C015 Certification Report
NexCode National Security Suite Release 3

File name: ISCB-5-RPT-C015-CR-v1a
Version: v1a
Date of document: 15 June 2011
Document classification: PUBLIC

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

CyberSecurity Malaysia
(726630-U)
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.
T +603 8946 0999
F +603 8946 0888
www.cybersecurity.my

C015 Certification Report
NexCode National Security Suite Release 3

15 June 2011

ISCB Department

CyberSecurity Malaysia

Level 8, Block A, Mines Waterfront Business Park,

No 3 Jalan Tasik, The Mines Resort City

43300 Seri Kembangan, Selangor, Malaysia

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

http://www.cybersecurity.my

Document Authorisation

DOCUMENT TITLE:	C015 Certification Report – NexCode National Security Suite Release 3
DOCUMENT REFERENCE:	ISCB-5-RPT-C015-CR-v1a
ISSUE:	v1a
DATE:	15 June 2011

DISTRIBUTION:	UNCONTROLLED COPY – FOR UNLIMITED USE AND DISTRIBUTION

Copyright Statement

Registered office:

Level 8, Block A,

Mines Waterfront Business Park,

No 3 JalanTasik, The Mines Resort City,

43300 Seri Kembangan

Selangor Malaysia

Registered in Malaysia – Company Limited by Guarantee

Company No. 726630-U

Printed in Malaysia

Forward

The Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme 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 15 June 2011, and the Security Target (Ref [6]). The certification report, Certificate of product evaluation and security target are posted on the MyCC Scheme Certified Product Register (MyCPR) at www.cybersecurity.my/mycc.

Disclaimer

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

Document Change Log

RELEASE	DATE	PAGES AFFECTED	REMARKS/CHANGE REFERENCE
v1	6 June 2011	All	Final Release.
v1a	15 June 2011	Page iv	Add the date of the certificate.

Executive Summary

The NexCode National Security Suite Release 3 from Nexbis Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL2) evaluation.

NexCode National Security Suite Release 3 is a software system that utilized mobile telephone technology with real-time information access to enhance the security of identification of documents that have a proprietary barcode, called NexCode.

The TOE is software that comprises of:

a) NexCode National Security Suite – Inventory Management System Release 3,

b) NexCode National Security Suite – Load Server System Release 3,

c) NexCode National Security Suite – Control Centre System Release 3 (web application),

d) NexCode National Security Suite – Gateway System Release 3,

e) NexCode National Security Suite – Mobile Application Release 3 (mobile application),

f) NexCode National Security Suite – Desktop Application Release 3 (desktop application).

The security functions of TOE that are within the scope of evaluation are authentication and identification, cryptographic support, security audit, protection of the TOE security functions, and TOE access. These security functions of the TOE will address the threats and Organisational Security Policies (OSPs) that are described in Section 4 of the Security Target (Ref [6]).

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for NexCode National Security Suite Release 3, the security requirements, and the evaluation assurance level at which the product is intended to satisfy the security requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

This report confirms the findings of the security evaluation of NexCode National Security Suite Release 3 to the Common Criteria (CC) evaluation assurance level EAL2. The report confirms that the product has met the target assurance level of EAL2 and the evaluation was conducted in accordance with the relevant criteria and the requirements of the Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme (Ref [4]). The evaluation was performed by the CyberSecurity Malaysia MySEF and was completed on 20 May 2011.

The Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the NexCode National Security Suite Release 3 evaluation meets all the conditions of the MyCC Scheme requirements and that the

product will be listed on the MyCC Scheme Certified Products Register (MyCPR) at www.cybersecurity.my/mycc.

It is the responsibility of the user to ensure that the NexCode National Security Suite Release 3 meets their requirements. It is recommended that a potential user of the NexCode National Security Suite Release 3 to refer to the Security Target (Ref [6]) and this Certification Report prior to deciding whether to purchase and deploy the product.

