Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2009/56

18 September 2009

Version 1.0

Amendment Record

Version	Date	Description
1.0	18/09/2009	Public release.

Executive Summary

1 The Target of Evaluation (TOE) is the MultiAppV1.0 Platform smartcard operating system which is designed to perform the interface between the card reader and the previously evaluated embedded integrated circuit.

2 This report describes the findings of the IT security evaluation of Gemalto's MultiAppV1.0 Platform, to the Common Criteria (CC) evaluation assurance level EAL2 . The report concludes that the product has met the target assurance level of EAL2 and that the evaluation was conducted in accordance with the Common Criteria and Australasian Information Security Evaluation Program (AISEP) requirements. The evaluation was performed by stratsec and was completed on 4 September 2009.

3 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that:

a) The TOE is used only in its evaluated configuration;

b) The TOE is operated according to the administrator's guidance;

c) Application developers are aware that their application controls access to secret data and internal authentication data. The application developer is responsible for ensuring that no functions exist to extract secret data and for ensuring that any implemented authentication/authorisation functions operate as specified;

d) Native code must not be executed from any third party applications; and

e) The purchaser ensures he obtains written advice from the supplier identifying any pre-installed applets and their purpose.

4 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

5 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at Ref [1] and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

6 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

7 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, MultiAppV1.0 Platform, against the requirements of the Common Criteria (CC) evaluation assurance level EAL2 , and

b) provide a source of detailed security information about the TOE for any interested parties.

