C051 Certification Report

ST3 Ace (ST3 Ace Token Manager v1.0.13.927, ST3 Ace Middleware v1.0.13.910, and SecureCOS Firmware v5.2)

File name: ISCB-5-RPT-C051-CR-v1a
Version: v1a
Date of document: 20 December 2013
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
T +603 8992 6888
F +603 8992 6841
H 1 300 88 2999

Corporate Office:
Level 5, Sapura@Mines
No 7, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.

www.cybersecurity.my

C051 Certification Report

ST3 Ace (ST3 Ace Token Manager v1.0.13.927, ST3 Ace Middleware v1.0.13.910, and SecureCOS Firmware v5.2)

20 December 2013

ISCB Department

CyberSecurity Malaysia

Level 5, Sapura@Mines,

No 3 Jalan Tasik, The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

Tel: +603 8992 6888 □Fax: +603 8992 6841

http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C051 Certification Report – ST3 Ace (ST3 Ace Token Manager v1.0.13.927, ST3 Ace Middleware v1.0.13.910, and SecureCOS Firmware v5.2)
DOCUMENT REFERENCE:	ISCB-5-RPT-C051-CR-v1a
ISSUE:	v1a
DATE:	20 December 2013

DISTRIBUTION:	UNCONTROLLED COPY - FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Level 5, Sapura@Mines,

No 3 Jalan Tasik,

The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Foreword

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme has been 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 MyCB 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 20 December 2012, 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 and the Common Criteria Portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

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 4 (Ref [3]), for conformance to the Common Criteria for IT Security Evaluation, version 3.1 revision 4 (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	10 December 2013	All	Final released.
v1a	20 December 2013	Page iv	Add the date of the certificate.

Executive Summary

ST3 Ace (ST3 Ace Token Manager v1.0.13.927, ST3 Ace Middleware v1.0.13.910, and SecureCOS Firmware v5.2) (hereafter referred as ST3 Ace) from SecureMetric Technology Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level 2 (EAL2) evaluation.

The TOE provides secure storage to store digital certificate(s) and cryptographic keys. The ST3 Ace follows the PKCS#11 standard and implements authentication via PIN to prevent unauthorised access to the token.

The TOE is comprised of the three following core components of the ST3 Ace product:

a) **SecureCOS Operating System**: The operating system (firmware) embedded in a microprocessor smart chip based USB token. The firmware provides the core cryptographic functionality of the TOE.

b) **ST3 Ace Middleware**: Two compiled binaries that utilise exported APIs to provide an interface to the core cryptographic security functionality of the TOE, providing developers with an easily accessible method for engaging PKI-related functionality to support the development of enterprise authentication and integrity solutions.

c) **ST3 Ace Token Manager**: The TOE provides an application for the user to manage the cryptographic key security of the TOE.

The middleware and Token Manager are installed on a host computer for third party application to communicate with SecureCOS and provides key security functionality of the TOE.

The scope of evaluation covers major security functions described as below:

a) **Cryptographic Operations**: The TOE provides cryptographic library, which includes 3DES, RSA, MD5 and SHA-1, for cryptographic operations that can be used by third party applications such as encryption and decryption of email. The third party applications are outside the TOE evaluation scope. The TOE also provides the functionality to digitally sign documents and files.

b) **User Authentication**: The TOE allows authorised users to access the TOE once the user is successfully identified and authenticated by the TOE. TOE user has to provide correct user PIN in order to access to TOE. The TOE enforces token blocking after 6 failed authentication attempts and Security Officer (SO) PIN is needed to unblock the token and reset the user PIN.

   The integration with the Token Management System Registration Authority (TMS RA) will allow a user to unblock the TOE and reset the User PIN without to deliver the physical token to the token management team. However, Secure Code is required in order to submit the unblock request or reset user PIN via TMS RA. TMS RA is outside the scope of the evaluation.

c) **Security Management**: The TOE provides management functions such as token management (name change, PIN change, unblock token) and object management (view object, export/import object).

