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-2015/30

Plateforme Java Card MAV31S en configuration ouverte de la carte à puce Optelio Contactless R7S masquée sur le composant P60D144JVA

(Version du patch : 1.4)

Paris, 31st August 2015

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

Certification report reference

ANSSI-CC-2015/30

Product name

Plateforme Java Card MAV31S en configuration ouverte de la carte à puce Optelio Contactless R7S masquée sur le composant P60D144JVA

Product reference

Version de la plateforme Java Card MultiApp : 3.1S

Version du patch : 1.4

Protection profile conformity

ANSSI-CC-PP-2010/03-M01 [PP JCS]

Java Card System – Open Configuration, version 3.0

Evaluation criteria and version

Common Criteria version 3.1 revision 4

Evaluation level

EAL 4 augmented

ALC_DVS.2, AVA_VAN.5

Developer(s)

Gemalto

**6 rue de la Verrerie,
92197 Meudon cedex, France**

NXP Semiconductors

**Box 54 02 40,
D-22502 Hambourg, Allemagne**

Sponsor

Gemalto

**6 rue de la Verrerie,
92197 Meudon cedex, France**

Evaluation facility

Serma Technologies

14 rue Galilée, CS 10055, 33615 Pessac Cedex, France

Recognition arrangements

CCRA

The product is recognised at EAL4 level.

SOG-IS

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” Plateforme Java Card MultiApp ID V3.1S en configuration ouverte de la carte à puce Optelio Contactless R7S masquée sur le composant P60D144JVA **,** patch 1.4 » developed by Gemalto .

This product is designed to provide security services for applets which will be installed on the smart card.

Other applications, out of the evaluation scope, are embedded in the product (ROM), particularly:

- eTravel EAC (native application) - passeport application
- eTravel SAC (native application) - passeport application
- IAS Classic v4.2 (Java application) for electronic signature purpose
- MOCA Server v1.0 (Java application) for Match On Card.

1.2. Evaluated product description

1.2.1. Introduction

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

This security target claims conformance to [PP JCS] protection profile.

1.2.2. Product identification

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

The certified version of the product can be identified using the Get Data command on
Card Identity Data (tag 0x0103), as follows:

Gemalto Family Name	Java Card	**B1**
Gemalto OS Name	MultiApp ID	**C7**
Gemalto Mask Number	MPH150	**F3**
Gemalto Flow Version	NA	**xx xx**
Gemalto Filter set	Version 1.4	**0104**

The TOE configurations can be uniquely identified using the Get Data command on
IC Data (tag 0x9F7F), as follows:

Chip Manufacturer	*NXP SEMICONDUCTORS*	**4790**
IC type	P60D144JVA	**6A15**
OS Identifier Provider	*GEMALTO*	**1981**
OS release Date	YDD	**3310**
OS release level	Revision 01 ; release revision 07	**0107**

The main difference between the product and the TOE (the platform) is applications loaded in pre-issuance on this smartcard are out of the evaluation scope.
All the applications in the product configuration given for evaluation are identified in the document [App_list] by their name and AID[1].
The Card Manager command Get Status can be used by the user to check which packages and applications are installed on his product.

1.2.3. Security Services

The product provides mainly the following security services:

- *Card Manager initialization* and card life cycle management;
- Applet loading , installation and extradition by the *Card Manager* (extradition allows to modify the security domain associated to an application) ;
- Delete application under *Card Manager* control ;
- Applet isolation done by the firewall ;
- Secure Application Programming Interface
- Secure Applet loading framework on *post-issuance* ;
- Applet isolation between different contexts and protection of the confidentiality and the integrity application data between application.

