C034 Certification Report

Northern Light Video Conferencing System (NLVC)

File name: ISCB-5-RPT-C034-CR-v1a
Version: v1a
Date of document: 22 March 2012
Document classification: PUBLIC

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

C034 Certification Report

Northern Light Video Conferencing System (NLVC)

22 March 2012

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:	C034 Certification Report - Northern Light Video Conferencing System (NLVC)
DOCUMENT REFERENCE:	ISCB-5-RPT-C034-CR-v1a
ISSUE:	v1a
DATE:	22 March 2012

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 22 March 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 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 March 2012	All	Final Released
v1a	22 March 2012	Page iv	Add the date of the certificate.

Executive Summary

The Northern Light Video Conferencing System (NLVC) (hereafter referred as NLVC) from JMCS Sdn Bhd is the Target of Evaluation (TOE) for this Evaluation Assurance Level (EAL) 2 evaluation.

NLVC is a multipoint-to-multipoint video conferencing system. It allows conferencing of any desired number of people around the world using existing LAN infrastructure, without affecting current applications. It is software based and uses non-proprietary hardware.

The TOE is software that comprises of three components:

- NLVC Client version 6.3.0.0. A user based GUI application that works on the end user's PC or NLVC boardroom codec system.
- NLVC Server Webadmin Tool version 7.0.0.1. A web based interface use to ease the administration of the TOE (NLVC Server).
- NLVC Server version 6.1-0.21. The main purpose is to maintain and control conference according to the Real Time Switching (RSW) control criteria used.

The security functions within the scope of the evaluation include:

- **Identification and Authentication** – the TOE provides identification and authentication of users before users are allowed to access the functionality of the TOE.
- **Secure communication** – the TOE provides a secure SSL session between the client and the server.
- **Security Management** – the TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.
- **User Data Protection** – the TOE manages access control on configuration data and functions based on user roles and access control lists.

The scope of the evaluation is defined by the Security Target (Ref [6]), which identifies assumptions made during the evaluation, the intended environment for NLVC, the security functional 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 describes the findings of the IT security evaluation of NLVC to the Common Criteria (CC) evaluation assurance level of EAL2. 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) Security Evaluation Facility (Stratsec MySEF) and was completed on 22 February 2012.

Malaysian Common Criteria Certification Body (MyCB), as the MyCC Scheme Certification Body, declares that the NLVC evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and the product will be listed on 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 NLVC meets their requirements and security needs. It is recommended that a potential user of the NLVC 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

1 Target of Evaluation 1

1.1 TOE Description 1
1.2 TOE Identification 1
1.3 Security Policy 2
1.4 TOE Architecture 3
1.5 Clarification of Scope 4
1.6 Assumptions 6
1.6.1 Usage Assumptions 6
1.6.2 Environment Assumptions 7
1.7 Evaluated Configuration 7
1.8 Delivery Procedures 7
1.9 Documentation 8

2 Evaluation 9

2.1 Evaluation Analysis Activities 9
2.1.1 Life-cycle support 9
2.1.2 Development 9
2.1.3 Guidance documents 9
2.1.4 IT Product Testing 10

3 Result of the Evaluation 18

3.1 Assurance Level Information 18
3.2 Recommendation 18

Annex A References 20

A.1 References 20
A.2 Terminology 20
A.2.1 Acronyms 20
A.2.2 Glossary of Terms 21

Index of Tables

Table 1: TOE identification 1
Table 2: Independent Functional Testing 10
Table 3: List of Acronyms 20
Table 4: Glossary of Terms 21

Index of Figures

Figure 1: NLVC System Architecture 3

1 Target of Evaluation

1.1 TOE Description

1 The Target of Evaluation (TOE), Northern Light Video Conferencing System (NLVC) (hereafter referred as NLVC) is a multipoint-to-multipoint video conferencing system. It allows conferencing of any desired number of people around the world using existing LAN infrastructure, without affecting current applications. It is software based and uses non-proprietary hardware. The TOE components include:

a) NLVC Client version 6.3.0.0. A user based GUI application that works on the end user's PC or NLVC boardroom codec system.

b) NLVC Server Webadmin Tool version 7.0.0.1. A web based interface use to ease the administration of the TOE (NLVC Server).

c) NLVC Server version 6.1-0.21. The main purpose is to maintain and control conference according to the Real Time Switching (RSW) control criteria used.