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for TOE, the security function requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Prospective consumers are advised to verify that their operating environment is consistent with the evaluated configuration, 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 ST3 Ace to the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2). This report confirms that 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 BAE Systems Detica evaluation facility (the 'Detica MySEF') and was completed on 26 November 2013.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangements on the Recognition of Common Criteria certificates and the product will be listed in the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc and the Common Criteria portal (the official website of the Common Criteria Recognition Arrangement) at www.commoncriteriaportal.org.

It is the responsibility of the user to ensure that ST3 Ace meets their requirements. It is recommended that a potential user of ST3 Ace to refer to the Security Target (Ref [6]) and this Certification report prior to deciding whether to purchase the product.

Table of Contents

1 Target of Evaluation 1

1.1 TOE Description 1
1.2 TOE Identification 2
1.3 Security Policy 3
1.4 TOE Architecture 3
1.4.1 Logical Boundaries 3
1.4.2 Physical Boundaries 4
1.5 Clarification of Scope 5
1.6 Assumptions 5
1.6.1 Usage assumptions 5
1.6.2 Environment assumptions 6
1.7 Evaluated Configuration 6
1.8 Delivery Procedures 6
1.9 Documentation 6

2 Evaluation 8

2.1 Evaluation Analysis Activities 8
2.1.1 Life-cycle support 8
2.1.2 Development 8
2.1.3 Guidance documents 8
2.1.4 IT Product Testing 9

3 Result of the Evaluation 13

3.1 Assurance Level Information 13
3.2 Recommendation 13

Annex A References 14

A.1 References 14
A.2 Terminology 14
A.2.1 Acronyms 14

A.2.2 Glossary of Terms 15

Index of Tables

Table 1: TOE identification 2
Table 2: Independent Functional Testing 9
Table 3: List of Acronyms 14
Table 4: Glossary of Terms 15

Index of Figures

Figure 1: TOE components 4

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), ST3 Ace (ST3 Ace Token Manager v1.0.13.927, ST3 Ace Middleware v1.0.13.910, and SecureCOS Firmware v5.2) (hereafter referred as ST3 Ace) is a PKI-related security solutions that provides secure storage to store digital certificate(s) and cryptographic keys. ST3 Ace follows PKCS#11 standard and implements authentication via PIN to prevent unauthorised access to the token.

2 The TOE is comprised of three main components of the ST3 Ace product as below:

a) **SecureCOS Operating System:** The operating system (firmware) embedded in a microprocessor smart chip based USB token. It provides the core cryptographic functionality of the TOE.

b) **ST3 Ace Middleware:** Two compiled binaries that utilise exported APIs to provide an interface to the core cryptographic security functionality of the TOE, providing developers with an easily accessible method for engaging PKI-related functionality to support the development of enterprise authentication and integrity solutions.

c) **ST3 Ace Token Manager:** This component provides an application interface for the user to manage the cryptographic key security of the TOE and perform functions such as changing User PINs and Certificate Management such as view, import, export, unblock token, deletion, renewal of certificate.

The middleware and Token Manager are installed on a host computer for third party application to communicate with SecureCOS and provides key security functionality of the TOE.

3 The scope of evaluation covers major security functions described as below:

a) **Cryptographic Operations**: The TOE provides cryptographic library, which includes 3DES, RSA, MD5 and SHA-1, for cryptographic operations that can be used by third party applications such as encryption and decryption of email. The third party applications are outside the TOE evaluation scope. The TOE also provides the functionality to digitally sign documents and files.

b) **User Authentication**: The TOE allows authorised users to access the TOE once the user is successfully identified and authenticated by the TOE. TOE user has to provide correct user PIN in order to access to TOE. The TOE enforces token blocking after 6 failed authentication attempts and Security Officer (SO) PIN is needed to unblock the token and reset the user PIN.