Table of Contents

Index of Tables

Index of Figures

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), NexCode National Security Suite Release 3, is a software system that utilized mobile telephone technology with real-time information access to enhance the security of identification of documents that have a proprietary barcode, called NexCode. The TOE component comprises of:

a) NexCode National Security Suite – Inventory Management System Release 3,

b) NexCode National Security Suite – Load Server System Release 3,

c) NexCode National Security Suite – Control Centre System Release 3 (web application),

d) NexCode National Security Suite – Gateway System Release 3,

e) NexCode National Security Suite – Mobile Application Release 3 (mobile application),

f) NexCode National Security Suite – Desktop Application Release 3 (desktop application).

1.2 TOE Identification

2 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	C015
TOE Name	NexCode National Security Suite
TOE Version	Release 3
Security Target Title	NexCode National Security Suite, Release 3 Security Target
Security Target Version	v8.4
Security Target Date	20 May 2011
Assurance Level	Evaluation Assurance Level 2 (EAL2)
Criteria	Common Criteria July 2009, Version 3.1, Revision 3
Methodology	Common Methodology for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3
Protection Profile Conformance	None

Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL2
Sponsor and Developer	Nexbis Sdn Bhd Level 40, Tower 2, PETRONAS Twin Towers, Kuala Lumpur City Centre, 50088 Kuala Lumpur
Evaluation Facility	CyberSecurity Malaysia MySEF

1.3 Security Policy

3 In order for NexCode National Security Suite Release 3 to work in a secure manner, the organisation that implements the TOE shall applied the organisation security policies, as described in Section 4.3 of the ST (Ref [6]), which include:

a) The TOE must allow only authorised username and authenticated password to gain access to the TOE. Access rights will be based on individual user or user group. Access to the TOE will be logged by the TOE.

b) The ability to access the TOE audit logs is to be restricted to the Auditor (who has been authorised to read the audit logs) only in order to protect the TOE assets.

1.4 TOE Architecture

4 NexCode National Security Suite Release 3 includes both logical and physical boundaries which are described in Section 2.3.1 of the Security Target (Ref [6]).

1.4.1 Logical Boundaries

5 Figure 1 below describes the component of NexCode National Security Suite Release 3 that comprises the TOE.

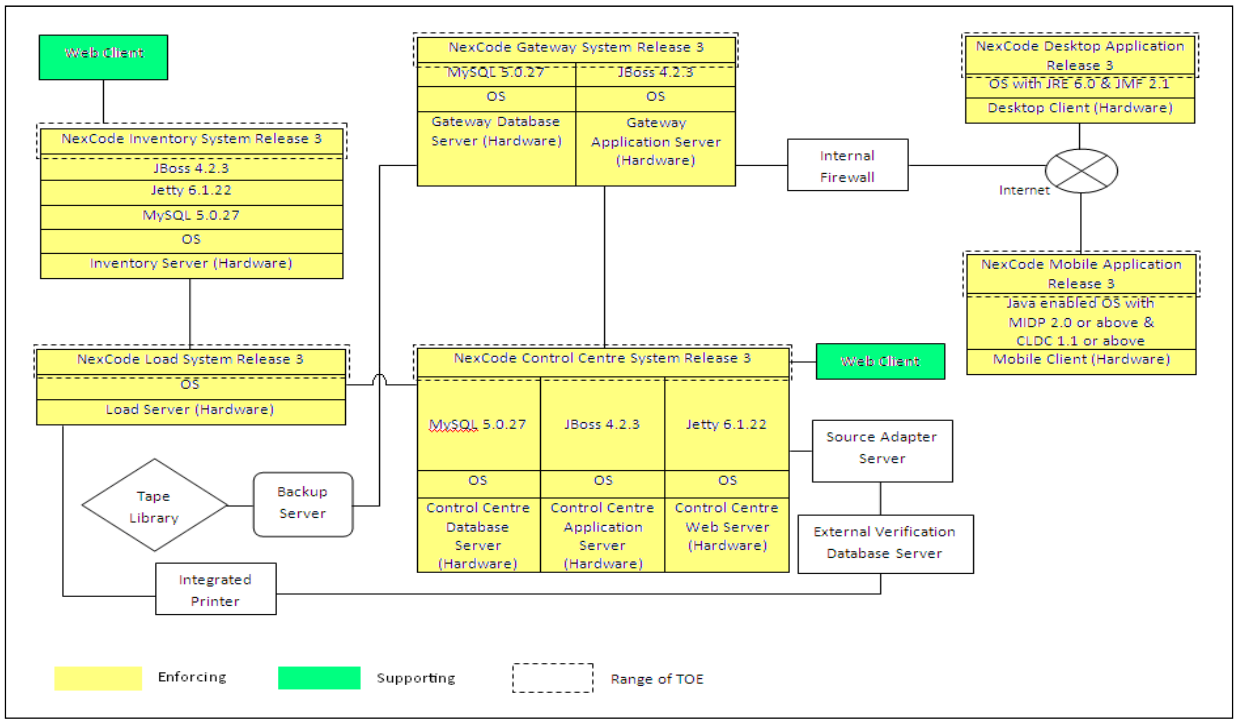

Figure 1: TOE Logical Scope

6 The TOE component comprises of the following:

a) **NexCode Inventory System Release 3** – Manages generation of TOE inventory files (NexCode 2D barcode images) and inventory reports. The TOE application server (JBoss 4.2.3), the TOE Web server (Jetty 6.1.22) and the TOE database server (MySQL 5.0.27) all reside in a single physical server named Inventory Server.

b) **NexCode Load System Release 3** – Handles inventory loading and stores the TOE inventory files for the NexCode Control Centre System Release 3. The Load Server manages storage and reference of TOE inventory files in a single physical server through UNIX-based scripts named Load Server.

c) **NexCode Control Centre System Release 3** – Manages the TOE inventory files in the Load Server, and handles the encryption of user passwords before they are stored into the database.

   i) The NexCode Control Centre System Release 3 is the component of the TOE that provides users with a Web application front-end for log-in, as well as for administration and configuration functions. Through this front-end, authorised users can also read various TOE user log reports in order to monitor and audit the usage of the TOE system.

   ii) The log information used for reporting and audit trails is stored within a database in the Control Centre Database server.

d) **NexCode Gateway System Release 3** – Handles data encryption, routing and connection between the gateway with the mobile client or the desktop client.

e) **NexCode Mobile Application Release 3 –** Handles mobile user functionality, scanning, and decoding through the mobile client.

f) **NexCode Desktop Application Release 3 –** Handles desktop user functionality, scanning, and decoding through the desktop client.

7 The TOE security functions comprises of the following:

a) User access and group access control, the TOE uses username and their corresponding password for authentication, allowing use of the TOE for authorised users only. The TOE is designed so that each user, or group of users, can be assigned security attributes, such as specific access rights and privileges, in the operation of the TOE.

b) Three times authentication failure, the TOE blocks access by disabling an existing user account after 3 unsuccessful authentication attempts.

c) Encrypted communication channel between TOE Gateway Server and enforcement tools, The TOE implements AES encryption on the data being transferred between the TOE Gateway Server and the NexCode Mobile Application or the NexCode Desktop Application.

d) Trusted TOE mobile application, the TOE implements signing and verification of the NexCode Mobile Application installed on the mobile client.

e) Audit trail and logging, the TOE is designed to recognize specific events within its operation and log them. These events include user log-ins and log-outs, a user accessing the NexCode Control Centre Release 3, the NexCode Mobile Application Release 3, or the NexCode Desktop Application Release 3.

f) Secure FTP on transferring TOE inventory files, the TOE implements usage of Secure FTP (SFTP) to transport generated inventory files (NexCode 2D barcode images) from the TOE Inventory Server to the TOE Load Server.

g) Login session idle time-out, the TOE implements a configurable session time-out upon the Web application of the NexCode Control Centre System Release 3, NexCode Inventory System Release 3, NexCode Mobile Application Release 3 and NexCode Desktop Application Release 3. By default, 15 minutes without user input causes the TOE to log out the current user, requiring him or her to log in again if use of the TOE is desired.

1.4.2 Physical Boundaries

8 Physically, the TOE is a system that requires separated servers, desktop PC, mobile phones, operating system, web server, database and other supporting softwares as described in Section 2.2.2 of the Security Target (Ref [6]). The software configuration of the TOE and non-TOE is described in Section 2.3.1.2 of the ST (Ref [6]).