2 The evaluated security functionalities for the TOE includes:

a) **Identification and Authentication** – the TOE requires that each user is successfully identified (User ID) and authenticated (password) before they are allowed to access the functionality of the TOE.

b) **Secure communication** – the TOE provides a secure SSL session between the client and the server in order to protect the video feeds and command data when transmitted between the client and the server.

c) **Security Management** – the TOE manages functions to ensure efficient and secure management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user. The roles maintained by the TOE are: Chairman, Participant, Observer, and Administrator. Each access control list maps users and roles to the operations that they are permitted to perform on the object.

d) **User Data Protection** – the TOE manages access control on configuration data and functions based on user role and access control lists.

1.2 TOE Identification

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

Table 1: TOE identification

Evaluation Scheme	Malaysian Common Criteria Evaluation and Certification (MyCC) Scheme
Project Identifier	C034
TOE Name	Northern Light Video Conferencing System (NLVC)

TOE Version	NLVC System version consist of: • NLVC Client version 6.3.0.0 • NLVC Server Webadmin Tool version 7.0.0.1 • NLVC Server version 6.1-0.21
Security Target Title	JMCS Northern Light Video Conferencing System Security Target
Security Target Version	1.2
Security Target Date	22 February 2012
Assurance Level	Evaluation Assurance Level 1 (EAL2)
Criteria	Common Criteria for Information Technology Security Evaluation, July 2009, Version 3.1 Revision 3 (Ref [2])
Methodology	Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3 (Ref [3])
Protection Profile Conformance	None
Common Criteria Conformance	CC Part 2 Conformant CC Part 3 Conformant Package conformant to EAL2
Sponsor and Developer	JMCS Sdn Bhd National Advances IPv6 Centre, Universiti Sains Malaysia, 11800 Penang, MALAYSIA
Evaluation Facility	STRATSEC.NET SDN BHD known as Stratsec MySEF

1.3 Security Policy

4 In order to provide user data protection, the TOE enforces access control policy on TOE configuration data and functions. Only Administrator can access the management functions through web interface that has access rights to TOE configuration data and TOE functions.

5 Users need to be identified and authenticated before the users can establish a video conferencing session. Only the Chairman can create and configure the session, invite the users, and choose the role of users using the NLVC Client.

6 The TOE also enforces communication policy on the establishment of a secure channel between the NLVC Clients and the NLVC Server. Only a NLVC Client with a valid certificate can establish a secure VPN channel with the NLVC Server.

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

1.4 TOE Architecture

8 The Security Target (Ref [6]) defines clearly both logical and physical boundaries.

9 Figure 1 below identifies the major architectural components that comprise the entire NLVC system and identifies all the major supporting elements that combine to deliver the system.

