



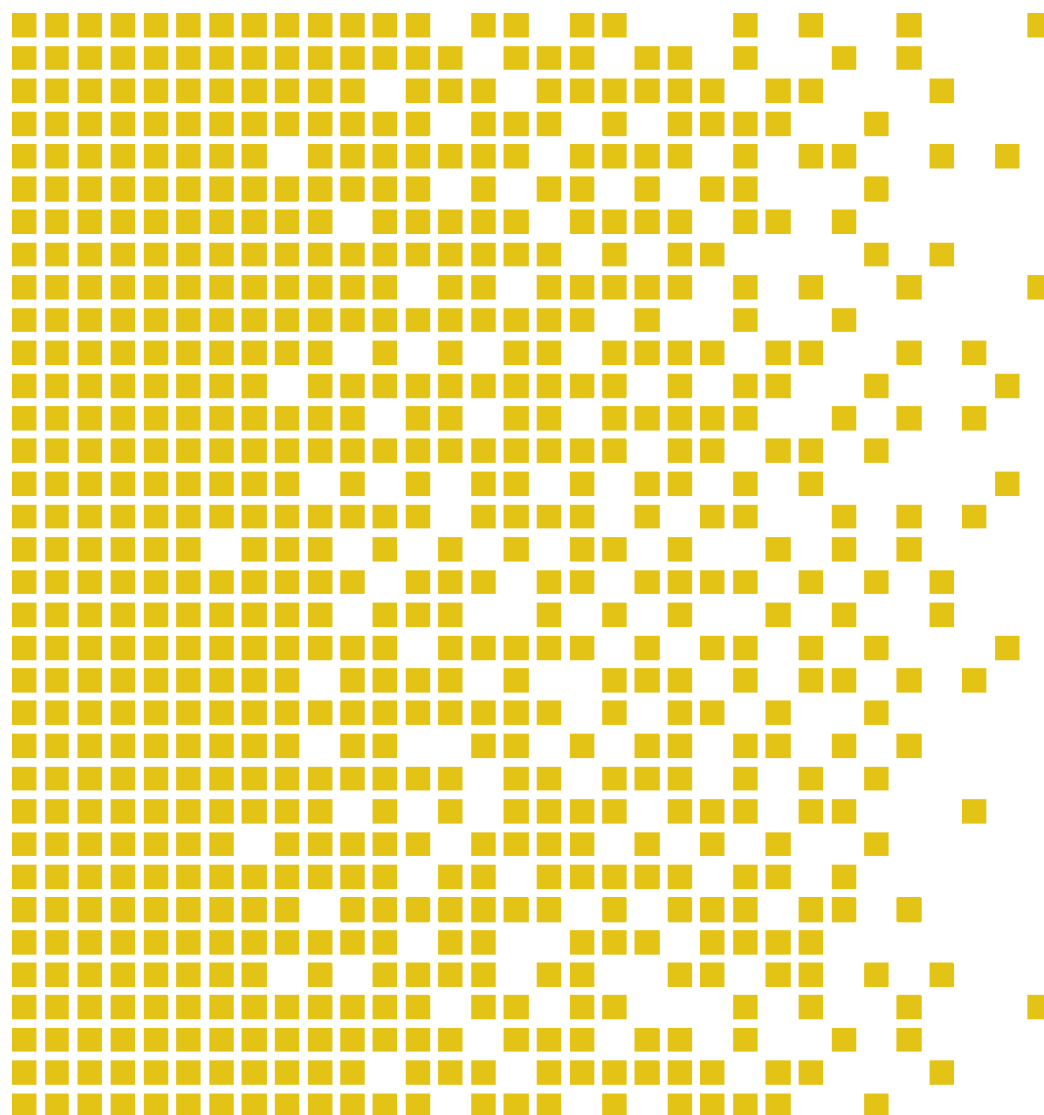
SERTIT

Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

SERTIT-052 CR Certification Report

Issue 1.0 21 August 2013

Huawei S2300, S2700, S5300, S5700, S6300, S6700, S7700, S9300,
S9700 Ethernet Switches V200R003



CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE SD 009 VERSION 2.1 11.11.2011

**ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN
THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

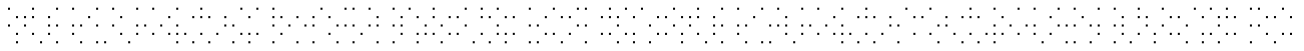
SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the Norwegian evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.



