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-2012/49

Mobile PayPass 1.0 application on Orange NFC V2 G1 release B platform on ST33F1ME

Paris, the 30th July 2012

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-2012/49

Product name (reference / version)

Mobile PayPass 1.0 on Orange NFC V2 G1 release B Card on ST33F1ME - Bridge AEPM configuration

(S1109398/S1105439 Bridge AEPM configuration / Release B)

TOE name (reference / version)

Mobile PayPass 1.0 application on Orange NFC V2 G1 release B platform on ST33F1ME

(S1109398 / Release B)

Protection profile conformity

none

Evaluation criteria and version

Common Criteria version 3.1 revision 3

Evaluation level

EAL 4 augmented

ALC_DVS.2, AVA_VAN.5

Developers

Gemalto

La Vigie, Av du Jujubier, ZI Athelia IV, 13705 La Ciotat Cedex, France

STMicroelectronics

190 avenue Celestin Coq, ZI de Rousset, B.P. 2, 13106 Rousset, France

Sponsor

Gemalto

La Vigie, Av du Jujubier, ZI Athelia IV, 13705 La Ciotat Cedex, France

Evaluation facility

THALES (TCS – CNES)

18 avenue Edouard Belin, BPI1414, 31401 Toulouse Cedex 9, France

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, 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 « Mobile PayPass 1.0- on Orange NFC V2 G1 release B Card on ST33F1ME - Bridge AEPM configuration, ref. S1109398/S1105439 Bridge AEPM configuration, release B » developed by Gemalto and STMicroelectronics.

The product is a (U)SIM[1] card intended to be plugged in a mobile handset supporting NFC[2] technologies. It embeds the Mobile PayPass v1.0 application which implements the "Payez Mobile" solution specified by AEPM (Association Européenne Payez Mobile). This application enables Contactless Mobile Payment (CMP) transactions via radio frequency.

This product is a specific implementation for the Orange Mobile Network Operator (MNO).

1.2. Evaluated product description

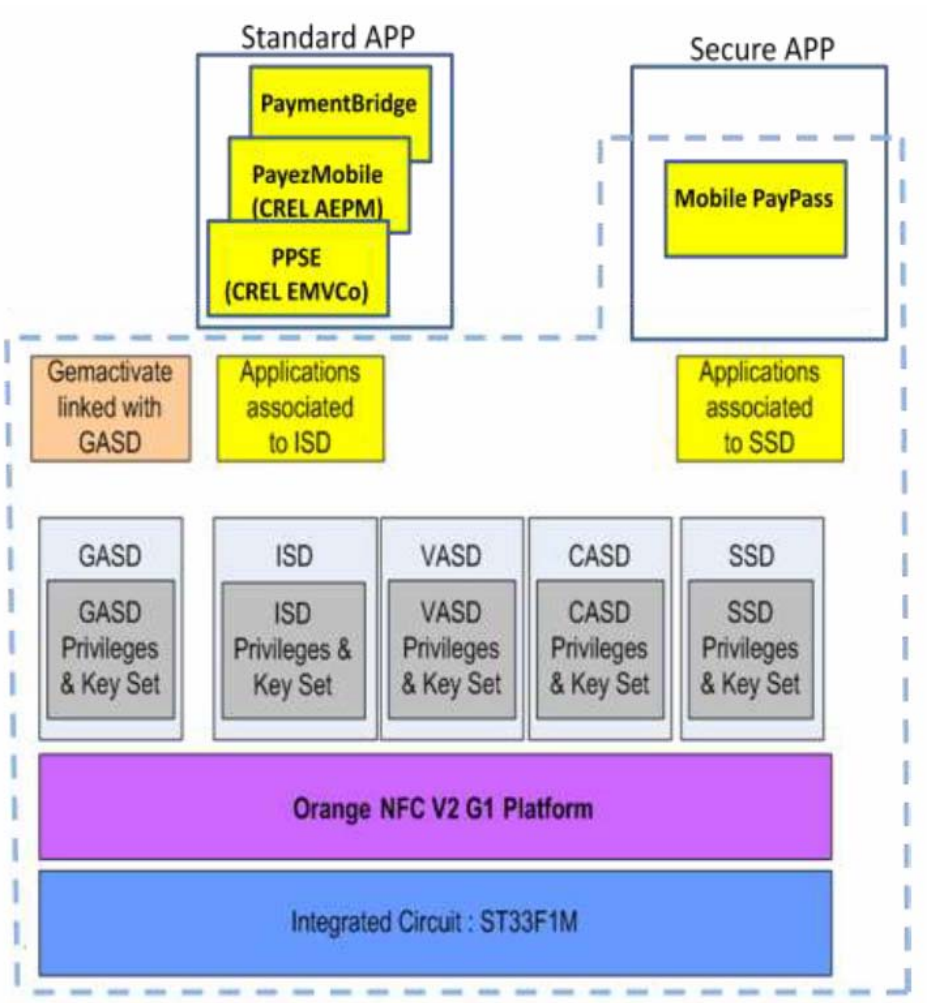
The security target [ST] defines the evaluated product, its evaluated security functionalities and its operational environment.

