C025 Certification Report

SecureToken ST3 version 1.0

File name: ISCB-5-RPT-C025-CR-v1a
Version: v1a

Date of document: 21 March 2011

Document classification: PUBLIC

For general inquiry about us or our services,
please email: mycc@cybersecurity.my

C025 Certification Report
SecureToken ST3 version 1.0

21 March 2011

ISCB Department

CyberSecurity Malaysia

Level 8, Block A, Mines Waterfront Business Park,

No 3 Jalan Tasik, The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

Tel: +603 8946 0999 Fax: +603 8946 0888

http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C025 Certification Report – SecureToken ST3 version 1.0
DOCUMENT REFERENCE:	ISCB-5-RPT-C025-CR-v1a
ISSUE:	v1a
DATE:	21 March 2011

DISTRIBUTION:	UNCONTROLLED COPY – FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 8, Block A,

Mines Waterfront Business Park,

No 3 JalanTasik, The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Forward

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme was established under the 9th Malaysian Plan to increase Malaysia's competitiveness in quality assurance of information security based on the Common Criteria (CC) standard and to build consumers' confidence towards Malaysian information security products.

The MyCC Scheme is operated by CyberSecurity Malaysia and provides a model for licensed Malaysian Security Evaluation Facilities (MySEFs) to conduct security evaluations of ICT products, systems and protection profiles against internationally recognised standards. The results of these evaluations are certified by the Malaysian Common Criteria Certification Body (MyCB) Unit, a unit established within Information Security Certification Body (ISCB) Department, CyberSecurity Malaysia.

By awarding a Common Criteria certificate, the ISCB asserts that the product complies with the security requirements specified in the associated Security Target. A Security Target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the Security Target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, its security requirements, and the level of confidence (i.e., the evaluation assurance level) that the product satisfies the security requirements.

This certification report is associated with the certificate of product evaluation dated 21 March 2011, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc.

Disclaimer

The Information Technology (IT) product identified in this certification report and its associate certificate has been evaluated at an accredited and licensed evaluation facility established under the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]) using the Common Methodology for IT Security Evaluation, version 3.1 revision 3 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 3 (Ref [2]). This certification report and its associated certificate apply only to the specific version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the MyCC Scheme and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced. This certification report and its associated certificate is not an endorsement of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certification report and its associated certificate, and no warranty of the IT product by CyberSecurity Malaysia or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
v1	8 March 2011	All	Final Released
v1a	21 March 2011	Page iv Page vii & Page 1	Add the date of the certificate. Change the TOE type to PKI-related security solutions.

Executive Summary

SecureToken ST3 Version 1.0 (hereafter referred as SecureToken ST3) from SecureMetric Technology Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 1 evaluation.

The TOE is PKI-related security solutions that comprise of:

- SecureCOS operating system.
- SecureCOS Middleware.
- SecureToken ST3 Management Tools.

SecureToken ST3 provides:

- a USB token with a security integrated circuit card (ICC) that is embedded with the SecureCOS and offers core PKI-related cryptographic functions;
- a software development kit (SDK) with source and headers files that can be used to support the development of enterprise applications;
- a range of utilities and token management applications that resides on a host PC;
- and a suite of middleware binaries that provide compiled APIs that serve as an interface to the token and associated security functionality (these also reside on the host PC)

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions, the intended environment and the security requirements for the TOE, in addition to the evaluation assurance level at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of SecureToken ST3, to the Common Criteria (CC) evaluation assurance level EAL1. The report confirms that the product has met the target assurance level of EAL1 and the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by the stratsec Security Evaluation Facility (STRATSEF) and was completed on 19 January 2011.

Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the SecureToken ST3 evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc.

It is the responsibility of the user to ensure that the SecureToken ST3 meets their requirement and security need. It is recommended that prospective users of SecureToken ST3 refer to the ST (Ref [6]), and read this Certification Report prior to deciding whether to purchase and deploy the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), SecureToken ST3 Version 1.0, is PKI-related security solution that comprises of:

- SecureCOS operating system. The operating system (firmware) embedded on the ICC on the token. The operating system provides the core cryptographic functionality of the TOE.
- SecureCOS Middleware. DLL file that provide exported APIs to provide an interface to the core cryptographic security functionality of the TOE by providing developer's with an easily accessible method for engaging PKI-related functionality.
- SecureToken ST3 Management Tools. The TOE provides two specific applications, one for the SO (administrator) and the second for the user, to manage the key security functionality of the TOE

2 The evaluated security functionalities for the TOE includes:

- Cryptographic Operation.
- User Authentication.
- Security Management.