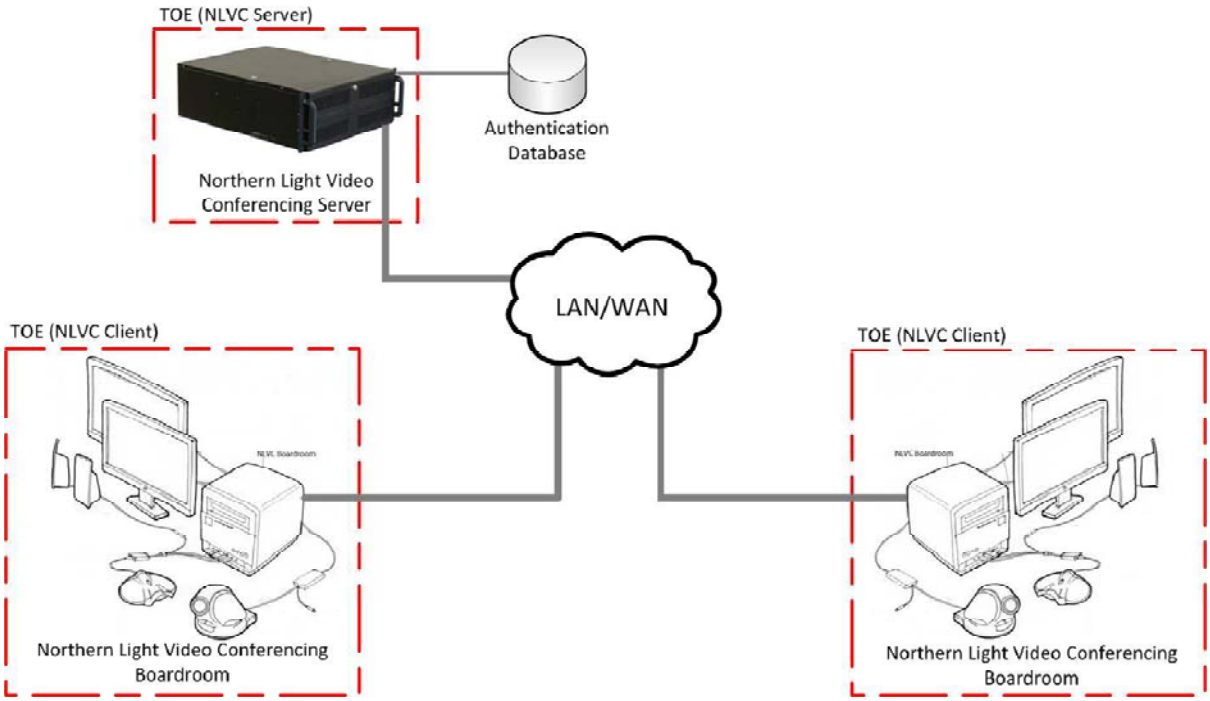

Figure 1: NLVC System Architecture

10 NLVC is a multipoint-to-multipoint video conferencing system that consists of NLVC Server and NLVC Client(s). It allows conferencing of any desired number of people around the world using existing LAN infrastructure. It is software based and uses non-proprietary hardware.

11 NLVC uses multicast technology within the LAN and unicast technology within the WAN. This enables NLVC to keep the conference bandwidth constant no matter how many users are connected to the conference.

12 NLVC also uses the RSW Control Criteria which is an advanced set of controls for Multimedia Conferencing that focused more on bandwidth reduction and prioritizes the participants to avoid confusion when everybody speaks up during conference.

13 Physically, the TOE comprises of 2 systems:

a) NLVC Server (version 6.1-0.21) – the main purpose is to maintain and control conference according to the RSW control criteria used. RSW control criterion is a set of rules that uses the client-server style of communication. NLVC Server

is managed through the Webadmin Tool (version 7.0.0.1) which is a web based interface for accessing the various user management and security function capabilities of the NLVC Server.

The functions of the server include:

- Controlling the conference using the chosen RSW control criteria.
- Allowing users to login into the system.
- Allowing users to change passwords.
- Establishing inter-server links (during multi-server conferences. However, this is not in the scope of the evaluation).

b) NLVC Client (version 6.3.0.0) – user based GUI application that is used to control and monitors the conference. It works on:

- end user's PC – can be any Windows based system; or
- NLVC boardroom codec system – a standalone platform with a high resolution monitor, Windows system, camera, and advanced echo cancellation system.

14 The secure installation of the operational environment is an important element in ensuring that the TOE is initialized correctly and protection from tampering. The Security Target assumes that the server is to be located in a secure area that is free from physical access to unauthorised parties. This would restrict access to the application through only logical access.

1.5 Clarification of Scope

15 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 administrator guidance that is supplied with the product.

16 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.** When a user logon using the NLVC Client, the TOE requires that the users identify and authenticate themselves before performing any TSF mediated action on behalf of the user. The TOE checks the credentials presented by the user upon the login module of the client against the authentication information in the database.

All users presented passwords are hashed before being used to authenticate the user or when users change their passwords and is being written to the database.

Administrators will login to the NLVC Server through Webadmin Tool interface which can only be accessed by the administrator.