Contents

1	Certification Statement	5
2	Abbreviations	6
3	References	8
4	Executive Summary	9
4.1	Introduction	9
4.2	Evaluated Product	9
4.3	TOE scope	9
4.4	Protection Profile Conformance	9
4.5	Assurance Level	10
4.6	Security Policy	10
4.7	Security Claims	10
4.8	Threats Countered	10
4.9	Threats Countered by the TOE's environment	10
4.10	Threats and Attacks not Countered	11
4.11	Environmental Assumptions and Dependencies	11
4.12	IT Security Objectives	11
4.13	Non-IT Security Objectives	12
4.14	Security Functional Requirements	12
4.15	Security Function Policy	13
4.16	Evaluation Conduct	13
4.17	General Points	13
5	Evaluation Findings	15
5.1	Introduction	16
5.2	Delivery	16
5.3	Installation and Guidance Documentation	16
5.4	Misuse	16
5.5	Vulnerability Analysis	16
5.6	Developer's Tests	17
5.7	Evaluators' Tests	17
6	Evaluation Outcome	17
6.1	Certification Result	17
6.2	Recommendations	17
	Annex A: Evaluated Configuration	18
	TOE Identification	18
	TOE Documentation	27
	TOE Configuration	27
	Environmental Configuration	28



1 Certification Statement

Huawei Technologies Huawei S2300, S2700, S5300, S5700, S6300, S6700, S7700, S9300, S9700 Ethernet Switches provides high-end networking capacities for telecom and enterprise core networks.

Huawei S2300, S2700, S5300, S5700, S6300, S6700, S7700, S9300, S9700 Ethernet Switches version V200R003 has been evaluated under the terms of the Norwegian Certification Scheme for IT Security and have met the Common Criteria Part 3 (ISO/IEC 15408) conformant requirements of Evaluation Assurance Level 3 augmented with ALC_CMC.4 for the specified Common Criteria Part 2 (ISO/IEC 15408) conformant functionality in the specified environment when running on the platforms specified in Annex A.

Author	Kvassnes, Kjartan Jæger	
	Certifier	
Quality Assurance	Arne Høye Røge	
	Quality Assurance	
Approved	Kjell W. Bergan	
	Head of SERTIT	
Date approved	21 August 2013	

2 Abbreviations

ACL	Access Control List
CC	Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)
CCRA	Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
EAL	Evaluation Assurance Level
EOR	Evaluation Observation Report
ETR	Evaluation Technical Report
EVIT	Evaluation Facility under the Norwegian Certification Scheme for IT Security
EWP	Evaluation Work Plan
GUI	Graphical User Interface
LMT	Local Maintenance Terminal
LPU	Line Process Unit
MCU	Main Control Unit
NTP	Network Time Protocol
POC	Point of Contact
PP	Protection Profile
QP	Qualified Participant
RMT	Remote Maintenance Terminal
SERTIT	Norwegian Certification Authority for IT Security
SFR	Security Functional Requirement
SFU	Switching Fabric Unit
SNMP	Simple Network Management Protocol
SPM	Security Policy Model
SPU	Service Process Unit
SRU	Switch Router Unit
ST	Security Target
STP	Spanning-Tree Protocol

TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
VP	Virtual Path
VRP	Versatile Routing Platform

