Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Northrop Grumman M5 Network Security SCS100 and SCS200 Software Build 5.3.6

Certification Report
2015/95

1 December 2015
Version 1.0

Amendment Record

Version	Date	Description
0.1	1 August 2015	Internal
1.0	1 December 2015	Final

Executive Summary

This report describes the findings of the IT security evaluation of Northrop Grumman M5 Security Network Secure Communication System (SCS) 100 and SCS 200 Software Build v5.3.6 against Common Criteria and Protection Profiles.

The Target of Evaluation (TOE) is Northrop Grumman M5 Network Security SCS100 and SCS200 Software Build v5.3.6. The TOE is a series of dedicated embedded, small form factor, hardware devices, which provides secure IP-based communication services over any internet connection. It is designed for use in varied environments including mobile networks and sometimes unpredictable situations, which may include environments such as hotel rooms, offices or battlefields. When deployed, the TOE forms a secure Dynamic Multipoint Virtual Protected Network (DMVPN) mesh network with other SCS devices, either via direct connection or over an internet connection. It provides a combination of routing functionality for an "all-in-one" mobile secure network solution. It also provides three network domains, each segregated by separate VPNs. These networks are intended for use with increasingly sensitive data, and each is afforded increased data transport protection.

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security Audit** – The TOE generates audit log records for a large range of events, including security events, configuration changes, user and administrator events, system events and errors
- **Cryptological Support** – baseline cryptological module is included to provide confidentiality and integrity services for authentication
- **User Data Protection** – The TOE zeroes any memory locations prior to use
- **Identification and Authentication** – The TOE requires users to provide unique identification and authentication data before any administration access to the system is granted
- **Security Management** – The TOE provides for an authorised Administrator role
- **Protection of the TSF** – The TOE provides a protection mechanism for its security functions, including cryptological keys and administrator passwords
- **TOE Access** – The TOE can be configured to terminate inactive sessions. The administrator can configure the idle timeout interval
- **Trusted Path / Channels** – The TOE creates trusted channels between itself and remote, trusted authorised IT product and remote administrator.

The report concludes that the product has complied with the Security Requirements for Network Devices, version 1.1 (NDPP) and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by BAE Systems Applied Intelligence and was completed on 24 June 2015.

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

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and Operate the TOE according to the vendor's product administrator guidance
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
d) The evaluators also recommend that the administrator verify the hash of the downloaded software.

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

It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 – Introduction

1.1 Overview

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

1.2 Purpose

The purpose of this Certification Report is to:

a) Report the certification of results of the IT security evaluation of the SCS100 and SCS200 Software Build v 5.3.6 against the requirements of the Common Criteria (CC) and the NDPP v1.1

b) Provide a source of detailed security information about the TOE for any interested parties.

This report should be read in conjunction with the TOE's Security Target (Ref 7) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

The TOE is a series of dedicated embedded hardware devices, which provides secure IP-based communication services over any internet connection. It is designed for use in varied environments and mobile networks and in unpredictable situations, which may include environments such as hotel rooms, offices or battlefields.

When deployed, the TOE forms a secure DMVPN mesh network with other SCS devices, either via direct connection or over an internet connection. It provides a combination of routing functionality for an "all-in-one" mobile secure network solution. It also provides three network domains, each segregated by separate VPNs. These networks are intended for use with increasingly sensitive data, and each is afforded increased data transport protection.

Table 1 Identification Information

Description	Version
Evaluation Scheme	Australasian Information Security Evaluation Program.
TOE	SCS-100 (Firmware 23) & SCS-200 RevC (Firmware 35d)

Software Version	Software Build: 5.3.6
Hardware Platforms	The SCS Modules use a customised version of SCS Linux (based on Fedora v12) as an operating system.
Security Target	Security Target for the SCS-100 & SCS-200 v1.5.3 28 July 2015
Evaluation Technical Report	Evaluation Technical Report SCS100 and SCS 200, v1.0 dated 05 November 2015, Document reference EFS-T033_ETR_v1.0
Criteria	Common Criteria for Information Technology Security Evaluation Part 2 Extended and Part 3 Conformant September 2012, Version 3.1.Rev4
Methodology	Common Methodology for Information Technology Security September 2012, Version 3.1.Rev4
Conformance	Security Requirements for Network Devices, Version 1.1, 08 June 2012 (NDPP)
Developer	Northrop Grumman M5 Network Security 218 Northbourne Avenue Braddon Canberra ACT 2612 Australia
Evaluation Facility	BAE Systems Applied Intelligence, Level 1, 14 Childers Street, Canberra 2600, ACT

Chapter 2 – Target of Evaluation

2.1 Overview

This chapter contains information about the Target of Evaluation (TOE), including a description of functionality provided, its architectural components, the scope of evaluation, security policies, and its secure usage.