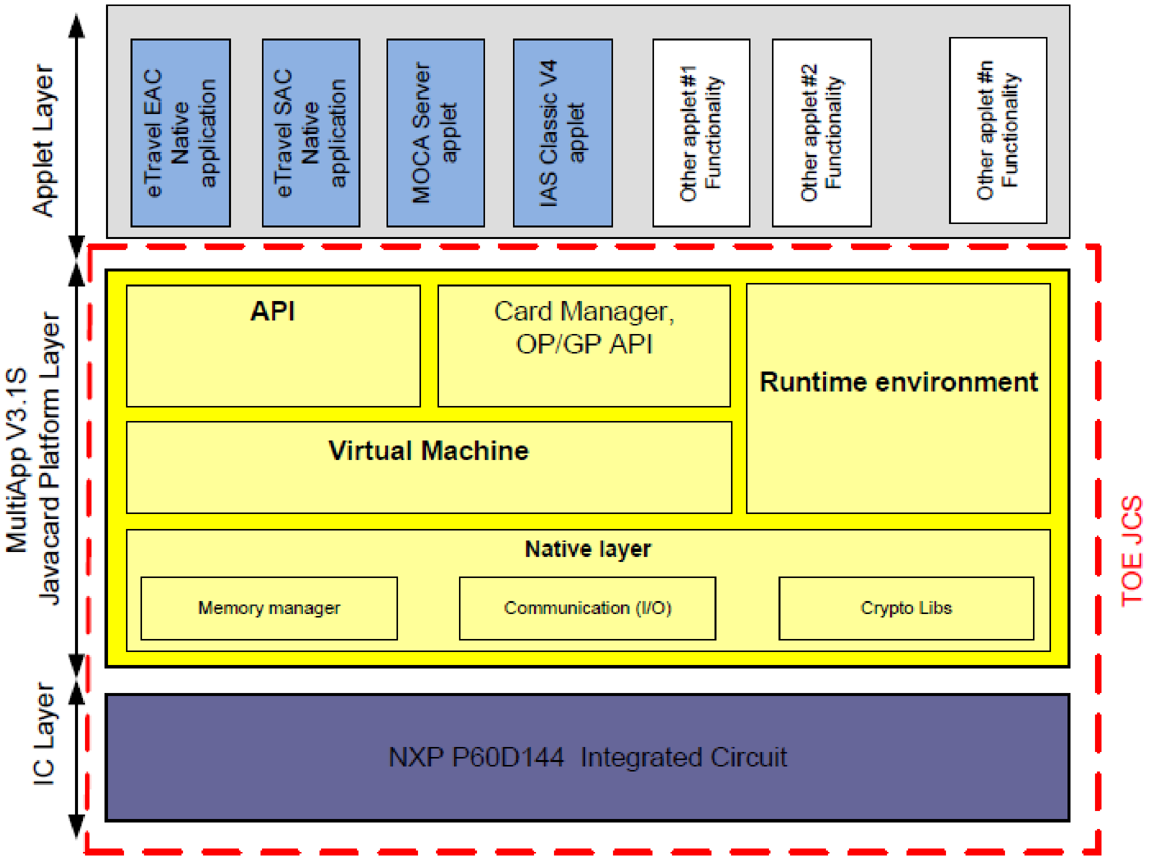
[1] *Application Identifier.*

1.2.4. *Architecture*

The platform Java Card on the smartcard MultiApp v3.1S consists of the following elements:

- Chip P60D144JVA, giving hardware-oriented services (memory management , I/O management, crypto processor management) ;
- A native layer composed of the following elements:
    - *Memory Management* ;
    - *Communication (I/O) management* ;
    - Crypto Libs management ;
- A Java Card System (JCS : *Java Card System*) composed of the following elements:
    - A *Runtime* environmeny (JCRE) ;
    - A Java Virtual Machine (*Virtual Machine*) ;
    - A programming interface (API) with the propriatary package « *com.gemalto.javacardx.pace* » ;
    - An application manager (*Card Manager*).