1.2.1. Architecture

The product is composed of the following components:

- The microcontroller ST33F1M revision E,
- A Java Card System which manages and executes applications. It also provides APIs to develop applications on top of it, in accordance with the Java Card specifications,
- GlobalPlatform (GP) packages, which provides an interface to communicate with the smart card and manage applications in a secure way,
- Platform APIs, which provides ways to specifically interact with (U)SIM applications,
- Telecom environment including network authentication applications (not evaluated) and Telecom communication protocol,
- GemActivate application to activate services in Post-Issuance,
- Mobile PayPass v1.0 secure application,
- PaymentBridge v1.0, PayezMobile v1.0 and PPSE v1.0 standards applications (also called basic applications).

[1] Universal Subscriber Identity Module
[2] Near Field Communication



In the previous figure doted lines identify the TOE: difference between the product and the TOE corresponds to the standard applications loaded on this smartcard.
Even if PaymentBridge v1.0, PayezMobile v1.0 and PPSE v1.0 standards applications are out of the scope of the TOE they have been taken into account in the evaluation process as it is mandated by [NOTE.10]. Indeed those 3 standards applications have been checked according the platform development constraint stated in the certification report [ANSSI-CC-2012/48].

Embedded applications on this product are exactly those identified in the previous certification report (see [ANSSI-CC-2012/11]). Only modifications on the platform, without any impact on the applications, have been performed between the two version of this smart card.

1.2.2. 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:

The following table provides commands and answers that permit to identify the applications considered during this evaluation after AID selection. Means to identify the others components of the product are provided in the certification report [ANSSI-CC-2012/48].

Application (commande)	ASCII answer	CHAR answer
Mobile PayPass v1.0 (About APDU 00 AB 00 00 40)	4D 6F 62 69 6C 65 20 50 61 79 70 61 73 73 20 53 54 4D 30 30 38 20 76 65 72 73 69 6F 6E 20 4D 50 50 76 31 5F 41 45 50 4D 76 33 5F 31 5F 30 5F 62 30 30 32 36 5F 31 31 30 38 32 39 5F 32 31 30 32	Mobile Paypass STM008 version MPPv1_AEPMv3_1_0_b0026_110829_2102
PaymentBridge v1.0 (About APDU 00 AB 00 00 40)	50 61 79 6D 65 6E 74 20 42 72 69 64 67 65 20 53 54 4D 30 30 38 20 76 65 72 73 69 6F 6E 20 4D 50 50 76 31 5F 41 45 50 4D 76 33 5F 31 5F 30 5F 62 30 30 32 36 5F 31 31 30 38 32 39 5F 32 31 30 32	Payment Bridge STM008 version MPPv1_AEPMv3_1_0_b0026_110829_2102
PayezMobile v1.0 (About APDU 00 AB 00 00 3C)	43 52 45 4C 20 50 61 79 65 7A 20 4D 6F 62 69 6C 65 20 76 65 72 73 69 6F 6E 20 4D 50 50 76 31 5F 41 45 50 4D 76 33 5F 31 5F 30 5F 62 30 30 32 36 5F 31 31 30 38 32 39 5F 32 31 30 32	CREL Payez Mobile version MPPv1_AEPMv3_1_0_b0026_110829_2102
PPSE v1.0 (About APDU 00 AB 00 00 33)	50 50 53 45 20 41 70 70 6C 69 63 61 74 69 6F 6E 20 4D 50 50 76 31 5F 41 45 50 4D 76 33 5F 31 5F 30 5F 62 30 30 32 37 5F 31 31 31 31 30 39 5F 31 35 35 33	PPSE Application MPPv1_AEPMv3_1_0_b0027_111109_1553

The following table provides the SHA1 and SHA2 hashes, calculated from the IJC file[1], of the applications considered during the evaluation:

	SHA1	**SHA2**
Mobile PayPass v1.0	68 B4 FF D2 56 63 96 17 F1 F1 69 18 16 76 B0 BC 41 10 9C 0D	83 3C C6 27 3E EB 56 CB D8 9D 7A C5 CA 91 D7 1C F2 2B 60 B1 6B 8E FA 38 CA 2E 75 11 00 86 89 E5
PaymentBridge v1.0	E7 CF D6 59 4F AD C7 39 72 D4 AF 87 9C 4C 8B 26 8A 2E 3D 62	44 3D 61 E3 CA 76 DC D2 CE 09 03 2B 08 C8 58 82 B7 5D 3D B9 A9 61 20 F0 68 E8 2D 85 2F E5 4C BD
PayezMobile v1.0:	40 84 B8 5A 74 4D 56 F6 D6 78 81 EF 28 03 19 DC D8 0D 52 59	82 22 0A 10 17 76 F8 CC 15 16 F3 2C 6B 39 B1 35 9A 7E 44 E1 B1 9F C3 03 4A 8E 5A 70 96 9E 1D 3D
PPSE v1.0	86 E7 AC 1E 72 6C 07 40 87 DA 0E 24 1C E9 85 4F 3D CE 53 DF	14 24 77 60 81 38 69 1A 70 99 C5 4D 80 5E DF 73 A2 AA 91 9F C4 17 A0 BA E1 47 C8 39 55 54 84 DF

1.2.3. Security services

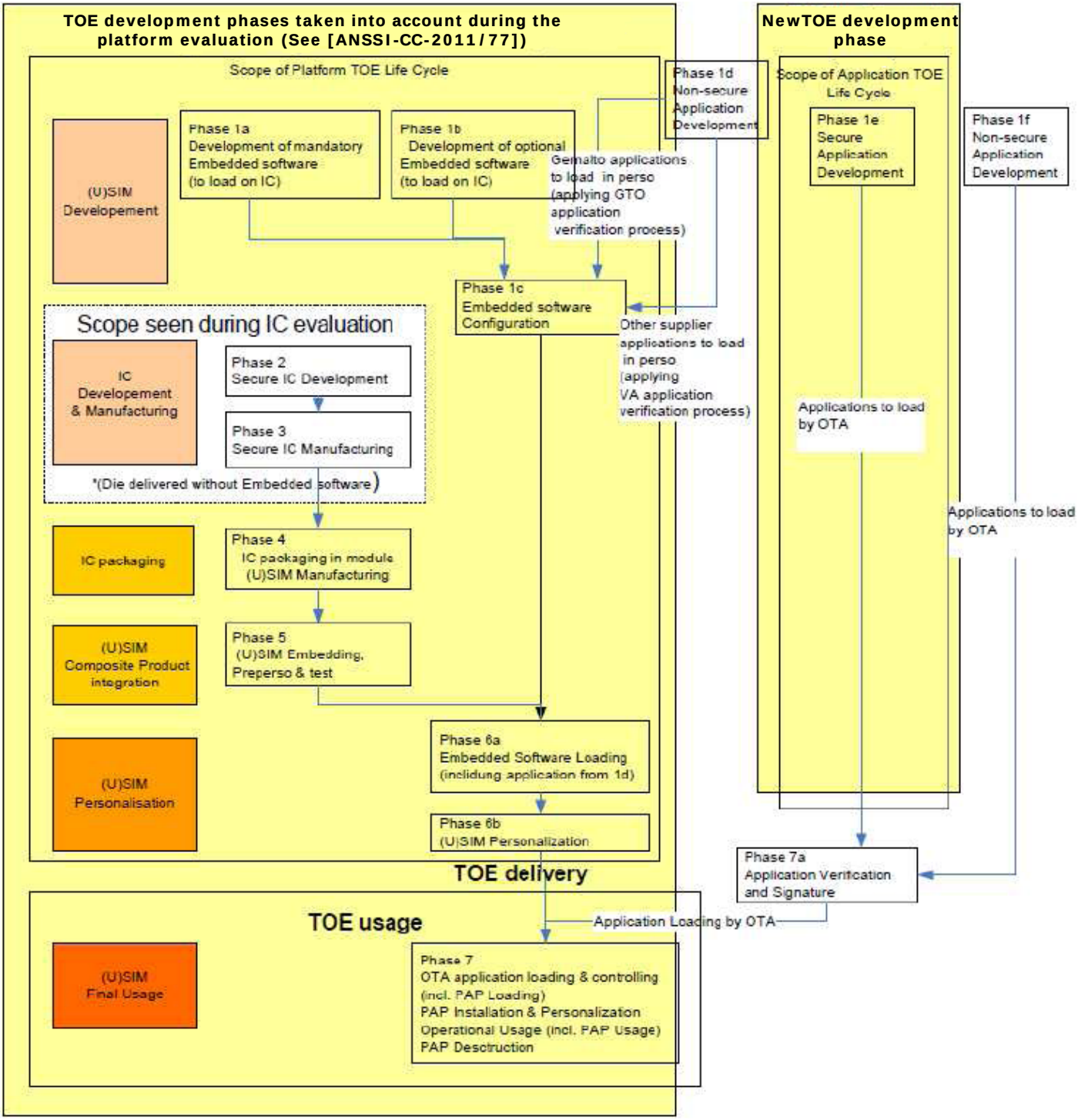
The product provides mainly the following evaluated security services:

- All those supported by the previously certified (U)SIM platform, see [ANSSI-CC-2012/48],
- And those supported by the Mobile PayPass application:
  - Offline communication with Point Of Sale terminal,
  - Offline Data Authentication,
  - Online Authentication and communication with the Bank Issuing,
  - Personal Code verification and management,
  - Transaction risk management analysis,
  - Transaction Certification,
  - Counter reset processing,
  - Script processing via OTA bearer,
  - Auditing,
  - Log reading and update,
  - Administration management (Contactless life cycle management).

[1] Files that correspond to adapted CAP files to be loaded in mobile environment.

1.2.4. Life cycle

The product's life cycle is organised as follow:



The microcontroller's and platform's development and manufacturing sites are identified in the certification report [ANSSI-CC-2012/48].

The application Mobile PayPass v1.0, PaymentBridge v1.0, PayezMobile v1.0 and PPSE v1.0 have been developed on the following site:

Application software development sites

8, rue de la Verrerie
92197 Meudon Cedex
France

12 Ayar Rajah Crescent
Singapour 139941
Singapour

Standards applications PaymentBridge, PayezMobile and PPSE could be loaded on the card:

- in pre-issuance, before card issuance to the end user, according to the audited processes of GEMALTO identified in the certification report [ANSSI-CC-2012/48],
- or in post-issuance through the mobile network (OTA[1] loading). The responsible of the loading process should then refer to the chapter 1.2.2 of this certification report to check, before signing it and sending ot to the (U)SIM cards, that the application to load corresponds to one of those that have been checked during the evaluation process.

1.2.5. Evaluated configuration

The certificate applies to the following configurations of the product:

- "Mobile PayPass 1.0- on Orange NFC V2 G1 release B on ST33F1ME Card - Bridge AEPM configuration, ref. S1109398/S1105439 Bridge AEPM configuration, release B" that contains the secure application Mobile Paypass v1.0 and the standard applications PaymentBridge v1.0, PayezMobile v1.0 and PPSE v1.0;
- "Mobile PayPass 1.0- on Orange NFC V2 G1 release B on ST33F1ME Card - Mastercard EMVCo configuration, ref. S1109398/S1105439 Mastercard EMVCo configuration, release B" that contains the secure application Mobile Paypass v1.0 and the standard application PPSE v1.0;
- "Mobile PayPass 1.0- on Orange NFC V2 G1 release B on ST33F1ME Card - AEPM France/WW configuration, ref. S1109398/S1105439 AEPM France/WW configuration, release B" that contains the secure application Mobile Paypass v1.0 and the standard applications PayezMobile v1.0 and PPSE v1.0;
- "Mobile PayPass 1.0- on Orange NFC V2 G1 release B on ST33F1ME Card - Bridge configuration, ref. S1109398/S1105439 Bridge configuration, release B" that contains the secure application Mobile Paypass v1.0 and the standard applications PaymentBridge v1.0 and PPSE v1.0.

Indeed all the 4 configurations of the product have been taken into account by the ITSEF during this evaluation.

[1] Over-The-Air

The open configuration of the product has been evaluated according to [NOTE.10]: this product corresponds to an open and isolating platform. Thus new applications loading that respect the constraints stated in chapter 3.2 and are loaded according to the audited process for pre-issuance loading do not impact the current certification report.

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].

In order to meet the specificities of smart cards, the [CC IC] and [CC AP] guides have been applied. Thus the reached VAN level have been determined according to the rating table of [CC AP] that is more demanding than the default one defined in [CC] used for other types of products (software product 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 "Orange NFC V2 G1 release B platform on ST33F1ME" at EAL4 level augmented with ALC_DVS.2 and AVA_VAN.5, compliant with the [PPUSIMB] protection profile, have been used. This platform has been certified under the reference [ANSSI-CC-2012/48].