The integration with the Token Management System Registration Authority (TMS RA) will allow a user to unblock the TOE and reset the User PIN without to deliver the physical token to the token management team. However, Secure Code is required in order to submit the unblock request or reset user PIN request to TMS RA. TMS RA is outside the scope of the evaluation.

c) **Security Management**: The TOE provides management functions such as token management (name change, PIN change, unblock token) and object management (view object, export/import object).

1.2 TOE Identification

4 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	C051
TOE Name	ST3 Ace
TOE Version	The TOE is consist of three components: • ST3 Ace Token manager (V1.0.13.927), • ST3 Ace Middleware (v1.0.13.910), and • ST3 Ace SecureCOS Firmware (v5.2)
Security Target Title	ST3 Ace Security Target
Security Target Version	1.1
Security Target Date	21 November 2013
Assurance Level	Evaluation Assurance Level 2 (EAL 2)
Criteria	Common Criteria for Information Technology Security Evaluation, September 2012, version 3.1 Revision 4 (Ref [2])
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation , September 2012, version 3.1 Revision 4 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 conformant CC Part 3 conformant Package conformant to EAL 2
Sponsor and Developer	SecureMetric Technology Sdn Bhd 2-2, Incubator 2, Technology Park Malaysia, Lebuhraya Sg. Besi – Puchong, Bukit Jalil, Kuala Lumpur, 57000 Malaysia
Evaluation Facility	Detica MySEF

1.3 Security Policy

5 The security policy of the TOE is expressed by the set of security functional requirements which may be found in Section 5.2 of the ST (Ref [6]).

1.4 TOE Architecture

6 The TOE includes both logical and physical boundaries which are described in Section 1.6 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

7 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 Operation**

The TOE provides key generation for RSA and 3DES. The TOE also performs key destruction by overwriting the memory space of the keys. This function overwrites the previous keys when the user deletes the expired certificate(s) and key(s).

The TOE performs RSA, 3DES, SHA-1 and MD5 operations. These operations are used by applications on the host system. The applications must comply with PKCS#11 and CSP standards and use the middleware of the TOE to access these functionalities provided by the TOE. The applications on the host system are outside the scope of this evaluation.

b) **User Authentication**

The TOE requires each user is successfully identified and authenticated before any interaction with protected resources is permitted. User of the TOE can authenticate to the TOE through the Token Manager application, which is outside the scope of evaluation. The Token Manager provides an interface to access management functions.

Users and the security officer must authenticate themselves to the TOE using their PINs. They will be allowed access to the TOE functions and resources after a successful authentication. The TOE maintains the status of user authentication by changing the authenticity value of a user to true if the Security Officer or user is successfully authenticated. The default value of the authenticity value is always false.

If the authentication fails more than 6 authentication attempts,, the access to the token will be blocked. Only the SO PIN is able to unblock a token. When this happens, the TOE will prevent all access to the TOE and TOE functionality. To unblock the token, the user must request a Secure Code from Token Management System Registration Authority (TMS RA). The TMS RA will send a Secure Code to user's registered mobile phone via SMS. On the Token Manager platform, the user must enter the Secure Code in order to decrypt the SO PIN.

The SO PIN is used at the back-end process to unblock a token for the user. The Token Manager unblocks the token by calling PKCS#11 C_InitPIN function.

c) **Security Management**

The TOE provides functions that allow management of the TOE and its security functions. The TOE maintains two (2) distinct roles to ensure that functions are restricted to those who have the privilege to access them: User and Security Officer (SO). The list below describes the management functions available to user and Security Officer:

i) token with default passwords (Security Officer);

ii) changing of user PIN (user);

iii) unblock token (Security Officer) – Secure Code is used to decrypt SO PIN; and

iv) import, export, delete digital certificate, enrolment and renewal (user).

1.4.2 Physical Boundaries

8 The TOE is comprised of the ST3 Ace operating system SecureCOS, the ST3 Ace middleware and the ST3 Ace Token Manager. SecureCOS is embedded into the memory of the secure microprocessor smart chip-based USB token. The middleware and the Token Manager are installed onto a host computer for third party applications to communicate with SecureCOS and to manage the key security functionality of the TOE. The TOE components are shown in Figure 1 below.

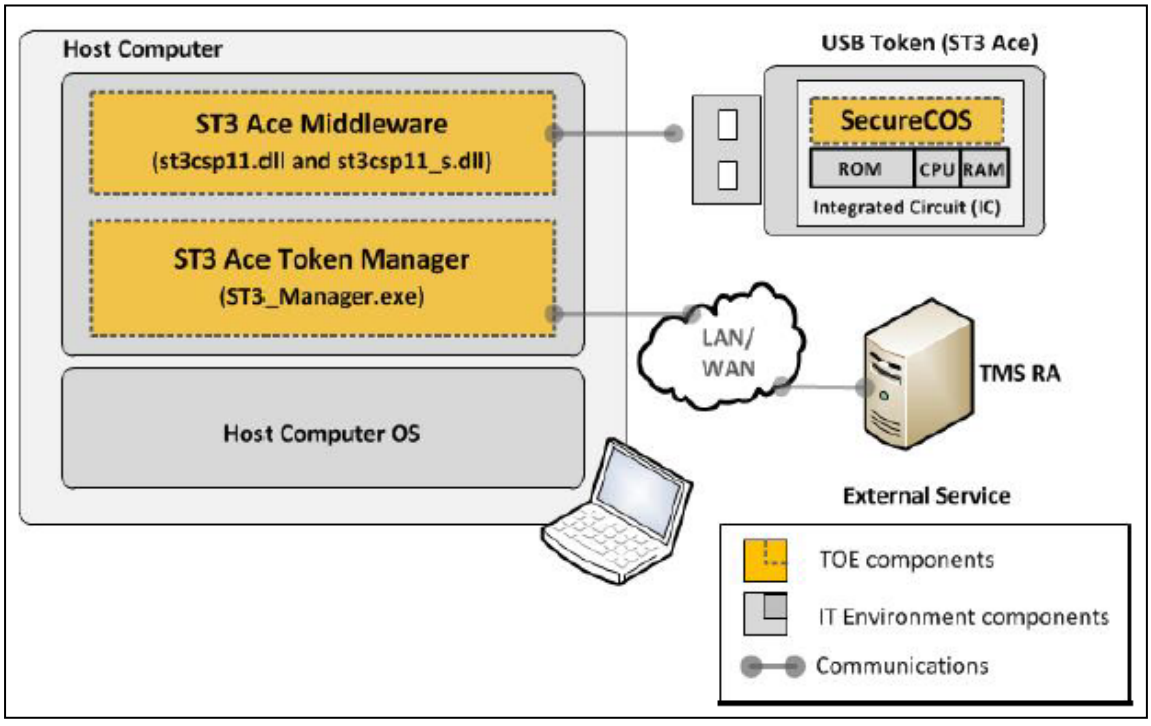

Figure 1: TOE components

9 The TOE is comprised of three main components of the ST3 Ace product as below:

a) **SecureCOS Operating System:** The operating system (firmware) embedded in a microprocessor smart chip based USB token. It provides the core cryptographic functionality of the TOE.

b) **ST3 Ace Middleware:** Two compiled binaries that utilise exported APIs to provide an interface to the core cryptographic security functionality of the TOE, providing developers with an easily accessible method for engaging PKI-related functionality to support the development of enterprise authentication and integrity solutions.

c) **ST3 Ace Token Manager:** This component provides an application interface for the user to manage the cryptographic key security of the TOE and perform functions such as changing User PINs and Certificate Management such as view, import, export, unblock token, deletion, renewal of certificate.

10 The integration with the Token Management System Registration Authority (TMS RA) will allow a user to unblock the TOE and reset the User PIN, without the need to deliver the physical token to the token management team. This function must first be enabled via the TMS RA by the token manager. TMS RA is outside the scope of this evaluation.

1.5 Clarification of Scope

11 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures in accordance with the guidance documentation that is supplied with the product.

12 Section 1.4 of this document described the scope of the evaluation which was limited to those claimed made in the Security Target (Ref [6]). Other components of ST3 Ace which includes the underlying hardware, operating system of the host, and other applications on the host specified in Section 1.5.3 of the Security Target (Ref [6]) are not part of TOE scope.

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

1.6 Assumptions

14 This section summarises the security aspects of the environment/configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and the requirements for secure operation of the TOE which is defined in subsequent sections and in the Security Target (Ref [6]).

1.6.1 Usage assumptions

15 The following is the assumption of the TOE usage that is required to ensure the security of the TOE:

a) The TOE user is not careless, wilfully negligent or hostile and possesses the necessarily privileges to access the information managed by the TOE.

1.6.2 Environment assumptions

16 The following is the assumption of the TOE environment that is required to ensure the security of the TOE:

a) The communication between the host computer and TOE is established correctly. It is also important to ensure that the host whereby the TOE is installed is configured correctly, patches and hardened to protect against unauthorised access, modification and deletion of TOE data.

1.7 Evaluated Configuration

17 The TOE is software that executes on a USB token (SecureCOS) and host computer (middleware and Token Manager). The underlying hardware and software that are used to support the TOE are listed on Section 1.5.3 of the Security Target (Ref [6]).

18 The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented preparative user guidance (Ref 22a)).

1.8 Delivery Procedures

19 ST3 Ace is delivered to the customer by SecureMetric Technology Sdn Bhd personnel using delivery procedures (Ref 21b)) to ensure that the TOE is securely transferred to respected customer. Before the TOE being delivered to the intended client, there are some steps need to be performed by the SecureMetric personnel as below:

a) Software installation including the TOE (Ref 22a)) and the underlying platform are installed based on the software/hardware specification.

b) The default PIN is created by the Security Officer at the TMS RA Server during initialisation and token registration.

c) Schedule is given out, via email or phone call, to end-user regarding the delivery of the TOE so that end-user will know when the TOE is expected to be delivered by representative of SecureMetric.

1.9 Documentation

20 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage of the product.

21 The following documentation is provided by the developer to the end user as guidance to ensure secure operation, and delivery of the product:

a) ST3 Ace: Token Manager User Guide, version 1.1, 17 October 2013

b) ST3 Ace: Lifecycle Documentation, version 1.2, 21 November 2013

c) ST3 Ace Guidance Documentation , version 1.2, 25 November 2013

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

a) ST3 Ace Installation Guide, version 1.0, September 2013

2 Evaluation

23 The evaluation was conducted in accordance with the requirements of the Common Criteria, version 3.1 Revision 4 (Ref [2]) and the Common Methodology for IT Security Evaluation (CEM), version 3.1 Revision 4 (Ref [3]). The evaluation was conducted at Evaluation Assurance Level 2 (EAL2). 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

24 The evaluation activities involved a structured evaluation of the TOE, including the following components:

2.1.1 Life-cycle support

25 An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the configuration items were clearly and uniquely labelled. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

26 The evaluators examined the lifecycle documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

2.1.2 Development

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

28 The evaluators examined the TOE design specification; they determined that the structure of the entire TOE is described in terms of subsystems. They also determined that, it provides a complete, accurate, and high-level description of the SFR-enforcing behaviour of the SFR-enforcing subsystems.

29 The evaluators examined the TOE security architecture description; they determined that the information provided in the evidence is presented at a level of detail commensurate with the descriptions of the SFR-enforcing abstractions contained in the functional specification and TOE design.

2.1.3 Guidance documents

30 The evaluators examined the TOE 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

31 Testing at EAL2 consists of assessing developer tests, perform independent function test, and perform penetration tests. The TOE testing was conducted by evaluators from Detica MySEF at BAE Systems Detica MySEF Lab, Kuala Lumpur. The detailed testing activities, including configurations, procedures, test cases, expected results and actual results are documented in a separate Test Plan Reports.

2.1.4.1 Assessment of Developer Tests

32 The evaluators verified that the developer has met their testing responsibilities by examining their test plans, and reviewing their test results, as documented in the Evaluation Technical Report (Ref [7]) (not a public document because it contains information proprietary to the developer and/or the evaluator).

33 The evaluators analysed the developer's test coverage and found them to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the interfaces in the functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

34 Independent functional testing is the evaluation conducted by evaluator based on the information gathered by examining design and guidance documentation, examining developer's test documentation, executing a sample of the developer's test plan, and creating test cases that augmented the developer tests.

35 The results of the independent test developed and performed by the evaluators to verify the TOE functionality are as follows.

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
To verify that the TOE generates TDES cryptographic key with key size of 128 bits that aligns with Annex E.4.1 of GP211	FCS_CKM.1a.1	CSP Interface	**PASS**. Result as expected.
To verify that the TOE generates RSA cryptographic key with key size of 1024 and 2048 bits that aligns with RSA PKCS#11	FCS_CKM.1b.1	PKCS#11 Interface	**PASS**. Result as expected.
To verify that the TOE overwrites the keys (e.g. RSA, TDES etc) as	FCS_CKM.4.1	CSP Interface	**PASS**. Result as

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
method of destroying them.			expected.
To verify that the TOE performs hashing using SHA-1 algorithm. These shall meet FIPS 180-2 standard.	FCS_COP.1c.1	CSP Interface	**PASS**. Result as expected.
To verify that the TOE shall perform hashing using MD5 algorithm. These shall meet FIPS 180-2 standard.	FCS_COP.1d.1	CSP Interface	**PASS**. Result as expected.
To verify that the TOE shall detect unsuccessful authentication upon 6 attempts when user enters their passphrase (PIN) to access security function.	FIA_AFL.1.1 FIA_AFL.1.2	• Token Manager Interface • PKCS#11 Interface • Memory Interface	**PASS**. Result as expected.
To verify that the TOE maintain the following list of security attributes belonging to individual users: • Token name • PIN • Certificate Name	FIA_ATD.1.1 FMT_SMR.1.1 FMT_SMR.1.2	• Token Manager Interface • PKCS#11 Interface • Memory Interface	**PASS**. Result as expected.
To verify that the TOE perform TDES encryption and decryption using TDES-CBC or TDES-ECB algorithm. The key sizes should match 112 bits for TDES 2 keys and 168 bits for TDES 3. These shall meet FIPS 46-3 standard.	FCS_COP.1a.1	• Token Manager Interface • PKCS#11 Interface • Memory Interface	**PASS**. Result as expected.
To verify that the TOE perform RSA encryption and decryption using RSA algorithm. The key sizes should match 1024 or 2048 bits. These shall meet RSA PKCS#11 standard.	FCS_COP.1b.1	• Token Manager Interface • PKCS#11 Interface • Memory Interface	**PASS**. Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
To verify that the TOE requires users to be successfully authenticated to enable TSF-mediated action.	FIA_UAU.2.1	• Token Manager Interface • PKCS#11 Interface • Memory Interface	**PASS**. Result as expected.
To verify that the TOE is capable of performing the following management functions: • Changing user PIN • Reset block status user • Import, export, delete digital certificate.	FMT_SMF.1.1 FMT_SMR.1.1 FMT_SMR.1.2	• Token Manager Interface • PKCS#11 Interface • Memory Interface	**PASS**. Result as expected.

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

2.1.4.3 Penetration Testing

37 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, functional specification, and TOE design and security architecture description.