This architecture is summarized in the following picture :


Applet Layer
eTravel EAC Native application
eTravel SAC Native application
MOCA Server applet
IAS Classic V4 applet
Other applet #1 Functionality
Other applet #2 Functionality
Other applet #n Functionality
MultiApp V3.1S Javacard Platform Layer
API
Card Manager, OP/GP API
Runtime environment
Virtual Machine
Native layer
Memory manager
Communication (I/O)
Crypto Libs
TOE JCS
IC Layer
NXP P60D144 Integrated Circuit

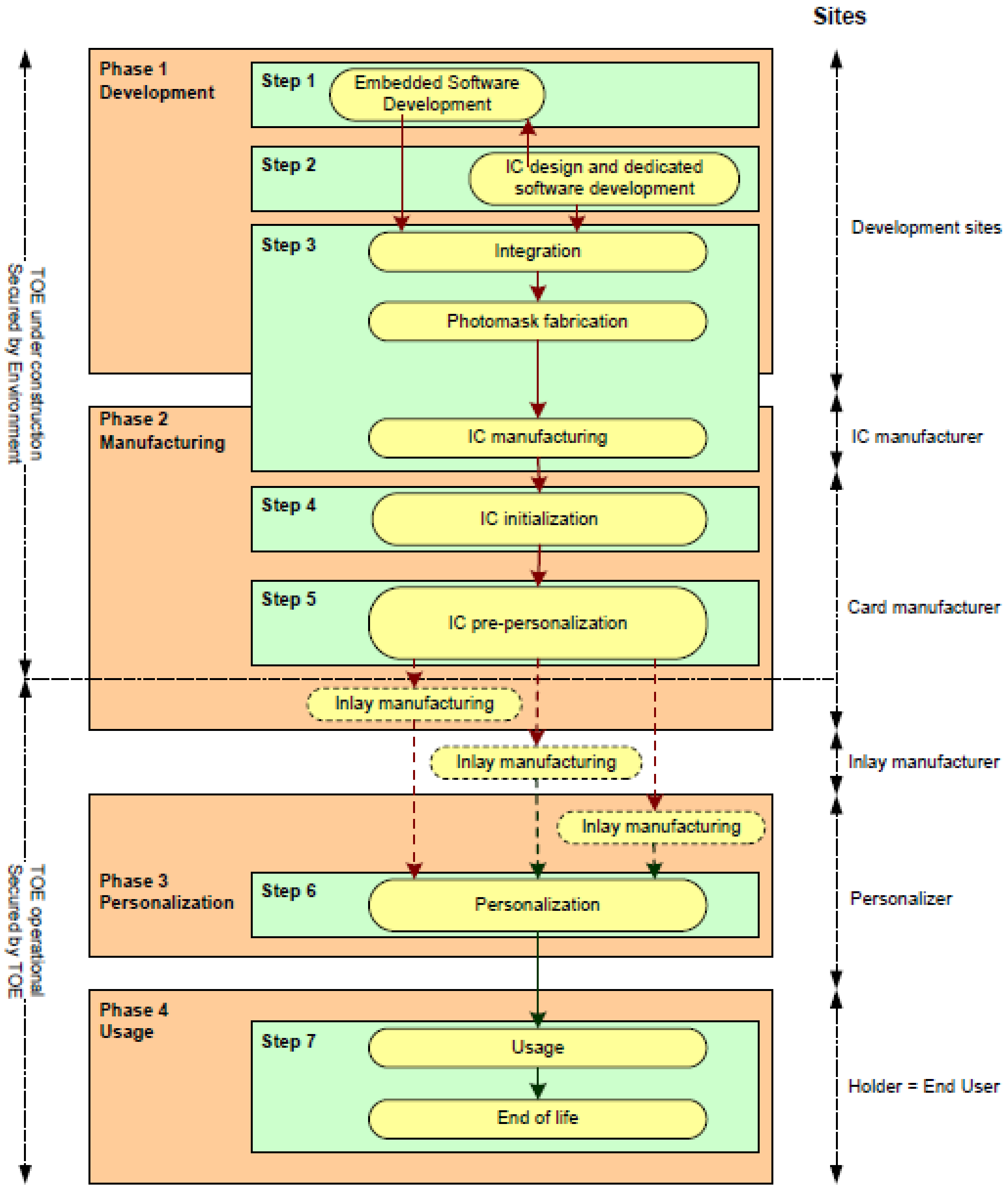
Picture 1 - Architecture and evaluation scope of the TOE

Applications already loaded on the product are all identified in the document [App_list]. Although these standard applications are not in the scope of the evaluation, they have been taken into account into the evaluation process in accordance with the requirements of

[NOTE.10]. Indeed, these standard applications have been verified in accordance with the development constraints for application described into [AGD-Dev_Basic].