2.2 Description of the TOE

The TOE is the Northrop Grumman M5 Network Security SCS100 and SCS200 v5.3.6. The TOE is a series of dedicated embedded hardware devices, which provides secure IP-based communication services over any internet connection. It is designed with small form factor for use in varied environments and mobile networks and sometimes unpredictable situations, which may include environments such as hotel rooms, offices or battlefields.

When deployed, the TOE forms a secure DMVPN mesh network with other SCS devices, either via direct connection or over an internet connection. It provides a combination of routing functionality for an “all-in-one” mobile secure network solution. It also provides three network domains, each segregated by separate VPNs. These networks are intended for use with increasingly sensitive data, and each is afforded increased data transport protection.

The Northrop Grumman M5 Secure Communications System (SCS) is a next-generation secure communications solution for military, government and large corporations. The SCS has been designed to allow mobile teams to securely exchange data in a cost-effective manner, with minimal administrative and configuration overheads.

The SCS products have been specifically designed for operation by non-IT specialists. The SCS-100 and SCS-200 devices feature intuitive graphical user interfaces that allow one-touch set up and simple configuration. To further assist the user, the system utilises network traffic, SNMP, and event log data to detect and repair faults and provide clear advice on system or device status. The system also features remote administration capabilities through the SCS-NMS (not included in the scope of this evaluation).

Each SCS device can manage multiple simultaneous external connections and select the optimal communications path based on performance and/or monetary considerations. Further, the SCS can sense and automatically establish connections with other SCS devices on the same network, further enhancing the communications paths at a system level.

The devices provide three network domains, each segregated by separate VPNs. These networks are intended for use with increasingly sensitive data, and each is afforded increased data transport protection.

- The Black network is protected by an IPsec tunnel. This network is designed for use with unsecured or public networks, such as a remote internet gateway. All communications, including those form the other networks, are routed through this tunnel.

- The Blue network runs within the Black network, and is segregated from the other networks and protected by an additional IPsec tunnel. This network is designed for communications with a remote network with higher security requirements.

- The Red network also runs within the Black network, and is segregated from the other networks and protected by specialised cryptography. This network is designed for communications with a remote network with higher security requirements than the Blue network.

2.3 TOE Functionality

The functionality defined in the Security Target that was subsequently evaluated is summarised as follows:

- **Security Audit** – The TOE generates audit log records for a large range of events, including security events, configuration changes, user and administrator events, system events and errors
- **Cryptological Support** – baseline cryptological module is included to provide confidentiality and integrity services for authentication
- **User Data Protection** – The TOE zeroes memory locations prior to use
- **Identification and Authentication** – The TOE requires users to provide unique identification and authentication data before any administration access to the system is granted
- **Security Management** – The TOE provides for an authorised Administrator role
- **Protection of the TSF** – The TOE provides a protection mechanism for its security functions, including cryptological keys and administrator passwords
- **TOE Access** – The TOE can be configured to terminate inactive sessions. The administrator can configure the idle timeout interval
- **Trusted Path / Channels** – The TOE creates trusted channels between itself and remote, trusted authorised IT product and remote administrator.

2.4 TOE Architecture

The TOE consists of the following major architectural components:

- Each of the SCS-100 and SCS-200 devices implement the core security functionality that meets the SFRs listed in the Security Target document.

- The SCS-100 is designed with size and portability in mind. It provides secure communication services for a single user.

- The SCS-200 provides secure communication services for one to four users. The SCS-200 also provides the ability to make use of external cryptographic modules. The SCS-200 includes two touch screen interfaces, allowing two separate configurations simultaneously.

2.5 Clarification of Scope

The evaluation was conducted in accordance with the Common Criteria and associated methodologies. The evaluated configuration is based on the default installation of the TOE with additional configuration implemented as per Secure Communications System (SCS) Family SCS-100 and SCS-200 Administrator Guide, (Ref 6). The scope of the evaluation was limited to those claims made in the Security Target (Ref 7).

