Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2009/60

28 September 2009

Version 1.0

Amendment Record

Version	Date	Description
1.0	28/09/2009	Public release.

Executive Summary

1 SanDisk's Cruzer Enterprise FIPS Edition is an encrypted USB storage device used for securely storing files on the FLASH memory of the device. The Cruzer Enterprise FIPS Edition is the Target of Evaluation (TOE), noting that the physical scope of the evaluation includes only the USB device circuit board. While the TOE interface to Central Management and Control (CMC) software was included in the evaluation, the CMC software itself was not evaluated.

2 The evaluated functionality of the TOE was:

a) **Cryptography.** The TOE generates 256-bit AES keys which do not leave the token. The TOE uses SHA-1 for password verification, AES key generation and storing the reference authentication data in an irreversible way. It also performs verification of 1024-bit RSA digital signatures to establish a secure channel with CMC software to verify the authenticity of firmware upgrades.

b) **Protection of secrets.** The TOE preserves the integrity and confidentiality of cryptographic keys and reference authentication data by providing physical and logical protection from unauthorised modification or disclosure.

c) **Authentication and access control.** The TOE requires the user of the host PC to be authenticated prior to accessing encrypted data stored on the TOE. It maintains an authenticated and lifecycle state that determines access to protected data. The TOE denies all access requests to the data stored on it when in lockdown mode or if the user is not successfully authenticated.

d) **Password security.** The TOE requires users to authenticate by entering the password created during initialisation in the Login Device Window each time it is started up. A lost or forgotten password cannot be recovered and either external management software is required to reset the password or the TOE needs to be reformatted and reinitialised which erases all previously stored data.

e) **Lockdown mode.** The TOE maintains a count of consecutive failed authentication attempts and if the count exceeds a preset maximum number of attempts the TOE enters lockdown mode. All access requests to the TOE are blocked in lockdown mode and the only way to recover the TOE is to reformat and initialise the device, which erases all previously stored data.

f) **Secure access.** The TOE can be securely administered using CMC software and can restrict access to only legitimate CMC software. The TOE is also capable of establishing a trusted channel between itself and any dedicated application being executed on the host PC.

g) **Secure firmware upgrade.** The TOE implements a mechanism for ensuring that only authentic firmware upgrades are implemented on the device. This is done by verifying the digital signature attached to the upgrade.

3 This report describes the findings of the IT security evaluation of SanDisk's Cruzer Enterprise FIPS Edition, to Common Criteria (CC) V3.1 evaluation assurance level EAL2 augmented with basic flaw remediation. The report concludes that the product has met the target assurance level of EAL2 and that the evaluation was conducted in accordance with Common Criteria and Australasian Information Security Evaluation Program (AISEP) requirements. The evaluation was performed by stratsec and was completed in July 2009.

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

a) order the TOE only in multiples of 20 units to ensure that tamper evidence is maintained during the delivery process;

b) ensure that critical or important data in the TOE is backed up to prevent data loss if the TOE is re-initialised; and

c) examine the internals of the device, by removing the outer casing and inspecting the epoxy covering the cryptographic controller for damage if tampering of the TOE is suspected or if the TOE has been out of the user's control for a significant period of time.

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

6 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

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

1.2 Purpose

8 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Cruzer Enterprise FIPS Edition, 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.

9 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

10 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.5.1 Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Cruzer Enterprise FIPS Edition
Software Version	Firmware v6.612 and v6.615
Security Target	SanDisk Cruzer Enterprise FIPS Edition Security Target, Version 1.1, 24 September 2009
Evaluation Level	EAL2
Evaluation Technical Report	Evaluation Technical Report for SanDisk Cruzer Enterprise FIPS Edition Firmware v6.612/v6.615 version 1.1, 16 September 2009
Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 2, September 2007 with interpretations as of 28 November 2008
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2007, Version 3.1 Revision 2, CCMB-2007-09-004

Conformance	CC Part 2 conformant. CC Part 3 Augmented with flaw remediation ALC_FLR.1
Sponsor/Developer	SanDisk 7 Atir Yeda Street Kfar Saba, 44425 Israel
Evaluation Facility	stratsec Suite 1, 50 Geils Court, Deakin, ACT 2600, Australia

Chapter 2 - Target of Evaluation

2.1 Overview

11 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

12 The TOE is the Cruzer Enterprise FIPS Edition, firmware versions 6.612 and 6.615 developed by SanDisk. The scope of the evaluation includes only the USB storage device circuit board. While the external casing provides a level of protection against environmental hazards (i.e. water, dust or physical damage), it may easily be removed to inspect the circuit board and does not provide any physical tamper evidence.