3 References

- [1] Huawei S Series Ethernet Switches V200R003 Security Target, Version 1.0, 2013-07-17.
- [2] Common Criteria Part 1, CCMB-2012-09-001, Version 3.1 R4, September 2012.
- [3] Common Criteria Part 2, CCMB-2012-09-002, Version 3.1 R4, September 2012.
- [4] Common Criteria Part 3, CCMB-2012-09-003, Version 3.1 R4, September 2012.
- [5] The Norwegian Certification Scheme, SD001E, Version 8.0, 20 August 2010.
- [6] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2009-07-004, Version 3.1 R3, September 2012.
- [7] Common Criteria EAL3+ Evaluation of Huawei S-Series Ethernet Switches V200R003, version 1.1, August 9, 2013.
- [8] S2350&S5300&S6300 Series Ethernet Switches V200R003 Product Documentation, version 1.0
- [9] S5700&S6700 V200R003 Product Documentation, version 1.0
- [10] S7700&S9700 Smart&Core Routing Switch V200R003 Product Documentation, version 1.0
- [11] S9300&S9300E Terabit Routing Switch V200R003 Product Documentation, version 1.0
- [12] S9300&S9300E V200R003 Product Documentation, version 1.0
- [13] CC Huawei S Series Ethernet Switches V200R003 - AGD_OPE, version 1.0
- [14] CC Huawei S Series Ethernet Switches V200R003 - AGD_PRE, version 1.0

4 Executive Summary

4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Huawei S2300, S2700, S5300, S5700, S6300, S6700, S7700, S9300, S9700 Ethernet Switches version V200R003 to the Sponsor, Huawei Technologies, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the Security Target[1] which specifies the functional, environmental and assurance evaluation requirements.

4.2 Evaluated Product

The versions of the product evaluated were Huawei S2300, S2700, S5300, S5700, S6300, S6700, S7700, S9300, S9700 Ethernet Switches version V200R003.

These products are also described in this report as the Target of Evaluation (TOE). The developer was Huawei Technologies.

Huawei S Series Ethernet Switches V200R003, the TOE, provides high-end networking capacities for telecom and enterprise core networks. It consists of both hardware and software.

At the core of each switch is the Versatile Routing Platform (VRP), the software for managing and running the router's networking functionality. VRP provides extensive security features. These features include different interfaces with according access levels for administrators; enforcing authentications prior to establishment of administrative sessions with the TOE; auditing of security-relevant management activities; as well as the correct enforcement of routing decisions to ensure that network traffic gets forwarded to the correct interfaces.

The Forwarding Engine is the actual hardware providing network traffic processing capacity.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

4.3 TOE scope

The TOE scope is described in the ST[1], chapter 1.4.2

4.4 Protection Profile Conformance

The Security Target[1] did not claim conformance to any protection profile.

4.5 Assurance Level

The assurance incorporated predefined evaluation assurance level EAL3, augmented by ALC_CMC.4. Common Criteria Part 3[4] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1[2].

4.6 Security Policy

The TOE security policies are detailed in the ST[1], chapter 3.2.

4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives meet and security functional requirements and security functions to elaborate the objectives. All of the SFR's are taken from CC Part 2[3]; use of this standard facilitates comparison with other evaluated products.

4.8 Threats Countered

- T.UnwantedL2NetworkTraffic
Unwanted L2 network traffic sent to the TOE will cause the MAC table gets updated dynamically by MAC learning function . This may due the MAC table overload. In the TOE Layer 2 switching network, loops on the network cause packets to be continuously duplicated and propagated in the loops, leading to the broadcast storm, which exhausts all the available bandwidth resources and renders the network unavailable.
- T.UnwantedL3NetworkTraffic
Unwanted L3 network traffic sent to the TOE will not only cause the TOE's processing capacity for incoming network traffic is consumed thus fails to process traffic expected to be processed, but an internal traffic jam might happen when those traffic are sent to the Control Plane. This may further cause the TOE to fail to respond to system control and security management operations. Routing information exchanged between the TOE and peer routes may also be affected due the traffic overload.
- T.UnauthenticatedAccess
A user who is not an administrator gains access to the TOE.
- T.UnauthorizedAccess
A user authorized to perform certain actions and access certain information gains access to commands or information he is not authorized for.
- T.Eavesdrop
An eavesdropper (remote attacker) is able to intercept, and potentially modify or re-use information assets that are exchanged between TOE and LMT/RMT.