2.5.1 Evaluated Functionality

All tests performed during the evaluation were taken from NDPP (Ref 4) and sufficiently demonstrate the security functionality of the TOE. Some of the tests were combined for ease of execution.

2.5.2 Non-evaluated Functionality and Services

Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref 5) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

The following components are considered outside of the scope of the TOE:

- The SCS-EI and associated remote infrastructure lies outside of the scope of this evaluation.
- Firewall functionality
- VPN Gateway Functionality

2.6 Security

2.6.1 Security Policy

The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected. The Security Target (Ref 7) contains a summary of the functionality to be evaluated:

- Security Audit
- Cryptographic Support
- User Data Protection / Information Flow Control
- Identification and Authentication – note that Telnet and FTP are considered to be out of scope
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Path/Channel

2.7 Usage

2.7.1 Evaluated Configuration

The TOE consists of the SCS-100 (Firmware 23) & SCS-200 RevC (Firmware 35d) and Software Build: 5.3.6. The evaluation was conducted on the default installation and configuration of the TOE with additional guidance and configuration information drawn from the Secure Communications System (SCS) Family SCS-100 and SCS-200 Administrator Guide (Ref 6).

2.7.2 Secure Delivery

To ensure that the software received is the evaluated product the customer must check the version details received against the list specified in the TOE. The customer should perform the following checks to ensure that they have received the correct version of the TOE:

- The shipping label should correctly identify the customer's name and address as well as the product
- The outside packaging should not appear to be tampered with so as to allow access to the contents, packing tape cut or the packaging resealed
- The inside packaging should be sealed and the seal itself should be intact
- Shipment of the device included a confirmation of the order number
- Verify that a shipment notification has been sent via email to the customer point of contact regarding the shipment of the order. The email should include details such as the purchase order number, Supplier order number (which is used to track a shipment), list of items that have been shipped (including any

serial numbers), and address/point of contact details for both the supplier and customer

- If the SCS device has been shipped directly to you, confirm the Bill of Materials (BOM) accompanying the delivery is correct.
- Media cards containing the SCS software are shipped separately and only once delivery receipt of the SCS device is communicated to Northrop Grumman M5.
- For instances where the SCS device(s) is collected in-person from Northrop Grumman M5, it is assumed the BOM and media cards are validated by the client.
- Media cards supplied with the SCS device are preconfigured according to client requirements. Operation of the SCS device in a Common Criteria compliant mode will have been configured prior to the cards being supplied. A checklist is provided in Attachment A of the Secure Communications System (SCS) Family SCS-100 and SCS-200 Administrator Guide (Ref 6).

2.7.3 Installation of the TOE

The Secure Communications System (SCS) Family SCS-100 and SCS-200 Administrator Guide (Ref 6) contains all relevant information for the secure configuration of the TOE.

2.8 Version Verification

The verification of the TOE is using SHA256 hashes.

- Via Command Line

  The version of SCS software running on the devices can be ascertained by checking the file /etc/scs_version. This version indicates the specific release of SCS software which comprises the software packages installed on the device.

  A hash (SHA256) can be used to verify the device is running the correct software packages. The hash is generated by querying and sorting the installed rpms and then redirecting the output through the hashing command

  ```
  $ rpm –qa | sort | sha256sum
  ```

  The result of this command can then compared to the known value of that particular version. Hashes can be obtained from NGM5.

  The SHA256 hash of the Black, Blue and Red images is supplied as part of this process.

- Via Restricted Shell

  reported via the following klish command:

  ```
  exec System version
  ```

- Via SCS UI

  This version number is also displayed on the information screen of the GUI.

- Via System Image

  The released software images for the SCS can also be verified provided this occurs prior to any client customization activities.

  ```
  $ sha256sum 200-black-rel-5.3.1.tgz
  ```

2.9 Documentation and Guidance

It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available to the consumer when the TOE is purchased. All guidance material is available from Northrop Grumman M5 website: http://www.northropgrumman.com/m5

All common criteria material is available at **www.commoncriteriaportal.org**. The Information Security Manual (ISM) is available at **www.asd.gov.au**.

2.10 Secure Usage

The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

Chapter 3 – Evaluation

3.1 Overview

This chapter contains information about the procedures used in conducting the evaluation, the testing conducted as part of the evaluation and the certification result.

3.2 Evaluation Procedures

The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the NDPP (Ref 4) and Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 4 Parts 2 and 3 (Ref 1 and 2).

The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 4 (Ref 3).

The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP).

In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref 10) were also upheld.