1.2.5. Life cycle

The product's life cycle is organised as follow:



The product has been developed on the following sites:

GEMALTO

12 Ayer Rajah Crescent
Singapor 139941
Singapour

GEMALTO

6 Rue de la Verrerie
92190 Meudon
France

GEMALTO

Avenue du Pic de Bertagne
13881 Gémenos
France

GEMALTO

Avenue du Jujubier, ZI Athelia IV,
16705 La Ciotat
France

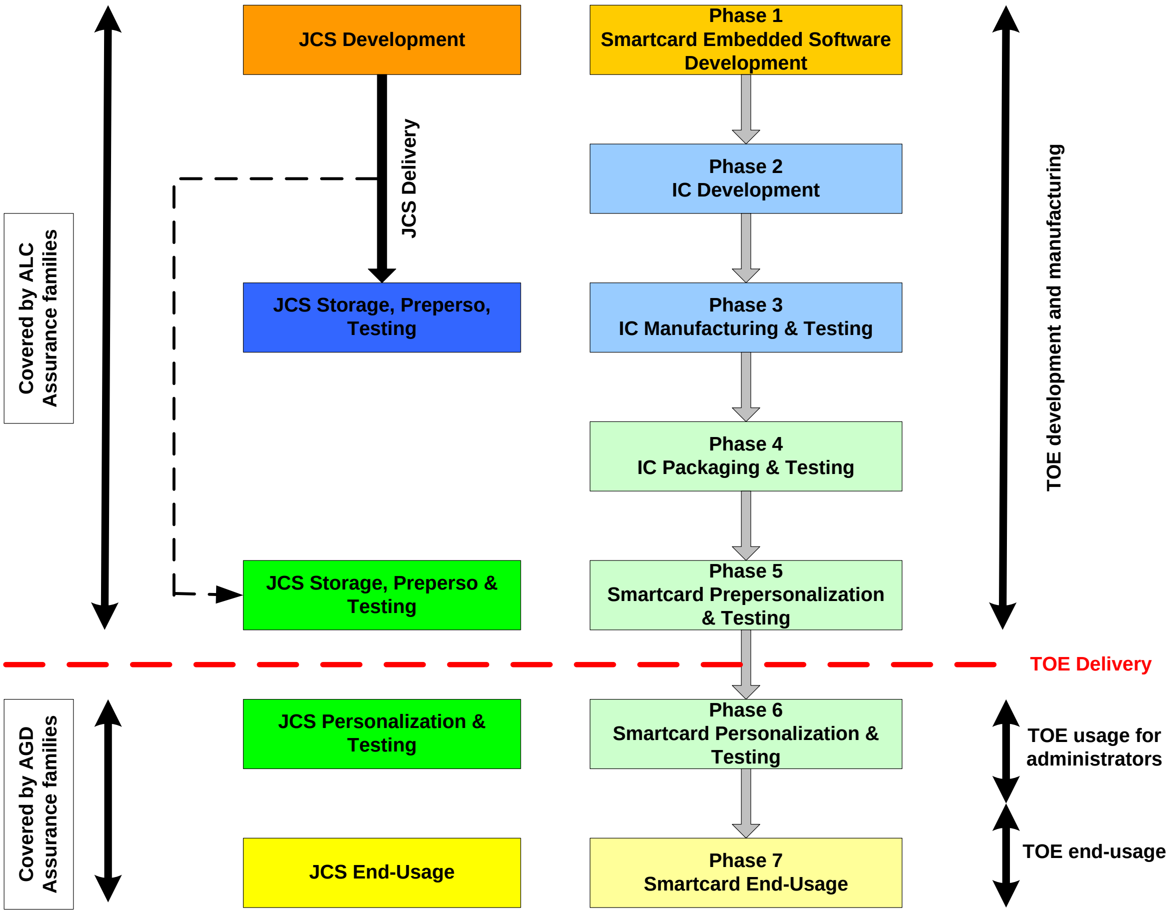
GEMALTO

Ul. Skarszewska 2
33-110 Tczew
Pologne

The IC is developed and manufactured by *NXP SEMICONDUCTORS*. Development and manufacturing sites of the IC are detailed in the certification report whose the reference is [BSI-DSZ-CC-0870-2014].