4.9 Threats Countered by the TOE's environment

There are no threats countered by the TOE's environment.

4.10 Threats and Attacks not Countered

No threats or attacks that are not countered are described.

4.11 Environmental Assumptions and Dependencies

The environment is supposed to provide supporting mechanism to the TOE:

- A Radius server for external authentication/authorization decisions;
- Peer router(s) for the exchange of dynamic routing information;
- A remote entities (PCs) used for administration of the TOE.
- An SNMP Server used for collecting SNMP traps

4.12 IT Security Objectives

The following objectives must be met by the TOE:

- **O.Forwarding (all series except S23XX-EI/S53XX-LI/S27XX-EI/S57XX-LI)**
The TOE shall forward network traffic (i.e., individual packets) only to the network interface that corresponds with a configured route for the destination IP address of the packet, or corresponds with a MAC address for the destination MAC address of the packet. When TOE works as Layer 2 forwarding device, users should be isolated between VLANs. And TOE can find the loops in the network, and block certain interfaces to eliminate loops.
- **O.Forwarding (S23XX-EI/S53XX-LI/S27XX-EI/S57XX-LI)**
The TOE shall forward network traffic (i.e., individual packets) only to the network interface that corresponds with a MAC address for the destination MAC address of the packet. Users should be isolated between VLANs. And TOE can find the loops in the network, and block certain interfaces to eliminate loops.
- **O.Communication**
The TOE must implement logical protection measures for network communication between the TOE and LMT/RMT from the operational environment.
- **O.Authorization**
The TOE shall implement different authorization levels that can be assigned to administrators in order to restrict the functionality that is available to individual administrators.
- **O.Authentication**
The TOE must authenticate users of its user access.
- **O.Audit**
The TOE shall provide functionality to generate audit records for security-relevant administrator actions.
- **O.Resource**
The TOE shall provide functionalities and management for assigning a priority (used as configured bandwidth), enforcing maximum quotas for bandwidth and MAC address table entries, to prevent internal collapse due to traffic overload

- **O.Filter**

The TOE shall provide ACL or packet filter to drop unwanted L2 or L3 network traffic.

4.13 Non-IT Security Objectives

The following objectives must be met by the operational environment:

- **OE.NetworkElements**

The operational environment shall provide securely and correctly working network devices as resources that the TOE needs to cooperate with. Behaviors of such network devices provided by operational environment shall be also secure and correct. For example, other routers for the exchange of routing information, PCs used for TOE administration, SNMP Servers and Radius servers for obtaining authentication and authorization decisions.

- **OE.Physical**

The TOE (i.e., the complete system including attached peripherals, such as a console, and CF card inserted in the Switch) shall be protected against unauthorized physical access.

- **OE.NetworkSegregation**

The operational environment shall provide segregation by deploying the management interface in TOE into an independent local -network.

- **OE.Person**

Personnel working as authorized administrators shall be carefully selected for trustworthiness and trained for proper operation of the TOE.

4.14 Security Functional Requirements

The following functional requirements are met by the TOE:

- FAU_GEN.1 Audit data generation
- FAU_GEN.2 | User identity association
- FAU_SAR.1 Audit review
- FAU_SAR.3 Selectable audit review
- FAU_STG.1 Protected audit trail storage
- FAU_STG.3 Action in case of possible audit data loss
- FCS_COP.1/AES Cryptographic operation
- FCS_COP.1/3DES Cryptographic operation
- FCS_COP.1/RSA Cryptographic operation
- FCS_COP.1/MD5 Cryptographic operation
- FCS_COP.1/HMAC-MD5 Cryptographic operation
- FCS_COP.1/DHKeyExchange Cryptographic operation
- FCS_CKM.1/AES Cryptographic key generation
- FCS_CKM.1/3DES Cryptographic key generation
- FCS_CKM.1/RSA Cryptographic key generation
- FCS_CKM.1/DHKey Cryptographic key generation
- FCS_CKM.1/HMAC Cryptographic key generation
- FCS_CKM.4/RSA Cryptographic key destruction

- FCS_CKM.4/3DES-AES-HMAC Cryptographic key destruction

4.15 Security Function Policy

The VRP is the control and management platform that runs on the SRU/MCU. The VRP supports IPv4/IPv6, and routing protocols such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), calculates routes, generates forwarding tables, and delivers routing information to the LPU(s). The VRP includes Service Control Plane (SCP), System Manage Plane (SMP), General Control Plane (GCP) and other TSF, non-TSF sub-systems.