3.3 Testing

3.3.1 Testing Coverage

All tests performed by the evaluators were taken from the NDPP. These tests are designed in such a way as to provide a full coverage of testing for all security functions claimed by the TOE. All SFRs listed in the Security Target and the Protection Profile packages were exercised during testing.

3.3.2 Test phases

Testing is determined in the assurance activities in the Protection Profiles. The evaluation was conducted in two phases.

a) The evaluators conducted testing of the TOE during the period of 23rd October 2014 to the 5th of November 2014. The evaluators additionally had to retest portions of the testing for FCS_TLS_EXT.1 on the 27th of March 2015 and the 24th of May 2015 due to issues discovered whilst undertaking cryptographic testing of the TOE using the CAVS tool. Additionally CAVS testing of the TOE was undertaken from the 2nd of February 2015 to the 8th of May 2015.

b) The evaluators obtained test results consistent with expected test results documented in the developer test documentation.

3.4 Entropy Testing

The entropy design description, justification, operation and health tests are assessed and documented in a separate report (Ref 11).

3.5 Penetration Testing

The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly-available information.

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

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

Chapter 4 – Certification

4.1 Overview

This chapter contains information about the result of the certification, an overview of the assurance provided and recommendations made by the certifiers.

4.2 Assurance

This certification is focused on the evaluation of product compliance with a Protection Profile that covers the technology area of network devices. Agencies can have confidence that the scope of an evaluation against an ASD approved Protection Profile covers the necessary security functionality expected of the evaluated product and known security threats will have been addressed.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with Protection Profiles (PPs). PPs provide assurance by a full security target and an analysis of the SFR in that ST, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

The analysis is supported by testing as outlined in the NDPP assurance activities, and a vulnerability analysis (based upon TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

Compliance also provides assurance through evidence of secure delivery procedures.

4.3 Certification Result

After due consideration of the conduct of the evaluation as reported to the certifiers and of the Evaluation Technical Report (Ref 8) the Australasian Certification Authority **certifies** the evaluation of the SCS100 and SCS200 v5.3.6 product performed by the Australasian Information Security Evaluation Facility, BAE Systems Applied Intelligence.

BAE Systems Applied intelligence **has determined** that SCS100 and SCS200 v5.3.6 uphold the claims made in the Security Target (Ref 7) and **has met** the requirements of NDPP.

The effectiveness and integrity of cryptographic functions are also within the scope of product evaluations performed in line with the Protection Profile.

The analysis is supported by testing as outlined in the NDPP assurance activities, and a vulnerability survey demonstrating resistance to penetration attackers with a basic attack potential. Compliance also provides assurance through evidence of secure delivery procedures. Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Recommendations

Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref 5) and New Zealand Government users should consult the GCSB.

In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed, the ACA also recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled
b) Configure and operate the TOE according to the vendor's product administrator guidance
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Function is preserved
d) The evaluators also recommend that the administrator verify the hash of the downloaded software, as obtained from Northrop Grumman M5.

Annex A – References and Abbreviations

A.1 References

1. Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, September 2012, Version 3.1 Revision 4

2. Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, September 2012, Version 3.1 Revision 4

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

4. US Government approved Protection Profile – Protection Profile for Network Devices (NDPP) version 1.1, 8 June 2012

5. 2015 Australian Government Information Security Manual (ISM), Australian Signals Directorate

6. Secure Communications System (SCS) Family SCS-100 and SCS-200 Administrator Guide, v0.3.1.1, 28 July 2015

7. Security Target: SCS100 and SCS200 Security Target version 1.5.3, 28 July 2015

8. Evaluation Technical Report for SCS100 and SCS200, version 1.0, 05 November 2015

9. SCS-100 & SCS-200 Test report version 1.0, 05 November 2015

10. Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, July 2, 2014.

11. SCSx00 – Entropy Documentation and assessment Release Date: 5 May 2015 Version: 1.1

12. NIST publication SP800-90A Recommendations for Random Number Generation Using Deterministic Random Bit Generation, January 2012.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
ASD	Australian Signals Directorate
BOM	Bill of Materials
CC	Common Criteria
CEM	Common Evaluation Methodology
DMVPN	Dynamic Multipoint Virtual Protected Network
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
GCSB	Government Communications Security Bureau
NMS	Network Management System
NDPP	US Government approved Protection Profile for Network Devices
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
SCS	Secure Communication System
SCS-EI	The SCS Enterprise Interface
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy