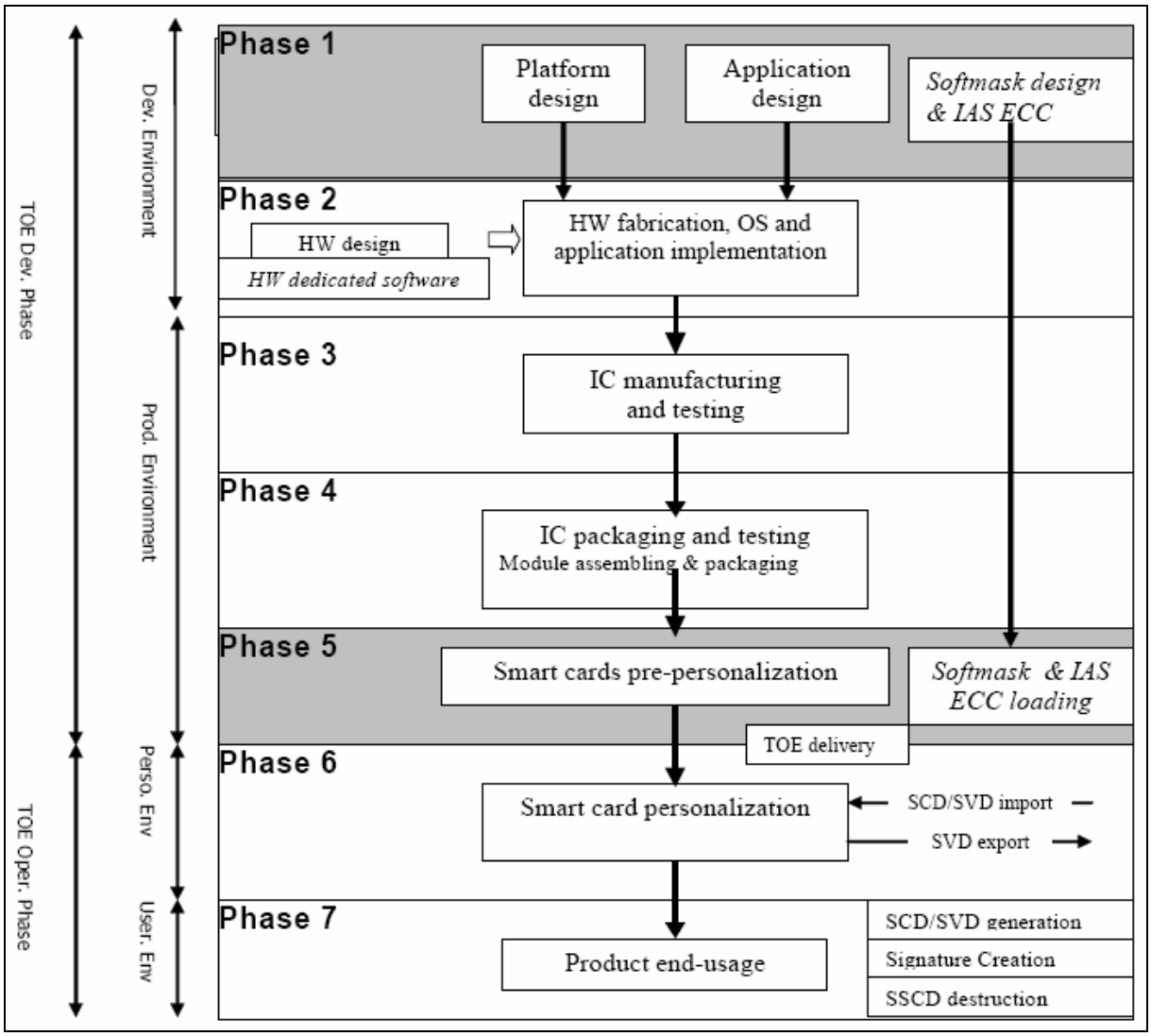
- IAS ECC applet loaded in EEPROM ;
- Soft mask (v1.2) loaded in EEPROM ;
- Multiapp hard mask in ROM ;
- Integrated Circuit.

The general structure is summarized in the figure below:



1.2.4. Life cycle

The product's life cycle is organised as follow (cf. [ST] chapter §1.4.3 TOE life-cycle) :



As show above, TOE delivery is done at the end of phase 5 (pre-personalization), after soft mask and applet loading.
Other phases, former to that delivery point, have been evaluated considering TOE in construction, phase 6 (personalization) have been evaluated regarding guidance, the evaluated product is the product used in phase 7 (use).

Applet, platform and soft mask have been developed on the following site:

Gemalto Meudon

6 rue de la Verrerie
92197 Meudon,
France.

Pre- personalization (phase 5), including applet loading, assembling and packaging (phase 4), have been done on Gemalto Gemenos site and Gemalto Vantaa site (back up):

Gemalto Gemenos

Avenue du Pic de Bretagne – BP 100
13881 Gémenos Cedex,
France.

Gemalto Vantaa

Turvalaaksonkaari 2 - P.O. Box 31
FI-01741 Vantaa,
Finlande

Microcontroller has been developed and produced by NXP on their sites (cf. [BSI-DSZ-CC-0411-2007-MA-04]), main:

NXP Semiconductors GmbH1

Stresemannallee 101
D-22502 Hamburg
Germany

For the evaluation, the evaluator considered:

- As product administrator :
  - The Smart Card product manufacturer : load applet and soft mask;
  - The Personalizer : load user data ;
  - The Card Issuer : typically a national administration, managing card personalization and, in the context of the digital signature, creating the user PIN (Personal Identification Number) and , potentially, import the first SCD in the TOE ;
- As product user :
  - The end-user, who, in the context of the digital signature, is also the signatory and so could sign with his/her SCD, destruct it or generate a new key pair SCD/SVD. At the first usage of the TOE, the Signatory must change his PIN code. A new PIN is also required each time a new SCD/SVD pair is generated.

All these roles are defined in the [ST] chapter §1.4.5 the actors and roles.

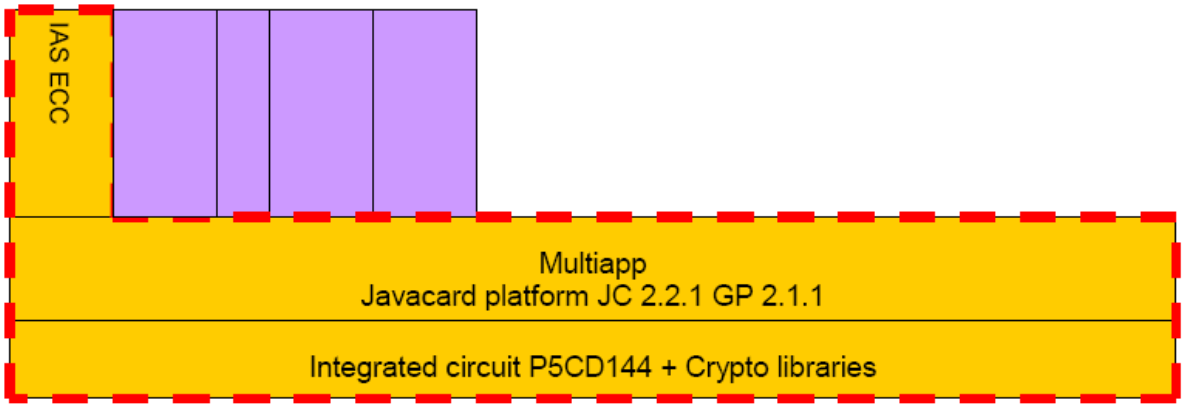
1.2.5. Evaluated configuration

The certificate applies to the smart card Integrated Circuit NXP P5CD144 (VOB), in contact configuration, with its embedded software including:

- The part of Java Card MultiApp platform (v1.0) providing a Card Manager and Global Platform (the remaining part is out of the evaluation scope);
- The Soft mask (v1.2),
- The digital signature IAS ECC v4.2.7.A application instanciated and activated.

Other applications may also be embedded in the product ROM (Read Only Memory); they are out of the scope of the evaluation. All these applications are deactivated in the evaluated product configuration.

The figure below represents the product. The TOE is bordered with bold and un-continuous line.



2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1** [CC], with 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.

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 NXP P5CD144V0B at EAL5 level augmented with ALC_DVS.2, AVA_MSU.3 and AVA_VLA.4, compliant with the [BSI-PP-0002-2001] protection profile, have been used. This microcontroller maintenance has been done by the BSI (cf. [BSI-DSZ-CC-0411-2007-MA-04]).

The evaluation technical report [ETR], delivered to ANSSI the 6th January 2010, provides details on the work performed by the evaluation facility and assesses that all evaluation tasks are "**pass**".

2.3. Cryptographic mechanisms robustness analysis according to ANSSI technical framework

The robustness of cryptographic mechanisms has been analysed by ANSSI according to ANSSI cryptographic framework [REF-CRY]. The results are stated in the cryptographic analysis report [ANA-CRY].

Cryptographic mechanisms can be considered conformant to the ANSSI cryptographic framework [REF-CRY] if guidance [GUIDES] is fully followed. In particular, regarding the product's qualification[1], [GUIDES] requires that the RSA keys used length must be higher or equal to 1 536 bits and requires the usage of SHA-256 algorithm.

The cryptographic implementation, evaluated by the evaluator, was found meeting the qualification[1] requirements at reinforced level.

These results have been taken into account in the evaluator vulnerability analysis and did not allow him highlighting exploitable vulnerabilities for the AVA_VAN.5 level targetted.

2.4. Random number generator analysis

The random number generator has been analysed by ANSSI.

It is a mix between physical generator and cryptographic reprocessing mechanism. This mechanism is found reaching the standard level as defined in the ANSSI cryptographic framework [REF-CRY].

Regarding physical generator, statistical analysis could not be performed by evaluator because of the non accessibility of the physical generator on the TOE. Nevertheless, some analyses were done by the ITSEF involved in the IC certification.

[1] Qualification process is described on ANSSI web site (cf. http://www.ssi.gouv.fr/site_article39.html)

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 evaluated product, Multiapp ID IAS ECC smart card: electronic signature application v4.2.7.A loaded on Multiapp v1.0 Java card platform with v1.2 soft mask embedded on NXP P5CD144 VOB, 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 specified in the security target [ST] and shall respect the recommendations in the guidance [GUIDES], in particular:

- To use RSA keys having their length higher or equal to 1 536 bits ;
- To use SHA-256 algorithm.

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 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, 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**	**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 procedure
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
	ADO_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 claim
	ASE_ECD	**1**	1	1	1	1	1	1	**1**	Extended component 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 specifications
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**	Independant 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: - MISTRAL Security Target v1.9, D1111555 Gemalto. For the needs of publication, the following security target has been provided and validated in the evaluation: - MultiApp ID IAS ECC - Security Target Jan 6, 2010 Gemalto.
[ETR]	Evaluation technical report : - Evaluation Technical Report - MISTRAL Project MISTRAL_ETR_v1.1 / 1.1 Serma Technologies.
[ANA-CRY]	ANSSI Cryptographic analysis report : Cotation de mécanismes cryptographiques - Qualification MISTRAL, N°2356/SGDN/ANSSI/DR, 22/09/2009.
[CONF]	Configuration list LIS: Configuration List – MISTRAL D1132920, V1.5, 06/01/2010 Gemalto.
[GUIDES]	Installation guidance: - Card Initialization Specification for MultiApp ID v1.0: MPH076 for IAS ECC products D1088720, v1.5 Gemalto. - Preparative procedure D1116279, v1.1 Gemalto. Administration guidance: - Card Personalization Specification requirement for SSCD security evaluation IASECCv4_002_CPS_Req_For_CC_Evaluation, v1.1 Gemalto. User guidance: - IAS-ECC Operational user guidance D1115162, v1.1 Gemalto.
[BSI-PP-0005-2002]	Protection Profile — Secure Signature-Creation Device Type 2, Version: 1.04, 25 July 2001. *Certified by the BSI (Bundesamt für Sicherheit in der Informationstechnik) under reference BSI-PP-0005-*

	2002T.
[BSI-PP-0006-2002]	Protection Profile — Secure Signature-Creation Device Type 3, Version: 1.05, 25 July 2001. *Certified by the BSI under reference BSI-PP-0006-2002T.*
[BSI-PP-0002-2001]	Protection Profile, Smart card IC Platform Protection Profile Version 1.0 July 2001. *Certified by the BSI (Bundesamt für Sicherheit in der Informationstechnik) sous la référence BSI-PP-0002-2001.*
[E-sign]	Application Interface for Smart Cards used as Secure Signature Creation Device CEN/ISSS WS/E-Sign Draft CWA Group K part 1 – Basic requirements. Version 1, Release 9 (17th September 2003) Application Interface for Smart Cards used as Secure Signature Creation Device CEN/ISSS WS/E-Sign Draft CWA Group K part 2 – Additional services. Version 0, Release:19 (12th December 2003)
[BSI-DSZ-CC-0411-2007-MA-04]	BSI maintenance report delivered on the 7th July 2009 for *NXP Smart Card Controller P5CD144V0B, P5CN144V0B and P5CC144V0B each with specific IC Dedicated Software*

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, September 2006, version 3.1, revision 1, ref CCMB-2006-09-001; Part 2: Security functional components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-002; Part 3: Security assurance components, September 2007, version 3.1, revision 2, ref CCMB-2007-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2007, version 3.1, révision 2, ref CCMB-2007-09-004.
[CC IC]	Common Criteria Supporting Document - Mandatory Technical Document - The Application of CC to Integrated Circuits, reference CCDB-2006-04-003 version 2.0, revision 1, April 2006.
[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.
[REF-CRY]	Cryptographic mechanisms - Rules and recommendations about the choice and parameters sizes of cryptographic mechanisms version 1.11, 24th October 2008, see www.ssi.gouv.fr