1.2 TOE Identification

3 The details of the TOE are identified in Table 1 below.

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C025
TOE Name	SecureToken ST3
TOE Version	1.0
Security Target Title	SecureMetric SecureToken ST3 Security Target
Security Target Version	1.0
Security Target Date	19 January 2011
Assurance Level	EAL 1
Criteria	Common Criteria Part 1, Common Criteria Part 2, Common Criteria Part 3 Version 3.1 Revision 3
Methodology	Common Methodology for IT Security Evaluation, version 3.1 revision 3 (Ref [3])

Protection Profile Conformance	None.
Common Criteria Conformance	CC Part 2 Conformant. CC Part 3 Conformant. Package conformant to EAL1.
Sponsor and Developer	SecureMetric Technology Sdn Bhd 2-2, Incubator 2, Technology Park Malaysia, Lebuhraya Puchong – Sg. Besi, Bukit Jalil , 57000 Kuala Lumpur, Malaysia.
Evaluation Facility	stratsec.net Sdn Bhd known as STRATSEF

1.3 Security Policy

4 The security policy of SecureToken ST3 is expressed by the set of security functional requirements which includes cryptographic support, identification and authentication, and security management. Further details on these security policies may be found in Section 4 of the ST (Ref [6]).

1.4 TOE Architecture

5 SecureToken ST3 includes both logical and physical boundaries.

6 Figure 1 below identifies the TOE architecture. The TOE is comprises of Secure COS Manager (User), Secure COS Manager (SO), and Secure Token ST3 Middleware.

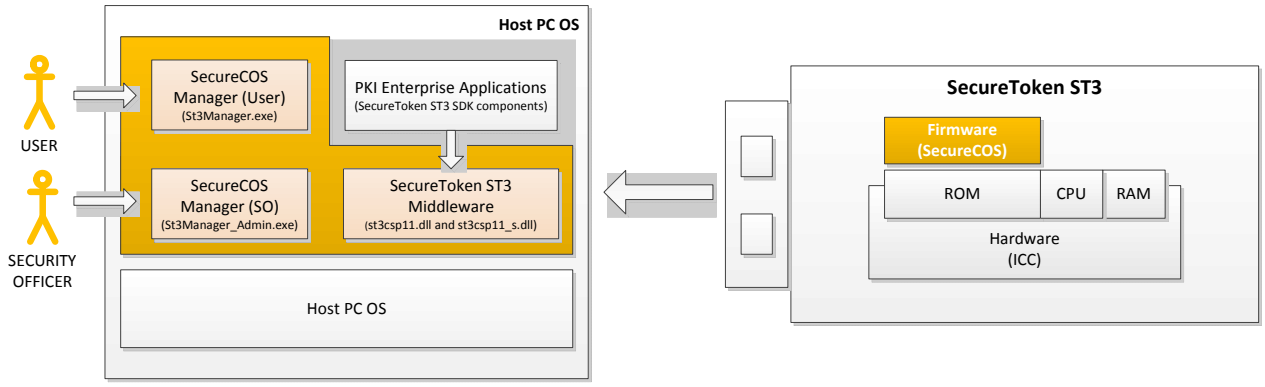

Figure 1: The architecture of SecureToken ST3

7 The following Table 2 describes the components construct the TOE:

Table 2: The component of the TOE

TOE Component	Description
SecureCOS	The operating system (firmware) embedded on the smartcard ICC. The operating system provides the core cryptographic functionality of the TOE.
SecureCOS PKI Hybrid Middleware (smsc_csp11.dll and smsc_csp11_s.dll)	Two compiled binaries that provide exported APIs to provide an interface to the core cryptographic security functionality of the TOE, providing developer's with an easily accessible method for engaging PKI-related functionality to support the development of enterprise authentication and integrity solutions.
SecureCos Card Managers (smscManager.exe and smscManager_Admin .exe)	The TOE provides two specific applications, one for the SO (administrator) and the second for the user, to manage the key security functionality of the TOE.

8 The underlying hardware that is used to support the TOE are:

- Any processor running the following platform:
  - Windows 98 SE
  - Windows ME
  - Windows 2000
  - Windows XP
  - Windows 2003
  - Windows Vista
- A USB port available on the computer and the BIOS supports USB devices, and the USB support feature in CMOS settings is enabled.
- SecureToken ST3 hardware token with pre-installed SecureCOS.

1.5 Clarification of Scope

9 The scope of the evaluation was limited to those claims made in the Security Target (Ref [6]) and includes only the following evaluated security functionality:

a) **Cryptographic Operations –** provides a cryptographic library for cryptographic operations that can be used by applications outside the TOE. It is supports RSA, Triple Des, SHA-1 and MD5 operations. The TOE also provides key generation for RSA and TDES, and key destruction by overwriting the memory space of the key.

b) **Identification and Authentication** – provides a platform to identify and authenticate authorized user to deploy the TOE. Administrator and user of the TOE can authenticate into the TOE through, Token Manager, an application which is outside the scope of evaluation. The Token Manager provides an interface to access management functions. Administrator and user need to present their PIN to the TOE for authentication. Only after a successful authentication will the TOE allows the users to access the TOE functions. The interfaces for the authentication for administrator and user are different so that the TOE will know if the authentication is for the administrator or the user.

c) **Security Management** – provides security features like user management such as creation of users with default passwords (administrator), changing of passwords (user, administrator), and import, export, delete digital certificate (user).

10 Potential consumers of the TOE are advised that some functions and services may not have been evaluated as part of the evaluation. Potential consumers of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration.

11 Functions and services which are not included as part of the evaluated configuration are as follows:

a) SecureToken ST3 hardware token with pre-installed SecureCOS.

b) Windows-based operating system (Windows 98 SE / Me / 2000 / 2003/ XP / Vista).

c) A USB port available on the computer and the BIOS supports USB devices, and the USB support feature in CMOS settings is enabled.

1.6 Assumptions

12 This evaluation was performed at EAL1. Therefore, no assumptions for the TOE were defined in the ST (Ref [6]).

1.7 Evaluated Configuration

13 The TOE is to be configured according to the preparative user guidance (Ref (19a).

14 The TOE is delivered as an application by the developer and developer will make changes to configuration based on preparative user guidance (Ref (19a):

a) Installation SecureToken ST3 Runtime Package

b) Supported Algorithm

c) Function Implementation

d) API Supported by SecureToken ST3.

1.8 Delivery Procedures

15 SecureToken ST3 is available on a CD and it is sealed to ensure the level of the integrity of the packaging process.

16 However, for this EAL1 evaluation, TOE Delivery (ALC_DEL) is not included in the scope of the evaluation. Thus, developer did not provide any documentation on TOE delivery and the evaluators did not verify any TOE delivery process. In section 2.5 of SecureMetric EAL1 Guidance Documents (SecureToken ST3), it states that the delivery process of the TOE is handled by the trusted third party entity such DHL, FedEx.

1.9 Documentation

17 To ensure continued secure usage of the product, it is important that the SecureToken ST3 is used in accordance with guidance documentation.

18 The following documentation is provided by the developer to the end user as guidance to ensure secure operation of the product:

a) SecureToken ST3 Developer's Guide Version 1.2, January 2009.

b) SecureToken ST3 User's Guide Version 1.2, January 2009.

19 The following documentation is used by the developer's authorised personnel as guidance to ensure secure installation of the product:

a) SecureToken ST3 Runtime Package Installation Guide Version 1.2, January 2009.

2 Evaluation

20 The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 1 (EAL1). The evaluation was performed conformant to the MyCC Scheme Policy (MyCC_P1) (Ref [4]) and MyCC Scheme Evaluation Facility Manual (MyCC_P3) (Ref [5]).

2.1 Evaluation Analysis Activities

21 The evaluation activities involved a structured evaluation of SecureToken ST3 Version 1.0, including the following components:

2.1.1 Life-cycle support

22 An analysis of the SecureToken ST3 configuration management system and associated documentation was performed. The evaluators confirmed that the configuration list which includes the TOE and the evaluation evidence were clearly and uniquely labelled.

2.1.2 Development

23 The evaluators analysed the SecureToken ST3 functional specification; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces (TSFIs), and how the TSF implements the security functional requirements (SFRs).

2.1.3 Guidance documents

24 The evaluators examined the SecureToken ST3 preparative user guidance and operational user guidance, and determined that it sufficiently and unambiguously described how to securely transform the TOE into its evaluated configuration, and how to use and administer the product in order to fulfil the security objectives for the operational environment. The evaluators examined and tested the preparative and operational guidance, and determined that they were complete and sufficiently detailed to result in a secure configuration.

2.1.4 IT Product Testing

25 Testing at EAL1 consists of performing independent function test, and performing penetration tests. SecureToken ST3 testing was conducted by tester from stratsec at stratsec Lab in Plaza Sentral where it was subjected to an independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Reports.

2.1.4.1 Independent Functional Testing

26 At EAL1, independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining functional specification and guidance documentation, and creating test cases to verify the behaviour of the TOE.

27 All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. Thirteen independent functional tests were developed and performed by the evaluators to verify the TOE functionality as follows:

Description	Security Function	TSFI	Results
The TDES cryptographic operation should align with FIPS 46-3 standard.	Cryptographic operation	CSP Interface	**PASS.** The output shows TOE supports TDES cryptographic key length of 168bits.
The RSA cryptographic operation shall align with RSA PKCS#11	Cryptographic operation	PKCS#11 Interface	**PASS.** The output shows that TOE only supports RSA cryptography key lengths of 1024 and 2048.
Hashing operation should operate with SHA-1 algorithm that meets FIPS 180-2 standard.	Cryptographic operation	CSP Interface	**PASS.** The output shows that TOE supports hash function based on SHA-1 with key length 160 bits.
Hashing should operate with MD5 algorithm that aligns with FIPS 180-2.	Cryptographic operation	CSP Interface	**PASS.** The output shows that TOE supports MD5 hash function with key length of 128bits.
TOE should generate TDES algorithm with keys length of 128bits that align with Annex E.4.1 of GP211	Cryptographic operation	CSP Interface	**PASS.** The output shows that TOE generates TDES key length of 128bits.
TOE should generate RSA key length 1024, 1152, 1280, 1536 and 2048 bits that align with RSA PKCS#1 standard.	Cryptographic operation	PKCS#11 Interface	**PASS.** The output shows that TOE only generates RSA key lengths of 1024 and 2048.
TOE should destroy	Cryptographic	PKCS#1	**PASS.** The output shows that

cryptographic keys when it generates new keys.	operation	1 Interface CSP Interface	old cryptographic keys that being overwritten is destroyed.
TOE shall detect incorrect authentication.	Identification and Authentication	PC/SC Interface	**PASS.** The output shows that incorrect user PIN authentication attempt is detected. 3 times attempt are allowed.
TOE shall maintain and stored PIN and assign certain rights to users' privilege.	Identification and Authentication	PC/SC Interface	**PASS.** The output shows that only valid user PIN able to open Certificate Manager.
TOE requires user authentication first before any action can be made.	Identification and Authentication	PC/SC Interface	**PASS.** The output shows that the user must successfully authenticate before any actions made.
TOE shall block PIN modification by normal user.	Security Management	PC/SC Interface	**PASS.** The output shows that the TOE shall restrict user PIN modification based on user management privilege.
TOE shall block user PIN modification to administrator by administrator.	Security Management	PC/SC Interface	**PASS.** The output shows that TOE shall restrict any modification attempt to Administrator PIN.
TOE shall block user modification to block Administrator.	Security Management	PC/SC Interface	**PASS.** The output shows that the TOE shall restrict any modification to block administrator.

Table 3: Independent Functional Testing

28 All tests performed by the evaluators produced the expected results and as such the TOE behaved as expected.

2.1.4.2 Penetration Testing

29 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, and functional specification.