Plateform Java Card life cycle (TOE) is a part of the product life cycle. It is composed of four phases :

- development ;
- storage, pre-personalization and test ;
- personalization and test ;
- final usage.


Covered by ALC Assurance families
JCS Development
JCS Delivery
JCS Storage, Preperso, Testing
JCS Storage, Preperso & Testing
Phase 1 Smartcard Embedded Software Development
Phase 2 IC Development
Phase 3 IC Manufacturing & Testing
Phase 4 IC Packaging & Testing
Phase 5 Smartcard Prepersonalization & Testing
TOE development and manufacturing
TOE Delivery
Covered by AGD Assurance families
JCS Personalization & Testing
JCS End-Usage
Phase 6 Smartcard Personalization & Testing
Phase 7 Smartcard End-Usage
TOE usage for administrators
TOE end-usage

[AGD-OPE] identifies recommendations regarding the delivery of new applications to be loaded into the card
[AGD-Dev_Basic] and [AGD-Dev_Sec] describe development rules for applications to be loaded into the card ;
[AGD-OPE-VA] describes verification rules which have to be applied by a verification authority.

For this evaluation, the evaluator has considered as product administrators the pre-personalizator, the personalizator and the card manager in charge of the card administration and as final users of the product the application developers to be loaded on the platform.

1.2.6. Evaluated configuration

The certificate applies to the open configuration of the product in accordance with [NOTE.10]:
The product corresponds to a partitioning open plateform. Any loading of new applications compliant with the constraints mentioned in chapter 3.2 of this certification report and realized with audited processes do not compromise this certification report.

All applications identified in [App_list] have been verified in accordance with requirements given in [AGD-OPE_VA].

2. The evaluation

2.1. Evaluation referential

The evaluation has been performed in compliance with **Common Criteria version 3.1 revision 4** [CC], with the Common Evaluation Methodology [CEM.

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

In order to meet the specificities of smart cards, the [JIWG IC] and [JIWG AP] guides have been applied. Thus the reached AVA_VAN level has been determined according to the rating table of the [JIWG AP] guide that is more demanding than the default one defined in [CC] used for other types of products (software products for example).

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 “P60D144JVA” at EAL5 level augmented with ASE_TSS.2, ALC_DVS.2 and AVA_VLA.5, compliant with the [BSI-PP-0035-2007] protection profile, have been used. This microcontroller has been certified the 19 February 2014 under the reference [BSI-DSZ-CC-0870-2014].

The evaluation relies on the evaluation results of the « Plateforme Java Card en configuration ouverte de la carte à puce MultiApp V3.1 masquée sur le composant P60D080PVC patch 1.4 » product certified the 22 December 2014 under the reference ANSSI-CC-2014/86 [ANSSI-CC-2014/86].

The evaluation technical report [ETR], delivered to ANSSI on the 5th of August 2015, 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 rating of cryptographic mechanisms according to the ANSSI technical reference framework [REF] has not been carried out. Nonetheless, the evaluation has not detected any design or manufacturing vulnerabilities for the targeted AVA_VAN.5 level.

2.4. Random number generator analysis

The hardware generator used by the final product has been evaluated during the microcontroller evaluation ([BSI-DSZ-CC-0870-2014]).

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 “Plateforme Java Card MAV31S en configuration ouverte de la carte à puce Optelio Contactless R7S masquée sur le composant P60D144JVA patch 1.4 ” submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL 4 augmented
with ALC_DVS.2 et AVA_VAN.5.

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 [GUIDES], in particular:

- All new applications loaded on this product (*post-issuance loading*) have to follow the platform development constraints ([AGD-Dev_Basic] and [AGD-Dev_Sec] according to the sensibility of the application;
- Certification authority has to apply [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	4	Complete functional specification
	ADV_IMP				1	1	2	2	1	Implementation representation of 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_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: - MAV31S Open Platform JCS Security Target, version 1.2, reference D1334796, July 2015, Gemalto. For the needs of publication, the following security target has been provided and validated in the evaluation: - Security Target Lite – MAV31S Open Platform, reference: D1334796, version 1.2p, July 2015, Gemalto.
[ETR]	Evaluation technical report : - DELPHES31S Project, reference DELPHES31S_ETR_JCS_v1.1, version 1.1, 5 August 2015,Serma Technologies.
[CONF]	Product Configuration List: - LIS: Configuration List for platform on MPH150, reference: D1348672, version 1.1, Gemalto. Applications and Packages verified Lists [App_list] : - Card Initialisation Specification – MultiApp v3.1 : MPH132Filter01, référence : MAV31_Santander_CIS, version 1.4, 23 July 2015, Gemalto
[GUIDES]	Product Installation Guidance [AGD_PRE] : - MultiApp ID V31S Software – AGD_PRE document – Javacard Platform, reference D1345062, version 1.0, 03 December 2014, Gemalto. Product Administration Guidance [AGD_OPE] : - MultiApp ID V31S Software – AGD_OPE document –Javacard Platform, reference D1345063, version 1.2 , 12 December 2014, Gemalto. Product User Guidances : - MultiApp ID Operating System – Reference manual, référence : D1203727D of March 19 2013, Gemalto ; - Guidance for application development [AGD_Dev_Basic] : Rules for applications on MultiApp certified product, référence : D1280572, version A00 of December 2012, Gemalto ; - Guidance for secure application development [AGD-Dev_Sec] : Guidance for secure application development on MultiApp platforms, reference : D1280580, version A00 of December 2012, Gemalto ; - Guidance for verification authority [AGD_OPE_VA] : Verification process of Third Party non sensitive applet loaded in POST-issuance, reference D1322491, version A00 February 2014, Gemalto.

[PP JCS]	“Java Card Protection Profile – Open Configuration”, version 3.0, May 18 2012. *Maintained by ANSSI under the* reference *ANSSI-CC-PP-2010/03-M01*.
[BSI-PP-0035-2007]	Protection Profile, Security IC Platform Protection Profile Version 1.0 August 2007. *Certified by BSI (Bundesamt für Sicherheit in der Informationstechnik) under the reference BSI-PP-0035-2007.*

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, September 2012, version 3.1, revision 4, ref CCMB-2012-09-001; Part 2: Security functional components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-002; Part 3: Security assurance components, September 2012, version 3.1, revision 4, ref CCMB-2012-09-003.
[CEM]	Common Methodology for Information Technology Security Evaluation : Evaluation Methodology, September 2012, version 3.1, révision 4, ref CCMB-2012-09-004.
[JIWG IC]	Mandatory Technical Document - The Application of CC to Integrated Circuits, version 3.0, February 2009.
[JIWG AP]	Mandatory Technical Document - Application of attack potential to smartcards, version 2.9, January 2013.
[COMP]	Mandatory Technical Document – Composite product evaluation for Smart Cards and similar devices, version 1.2, January 2012.
[NOTE.10]	« Note d’application - Certification d'applications sur “plateformes ouvertes cloisonnantes” », référence ANSSI-CC-NOTE-10/1.0, voir www.ssi.gouv.fr.
[CC RA]	Arrangement on the Recognition of Common Criteria certificates in the field of information Technology Security, July 2014.
[SOG-IS]	« Mutual Recognition Agreement of Information Technology Security Evaluation Certificates », version 3.0, 8 January 2010, Management Committee.

[REF]	Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques, version 1.20 of January 26 2010 annexed to the General Security Reference Framework, see www.ssi.gouv.fr.