9 The Security Target assumes that the all the servers are to be located in a secure area that is free from physical access to unauthorised parties.

1.5 Clarification of Scope

10 The TOE is designed to be suitable for use in well-protected environments that have effective countermeasures, particularly in the areas of physical access, personnel and

communication security in accordance with user guidance that is supplied with the product.

11 Figure 1 in Section 1.4.1 of this document shows the scope of the evaluation. 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) **Identification and Authentication** – TOE user with unique username is authenticated by password with access rights controlled by either an individual user or a user group within NexCode Control Centre System Release 3, NexCode Inventory System Release 3, NexCode Mobile Application Release 3 and NexCode Desktop Application Release 3. User login will be blocked upon three consecutive attempts of incorrect password entry in accessing NexCode Control Centre System Release 3.

b) **Cryptographic Support** – Data transferred between the TOE Gateway Server Release 3 and the NexCode Mobile Application Release 3 or the NexCode Desktop Application Release 3 is encrypted using AES encryption. The TOE implements signing and verification of the NexCode Mobile Application Release 3 installed on the mobile client. A signing certificate used on an application serves to protect the integrity of that application by applying a digital signature that is independently verified by VeriSign.

c) **Security Audit Data Generation** – All TOE user access login or logout and all action taken against any TOE data is logged and auditable.

d) **Protection of the TOE Security Function –** Usage of Secure FTP (SFTP) to transfer generated TOE inventory files (NexCode 2D barcode images) from the TOE Inventory Server to the TOE Load Server.

e) **TOE Access –** The TOE user login session is timed-out within NexCode Control Centre System Release 3, NexCode Inventory System Release 3, NexCode Mobile Application Release 3 and NexCode Desktop Application Release 3 upon a configured idle time (default 15 minutes) to prevent unauthorised TOE users from accessing it.

12 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.

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

a) Hardware servers;

b) Operating Systems on which the TOE is installed on;

c) Database Software on which the TOE is dependent on as its database, including External Verification Database Server and Source Adapter Server;

d) Storage devices such as Backup Server and Tape Library;

e) Integrated Printer for NexCode 2D barcode image;

f) Other supporting software;

i) Apache Tomcat version 6.0.14

ii) Java ME with MIDP 2.0

iii) Java Media Framework 2.1

iv) Java Runtime Environment 6.0

v) Java SDK Version 1.5.0.11

vi) JBoss Application Server version 4.2.3

vii) Jetty Web Server Version 6.1.22

viii) MySQL Server version 5.0.27

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 that required for secure operation of the NexCode National Security Suite Release 3 as defined in subsequent sections and in the Security Target.

1.6.1 Environment assumptions

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

a) Only authorised personnel can access the data centre and servers where the TOE installed.

b) The TOE operating environment will provide reliable timestamp.

1.7 Evaluated Configuration

16 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 preparative user guidance (Ref 25a)).

17 The TOE is delivered and installed by the developer's trusted and authorised personnel. During installation, the developer's trusted and authorised personnel will make changes to configuration based on preparative user guidance (Ref 25a)) as following:

a) Operating system installation and configuration

b) Application tools installation and configuration

c) Application installation and configuration

d) SFTP installation and configuration

e) SSL installation and configuration

1.8 Delivery Procedures

18 NexCode National Security Suite Release 3 is delivered to the user using the procedure described in the Delivery Procedure (Ref 25b)) which ensures that NexCode National Security Suite Release 3 is securely transferred from development environment into the responsibility of the user. The delivery procedures are outlined below.

19 The sales transaction is initiated when the end-user expresses interest in purchasing the TOE, and Nexbis Sdn Bhd responds with a sales quotation document.

20 A Purchase Order is then sent from the end-user to Nexbis Sdn Bhd and sales contract is established. Schedules are then arranged for the TOE to be delivered to the end-user.

21 The TOE is copied from the development machines of Nexbis Sdn Bhd by trusted and authorised Nexbis Sdn Bhd personnel, and stored on read-only CD media. It is then physically delivered by them to the end-user site, where it is installed by Nexbis Sdn Bhd personnel for the end-user.