13 The TOE is an encrypted U3 capable USB storage device used for securely storing files on the flash memory of the device. The TOE is also capable of authenticating end users and encrypting and decrypting files stored on the device's non-volatile memory. Data is decrypted by the TOE as required when it is read from encrypted non-volatile storage, all other data remains encrypted on the non-volatile memory of the device. The security features of the TOE includes cryptography, protection of secrets, authentication and access control, password security, lockdown mode, secure access and secure firmware upgrade.

14 The TOE maintains an unencrypted, read-only, CD-ROM emulation partition which contains the software used to interface with the TOE authentication functions.

15 Further details on the TOE and its operating environment are provided in Section 2.4 of the Security Target (Ref [1]).

2.3 TOE Architecture

16 The TOE's major architectural components are described in the Security Target (Ref [1]).

17 The TOE is represented by the following subsystems:

a) Hardware subsystem,

b) Flash Memory subsystem,

c) Physical Communication Layer subsystem,

d) USB Device Layer subsystem,

e) USB Services Layer subsystem, and

f) Service Implementation subsystem.

18 The Developer's Architectural Design identifies the following components of the TOE:

a) Hardware subsystem.

- Provides the necessary hardware primitives and routines for the TOE and implements the essential symmetric cryptographic functions. These include the AES cryptographic engine and the random number generator used for implementing cryptographic services. The hardware subsystem also provides the physical connectivity of the TOE to the host PC via a physical USB interface.

b) Flash Memory subsystem.

- Provides the storage used by the other subsystems to store data persistently within the TOE.

c) Physical Communication Layer subsystem.

- Provides the physical communication layer services described in the U3 API. This subsystem performs physical layer API services and relays protocol messages between the host PC and the TOE USB Device layer subsystem.

d) USB Device Layer subsystem.

- Provides the device layer services described in the U3 API. The device layer API services include receiving protocol messages to the host PC and relaying protocol messages between the physical communication layer subsystem and USB Services layer subsystem of the TOE.

e) USB Services Layer subsystem.

- Provides the service layer services described in the U3 API. This subsystem performs the USB Services layer API services and triggers the corresponding functions in the Service Implementation subsystem.

f) Service Implementation subsystem.

- Implements all API commands defined in the U3 Specification as supported by the USB Services layer subsystem. This subsystem interacts with the USB Services layer subsystem and the Hardware subsystem. The essential SFR-enforcing functionalities implemented in the subsystem are secure

sessions, user authentication, access control, security management and secure start-up of the TOE.

2.4 Clarification of Scope

19 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]). The scope of the evaluation includes only the SanDisk Cruzer Enterprise USB storage device. An evaluation copy of the CMC server software, which can securely administer the TOE, may be included on a CD with the TOE. The CMC server software provides a valid interface to the TOE, but is not included in the evaluation. This interface has been included in the independent testing. The TOE is also a U3 capable device and therefore supports a subset of the U3 Device API – there is currently no publicly available SDK for the TOE and the evaluators tested the APIs using an older U3 Device API SDK. Due to hardware differences between the TOE and other U3 devices, the evaluators were unable to exercise login and logout related functions via the API.