30 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential. The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialist expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation.

31 The results of the penetration testing note that there is no vulnerability or residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment

32 The penetration tests focused on :

a) USB Sniffing

2.1.4.3 Testing Results

33 Tests conducted for the SecureToken ST3 produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

34 Based on the results of penetration testing, the evaluators determined that the TOE is resistant to an attacker possessing a basic attack potential.

3 Result of the Evaluation

35 After due consideration during the oversight of the execution of the evaluation by the certifiers and of the Evaluation Technical Report (Ref [7]), the Malaysian Common Criteria Certification Body certifies the evaluation of SecureToken ST3 performed by the stratsec Security Evaluation Facility which known as STRATSEF.

36 STRATSEF found that SecureToken ST3 upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) assurance level EAL1.

37 Certification is not a guarantee that a TOE is completely free of exploitable vulnerabilities. There will remain a small level of risk that exploitable vulnerabilities remain undiscovered in its claimed security functionality. This risk is reduced as the certified level of assurance increases for the TOE.

3.1 Assurance Level Information

38 EAL1 provides a basic level of assurance by a limited Security Target and an analysis of the security functions in that Security Target, using a functional and interface specification and guidance documentation, to understand the security behaviour.

39 The analysis is supported by a search for potential vulnerabilities in the public domain and independent testing (functional and penetration) of the TOE security functions.

40 EAL1 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

3.2 Recommendation

41 In addition to ensure secure usage of the product, below are additional recommendations for SecureToken ST3 consumers:

a) Potential purchasers of the TOE should review the intended operational environment and ensure that they are comfortable that the stated security objectives for the operational environment can be suitably addressed.

b) The developers should make themselves familiar with the developer guidance provided with the TOE and pay attention to all security warnings.

Annex A References

A.1 References

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

[2] The Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009.

[4] MyCC Scheme Policy (MyCC_P1), v1a, CyberSecurity Malaysia, December 2009.

[5] MyCC Scheme Evaluation Facility Manual (MyCC_P3), v1, December 2009.

[6] SecureMetric SecureToken ST3 Security Target, Version 1.0, 19 January 2011.

[7] Evaluation Technical Report EAL1 Evaluation of SecureMetric SecureToken ST3 Security Target, Version 1.0, 19 January 2011.

A.2 Terminology

A.2.1 Acronyms

Table 4: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CEM	Common Evaluation Methodology (ISO/IEC 18045)
CCRA	Common Criteria Recognition Arrangement
ICC	Integrated Circuit Card
IEC	International Electrotechnical Commission
ISO	International Standards Organisation
ISCB	Information Security Certification Body
MyCB	Malaysian Common Criteria Certification Body
MyCC	Malaysian Common Criteria Evaluation and Certification Scheme
MyCPR	MyCC Scheme Certified Products Register
MySEF	Malaysian Security Evaluation Facility
PP	Protection Profile
ST	Security Target

Acronym	Expanded Term
TOE	Target of Evaluation
SO	Security Officer

A.2.2 Glossary of Terms

Table 5: Glossary of Terms

Term	Definition and Source
CC International Interpretation	An **interpretation** of the CC or CEM issued by the CCMB that is applicable to all CCRA participants.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology. An interpretation may be either a **national interpretation** or a **CC international interpretation**.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.

Term	Definition and Source
Maintenance Certificate	The update of a Common Criteria certificate to reflect a specific version of a product that has been maintained under the MyCC Scheme.
ISCB Personnel	Includes all members of the Certification Subcommittee, the Scheme Manager, the Senior Certifier, Certifiers and the Quality Manager.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.
FIPS 46-3	It is a Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology for DATA ENCRYPTION STANDARD.
PKCS#1	It is the first of a family of standards called Public-Key Cryptography Standards (PKCS), published by RSA Laboratories. It provides the basic definitions of and recommendations for implementing the RSA algorithm for public-key cryptography.
RSA	It is an algorithm for public-key cryptography.
GP211	Global Platform Card Specification – v2.1.1, March 2003.
MD5	MD5 (Message-Digest algorithm 5) is a cryptographic hash function with a 128-bit hash value.

--- END OF DOCUMENT ---