38 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 (specialised expertise);

c) Knowledge of the TOE;

d) Window of opportunity; and

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

39 The penetration tests focused on USB packet sniffing to ensure that the TOE prevents an attacker from sniffing all the USB transactions at host controller.

40 The results of the penetration testing note that there is no residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated

configuration and in secure environment as specified in Section 1.5.3 of the Security Target (Ref [6]).

2.1.4.4 Testing Results

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

42 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

43 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 ST3 Ace performed by Detica MySEF.

44 Detica MySEF found that ST3 Ace upholds the claims made in the Security Target (Ref [6]) and supporting documentation, and has met the requirements of the Common Criteria (CC) Evaluation Assurance Level 2 (EAL2).

45 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

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

47 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.

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

3.2 Recommendation

49 In addition to ensure secure usage of the product, below are additional recommendations for ST3 Ace users:

a) The users of the TOE shall adhere to developer guidance provided with the TOE and alert with all security warning.

b) The underlying operating system and database server are patched and hardened to protect against known vulnerabilities and security configuration issues.

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 4, September 2012.

[3] The Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012.

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

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

[6] SecureMetric ST3 Ace Security Target, version 1.1, 21 November 2013

[7] Evaluation Technical Report SecureMetric ST3 Ace, version 2.1, 26 November 2013

A.2 Terminology

A.2.1 Acronyms

Table 3: 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
EAL	Evaluation Assurance Level
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardization
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

Acronym	Expanded Term
ST	Security Target
TOE	Target of Evaluation
TMS RA	Token Management System Registration Authority
TSF	TOE Security Function
TSFI	TOE Security Function Interface

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Authentication	It is information used to verify the claimed identity of a user.
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
Certifier	The certifier responsible for managing a specific certification task.
Cipher-block chaining (CBC)	In the cipher-block chaining (CBC) mode, each block of plaintext is XORed with the previous ciphertext block before being encrypted.
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Electronic codebook (ECB)	The message is divided into blocks and each block is encrypted separately.
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

Term	Definition and Source
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.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
FIPS 180-2	Federal Information Processing Standards Publications (FIPS PUBS) 180-2 are issued by the National Institute of Standards and Technology (NIST) for technical publication defining Secure Hash standards.
FIPS 46-3	Federal Information Processing Standards Publications (FIPS PUBS) 46-3 are issued by the National Institute of Standards and Technology (NIST) for technical publication defining Data Encryption standards.
GP211	Global Platform Card Specification – v2.1.1, March 2003.
Integrated circuit (IC)	Electronic component(s) designed to perform processing and/or memory functions.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.
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.
MD5	MD5 (Message-Digest algorithm 5) is a cryptographic hash function with a 128-bit hash value.
Personalisation	The process by which personal data are brought into the TOE before it is handed to the card holder.
PIN	A numeric password shared between a user and a system that can be used for user authentication.
PKCS#11	The first in the Public-Key Cryptography Standards (PKCS) library published by RSA Laboratories. It provides the basic definitions of, and recommendations for, implementing the RSA algorithm for public-key cryptography.
RSA	An algorithm for public-key cryptography published by RSA Laboratories.
SecureCode	Unique code is sent through to the user's registered mobile number that will be used to decrypt the SO PIN for the user to unblock the token.

Term	Definition and Source
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
Security Officer (SO)	A user authorised to perform TOE personalisation, or other TOE Security Officer functions.
SHA-1	A cryptographic hash function designed by the National Security Agency (NSA) and published by the NIST as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm. It produces a 160-bit hash value.
Smart Card	A credit card sized chip card with embedded integrated circuits. Often used to store keys for authentication.
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.
TDES	A block cipher which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block.
TSF data	Data created by and for the TOE, that might affect the operation of the TOE
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
User data	Data created by and for the user that does not affect the operation of the TSF.

--- END OF DOCUMENT ---