8 This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

9 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

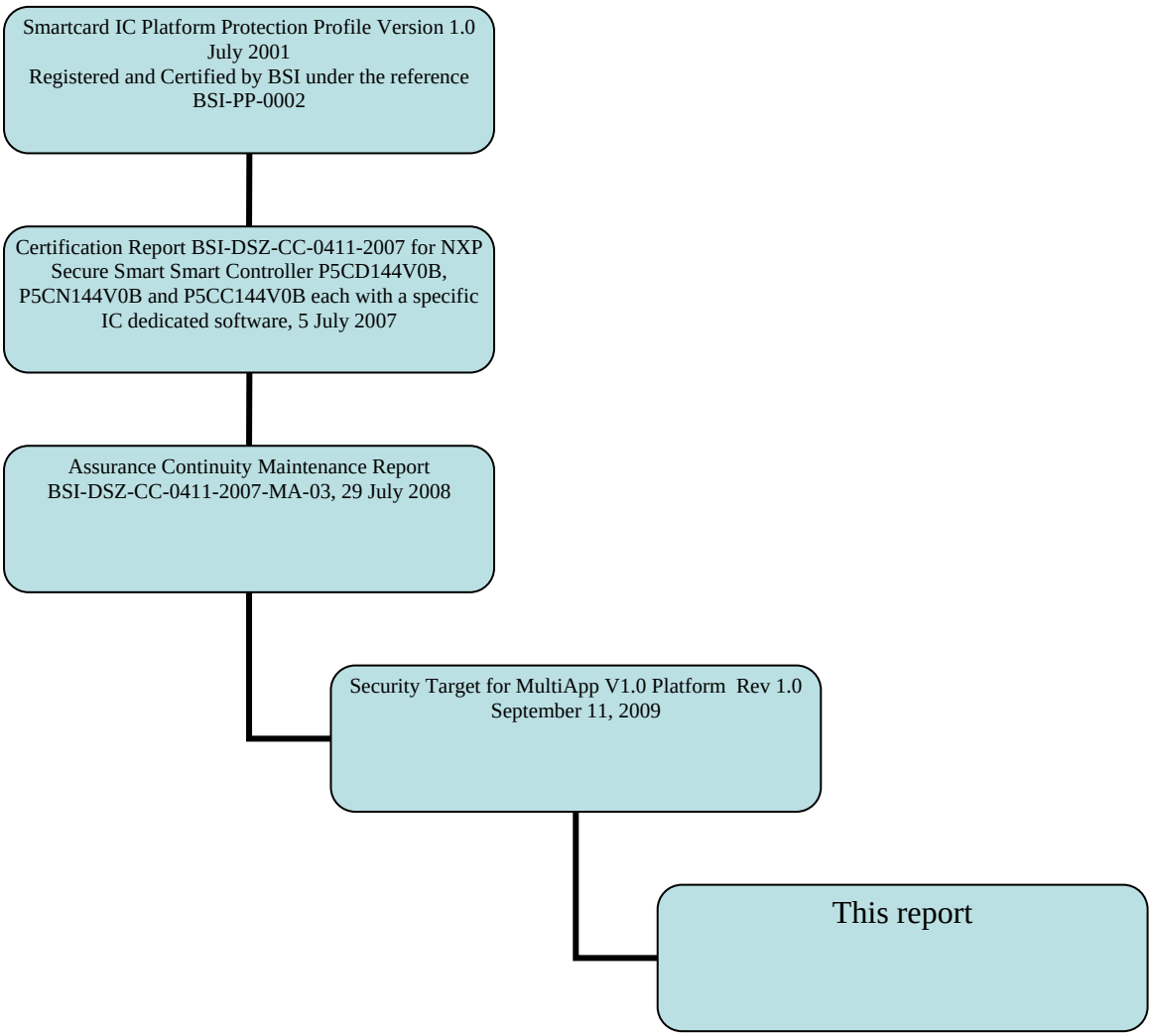
Table 1:Identification Information

Item	**Identifier**
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	MultiAppV1.0 Platform
Software Version	MultiAppV1.0 Platform
Security Target	MultiAppV1.0 Platform: Security Target
Evaluation Level	EAL2
Evaluation Technical Report	Evaluation Technical Report for MultiAppV1.0 Platform 4 September 2009
Criteria	Common Criteria Version 3.1, Revision 2, September 2007, with interpretations as of 24 March 2009.
Methodology	Common Criteria, Common Methodology for Information Technology Security Evaluation, Evaluation methodology

	September 2007 Version 3.1 Revision 2 with interpretations as of 24 March 2009
Conformance	CC Part 2 conformant CC Part 3 conformant
Sponsor	Gemalto, 6 rue de la Verrerie, 92197 Meudon Cedex, France
Developer	Gemalto, 6 rue de la Verrerie, 92197 Meudon Cedex, France
Evaluation Facility	stratsec, Unit 1 , 50 Geils Court, Deakin, ACT 2600

1.4 Document Tracking

The hierarchical relationship between this certification report and related documents is shown below.



Chapter 2 - Target of Evaluation

2.1 Overview

10 This chapter contains information about the TOE, including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

11 The TOE is the MultiAppV1.0 Platform developed by Gemalto. Its primary role is as a smart card operating system which is hosted on an evaluated hardware device conformant to the Protection Profile BSI-PP-0002 (Ref [2]).

12 The TOE is a versatile operating system that allows several applications to share a dedicated security domain. The smartcard Integrated Circuit with Embedded Software supports e-Identity applications which can be used by citizens in a hostile e-security environment.

13 The TOE is a smart card OS that complies with two major industry standards:

a) Sun's Java Card 2.2.1, which consists of the Java Card 2.2.1 ,Virtual Machine, Java Card 2.2.1 Runtime Environment and the Java Card 2.2.1 Application Programming Interface; and

b) The GlobalPlatform Card Specification version 2.1.1

14 The TOE contains the following components

a) The Native Layer that provides the basic card functionalities (memory management, I/O management and cryptographic libraries) with native interface with the dedicated IC. The cryptographic library includes TDES, RSA standard and CRT (up to 2048), ECDSA, ECDH, hashing (SHA-1, SHA-256), and RNG;

b) The Java Card Runtime Environment, which provides a secure framework for the execution of Java Card programs and data access management (firewall);

c) The Java Card Virtual Machine, which provides the secure interpretation of bytecodes;

d) The API including the standard Java Card API, the JCF API (Biometry) and Gemalto proprietary API; and

e) The Open Platform Card Manager, which provides card, key and application management functions (contents and life-cycle) and security control.

2.3 Security Policy

15 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The TSP is defined in the Security Target (Ref [1]). A summary of the TSP is provided below:

a) The platform is conformant to Java Card 2.2.1 and GP 2.1.1 standards and allows the e-Identity application (a Java Card applet) to operate in a secure environment.

b) The platform shall ensure that only S.Card_Manager can perform the following secure operations: load, install and delete applications.

c) The platform shall provide the applications with a secure execution environment as well as a mechanism for secure data sharing.

d) The platform shall provide the applications with cryptographic services, in particular, RSA (up to 2048), ECDSA, ECDH, AES, TDES, SHA-1, SHA-256 and RNG.

2.4 TOE Architecture

16 The TOE consists of the following major architectural components:

a) Java card API;

b) Java card kernel;

c) Card manager ;

d) Runtime environment;

e) Virtual machine;

f) Native layer –

   i. memory manager;

   ii. communications (I/O) ; and

   iii. crypto libraries;

g) Hardware drivers; and

h) IC P5CD144.

The ‘open card’ operating system allows post issuance downloading of applets .

2.5 Clarification of Scope

17 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.5.1 Evaluated Functionality

18 The TOE provides the following evaluated security functionality:

a) Security audit;

b) Cryptographic support;

c) User data protection;

d) Identification and authentication;

e) Security management;

f) Protection of the TOE Security function; and

g) Trusted path/channel.

2.5.2 Non-evaluated Functionality and Services

19 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information and Technology Security Manual (ISM) (Ref [3]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

20 The functions and services that have not been included as part of the evaluation are provided below:

a) Java card applications;

b) holograms and security printing (i.e. microprinting);

c) OATH which provides one time password (OTP) authentication service following the OATH standard;

d) Gemsafev2 which provides electronic signature services;

e) IAS Premium which provides electronic signature services;

f) Cryptomanager provides the biometric Match-On-Card service (by Precise Biometrics);

g) MPCOS which is a card operating system; and

h) Paypass MCHIP which is a MasterCard application.

2.6 Usage

2.6.1 Evaluated Configuration

21 This section describes the configuration of the TOE that was included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in this defined evaluated configuration. Australian Government users should refer to ISM (Ref [3]) to ensure that this configuration meets the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

22 The TOE is comprised of the following software components:

a) MultiAPPV1.0 Platform;

23 The TOE relies on the following hardware:

a) The TOE is an IC module comprised of a Java based smartcard operating system delivered on an integrated circuit (P5CD144) ready to be installed on plastic card packaging. It is personalised securely with the customers required applications. There is no specific evaluation configuration for the operating system required by the developer however care must be taken that the TOE is prepared in a secure manner.

2.6.2 Delivery procedures

24 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product. The TOE is delivered as an IC Module, i.e. an IC with contacts that is not encased in a plastic form. While Gemalto has physical procedures to combat theft during delivery, these were not considered as part of the evaluation.

25 The TOE delivery is secured by a mutual authentication exchange between the TOE and the terminal. The terminal will have been loaded with appropriate key provided by Gemalto. The key exchange is described at a high level in the following sections.

26 The customer will check TOE authenticity by performing the following mutual authentication steps:

a) Init Update command ;

b) Check Card Cryptogram; and

c) External Authenticate command.

27 Once these steps have been completed, the personaliser can be confident that the received modules are authentic and have been correctly initialised.

2.6.3 Definition of an Exchange KEY: ZMK

28 The Key issuer Key management software must integrate some facilities in order to:

a) Generate randomly a ZMK in 3 parts using a HSM + KCV and print the values,

b) Store the ciphered ZMK in a database,

c) Each Key Custodian (3 key custodians) sends his Clear ZMK Key Component to the receiver Key Custodians by personal mail.

29 The Key receiver Key management software must integrate some facilities in order to:

a) Receive the 3 ZMK key parts (3 key custodians);

b) Check the KCV for each part; and

c) Recombine the ZMK, check the KCV of the recombined Key, and store the encrypted ZMK key.

Gemalto can be Key Issuer or Key Receiver. In both cases Gemalto will use a HSM to receive or generate the ZMK key parts. The customer can decide to generate or receive the ZMK keys using a system which is not based on a HSM. In this case the security may be lower.