22 The TOE is identified by the end-user as the version of the product is displayed on the label of the Compact Discs (CD) media for TOE delivery.

1.9 Documentation

23 To ensure continued secure usage of the product, it is important that the NexCode National Security Suite Release 3 is used in accordance with guidance documentation.

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

a) NexCode National Security Suite Release 3 Operational User Guidance, version 1.3, 14 October 2010

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

a) NexCode National Security Suite Release 3 Preparative Procedure, version 1.3, 14 October 2010

b) NexCode National Security Suite Release 3 Delivery Procedures version 1.1, 14 October 2010

2 Evaluation

26 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 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

27 The evaluation activities involved a structured evaluation of NexCode National Security Suite Release 3, including the following components:

2.1.1 Life-cycle support

28 An analysis of the NexCode National Security Suite Release 3 configuration management system and associated documentation was performed. The evaluators found that the NexCode National Security Suite Release 3 configuration items 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. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

29 The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of NexCode National Security Suite Release 3 during distribution to the consumer.

2.1.2 Development

30 The evaluators analysed the NexCode National Security Suite Release 3 functional specification; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces (TSFIs), and how the TSF implements the security functional requirements (SFRs).

31 The evaluators analysed the NexCode National Security Suite Release 3 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

32 The evaluators examined the NexCode National Security Suite Release 3 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

33 Testing at EAL2 consists of performing functional testing based on the developer's test case, independent function test, and performing penetration tests. The NexCode National Security Suite Release 3 testing was conducted at CyberSecurity Malaysia MySEF where it was subjected to a functional testing, 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

34 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).

35 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

36 At EAL2, 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.

37 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	TEST RESULT
Test that comprises a series of test cases on TOE security functions to verify unique identification & authentication by password with access rights controlled by either an individual user	ITSF.I&AUTH	Inventory-WebClient Interface Control Centre-WebClient Interface Mobile-Gateway Interface Desktop-Gateway Interface	PASS

DESCRIPTION	SECURITY FUNCTION	TSFI	TEST RESULT
or a user group within TOE			
Test that comprises a series of test cases on TOE security functions to verify that the TOE user login will be blocked upon three consecutive attempts of incorrect password entry in accessing TOE.	ITSF.RETRY_FAIL	Control Centre–WebClient Interface	PASS
Test that comprises a series of test cases on TOE security functions of data transferring between the TOE Gateway Server and the mobile client or the desktop client that will be encrypted using AES encryption.	ITSF.ENCRY_DAT	Gateway–MobileDesktop Interface Mobile–Gateway Interface Desktop–Gateway Interface	PASS
Test that comprises a series of test cases on TOE security functions to verify that the TOE Mobile Application that is installed on the mobile client is signed and verified.	ITSF.SIGN_MOB	Mobile–Gateway Interface	PASS
Test that comprises a series of test cases on TOE security functions of audit trail and logging to TOE web application, the NexCode Mobile Application and the NexCode Desktop Application. The auditable events are: 1. All TOE user access login or logout 2. All action taken against	ITSF.AT&L	Inventory–WebClient Interface Control Centre–WebClient Interface Mobile–Gateway Interface Desktop–Gateway Interface	PASS

DESCRIPTION	SECURITY FUNCTION	TSFI	TEST RESULT
any TOE data These audit trails are provided reliable time stamps for use in collected audit data by IT Environment. This test group also will cover storing of audit data in the IT Environment, which the TOE relies on to protect as well.			
Test that comprises a series of test cases on the TOE security functions to verify the usage of the Secure FTP (SFTP) to transfer generated TOE inventory files (NexCode 2D barcode images) from the TOE Inventory Server to the TOE Load Server.	ITSF.SEC_DATA		PASS
Test that comprises a series of test cases on TOE security functions to verify TOE user login session is timed-out within TOE web application upon a configured idle time (default 15 minutes) to prevent unauthorised TOE users from accessing it.	ITSF.TIMEOUT	Inventory-WebClient Interface Control Centre-WebClient Interface Mobile-Gateway Interface Desktop-Gateway Interface	PASS

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

2.1.4.3 Penetration Testing

39 The evaluators performed a vulnerability analysis of the TOE in order to identify potential vulnerabilities in the TOE. This vulnerability analysis considered public

domain sources and an analysis of guidance documentation, and functional specification.

40 From the vulnerability analysis, the evaluators conducted penetration testing to determine whether potential vulnerabilities could be exploited in the intended operating environment of the TOE, to attack performed by an attacker possessing a basic attack potential. The following factors have been taken into consideration during the penetration tests:

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

b) Specialist technical expertise required (specialist expertise);

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

d) Window of opportunity; and

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

41 The penetration tests focused on:

a) Generic vulnerabilities;

b) Bypassing;

c) Tampering; and

d) Direct attacks.

42 The results of the penetration testing note that there is no vulnerability or residual vulnerability found. However, it is important to ensure that the TOE is use only in its evaluated configuration and in secure environment. All hardware and software use by the TOE in its environment should be updated and harden, and should be located in physical secure area.

2.1.4.4 Testing Results

43 Tests conducted for the NexCode National Security Suite Release 3 produced the expected results and demonstrated that the product behaved as specified in its Security Target and functional specification.

3 Results of the Evaluation

44 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 NexCode National Security Suite Release 3 performed by the CyberSecurity Malaysia MySEF.

45 The CyberSecurity Malaysia MySEF found that NexCode National Security Suite Release 3 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 EAL2.

46 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

47 EAL2 provides a basic level of assurance by a limited Security Target and an analysis of the security functions in that Security Target, using a functional and interface specification and guidance documentation of TOE to understand the security behaviour.

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

49 EAL2 also provides assurance through unique identification of the TOE and of the relevant evaluation documents.

3.2 Recommendation

50 In addition to ensure secure usage of the product, below are additional recommendations for NexCode National Security Suite Release 3 consumers:

a) Use the product only in its evaluated configuration;

b) User should follow closely the operational user guidance document to ensure proper usage of the TOE; and

c) Supported hardware and software use by the TOE in its operating environment should be harden and configure according to good practise in order to avoid unauthorised user from getting access to the environment and the TOE.

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] NexCode National Security Suite, Release 3 – Security Target, Version 8.4, 20 May 2011

[7] Evaluation Technical Report NexCode National Security Suite Release 3, Version 1.2, 20 May 2011

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
IEC	International Electrotechnical Commission
ISCB	Information Security Certificaiton Body
ISO	International Standards for Organisation
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

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
Auditor	A person appointed to collect and evaluate evidence of an organisation's information systems, practices, and operations; the evaluation of obtained evidence determines if the information systems are safeguarding assets, maintaining data integrity, and operating effectively to achieve the organisation's goals or objectives.
Certificate	The official representation from the CB of the certification of a specific version of a product to the Common Criteria.
Certification Body	An organisation responsible for carrying out **certification** and for overseeing the day-today operation of an **Evaluation and Certification Scheme**. Source CCRA
Consumer	The organisation that uses the certified product within their infrastructure.
Developer	The organisation that develops the product submitted for CC evaluation and certification.
Evaluation	The assessment of an IT product, IT system, or any other valid target as defined by the scheme, proposed by an applicant against the standards covered by the scope defined in its application against the certification criteria specified in the rules of the scheme. Source CCRA and MS ISO/IEC Guide 65
Evaluation and Certification Scheme	The systematic organisation of the functions of **evaluation** and **certification** under the authority of a **certification body** in order to ensure that high standards of competence and impartiality are maintained and that consistency is achieved. Source CCRA.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.
Certifier	The certifier responsible for managing a specific certification task.

Term	Definition and Source
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.
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.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
Security Evaluation Facility	An organisation (or business unit of an organisation) that conducts ICT security evaluation of products and systems using the CC and CEM in accordance with Evaluation and Certification Scheme policy
Sponsor	The organisation that submits a product for evaluation and certification under the MyCC Scheme. The sponsor may also be the developer.
System Administrator	A person employed to maintain and operate a computer system and/or network.

--- END OF DOCUMENT ---