CyberSecurity MALAYSIA
An agency under MOSTI

MOSTI
Ministry of Science,
Technology and Innovation

C037 Certification Report

Keyper Hardware Security Module (HSM) v2.0

File name: ISCB-5-RPT-C037-CR-v1a

Version: v1a

Date of document: 4 January 2013

Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)

T +603 8946 0999
F +603 8946 0888

Corporate Office:
Level 8, Block A
Mines Waterfront Business Park
No 3 Jalan Tasik, The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia.
www.cybersecurity.my

Securing Our Cyberspace

C037 Certification Report

Keyper Hardware Security Module (HSM) v2.0

4 January 2013

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:	C037 Certification Report – Keyper Hardware Security Module (HSM) v2.0
DOCUMENT REFERENCE:	ISCB-5-RPT-C037-CR-v1a
ISSUE:	v1a
DATE:	4 January 2013

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 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 4 January 2013, 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).

Reproduction of this report is authorised provided the report is reproduced in its entirety.

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	21 December 2012	All	Final Released
v1a	4 January 2013	Page iv	Add the date of the certificate.

Executive Summary

The Keyper Hardware Security Module (HSM) v2.0 from AEP Networks Ltd. is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 4 augmented with AVA_VAN.5 evaluation.

Keyper Hardware Security Module (HSM) v2.0 or the TOE is a dedicated hardware product which provides secure digital signature services, cryptographic services and key management services to applications that reside on physically separate host computer systems. The TOE is a secure module that is contained within an outer casing. The outer casing includes a Keypad, LCD screen, smart card reader and a number of external ports; they are out of the evaluation scope. The TOE is tamper reactive; and has been validated against the requirements for the FIPS PUB 140-2 at level 4. Keyper Hardware Security Module (HSM) v2.0 is intended for use in a dedicated network with devices and applications that make use of its cryptographic functions. Keyper Hardware Security Module (HSM) v2.0 should be provided appropriate physical and logical protections.

The TOE encompasses two models: AEP Keyper Enterprise (Hardware: 9720, Software: 011126) and AEP Keyper Professional (Hardware: 9720, Software: 010405). Both models share the same features and architecture (the only difference is performance), therefore both models shall be considered together. Two additional “High Availability” models also exist, however they are out of the scope of this evaluation.

The functions of the TOE that are within the scope of evaluation covering the secure key management, secure key storage, cryptographic operation, user authentication, access control for key management functions, auditing of security relevant events, self-test, tamper protection and management of the security functions.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for the TOE, the security functional 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 the TOE to the Common Criteria (CC) Evaluation Assurance Level 4 (EAL4) Augmented with AVA_VAN.5. The 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 the Stratsec.net Sdn Bhd (‘Stratsec’) evaluation facility (the ‘Stratsec MySEF’) and completed on 13 December 2012.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the TOE evaluation meets all the Arrangement 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 the Keyper Hardware Security Module (HSM) v2.0 meets their requirements. It is recommended that a potential user of the Keyper Hardware Security Module (HSM) v2.0 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 The Physical Boundaries 4

1.5 Clarification of Scope 4

1.6 Assumptions 5

1.6.1 Usage assumptions 5

1.6.2 Environmental assumptions 5

1.7 Evaluated Configuration 6

1.8 Delivery Procedures 6

1.9 Documentation 7

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 9

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 15

A.1 References 15

A.2 Terminology 15

A.2.1 Acronyms 15

A.2.2 Glossary of Terms 16

Index of Tables

Table 1: TOE identification 2
Table 2: Independent Functional Testing 10
Table 3: List of Acronyms 15
Table 4: Glossary of Terms 16

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), Keyper Hardware Security Module (HSM) v2.0 is a hardware-based and dedicated security device which generates, stores, protects and manages digital cryptographic keys.

2 The TOE encompasses two models: AEP Keyper Enterprise (Hardware: 9720, Software: 011126) and Professional (Hardware: 9720, Software: 010405). Both models share the same features and architecture (the only difference is performance), therefore both models shall be considered together. Two additional "High Availability" models also exist, however they are out of the scope of this evaluation.

3 The TOE communicates with applications on host computer systems through a standard network interface (100BASE-T Fast Ethernet). Host applications communicate with the TOE via an AEP produced 'Provider', which performs a similar function to a software driver. There are four 'Providers' (PKCS11 Provider, RSA Full Provider (MSCAPI), SChannel Provider (MSCAPI) and OpenSSL Provider) which may be selected based on host application requirements (note that the provider is not included in the scope of this evaluation).

4 The TOE is a secure module that is contained within an outer casing. The outer casing includes a Keypad, LCD screen, smart card reader and a number of external ports. The TOE is tamper reactive; and has been validated against the requirements for the FIPS PUB 140-2 at level 4. The device is intended for use in a dedicated network with devices and applications that make use of its cryptographic functions. The device should be provided appropriate physical and logical protections.

5 In addition to the Ethernet interface, the TOE provides interfaces for import/export of cryptographic keys via smartcards. Key management operations take place via a keypad/LCD and smart card reader. The TOE also implements a cryptographic policy that restricts specific roles to specific tasks associated with managing keys and the device.

6 The TOE is intended to be deployed as a core component of a critical enterprise cryptographic system where the generation, protection and management of cryptographic keys are all priorities. It can be deployed as part of any cryptographic system that uses digital keys. The keys are anticipated to be of high-value, therefore the TOE must provide a high-level of assurance in protection of the digital keys, that is, that there would be a significant negative impact if the keys were compromised.

7 In the context of the evaluation, the TOE is expected to provide the following major security features:

a) Secure generation, distribution and destruction of cryptographic keys.

b) Secure storage and management of keys throughout their lifecycle.

c) User authentication to facilitate controlled access to cryptographic key management and TOE management functions by trusted personnel only.

d) Security management to enable role-based management of the core functions of the TOE.

e) Access control for key management functions to ensure that only specified roles are permitted to perform defined tasks.

f) Auditing of security relevant events to provide suitable accountability.

g) Self-test of the core cryptographic functions and algorithms of the TOE.

h) Tamper protection to ensure that the TOE is adequately protected from unauthorised physical access.

1.2 TOE Identification

8 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	C037
TOE Name	Keyper Hardware Security Module (HSM) v2.0: a) Enterprise (Hardware: 9720, Software: 011126) b) Professional (Hardware: 9720, Software: 010405)
TOE Version	Version 2.0
Security Target Title	Security Target for the Keyper Hardware Security Module (HSM) v2.0
Security Target Version	v1.3
Security Target Date	13 December 2012
Assurance Level	Evaluation Assurance Level 4 augmented (EAL4+) with AVA_VAN.5
Criteria	Common Criteria for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3 (Ref [2])
Methodology	Common Evaluation Methodology for Information Technology Security Evaluation, July 2009, 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 EAL4+ AVA_VAN.5
Sponsor and Developer	AEP Networks Ltd.

	Knaves Beech Business Centre Loudwater, Buckinghamshire HP10 9UT United Kingdom Tel: +44 1628 642 600 Fax: +44 1628 642 605
Evaluation Facility	Stratsec MySEF

1.3 Security Policy

9 Keyper Hardware Security Module (HSM) v2.0 implements a cryptographic operations and key management security policy to manage cryptographic key generation, archiving, recovery and destruction.

10 The details of the security policy are described in Sections 5 and 7 of the Security Target (Ref [6]).

1.4 TOE Architecture

11 Keyper Hardware Security Module (HSM) v2.0 includes both logical and physical boundaries which are described in detail Section 1.7 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

12 Keyper firmware includes the Keyper HSM Application, support libraries and other components, the operating environment, and a set of hardware drivers. The details of Keyper firmware components are described in Section 1.7.2 of the Security Target (Ref [6]).

13 The Keyper HSM Application (along with Keyper hardware components) implements and controls the security features listed below:

a) **Secure key management** – The TOE provides the means to generate and manage cryptographic keys for use with its various cryptographic functions.

b) **Secure key storage** – the TOE provide the means to securely store sensitive cryptographic keys, using a dedicated hardware device and tamper mechanisms.

c) **Cryptographic operations** – The TOE implements several cryptographic algorithms in hardware and software. These algorithms are used internally by the TOE and are also provided to users by the HSM Crypto Manager. The TOE implements asymmetric and symmetric encryption algorithms, key generation algorithms and cryptographic checksum algorithms and offers functions for data signing, encryption, secure storage and integrity checking.

d) **User authentication** – The TOE provides a mechanism for secure authentication using smart cards.

e) **Security management** – The TOE implements a set of functions and mechanisms to securely manage the TSF and TSF data.

f) **Access control** – The TOE implements two statically defined roles that are used primarily for segmenting access control. Each role has statically defined access to certain functions. Assumption of a role requires multiple smart card authentications.

g) **Auditing** – The TOE logs significant events to an internal audit log with at minimum a timestamp and error code.

h) **Self-test** – The TOE implements a set of self-tests that verify the TOE's hardware components, cryptographic algorithms, random number generator and firmware integrity.

i) **Tamper protection** – The TOE includes inbuilt tamper detection mechanisms that trigger tamper response mechanisms which wipe sensitive data and transition the TOE to a secure tamper state. An inbuilt battery allows the TOE to detect and react to tampers even when mains power is lost.

1.4.2 The Physical Boundaries

14 The TOE is a hardware module with a tamper resistant casing installed within a small standalone desktop unit. The physical TOE boundary includes the tamper reactive mesh casing, which surrounds the secure module. The keypad, LCD display, smartcard reader and miscellaneous external circuitry are excluded from the physical scope.

15 The physical scope of the TOE includes the Keyper firmware and configuration data which are stored in the TOE's FLASH memory.

16 The details of TOE physical scope are described in Section 1.7.1 of the Security Target (Ref [6]).

1.5 Clarification of Scope

17 The TOE provides a level of protection that is appropriate for an assumed non-hostile and well-managed user community in accordance with administrator guidance that is supplied with the product. While the TOE is designed to protect its user community against deliberate and pre-planned attempts to breach system security, it is not intended for situations in which determined attempts by hostile insiders use sophisticated attacks from within the physical zone, nor could it provide complete protection against authorised user intentionally or carelessly disclosing the secret information under their control.

18 Section 1.4 of this document described the scope of the evaluation which was limited to those claims made in the Security Target (Ref [6]).

19 It should be noted that the TOE is a hardware secure module with a tamper reactive casing installed within a small standalone desktop unit. 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.

1.6 Assumptions

20 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 that required for secure operation of the Keyper Hardware Security Module (HSM) v2.0 as defined in subsequent sections and in the Security Target Ref ([6]).

1.6.1 Usage assumptions

21 Assumptions for the TOE usage listed in the Security Target are:

a) The Certification-service-provider (CSP) reviews the audit trail generated and exported by the TOE. The client application receives and stores the audit trail of the TOE for review by the System auditor of the CSP according to the audit procedure of the CSP.

b) The client-application is assumed as user of the TOE in the Operator role. Other users authorised for the TOE Operator services may be not be known to the TOE itself. The TOE environment performs identification and authentication for theses individual users and allows successfully authenticated users to use the client application as their agent for the Operator services.

1.6.2 Environmental assumptions

22 Assumptions for the TOE environment listed in the Security Target are:

a) The TOE environment ensures the confidentiality, integrity and availability of their security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE.

b) The TOE environment ensures the availability of the backup data. Examples of these data are verification authentication data, cryptographic key material and documentation of TOE configuration data.

c) DTBS-representation submitted to the TOE is assumed to be correct. This requires that the DTBS (e.g. the certificate content data) has been initialised correctly and maintains this correctness until it is passed to the TOE. This requires the DTBS to be correctly defined during the registration process, be transferred with integrity protection between the systems involved in the process (e.g. registration and certificate generation), be processed in a correct way by the client application, being hashed correctly (in the case the hashing is done by the client application and not by the TOE) and passed correctly to the TOE.

The TOE environment will probably use its own mechanisms to ensure this correctness during processing and transmission. This will for example include mechanisms that can be used to verify the integrity and authenticity of user data when passed between different entities within the TOE environment. Specific instantiations of the TOE may have additional functions that can be used by the TOE environment to maintain the integrity of user data outside of the TOE, but those functions are not mandated in this evaluation scope.

1.7 Evaluated Configuration

23 This section describes the configurations of the TOE that are included within the scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in the defined evaluated configuration according to the documented preparative user guidance specified in Section 1.9 of this document.

24 The evaluated configuration for the TOE encompasses two Keyper HSM models:

a) AEP Keyper Enterprise (Hardware: 9720, Software: 011126), and

b) AEP Keyper Professional (Hardware: 9720, Software: 010405).

1.8 Delivery Procedures

25 Keyper Hardware Security Module (HSM) v2.0 is sent to the customers using the delivery procedure (Ref [8]), which ensures that the TOE is securely transferred from the development environment into the responsibility of the customer. The delivery procedures are outlined below.

26 Prior to a Keyper Hardware Security Module (HSM) v2.0 being shipped, a number of details and functions are recorded and tested. The AEP Keyper Shipment Checklist is used to ensure the unit is in correct working order and that it has not been tampered with prior to shipment. Prior to shipment, the Keypers are stored within a secure facility at AEP.

27 Keyper Hardware Security Module (HSM) v2.0 is shipped together with a power unit, a CDROM containing Keyper drivers, an Ethernet cable and a set of blank smart cards. Keyper Hardware Security Module (HSM) v2.0 is shipped within a tamper-evident bag and shipped to the client along with a bill of materials, using a standard courier service. Each tamper evident bag has a unique serial number that can be used for identification. The unique serial number for each tamper bag is recorded and filed by AEP Networks Ltd. A notification is sent to the customer upon shipment of the Keyper Hardware Security Module (HSM) v2.0. The notification contains shipment details, a tracking number and the unique tamper bag serial number, which can be used to verify the integrity of the tamper bag upon receipt.

28 Upon receipt of the Keyper Hardware Security Module (HSM) v2.0, the recipient will ensure that it has been delivered in a secure manner by ensuring the tamper proof bag has not being tampered. The recipient should also check that the Keyper Hardware Security Module (HSM) v2.0 is in the Initialised State. If it is in the Initialised State then follow the instructions in Section 6 of the Keyper Manual (Ref 31b)). If not, it is assumed that it has been compromised and should be returned to AEP Networks Ltd.

29 The recipient can verify the firmware version of Keyper Hardware Security Module (HSM) v2.0 in Initialised State based on Section 6.7 of the AEP Keyper v2 Enterprise and Professional Manual (Ref 31b)). There are four parts to the firmware: the Boot Loader, the Loader, the Application and the Common Section (version of the hardware support library in use).

1.9 Documentation

30 To ensure continued secure usage of the product, it is important that the Keyper Hardware Security Module (HSM) v2.0 is used in accordance with guidance documentation.

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

a) AEP Keyper version 2 with PKCS#11 version 4.10 for AEP Keyper Enterprise and Professional Installation, Upgrade and Troubleshooting Guide, rev 7, 23 February 2010.

b) AEP Keyper v2 Enterprise and Professional (FIPS 140-2 level 4 certificate 1340) Manual, Part Number 011127, Revision 2.0, rev 7, 23 February 2010.

c) AEP Keyper version 2 Utilities for AEP Keyper Enterprise and Professional Manual, Part Number 010955, rev 2, 23 September 2009.

2 Evaluation

32 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 4 (EAL4) augmented with AVA_VAN.5. 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

33 The evaluation activities involved a structured evaluation of Keyper Hardware Security Module (HSM) v2.0, including the following components:

2.1.1 Life-cycle support

34 An analysis of the Keyper Hardware Security Module (HSM) v2.0 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, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorised access to the configuration items.

35 It is evaluated that the implemented configuration management system can control changes to those items that have been placed under configuration management system. The developer's configuration management system was also observed during the site visit, and it was found security flaws under configuration management ensures that security flaw reports are not lost or forgotten, and allows a developer to track security flaws to their resolution. This is evaluated to be consistent with the provided evidence.

36 During the site visit the evaluators examined the development security documentation and determined that it detailed sufficient security measures for the development environment to protect the confidentiality and integrity of the Keyper Hardware Security Module (HSM) v2.0 design and implementation. The evaluators confirmed that the developer used a documented life-cycle model which provides necessary control over the development and maintenance of Keyper Hardware Security Module (HSM) v2.0 by using the procedures, tools and techniques described by the life-cycle model.

37 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of Keyper Hardware Security Module (HSM) v2.0 during distribution to the consumer.

2.1.2 Development

38 The evaluators analysed the Keyper Hardware Security Module (HSM) v2.0 functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF

subsystems and modules. The design described the TOE subsystems to sufficiently determine the TSF boundary, and provides a description of the TSF internals in terms of modules. It provides a detailed description of the SFR-enforcing modules and enough information about the SFR supporting and SFR-non-interfering modules for the evaluator to determine that the SFRs are completely and accurately implemented.

39 The evaluators analysed the Keyper Hardware Security Module (HSM) v2.0 security architectural description and determined that the delivery and installation process was secure and the security functions are protected against tamper and bypass. The evaluators also independently verified that the correspondence mappings between the design documents were correct.

2.1.3 Guidance documents

40 The evaluators examined the Keyper Hardware Security Module (HSM) v2.0 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

41 Testing at EAL4 consists of assessing developer tests, independent function test, and performing penetration tests. Keyper Hardware Security Module (HSM) v2.0 testing was conducted by tester from Stratsec.net MySEF at Stratsec.net MySEF Lab, Kuala Lumpur and at the developer’s site where it was subjected to comprehensive suite of formally documented, 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 Plan Reports.

2.1.4.1 Assessment of Developer Tests

42 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).

43 The evaluators analysed the developer’s test coverage and depth analysis, 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 implementation representative, functional specification, TOE design and security architecture description was complete.

2.1.4.2 Independent Functional Testing

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

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

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULTS
To test that the TOE implement Secure Key Management and Access Control security features that control who can access resources	FCS_CKM.1, FCS_RND.1, FCS_CKM.2, FCS_CKM.4, FCS_COP.1a, FCS_COP.1b, FCS_COP.1c, FPT_ITC.1, FPT_ITI.1, FMT_MSA.1, FMT_MSA.2, FMT_MSA.3, FMT_SMF.1.1, FDP_ACF.1b.1, FDP_ACF.1b.2 FDP_ACF.1a.1, FDP_ACF.1a.2, FDP_ACF.1a.3, FDP_ACF.1a.4, FDP_ACC.1a, FDP_ACC.1b, FDP_RIP.1, FDP_SDI.2	EP_SCC4 EP_MII EP_FRONTPANEL EL_SMARTCARD EL_HUIM EL_HM EP_POWER (Power) EP_TAMPER (Tamper) EL_HCM (HSM Crypto Manager)	**PASS.** The TOE does implement Secure Key Management and Access Control security features.
To test that the TOE implement User Authentication in identifying the user and verifying that the user is allowed to access some restricted service. In conjunction with user authentication, the TOE also applies Security Management function for administrator to control users.	FIA_SOS.1, FIA_UAU.1, FIA_UID.1, FMT_SMF.1, FMT_SMR.1, FMT_MTD.1a, FMT_MTD.1b, FDP_ACF.1a.2	EP_SCC3 EP_SCC4 EP_MII EP_FRONTPANEL EP_TAMPER EP_POWER EL_SMARTCARD EL_HUIM EL_HCM EL_FRONTPANEL EL_HM	**PASS.** The TOE does implement User Authentication applies Security Management function.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULTS
To test that the TOE implement BIST (Built-In Self Tests) capable of providing the full range of required self-tests	FPT_TST.1 and FPT_FLS.1.	None	**PASS**. The TOE does implement BIST (Built-In Self Tests)
To test that the TOE implement Tamper Protection that support both internal and external sources of tamper.	FPT_RCV.1, FPT_PHP.2 and FPT_PHP.3.	EP_SCC3 EP_SCC4 EP_MII EL_SMARTCARD EL_HUIM EL_HCM EL_HM EL_FRONTPANEL EP_TAMPER EP_POWER	**PASS**. The TOE does implement Tamper Protection that supports both internal and external sources of tamper.
To test that the TOE implement Auditing for all security relevant operations	FAU_GEN.1, FAU_GEN.2 and FPT_STM.1.	EP_SCC4 EP_MII EP_FRONTPANEL EL_HUIM EL_HCM EL_HM EP_TAMPER EL_SMARTCARD EP_POWER	**PASS**. The TOE does implement Auditing functionality

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

2.1.4.3 Penetration Testing

47 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE and to determine whether these were exploitable in the intended operating environment of the TOE. This vulnerability analysis considered public domain sources and an analysis of guidance documentation, functional specification, TOE design, security architecture description, and implementation representation.

48 From the vulnerability analysis, the evaluators conducted penetration testing to determine that the TOE, in its operational environment, is resistant to attack performed by an attacker possessing a High attack potential. The following factors have been taken into consideration during penetration tests:

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

b) Specialist technical expertise required (specialised expertise);

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

d) Window of opportunity; and

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

49 The penetration tests focused on:

a) Man in the middle attack;

b) Fuzzing;

c) Firmware integrity;

d) Hardware attack; and

e) PIN characters modification.

50 It should be noted that detailed SPA and DPA testing was not performed. As the TOE is assumed to be in a secure environment, only accessible to people with the ability to extract the keys from the TOE using legitimate interfaces. Therefore this testing was deemed unnecessary.

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

2.1.4.4 Testing Results

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

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

3 Result of the Evaluation

54 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 Keyper Hardware Security Module (HSM) v2.0 performed by the Stratsec.net MySEF.

55 The Startsec.net MySEF found that Keyper Hardware Security Module (HSM) v2.0 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 EAL4+ AVA_VAN.5.

56 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

57 EAL4 provides assurance by a full Security Target (ST) and an analysis of the security functions in the ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation to understand the security behaviour.

58 The analysis is supported by independent testing of the TOE security functions, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, implementation representation, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an Enhance-Basic attack potential. However, in this evaluation, the penetration testing is performed by the evaluator assuming an attack potential of High based on AVA_VAN.5 requirements.

59 EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

3.2 Recommendation

60 In addition to ensure secure usage of the product, below are additional recommendations for Keyper Hardware Security Module (HSM) v2.0 consumers and developer:

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

b) Appropriate network layer protection, the network on which the TOE is installed must be both physically and logically protected, commensurate with the sensitivity of the TOE keys;

c) Maintain the confidentiality, integrity and availability of security relevant data for TOE initialisation, start-up and operation if stored or handled outside the TOE;

d) System Auditor should review the audit trail generated and exported by the TOE periodically;

e) System Administrator ensures that the TOE is correctly configured and implements a network that maintains this correctness of the DTBS (e.g. the certificate content data) until it is passed to the TOE;

f) Implement appropriate physical protection of the TOE to ensure access to network ports, smart card readers, and PIN pads are restricted;

g) Check the serial numbers of the tamper evident bags on delivery of the TOE;

h) Ensure that AAK, SMK, and application key cards are stored in safe locations when not in use; and

i) Set the TOE to require operator intervention to restore TOE functionality.

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] Security Target for the Keyper Hardware Security Module (HSM) v2.0, v1.3, 13 December 2012.

[7] Evaluation Technical Report Keyper Hardware Security Module (HSM), v1.0, 13 December 2012.

[8] Delivery process for the Keyper Hardware Security Module (HSM) v2.0, v1.0, 13 December 2012.

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)
CEN	European Committee for Standardization
CWA	CEN workshop agreement European Committee for Standardization
CCRA	Common Criteria Recognition Arrangement
CSP	Certification–service–provider
CSP–SCD	CSP signature creation data
CSP–SVD	CSP signature verification data
DTBS	Data to be signed

Acronym	Expanded Term
HSM	Hardware security module
IEC	International Electrotechnical Commission
ISCB	Information Security Certification Body
ISO	International Standards Organisation
ISMK	Internal storage master key
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
RAD	Reference authentication data
SCD	Signature-creation data
SMK	Storage master key
SVD	Signature-verification data
ST	Security Target
TOE	Target of Evaluation

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Adapter Authorisation Key (AAK)	The AAK protects the TOE from unauthorised access by providing the means to authenticate Security Officer smart cards. There is only one AAK per device which is generated in the TOE during the initialisation phase.
Administrator	A CSP user role that performs TOE initialisation or other TOE administrative functions. These tasks are mapped to the Security Officer.
Application Keys	Application Keys are generated by a request for cryptographic services from an external application. An Application Key is protected along with key policy and identifiers and wrapped by the SMK for protection during backup or restore.
Auditor	A user exporting the TOE audit data and reviewing the audit data with tools in the TOE environment.
Authentication data	Information used to verify the claimed identity of a user.

Term	Definition and Source
Backup	Backup of the CSP-SCD, the TSF data and the system data (backup data) sufficient to recreate the state of the TOE at the time the backup was created.
Certificate	An electronic attestation which links the SVD to a person and confirms the identity of that person.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA.
Certification-service-provider (CSP)	An entity or a legal or natural person who issues certificates or provides other services related to electronic signatures.
CSP signature creation data (CSP-SCD)	SCD which is used by the CSP for the creation of advanced electronic signatures in qualified certificates or for signing certificate status information.
CSP signature verification data (CSP-SVD)	SVD which corresponds to the CSP-SCD and which is used to verify the advanced electronic signature in the qualified certificate or for signing certificate status information.
Consumer	The organisation that uses the certified product within their infrastructure.
CEN workshop agreement (CWA)	A consensus-based specification, drawn up in an open workshop environment of the European Committee for Standardization (CEN).
Data to be signed (DTBS)	The complete electronic data to be signed, such as QC content data or certificate status information.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Digital signature	Data appended to, or a cryptographic transformation of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. [ISO 7498-2]
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.
Internal Storage Master Key (ISMK)	The purpose of the ISMK is to protect the internal store.

Term	Definition and Source
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.
Certifier	The certifier responsible for managing a specific certification task.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
Hardware security module (HSM)	The cryptographic module used to generate the advanced signature in qualified certificates and which represents the TOE.
Reference authentication data (RAD)	Data persistently stored by the TOE for verification of the authentication attempt as authorised user.
Restore	Action of importing of the backup data to recreate the state of the TOE at the time the backup was created.
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
Signature-creation data (SCD)	Unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature.
Signature-verification data (SCD)	Data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature.
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.
Storage master key (SMK)	The purpose of the SMK is to protect the smart card store.
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 ---