2.6.4 Delivery of the Keys

30 The TOE is sent to the personaliser (customer), protected by a set of keys, comprising Root_KAUT, Root_KA, & Root_KC.

2.6.5 Application Key Exchange

31 The Gemalto Key management software integrates some facilities in order to:

i. Generate the Application Master keys and store them ciphered in a database; and

ii. Send the Application Master Keys ciphered by the ZMK previously defined between Key Issuer and Key receiver.

32 The Customer Key management software must integrate some facilities in order to:

i. receive the encrypted Application Master keys,

ii. decrypt the Application Master keys using ZMK,

iii. check the Application Keys KCV, and

iv. store the Applications Keys.

2.6.6 Determining the Evaluated Configuration

33 To check the TOE version is correct, the personaliser should issue an ATR command to the TOE. The ATR expected is:

34 3B FD 96 00 00 81 31 80 43 80 31 80 65 B0 85 01 00 D6 83 01 90 00 BC. The ATR is not sufficient in itself to identify the TOE. In addition, to fully identify the TOE the personaliser should issue the GetData Identity (tag 0103) command. The answer expected to the get data command is: B085142401204070514400000000000000000000000000000000000000000

35 The fields are listed in Table 2.

Table 2:

Group	Byte	Description	Value	Length
R&D	00	Gemalto Family Name – Javacard	**B0h**	1
	01	Gemalto OS name – MultiApp ID V1.0	**85h**	1
	02	Gemalto Mask Number – MPH076	**14h**	1
	03	Gemalto Product Name: Australia products	**24h**	1
	04	Gemalto Flow version	**01h**	1
	05	Gemalto Filter Set – Filter V2.0	**20h**	1
	06	Chip Manufacturer – NXP	**4070h**	2
	08	Chip Version – P5CD144	**5144h**	2
	10	RFU	**0000h**	2
Manufacturing	-	RFU	**00..00h**	06
Personnalization	xxh	RFU	**00..00h**	11

36 Additional information such as Chip Serial Number can be checked with the command GetData CPLC (tag 9F7F). For example answer:4070514412918 ‘05312008127000006F63E0412929107129391071294910700000001000000000000000’ .The ROM identifiers (in the mask – 10 bytes) are listed in the Table 3.

Table 3: ROM Identifiers

Length	*Description*
2	IC Fabricator
2	IC Type
2	Operating System Identifier
2	Operating System release date
2	Operating System release level

EEPROM identifiers (initialisation – 16 bytes) are listed in Table 4.

Table 4: EEPROM Identifiers (initialisation – 16 bytes)

Length	*Description*
2	IC Fabrication Date*
4	IC Serial Number*
2	IC Batch Identifier*
2	IC Module Fabricator
2	IC Module Packaging Date
2	ICC Manufacturer
2	IC Embedding Date

*Note: First 8 bytes of initialisation data define the Card Serial Number (CSN).

EEPROM identifiers (pre-personalisation – 8 bytes) are listed in Table 5

Table 5: EEPROM Identifiers (pre-personalisation – 8 bytes)

Length	*Description*
2	IC Pre-Personalizer
2	IC Pre-Personalization Date
4	IC Pre-Personalization Equipment Identifier

EEPROM identifiers (personalisation – 8 bytes) are listed in Table 6.

Table 6: EEPROM identifiers (personalisation – 8 bytes)

Length	*Description*
2	IC Personalizer
2	IC Personalization date
4	IC Personalization Equipment Identifier

2.6.7 Documentation

37 It is important that the TOE is used in accordance with guidance documentation (Ref [4]) in order to ensure secure usage. The following documentation is available upon request :

a) MultiApp V1.0 Preparative User Guide, version 1.1;

b) MultiApp V1.0 Operational User Guide, version 1.1;

c) MultiApp ID Combi and Derived Products Reference Manual;

d) User Guide for JLEP2 Platform Release 1.0.

2.6.8 Secure Usage

38 The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

39 The following assumptions were made:

i. All applets shall be successfully verified by an off–card Java Card Bytecode Verifier (JC_BV22).

ii. All applets to be added on the platform shall not contain native code.