The evaluation relies on the evaluation results of the "Application Mobile PayPass 1.0 sur plateforme Orange NFC V2 G1 sur composant ST33F1ME" product certified the under the reference [ANSSI-CC-2012/11].

The evaluation technical report [ETR], delivered to ANSSI the 8th June 2012, 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 according to [REF-CRY] hasn't been performed. Nevertheless the evaluation hasn't lead to the identification of design or construction vulnerabilities for the targeted AVA_VAN level.

2.4. Random number generator analysis

The random number generator has been studied during the platform evaluation (see [ANSSI-CC-2012/48]).

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 "Mobile PayPass 1.0- on Orange NFC V2 G1 release B on ST33F1ME Card - Bridge AEPM configuration, ref. S1109398/S1105439 Bridge AEPM configuration, release B" submitted for evaluation fulfils the security features specified in its security target [ST] for the evaluation level EAL4 augmented by ALC_DVS.2 and 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 guidance [GUIDES] and [GUIDESptfe]. In particular:

- Applications developers must follow the guidance for basic applications development [AGD-Dev_Basic]or the guidance for secure applications development [AGD-Dev_Sec] depending of the sensibility of the targeted application;
- The Verification Authority must follow the guidance for verification authority [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:

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 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_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: - "Security Target - Mobile PayPass 1.0 on Orange NFC V2 G1", reference R0 R21486_001_CCD_ASE, release 2.01. For the needs of publication, the following security target has been provided and validated in the evaluation: - "Security Target - Mobile PayPass 1.0 on Orange NFC V2 G1", reference R0 R21486_001_CCD_ASE, release 2.01p.
[ETR]	Evaluation technical report : - "Evaluation technical report - Project: ALLEGRO-OR2", reference ALGO2_ETR, revision 2.0.
[CONF]	- « Configuration list 1 », reference LIS_MPP1.0_MPPv1_AEPMv3_Orange2___MPPv1_AEP Mv3_1_0_CAR, release 1.70 ; - « Configuration list 2 », reference LIS_MPP1.0_MPPv1_AEPMv3_Orange2___MPPv1_AEP Mv3_1_0_CAR, release 1.9 ; - « Configuration list 3 », reference R0R21486_001_DAL___30-03-2012.xls, release A08.
[GUIDES]	Preparative guidance : - "Mobile Paypass 1.0 Preparation Guidance", reference R0R21486_009_CCD_AGD-PRE, version 2.01; - "Mobile MasterCard Paypass – Card Applications V1.0 - Installation Guide", reference D2148603, version 1.0.0; Operational guidance: - "Mobile Paypass 1.0 Guidance for administration", reference R0R21486_008_CCD_AGD-OPE, version 2.01; - "Mobile MasterCard Paypass – Card Applications V1.0 - Administration Guide", reference D2148601, version 1.0.0; - "Mobile MasterCard Paypass Card Applications V1.0, Developing Client Applications Guide", reference, D2148602, version 1.0.0.
[GUIDESptfe]	Preparative guidance of the platform: - Acceptance and installation guidance [AGD-PRE]: "Orange NFC V2 G1 card - Preparation Guidance", reference D1226480, release 1.2; Operational guidance of the platform: - Administration guidance [AGD-OPE] : "Orange NFC V2 G1 card - Guidance for Administration", reference D1226483, release 1.5; - Guidance for application development • Guidance for basic application development [AGD-Dev_Basic]: "Rules for applications on Upteq mNFC certified product", reference D1186227, release A092;

	• Guidance for secure application development [AGD-Dev_Sec]: "Guidance for secure application development on Upteq mNFC platforms", reference D1188231, release A07; - Guidance for Verification Authority [AGD-OPE_VA]: "Guidance for Verification Authority of Orange NFC V2 G1 card", reference D1226483v, release 1.5.
[ANSSI-CC-2012/11]	Mobile PayPass 1.0 application on Orange NFC V2 G1 platform on ST33F1ME *Certified by ANSSI under the reference ANSSI-CC- 2012/11.*
[ANSSI-CC-2012/48]	Orange NFC V2 G1 release B platform on ST33F1ME *Certified by ANSSI under the reference ANSSI-CC- 2012/48.*

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, 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.
[NOTE.10]	« Application note - Certification of applications on "open and cloisonning platform" », reference ANSSI-CC-NOTE/10.0EN, see ssi.gouv.fr
[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, 8th 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 annexée au Référentiel général de sécurité, voir www.ssi.gouv.fr