2.4.1 Evaluated Functionality

20 The TOE provides the following evaluated security functionality:

Table 2 SanDisk Cruzer Enterprise FIPS Edition Security Features

Security Function	Description
Cryptography	256-bit AES keys are generated on the device. The cryptographic key is never exported from the TOE. Data decryption is dynamic. Only the file required by the host PC is decrypted and sent to the PC. The device also implements secure hashing for password verification and AES key generation using SHA-1. SHA-1 is also used for storing the reference authentication data in an irreversible way. Verification of 1024-bit RSA digital signatures is implemented to establish a secure channel between the TOE and CMC software and for verifying the authenticity of firmware upgrades.
Protection of secrets	The secrets – cryptographic keys and reference authentication data – persistently stored on the device are protected physically and logically from any unauthorised modification and disclosure deemed as violations of the integrity and confidentiality of those secrets.
Authentication and access control	The user of the host PC is authenticated prior to access being granted to the software running on the host PC to access the encrypted data persistently stored on the device. The device maintains authentication and lifecycle states on which are based the granting and denying of access requests to protected

Security Function	Description
	data. The authentication state is set upon each successful authentication and cleared upon a logout command and when the device is powered up. The lifecycle state is determined by the existence of a root key: if the root key does not exist, the TOE is not initialised and is in the initialisation state. If the root key exists, the TOE is in the operational state. If the user is not successfully authenticated or if the TOE is in a Lockdown state, all access requests to the data stored on the device are denied. TOE initialisation, including the generation of the AES key, is only allowed if the user is not currently logged in to the TOE.
Password security	Authentication is based on a password that the owner of the device creates during initialisation of the device. Each time the device is inserted into a USB slot, the USB Start-up window appears and once the start-up is complete, a Login Device Window appears for the user to enter the password. The entered password is sent to the USB Token where TOE software compares it to the stored reference password. Depending on the comparison result the authentication state is set, or the counter keeping track of the number of consecutive authentication failures is incremented. The counter (NOA – Number of Attempts) is used for determining a possible password guessing attack. If the password is known to the user, it can at any time be changed through the Cruzer Enterprise Settings dialogue. A lost or forgotten password cannot be recovered and either external management software is needed to reset the password or the device has to be reformatted and re-initialised. In the latter case, all data previously stored on the TOE is lost.
Lock-down mode	The Cruzer Enterprise maintains a counter of consecutive, failed authentication attempts - NOA. If that number exceeds a pre-set threshold (MAXNOA – the maximum number of attempts), the TOE enters a Lockdown mode in which all access requests are blocked. If the TOE is in Lockdown mode, the only way to recover the TOE is to reformat and re-initialise the device in which case all data previously stored on the TOE is lost.
Secure access	The CMC Software can be used for securely administering the TOE. The legitimacy and authenticity of the CMC Software can be established by the TOE and access to the TOE restricted only

Security Function	Description
	to a legitimate CMC instance. On registration with the CMC instance, the TOE stores a public key issued by the CMC. This key is used to verify the authenticity of the CMC instance and to establish a trusted channel between itself and the valid CMC instance. If the managed TOE is not able to authenticate to its CMC instance, it will not allow the user to authenticate. Alternatively an SDK is available from SanDisk for customers to develop their own management software. The SDK uses the same mechanism (described above) to allow managed TOE instances to verify the authenticity of the management software.
Secure firmware upgrade	The Cruzer Enterprise implements a mechanism for firmware upgrading, and ensures that only authentic upgrades are implemented on the device. An authentic upgrade can be detected by verifying the digital signature attached to the upgrade. Only upgrades signed by SanDisk are deemed authentic. Firmware updates are self-installing executables that may be installed manually (in the case of an unmanaged TOE) or pushed to each managed TOE by the CMC management software. No firmware upgrades were available at the time of testing and changing the firmware revision will cause the device to be outside of the evaluated configuration.

2.4.2 Non-evaluated Functionality

21 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 ICT Security Manual (ISM) (Ref [2]) 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).

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

a) Computing platform hardware;

b) Microsoft Windows operating systems;

c) CMC Server software; and

d) Firmware upgrades

2.5 Usage

2.5.1 Evaluated Configuration

23 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration. Australian Government users should refer to the ISM (Ref [2]) for guidance on Australian Government policy requirements. New Zealand Government users should consult the GCSB.

24 The evaluated configuration of the TOE is based on the default installation of the TOE. The host PC must run the operating system platform that controls the USB interface. The operating system platforms supported are

- Microsoft Windows 2000 SP4 or higher,
- Microsoft Windows XP SP1 or higher,
- Microsoft Windows XP 64-bit SP1,
- Microsoft Windows 2000 Server,
- Microsoft Windows 2003 Server (Standard and Enterprise editions), and
- Windows Vista (all editions).

25 A USB 2.0 port is required for Microsoft Windows 2000 users without administrative privileges. Additionally, some administrative features of the TOE are only available in the presence of the SanDisk CMC server software. The CMC Software is not part of the TOE but the TOE implements features to authenticate the CMC Software and establish a trusted channel between itself and legitimate CMC Software.

2.5.2 Delivery procedures

26 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product.

27 Each final package that a customer receives consists of the USB storage device. ModusLink, which provides supply chain and inventory management solutions, packs twenty final packages into a carton, seals the carton and puts it into inventory storage. The Distributors, which are SanDisk Enterprise customers, keep inventory for Value Added Reseller (VAR) orders and fulfils an order based on the quantity required. If the order is not a multiple of 20, the Distributors can open the sealed carton to fulfil that order. The evaluated product must be ordered in multiples of 20 units to ensure that tamper evidence is preserved throughout the distribution and delivery process.

28 The VAR purchases devices from the Distributors according to the end customer orders, but does not keep inventory. The end customer receives the products from the VAR.

2.5.3 Determining the Evaluated Configuration

29 Upon receiving a sealed pack of twenty, the administrator must inspect the sealing of the packaging. If any of the sealed tape is damaged, if the carton is damaged or if there is any other physical evidence of possible tampering or accidental damage with the package, the products must be rejected and returned to the VAR.

30 The evaluated product is verified by examination of the casing, which should have "Cruzer Enterprise FIPS Edition" printed on it, the size of the USB storage device engraved on a metal plate, and 'SanDisk' printed on the cap. The user will also have to initialise the TOE (by supplying a password for the storage encryption) and check that the firmware version matches version 6.612 or version 6.615. The part number must include CZ32 e.g.SDCZ32-001G. Part numbers containing CZ22 are for the non-FIPS edition Cruzer Enterprise product. The firmware version may also be confirmed via U3 API calls without the need to initialise the device or authenticate to the device.

31 On receipt of a box of 20 TOEs, the administrator may choose to open the case on a random TOE to check for tampering in transit i.e. check for additional components such as a USB logger.

2.5.4 Documentation

32 It is important that the TOE is used in accordance with guidance documentation in order to ensure its secure usage. The following documentation is provided with the TOE:

a) Cruzer Enterprise USB Driver User Guide, revision 1.0, May 2007 (Ref [3])

b) Cruzer Enterprise CMC User Guide, revision 2.1, January 2008 (Ref [4])

c) Cruzer Enterprise CMC Setup and Deployment Guide, revision 2.1, January 2008 (Ref [5])

2.5.5 Secure Usage

33 The evaluation of the TOE did not take into account any assumptions about its operational environment.

34 The TOE assists in meeting the following organisational security policies (OSP):

Table 3 Organisational Security Policies

OSP Identifier	OSP Description
OSP.CMC	Administration and operation of the TOE is governed by a policy that states the conditions under which the CMC software can be used for administering the TOE and that no other software can be used for administering it. The CMC software must reside in a host PC that is operated by trusted administrators in secure premises that prevents physical

OSP Identifier	OSP Description
	access by parties other than the administrators. The host PC of the CMC software should not be connected to public networks. If it is then the administrator must ensure that illegitimate access through the network to the host PC and to the software residing on it are prevented.
OSP.INIT	Initialisation of the TOE is governed by a policy that states the criterion for trustworthiness to the host PCs on which the TOE may be initialised. The TOE initialisation must take place in a trusted host PC not connected to any network. The trustworthiness of the host PC must be asserted by it residing in physically secure premises and only administered by trustworthy administrators. An administrator must be present and supervise each TOE initialisation taking place using the host PC.
OSP.CERT	The issuance of firmware upgrades is governed by a policy stating the requirements for trustworthiness of the signature keys, signature computation for the upgrades, and issuance of public key certificates for the upgrade issuing authority. The public key certificates should be valid X.509 (or equivalent) certificates and represent signing keys of RSA with at least 512bit keys or other algorithms with at least similar theoretical strength than RSA with 512bit keys. The organisation using the TOE must identify trustworthy certification authorities and ensure that each public key certificate is produced by a trusted certification authority.

Chapter 3 - Evaluation

3.1 Overview

35 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

36 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation (Refs [6], [7], [8]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) (Ref [9]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [10], [11], [12], [13]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [14]) were also upheld.

3.3 Functional Testing

37 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed 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 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. The developers confirmed that the actual test results were consistent with the expected test results.

3.4 Penetration Testing

38 Penetration testing was conducted based on an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description, implementation representation as well as available public information. The evaluators used these tests 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 testing:

a) Time taken to identify and exploit;

b) Specialist technical expertise required;

c) Knowledge of the TOE design and operation;

d) Window of opportunity; and

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

39 The analysis conducted by the evaluators and the subsequent testing effort indicated that the TOE will resist an attacker with a Basic attack potential. This is consistent with the requirements of the EAL 2+ assurance level.

Chapter 4 - Certification

4.1 Overview

40 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

41 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report (Ref [15]), the Australasian Certification Authority certifies the evaluation of Cruzer Enterprise FIPS Edition performed by the Australasian Information Security Evaluation Facility, stratsec.

42 stratsec has found that Cruzer Enterprise FIPS Edition upholds the claims made in the Security Target (Ref [1]) and has met the requirements of Common Criteria (CC) evaluation assurance level EAL2+.

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

4.3 Assurance Level Information

44 EAL2 provides assurance by a full security target and an analysis of the security functions 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.

45 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results and an independent vulnerability analysis demonstrating resistance to penetration attackers with a Basic attack potential.

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

4.4 Recommendations

47 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 the ISM (Ref [2]) and New Zealand Government users should consult the GCSB.

48 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [16]), the ACA also recommends that users:

a) order the TOE only in multiples of 20 units to ensure that tamper evidence is maintained during the delivery process;

b) ensure that critical or important data in the TOE is backed up to prevent data loss if the TOE is re-initialised; and

c) have suitably qualified personnel examine the internals of the device for evidence of tampering, if the TOE has been out of the user's control for a significant period of time or if tampering is suspected.

Annex A - References and Abbreviations

A.1 References

[1] SanDisk Cruzer Enterprise FIPS edition Security Target EAL2 Augmented with ALC_FLR.1 version 1.1, 24 September 2009

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

[3] Cruzer Enterprise USB Drive. User Guide, Revision 1.0. Document No. UG-CRE-0507-14. SanDisk Corporation, May 2007.

[4] Cruzer Enterprise CMC User Guide, Revision 2.1. Document number UG-CMC-0807-21. SanDisk Corporation, January 2008.

[5] Cruzer Enterprise CMC Setup and deployment Guide, Revision 2.1. Document number IG-CMC-0807-22. SanDisk Corporation, January 2008.

[6] 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 2008-05-29

[7] 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 2008-05-29

[8] 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 2008-05-29

[9] Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 2 September 2007, CCMB-2007-09-004 Incorporated with interpretations as of 2008-05-29

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

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

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

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

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

[15] Evaluation Technical Report for SanDisk Cruzer Enterprise FIPS Edition Firmware v6.612/v6.615, version 1.1, 16 September 2009.

[16] SanDisk Cruzer Enterprise FIPS edition Assurance class AGD: Guidance documents EAL2 augmented with ALC_FLR.1 version 1.0, August 2009

A.2 Abbreviations

ACA	Australasian Certification Authority
AES	Advanced Encryption Standard
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ALC	Assurance: Life-cycle
API	Application Programming Interface
CC	Common Criteria
CCMB	Common Criteria Maintenance Board
CD-ROM	Compact Disk – Read Only Memory
CEM	Common Evaluation Methodology
CMC	Central Management and Control
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
FLR	Flaw Remediation
GCSB	Government Communications Security Bureau
ISM	Information Security Manual
MAXNOA	Max Number Of Attempts
NOA	Number Of Attempts
OSP	TOE Organisational Security Policy
RSA	Rivest, Shamir, Adleman (cryptographic algorithm)
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
U3	U3 LLC, Redwood City CA (USB auto-boot protocol)
USB	Universal Serial Bus
VAR	Value Added Reseller