Chapter 3 - Evaluation

3.1 Overview

40 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

41 The criteria against which the TOE has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 2 (Refs [5], [6] and [7]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) Version 3.1 Revision 2 (Ref [8]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [9], [10] , [11] and [12]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [13]) were also upheld.

3.3 Functional Testing

42 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators reported analysing the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators reported that they drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

3.4 Penetration Testing

43 The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly available information.

Chapter 4 - Certification

4.1 Overview

44 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

45 After due consideration of the conduct of the evaluation where witnessed by the certifiers, and of the Evaluation Technical Report (Ref [14]), the Australasian Certification Authority certifies the evaluation of MultiAppV1.0 Platform performed by the Australasian Information Security Evaluation Facility, stratsec.

46 stratsec has found that MultiAppV1.0 Platform upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria evaluation assurance level EAL2 .

47 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

48 EAL2 provides assurance by a complete security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

49 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

50 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

4.4 Recommendations

51 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref [3]) and New Zealand Government users should consult the GCSB.

52 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [4]), the ACA also recommends that users and administrators ensure that :

a) The TOE is used only in its evaluated configuration;

b) The TOE is operated according to the administrator's guidance;

c) Application developers are aware that their application controls access to secret data and internal authentication data. The application developer is responsible for ensuring that no functions exist to extract secret data and for ensuring that any implemented authentication/authorisation functions operate as specified;

d) Native code must not be executed from any third party applications; and

e) The purchaser ensures that he obtains written advice from the supplier identifying any pre-installed applets and their purpose.

Annex A - References and Abbreviations

A.1 References

[1] MultiappV1.0 Platform: Security Target, Rev 1.0, September 11, 2009.

[2] EUROSMART, European Smartcard Industry Association, Smartcard IC Platform Protection Profile, Version 1.0 July 2001 developed by Atmel Smart Card ICs Hitachi Europe Ltd Infineon Technologies AG Philips Semiconductors. Register and Certified by Bundesamt fur Sicherheit in der Informationstechnik (BSI) under the reference BSI-PP-0002

[3] Australian Government Information and Communications Technology Security Manual (ISM), 2008, Defence Signals Directorate, (available at www.dsd.gov.au).

[4] User Documentation:

a) MultiApp V1.0 Preparative User Guide, version 1.1;

b) MultiApp V1.0 Operational User Guide, version 1.1;

c) MultiApp ID Combi and Derived Products Reference Manual; and

d) User Guide for JLEP2 Platform Release 1.0 .

[5] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 3.1, Revision 1, September 2006, CCMB-2006-09-001, Incorporated with interpretations as of 2009-03-24

[6] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components (CC), Version 3.1, Revision 2 , September 2007, CCMB-2007-09-002, Incorporated with interpretations as of 2009-03-24

[7] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components (CC), Version 3.1, Revision 2, September 2007, CCMB-2007-09-003, Incorporated with interpretations as of 2009-03-24.

[8] Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 2 September 2007, CCMB-2007-09-004 Incorporated with interpretations as of 2009-03-24

[9] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[10] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.1,29 September 2006, Defence Signals Directorate.

[11] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate.

[12] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September 2006, Defence Signals Directorate.

[13] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[14] Evaluation Technical Report for Multiapp V1.0 Platform, Version 1.1, Gemalto Pty Ltd, 4 September 2009.

A.2 Abbreviations

AES	Advanced Encryption Standard
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ATR	answer to reset command
CC	Common Criteria
CEM	Common Evaluation Methodology
DFA	Differential Fault Analysis
DPA	Differential Power Analysis
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman (ECDH) key agreement protocol
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
HSM	Hardware Security Module
IC	Integrated circuit
KCV	Key check value
MPCOS	Card operating system
OATH	Provides OTP following the OATH standard.
OTP	One time password.
PayPass MCHIP	Mastercard application
PP	Protection Profile
RNG	Random Number Generator
RSA	algorithm for public-key cryptography
SFP	Security Function Policy
SFR	Security Functional Requirements
SHA	Secure Hash Algorithm
SPA	Simple Power Analysis
ST	Security Target
TDES	Triple DES
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy

ZMK	Zone Master Key