The TOE also checks the authenticity of the NLVC Clients when they are requesting to establish a secure channel to the NLVC Server. This is done through the use of digital certificates which are pre-installed on the client side.

b) **Secure communication** - The TOE protects the video feeds, audio and command data from disclosure when they are transmitted between the server and the client through the establishment of secure SSL channel. The VPN API (server) will invoke open-source OpenVPN server program and wait for VPN API (client) connection. The VPN API (client) will connect to VPN API (server) by establishing TLS based dynamic key exchange using client certificates. Once the SSL authentication is done, a SSL tunnel will be established.

c) **Security management** - The TOE contains various management functions to ensure efficient and secure management of the TOE as follows:

i) User Management - only Administrator is allowed to query, create, delete, and modify user. All users can change their password only.

ii) Permission Management for Functions and Data - the person who starts the video session will have the Chairman role. Only the Chairman can invite users to the video conferencing session and assign them roles (Participants or Observers). The Administrator of the TOE can configure the certificate settings on the NLVC Server for identification and authentication of NLVC Clients.

iii) Configuration of session - when the user setup the video conferencing session, he/she can edit the settings of the video conferencing (SSL, protocols, etc).

The TOE maintains 4 roles within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions. The roles maintained by the TOE are: Chairman, Participant, Observer and Administrator.

The TOE allows no one to change the default values of the TSF data and security attributes of the TOE but only allows the Administrator to change the security attributes for the identification and authentication of NLVC client through digital certificates.

d) **User data protection** – The access control function permits a user to access configuration data and functions only if a user role of the user has permission to perform the requested action. It also permits a NLVC Client with a valid certificate to request to establish a secure SSL channel with the NLVC Server.

Users will be assigned a role after they have been identified and authenticated. The following user assignment rules are enforced:

i) When no user authentication has taken place, the user has been assigned no role. Only authenticated user can access the TOE functions.

ii) When the user successfully authenticates himself/herself, he can be assigned any of the 4 roles depending on the event:

- Conference Roles:

1. **Chairman** (creator) – can view, listen and transmit audio and video streams in a conference session. Once a user creates a conference, he is automatically the “Chairman” and can invite user into their conference. Chairman is always active.

2. **Participant** – can view and listen to audio, video streams in a conference session. Once he is active, he could transmit audio and video. This role is assigned by Chairman during conference invitation.
3. **Observer** – can only view and listen to others audio and video streams in a conference session. He can change status to active by requesting to become "active". This role is assigned by Chairman during conference invitation.

o Administrator Roles:

1. **Administrator** – can perform users' management and monitor system status through Webadmin Tool interface to the TOE.

iii) Users can only operate in the organisation that they are assigned to. Only Administrator has access to all organisations data.

17 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.

18 Functions and services which are not included as part of the evaluated configuration, but these IT environment are required to ensure that the TOE perform in its intended operations, are as follows:

a) A Hardware Server;

b) An Operating System on which the TOE is installed on;

c) A Database Software on which the TOE is dependent on as its database;

d) Other supporting software;

i) SSH server v4.3.

ii) Apache web server v2.2.3-6.

iii) Yum v3.0.5-1

iv) OpenVPN v2.0.9-1

1.6 Assumptions

19 This section summarises the security aspects of the environment or configuration in which the IT product is intended to operate. Consumers should understand their own IT environments and what is required for secure operation of the TOE as defined in the Security Target (Ref [6]). Consumers can make informed decisions about the risks associated with using the TOE by considering assumptions about usage and environment settings as requirements for the product's installation and its operating environment, to ensure its proper and secure operation.

1.6.1 Usage Assumptions

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

a) The administrator who manages the TOE is not hostile and is competent.

b) All management of the TOE will be performed through the management interfaces of the TOE and not through the underlying environment.

1.6.2 Environment Assumptions

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

a) The TOE environment will provide appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, RDBMS, and Web Server).

b) Those responsible for the TOE must ensure that the TOE environment is free of vulnerabilities that allow an attacker to bypass the TOE security functions.

c) The IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

d) The databases in the TOE environment have been correctly configured according to the principle of least privilege.

e) The encryption of user password in the TOE environment has been performed to ensure confidentiality or integrity of user or management data.

1.7 Evaluated Configuration

22 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 and operational user guidance, and only by trustworthy staff.

23 The TOE, and its supporting hardware and software listed in the Security Target (Ref [6]) are configured based on secure installation guidance as follows:

a) Installation and configuration of NLVC Server.

b) Installation and configuration of OpenVPN.

c) Installation and configuration of web administration page.

d) Installation and configuration of the NLVC Client.

1.8 Delivery Procedures

24 NLVC is delivered to the end-user (i.e. the Administrator) by JMCS's trusted representative. Before the TOE is delivered, all necessaries steps are performed by JMCS representative, including:

a) The NLVC System components to be delivered consist of NLVC Client (NLVC Boardroom codec System(s)) and NLVC Server.

b) Software installation including the TOE (according to the Getting Started with NLVC Boardroom Codec System and Northern Light Video Conferencing Server User Guide) and the underlying platform are installed by JMCS's representative along with the hardware specification.

c) Default accounts and passwords are created by JMCS's representative.

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

25 Once the TOE has been installed and configured, user then has to check and verify the version of the components according to the methods listed in Section 3.3 of JMCS NLVC System Guidance Documentation (Ref [8]).

1.9 Documentation

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

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

a) JMCS NLVC System Guidance Documentation (Ref [8]).

b) Northern Light Video Conferencing System (NLVC) User Guide.chm, v1.0

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

a) Northern Light Video Conferencing Server User Guide, v6.0.1, 17 February 2011.

b) Getting Started with NLVC Boardroom Codec System v6.3, October 2010

2 Evaluation

29 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

30 The evaluation activities involved a structured evaluation of NLVC, including the following components:

2.1.1 Life-cycle support

31 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, and that the access control measures as described in the configuration management documentation are effective in preventing unauthorized access to the configuration items. The developer's configuration management system was evaluated, and it was found to be consistent with the provided evidence.

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

2.1.2 Development

33 The evaluators analysed the TOE 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).

34 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.

35 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

36 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

37 Testing at EAL2 consists of assessing developer tests, independent function test, and performing penetration tests. NLVC testing was conducted by Stratsec MySEF at Stratsec lab in Plaza Sentral, 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

38 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).

39 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

40 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.

41 The results of the independent test developed and performed by the evaluators to verify the TOE functionality as follows:

Table 2: Independent Functional Testing

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
The TSF shall perform [**hashing**] in accordance with a specified cryptographic algorithm [**SHA256**] and cryptographic key sizes [**none**] that meet the following: [**FIPS 180-2**]	FCS_COP.1 Cryptographic operation	Webadmin Interface	**PASS**. Result as expected.
The TSF shall enforce the [**Access Control SFP**] on [	FDP_ACC.1 Subset access control	• NLVC Client Interface • Webadmin	**PASS**. Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
Subjects: **a) TOE users** **Objects:** **a) TOE configuration data** **b) Functions** **Operations:** **Manipulate**]		Interface	
FDP_ACF.1.1 The TSF shall enforce the [**Access Control SFP**] to objects based on the following: [**Subject attribute:** **a) ID of the user** **b) corresponding user role** **Object attributes:** **Access Control List**] **FDP_ACF.1.2** The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**The operation is allowed, if:** **a) The Access Control List for an object permits the user ID to access that object; AND** **b) The Access Control List for an object permits the User Role to access that**	FDP_ACF.1 Security attribute based access control	• NLVC Client Interface • Webadmin Interface	**PASS**. Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
Object.] **FDP_ACF.1.3** The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**the Administrator role can access all functions and data**]. **FDP_ACF.1.4** The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**None**].			
The TSF shall enforce the [**Communication SFP**] on [**NLVC server and client when the client machine requests a secure channel between the NLVC server and client for transmitting and receiving and transmitting user data**]	FDP_IFC.1 Subset information flow control	• NLVC Client Interface • VPN API	**PASS**. Result as expected.
FDP_IFF.1.1 The TSF shall enforce the [**Communication SFP**] based on the following types of subject and information security attributes: [**a) Identification and authentication of the client machine**].	FDP_IFF.1 Simple security attributes	• NLVC Client Interface • VPN API	**PASS**. Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [a) **For the transmission of user data from the NLVC server and the NLVC client; the requesting client machine has been identified as authorised by the server using certificates.**] **FDP_IFF.1.3** The TSF shall enforce the [**no additional information flow control SFP rules**]. **FDP_IFF.1.4** The TSF shall provide the following [**no additional SFP capabilities**]. **FDP_IFF.1.5** The TSF shall explicitly authorise an information flow based on the following rules: [**none**]. **FDP_IFF.1.6** The TSF shall explicitly deny an information flow based on the following rules: [**none**].			

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
The TSF shall enforce the [**Communication SFP**] to prevent the [***disclosure, modification***] of user data when it is transmitted between physically-separated parts of the TOE.	FDP_ITT.1 Basic internal transfer Protection	• NLVC Client Interface • VPN API	**PASS**. Result as expected.
FIA_UAU.2a The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. **FIA_UID.2a** The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.	FIA_UAU.2 User authentication before any action FIA_UID.2 User identification before any action	• Webadmin Interface • VPN API	**PASS**. Result as expected.
FIA_UAU.2b The TSF shall require each **NLVC Client** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user. **FIA_UID.2b** The TSF shall require each **NLVC Client** to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.	FIA_UAU.2 User authentication before any action FIA_UID.2 User identification before any action	• NLVC Client Interface • VPN API	**PASS**. Result as expected.
The TSF shall restrict the ability to [***determine the***	FMT_MOF.1 Management of	• Webadmin	**PASS**. Result as

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
behaviour of, disable, enable, modify the behaviour of] the functions [**all functions**] to [**the users with appropriate permissions**].	security functions behaviour	Interface • NLVC Client Interface	expected.
FMT_MSA.1a The TSF shall enforce the [**Access Control SFP**] to restrict the ability to [***write or delete***] the security attributes [**that map user IDs to roles only the users that are mapped**] to [**none**]. **FMT_MSA.1b** The TSF shall enforce the [**Communication SFP**] to restrict the ability to [***create, modify, delete***] the security attributes [**identification and authentication of NLVC clients**] to [**Administrator**].	FMT_MSA.1 Management of security attributes	NLVC Client Interface	**PASS**. Result as expected.
FMT_MSA.3.1 The TSF shall enforce the [**Access Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP. **FMT_MSA.3a.2** The TSF shall allow ~~the~~ [**none**] to specify alternative initial values to override the default values when an object or	FMT_MSA.3 Static attribute initialisation	Webadmin Interface	**PASS**. Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
information is created.			
FMT_MSA.3.1 The TSF shall enforce the [**Communication SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP. **FMT_MSA.3b.2** The TSF shall allow the [**administrator**] to specify alternative initial values to override the default values when an object or information is created.	FMT_MSA.3 Static attribute initialisation	Webadmin Interface	**PASS.** Result as expected.
Default The TSF shall restrict the ability to [***change_default, query, modify, delete***] the [**TOE configuration data**] to [**Users with appropriate permission**].	FMT_MTD.1/Default Management of TSF data	• Webadmin Interface • NLVC Client Interface	**PASS.** Result as expected.
The TSF shall restrict the ability to [***query, modify, delete, clear*** **[Create]**] the [**User accounts**] to [**Administrator**].	FMT_MTD.1/user Management of TSF data	• Webadmin Interface • NLVC Client Interface	**PASS.** Result as expected.
The TSF shall restrict the ability to [***modify***] the [**User password**] to [**users (that is related to the password)**].	FMT_MTD.1/password Management of TSF data	• Webadmin Interface • NLVC Client Interface	**PASS.** Result as expected.
The TSF shall be capable of performing the following management functions: [**security attribute management, TSF data management, and security function**	FMT_SMF.1 Specification of Management Functions	• Webadmin Interface • NLVC Client Interface	**PASS.** Result as expected.

DESCRIPTION	SECURITY FUNCTION	TSFI	RESULT
management].			
TSF shall maintain the roles [**chairman, participant, observer and administrator**]	FMT_SMR.1 Security roles	Webadmin Interface	**PASS.** Result as expected.
The TSF shall protect TSF data from [***disclosure***] when it is transmitted between separate parts of the TOE.	FPR_ITT.1 Basic internal TSF data transfer protection	VPN API	**PASS.** Result as expected.

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

2.1.4.3 Penetration Testing

43 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, TOE design and security architecture description.

44 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.

45 The penetration tests focused on:

a) Information leakage; and

b) Cross-Site Scripting.

46 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.

2.1.4.4 Testing Results

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

3 Result of the Evaluation

48 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 NLVC performed by the Stratsec Security Evaluation Facility which known as Stratsec MySEF.

49 Stratsec MySEF found that NLVC 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.

50 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 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

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

52 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.

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

3.2 Recommendation

54 In addition to ensure secure usage of the product, below are additional recommendations for NLVC users:

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) Those responsible for the server must ensure that appropriate authentication and authorization controls for all users and administrators in the underlying environment (including the Operating System, RDBMS, and Web Server) and must ensure that appropriate network layer protection, such as firewall is in place that only permits access through web ports for external users to access the web-server.

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

d) That all SSL certificates are maintained and valid (not revoked or expired), are sourced from a trusted entity.

e) The servers that host the web and database servers are hosted in a secure operating facility with restricted physical access and on dedicated hardware.

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] JMCS Northern Light Video Conferencing System Security Target, Version 1.2, 22 February 2012.

[7] Evaluation Technical Report EAL2 Evaluation of JMCS Northern Light Video Conferencing (NLVC) System, Version 1.0, 23 February 2012.

[8] JMCS Northern Light Video Conferencing System Guidance Documentation, version 1.0, 22 February 2012.

A.2 Terminology

A.2.1 Acronyms

Table 3: List of Acronyms

Acronym	Expanded Term
CB	Certification Body
CC	Common Criteria (ISO/IEC15408)
CCRA	Common Criteria Recognition Arrangement
CEM	Common Evaluation Methodology (ISO/IEC 18045)
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

Acronym	Expanded Term
MySEF	Malaysian Security Evaluation Facility
NLVC	Northern Light Video Conferencing System
PP	Protection Profile
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

A.2.2 Glossary of Terms

Table 4: Glossary of Terms

Term	Definition and Source
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.
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.
Evaluator	The evaluator responsible for managing the technical aspects of a specific evaluation task.

Term	Definition and Source
Hashing	A procedure or mathematical function that changes large data into smaller data. Mostly, the value is used to check any modification in the data and to ensure that an attacker cannot see sensitive information in plain text.
Interpretation	Expert technical judgement, when required, regarding the meaning or method of application of any technical aspect of the criteria or the methodology.
LAN (Local Area Network)	A computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building.
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.
Multicast Technology	Data transmission technology that transmit data only to interested destinations by using special address assignments.
MyCB Personnel	Includes all members of the Certification Subcommittee, the Scheme Manager, the Senior Certifier, Certifiers and the Quality Manager.
National Interpretation	An **interpretation** of the CC, CEM or MyCC Scheme rules that is applicable within the MyCC Scheme only.
OpenVPN	An open source software application that implements virtual private network.
RSW (Real Time Switching) Control Criteria	RSW Control Criteria is an advanced set of controls for Multimedia Conferencing that focused more on bandwidth reduction and prioritizes the participants to avoid confusion when everybody speaks up during conference.
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.
SSL (Secure Socket Layer)	Protocol that helps to protect data integrity that is transmitting in the network by encrypting the data itself.
TSF data	Data created by and for the TOE, which might affect the operation of the TOE.
TSP	TOE Security Policy, a set of rules that regulate how assets are managed, protected and distributed.

Term	Definition and Source
Unicast Technology	Data transmission technology that transmit the same data to all possible destinations.
User	It means any entity (human user or external IT entity) outside the TOE that interacts with the TOE. In this case, users of the TOE are developers who will build custom application to run over the TOE and users of the custom applications.
VPN (Virtual Private Network)	A techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.
WAN (Wide Area Network)	A computer network that covers a broad area / public telecommunication infrastructure, such as internet.

--- END OF DOCUMENT ---