There is one difference between the software architecture of Box Switch and the Chassis Switch: in Box Switches the LPU and VP are done in SW, but in Chassis Switches, this is done in HW.

Note that for the S23xx-EI/S53xx-LI and S27xx-EI/S57xx-LI (who do not support L3 forwarding) and the S53xx-SI and S57xx-SI (who only support static routing), the software architecture is identical, but the commands required to support non-existing functionality will simply return error messages.

4.16 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001[5]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security (CCRA), and the evaluation was conducted in accordance with the terms of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target[1], which prospective consumers are advised to read. To ensure that the Security Target[1] gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[6].

SERTIT monitored the evaluation which was carried out by the Brightsight B.V. Commercial Evaluation Facility (CLEF/EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT in 9 August 2013. SERTIT then produced this Certification Report.

4.17 General Points

The evaluation addressed the security functionality claimed in the Security Target[1] with reference to the assumed operating environment specified by the Security Target[1]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.



Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.

5 Evaluation Findings

The evaluators examined the following assurance classes and components taken from CC Part 3[4]. These classes comprise the EAL 3 assurance package augmented with ALC_FLR.2.

Assurance class	Assurance components	
Development	ADV_ARC.1	Security architecture description
	ADV_FSP.3	Functional specification with complete summary
	ADV_TDS.2	Architectural design
Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
Life-cycle support	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS.3	Implementation representation CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_DVS.1	Identification of security measures
	ALC_FLR.2	Flaw reporting procedures
	ALC_LCD.1	Developer defined life-cycle model
Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
Tests	ATE_COV.2	Analysis of coverage
	ATE_DPT.1	Testing: basic design
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

All assurance classes were found to be satisfactory and were awarded an overall "pass" verdict.

5.1 Introduction

The evaluation addressed the requirements specified in the Security Target[1]. The results of this work were reported in the ETR[7] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated versions of its components have been supplied, and to check that the security of the TOE has not been compromised in delivery.

5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance in the Operational User Guidance[13][14] and Preparative Procedures documents provided by the developer.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The guidance should always follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

The TOE are substantially similar to other router/switches on the market. This technology is well-established. The technology and possible vulnerabilities are described in a series of public documents.

The evaluators assessed all possible vulnerabilities found during evaluation. Potential vulnerabilities were found but only one turned out to be possibly exploitable. The developer has updated the guidance to enhance the secure configuration of the TOE, and as a result this issue has become moot.

5.6 Developer's Tests

The developer test effort is considered already fairly complete. Any major missing features reported by the evaluators are added to the developer test set. Nevertheless the evaluator has defined 11 additional tests.

The Developer Test Plan consists of 11 different categories, each containing between 1 and 13 tests. The categories are based on major groupings of security functionality, and in combination cover all SFRs and TSFIs.

5.7 Evaluators' Tests

For independent testing, the evaluator has chosen to perform some additional testing although the developer's testing was extensive but some additional assurance could be gained by additional testing.

For independent testing, the evaluator has made a sample of one test of each category, with one exception, as that category has only one test and this test was sufficiently repeated later on

6 Evaluation Outcome

6.1 Certification Result

After due consideration of the ETR[7], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Huawei S2300, S2700, S5300, S5700, S6300, S6700, S7700, S9300, S9700 Ethernet Switches version V200R003 meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level 3 augmented with ALC_CMC.4 for the specified Common Criteria Part 2 conformant functionality, in the specified environment, when running on platforms specified in Annex A.

6.2 Recommendations

Prospective consumers of Huawei S2300, S2700, S5300, S5700, S6300, S6700, S7700, S9300, S9700 Ethernet Switches version V200R003 should understand the specific scope of the certification by reading this report in conjunction with the Security Target[1]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above under Section 4.3 "TOE Scope" and Section 0 "Evaluation Findings".

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

Annex A: Evaluated Configuration

TOE Identification

The TOE consists of Huawei S2300, S2700, S5300, S5700, S6300, S6700, S7700, S9300, S9700 Ethernet Switches V200R003

There are some minor security differences between the various series: not all series support all functionality:

- The S23xx-EI/S53xx-LI and S27XX-EI/S57XX-LI do not support L3 forwarding
- The S53xx-SI and S57xx-SI only support static routing and no OSPF/BGP

MODEL TYPES	Typical System Configuration and Physical Parameters		
S2300	Item	Typical Configuration	Remark
	Processing unit	Main frequency: 1GHZ	-
	SDRAM	256MB	-
	Flash	200MB	-
	CF card	-	-
	Switching capacity	S2350-20TP-PWR-EI-AC:11.2Gbit/s S2350-28TP-EI-AC: 12.8 Gbit/s S2350-28TP-PWR-EI-AC:12.8 Gbit/s (bidirectional)	-
	Forwarding capacity	S2350-20TP-PWR-EI-AC: 8.33Mpps S2350-28TP-EI-AC: 9.52Mpps S2350-28TP-PWR-EI-AC: 9.52Mpps	-
S5300	Item	Typical Configuration	Remark
Processing unit	Main frequency: 5300EI: 533MHZ 5300SI: 800MHZ	-	

		5300HI: 1GHZ 5300LI: 1GHZ 5310EI: 1GHZ	
	SDRAM	5300EI: 256MB 5300SI: 256MB 5300HI: 512MB 5300LI: 256MB 5310EI: 512MB	-
	Flash	5300EI: 32MB 5300SI: 32MB 5300HI: 64MB 5300LI: 200MB 5310EI: 200MB	-
	CF card	-	-
	Switching capacity	5324TP-SI: 48Gbit/s 5348TP-SI: 96Gbit/s 5328C-EI/SI: 128Gbit/s 5352C-EI/SI: 176Gbit/s 5300-28P-LI: 56Gbps 5300-52P-LI: 104Gbps 5300-28X-LI: 128Gbps 5300-10P-LI: 26Gbps (bidirectional)	-
	Forwarding capacity	5324TP-SI: 35.7Mpps 5348TP-SI: 71.4Mpps 5328C-EI/SI: 95.2Mpps 5352C-EI/SI: 130.9Mpps 5300-28P-LI: 41.66Mpps 5300-52P-LI: 77.4Mpps	-

		5300-28X-LI: 95.2Mpps 5300-10P-LI: 15Mpps	
S6300	Item	Typical Configuration	Remark
	Processing unit	Main frequency: 1 GHz	-
	SDRAM	512 MB	-
	Flash	64 MB	-
	CF card	-	-
	Switching capacity	6324: 480Gbit/s 6348: 960Gbit/s (bidirectional)	-
	Forwarding capacity	6324: 357Mpps 6348: 714Mpps	-
S2700	Item	Typical Configuration	Remark
	Processing unit	Main frequency: 1GHZ	-
	SDRAM	256MB	-
	Flash	200MB	-
	CF card	-	-
	Switching capacity	S2750-20TP-PWR-EI-AC:11.2Gbit/s S2750-28TP-EI-AC: 12.8 Gbit/s S2750-28TP-PWR-EI-AC:12.8 Gbit/s S2751-28TP-PWR-EI-AC:12.8 Gbit/s	-

		(bidirectional)	
	Forwarding capacity	S2750-20TP-PWR-EI-AC: 8.33Mpps S2750-28TP-EI-AC: 9.52Mpps S2750-28TP-PWR-EI-AC: 9.52Mpps S2751-28TP-PWR-EI-AC: 9.52Mpps	-
S5700	Item	Typical Configuration	Remark
	Processing unit	Main frequency: 5700EI: 533MHZ 5700SI: 800MHZ 5700HI: 1GHZ 5700LI: 1GHZ 5710EI: 1GHZ 5710HI: 1GHz	-
	SDRAM	5700EI: 256MB 5700SI: 256MB 5700HI: 512MB 5700LI: 256MB 5710EI: 512MB 5710HI: 512MB	-
	Flash	5700EI: 32MB 5700SI: 32MB 5700HI: 64MB 5700LI: 200MB 5710EI: 200MB	-
	CF card	-	-
	Switching capacity	5724TP-SI: 48Gbit/s 5748TP-SI: 96Gbit/s 5728C-EI/SI: 128Gbit/s	-

		5752C-EI/SI: 176Gbit/s 5700-28P-LI: 56Gbps 5700-52P-LI: 104Gbps 5700-28X-LI: 128Gbps 5700-52X-LI: 256Gbps 5700-10P-LI: 26Gbps 5710-108C-HI: 672Gbs (bidirectional)	
	Forwarding capacity	5724TP-SI: 35.7Mpps 5748TP-SI: 71.4Mpps 5728C-EI/SI: 95.2Mpps 5752C-EI/SI: 130.9Mpps 5700-28P-LI: 41.66Mpps 5700-52P-LI: 77.4Mpps 5700-28X-LI: 95.2Mpps 5700-52X-LI: 132Mpps 5700-10P-LI: 15Mpps S5710-108C-HI: 504Mpps	-
S6700	Item	Typical Configuration	Remark
	Processing unit	Main frequency: 1 GHz	-
	SDRAM	512 MB	-

	Flash	64 MB	-
	CF card	-	-
	Switching capacity	6724: 480Gbit/s 6748: 960Gbit/s (bidirectional)	-
	Forwarding capacity	6724: 357Mpps 6748: 714Mpps	-
S9303 S7703	Item	Typical Configuration	Remark
	Processing unit	Main frequency: 500 MHz	-
	SDRAM	512 MB	
	NVRAM	512 KB	-
	CF card	512 MB	CF cards with different capacities can be configured. Can be used as a mass storage device for storing data files. There are two CF cards on the SRU.
	Switching capacity	1440 Gbit/s	-
	Forwarding capacity	540 Mpps	-
	Max MCU slots	2	MCUs work in 1:1 redundancy.
	Max LPU slots	3	-
	Maximum interface rate per LPU	40*10 Gbit/s	-

S9306 S7706	Item	Typical Configuration	Remark
	Processing unit	Main frequency: 700 MHz	-
	SDRAM	1 GB	
	NVRAM	512 KB	-
	CF card	512 MB	CF cards with different capacities can be configured. Can be used as a mass storage device for storing data files. There are two CF cards on the SRU.
	Switching capacity	2T Gbit/s	-
	Forwarding capacity	1320 Mpps	-
	Max SRU slots	2	SRUs work in 1:1 redundancy.
	Max LPU slots	6	-
	Maximum interface rate per LPU	40*10 Gbit/s	-
S9312 S7712	Item	Typical Configuration	Remark
	Processing unit	Main frequency: 700 MHz	-
	SDRAM	1 GB	
	NVRAM	512 KB	-
	CF card	512 MB	CF cards with different capacities can be configured. Can be used as a mass storage device for storing data files.

			There are two CF cards on the SRU.
	Switching capacity	2T Gbit/s	-
	Forwarding capacity	1320 Mpps	-
	Max SRU slots	2	SRUs work in 1:1 redundancy.
	Max LPU slots	12	-
	Maximum interface rate per LPU	40*10 Gbit/s	-
S9303E	Item	Typical Configuration	Remark
S9703	Processing unit	Main frequency: 500 MHz	-
	SDRAM	512 MB	
	NVRAM	512 KB	-
	CF card	512 MB	CF cards with different capacities can be configured. Can be used as a mass storage device for storing data files. There are two CF cards on the SRU.
	Switching capacity	1440 Gbit/s	-
	Forwarding capacity	540 Mpps	-
	Max MCU slots	2	MCUs work in 1:1 redundancy.
	Max LPU slots	3	-
	Maximum interface rate per LPU	40*10 Gbit/s	-

S9306E S9706	Item	Typical Configuration	Remark
	Processing unit	Main frequency: 1.2G MHz	-
	SDRAM	2GB	
	NVRAM	512 KB	-
	CF card	512 MB	CF cards with different capacities can be configured. Can be used as a mass storage device for storing data files. There are two CF cards on the SRU.
	Switching capacity	3.84T Gbit/s	-
	Forwarding capacity	2880 Mpps	-
	Max SRU slots	2	SRUs work in 1:1 redundancy.
	Max LPU slots	6	-
	Maximum interface rate per LPU	40*10 Gbit/s	-
S9312E S9712	Item	Typical Configuration	Remark
	Processing unit	Main frequency: 700 MHz	-
	SDRAM	2 GB	
	NVRAM	512 KB	-
	CF card	512 MB	CF cards with different capacities can be configured. Can be used as a mass storage device for storing data files.

			There are two CF cards on the SRU.
	Switching capacity	3.84T Gbit/s	-
	Forwarding capacity	2880 Mpps	-
	Max SRU slots	2	SRUs work in 1:1 redundancy.
	Max LPU slots	12	-
	Maximum interface rate per LPU	40*10 Gbit/s	-

TOE Documentation

The supporting guidance documents evaluated were:

- [a] S2350&S5300&S6300 Series Ethernet Switches V200R003 Product Documentation, version 1.0
- [b] S5700&S6700 V200R003 Product Documentation, version 1.0
- [c] S7700&S9700 Smart&Core Routing Switch V200R003 Product Documentation, version 1.0
- [d] S9300&S9300E Terabit Routing Switch V200R003 Product Documentation, version 1.0
- [e] S9300&S9300E V200R003 Product Documentation, version 1.0
- [f] CC Huawei S Series Ethernet Switches V200R003 - AGD_OPE, version 1.0
- [g] CC Huawei S Series Ethernet Switches V200R003 - AGD_PRE, version 1.0

Further discussion of the supporting guidance material is given in Section 5.3 "Installation and Guidance Documentation".

TOE Configuration

The following configuration was used for testing:

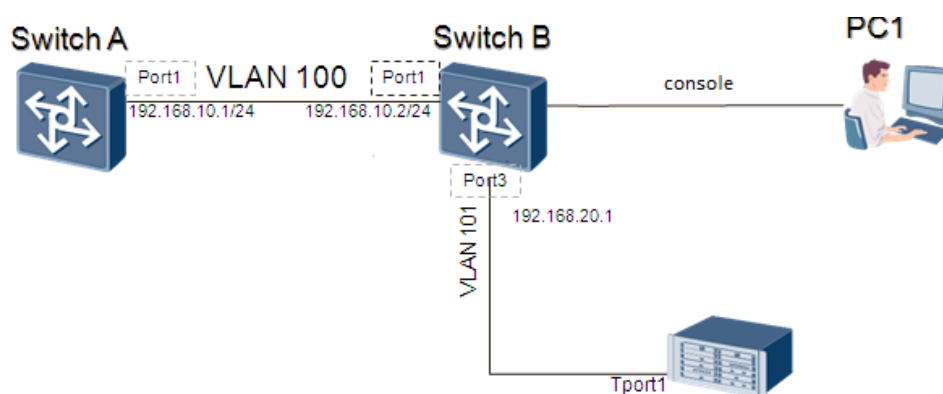
Item	Identifier
HARDWARE	One of the hardware models listed in section TOE Identification
SOFTWARE	Product software version V200R003, VRP

Version 5 Release 13, VxWorks version
5.5.1 configured according to [AGD_PRE].

MANUALS	S2350&S5300&S6300 Series Ethernet Switches V200R003 Product Documentation, version 1.0 S5700&S6700 V200R003 Product Documentation, version 1.0 S7700&S9700 Smart&Core Routing Switch V200R003 Product Documentation, version 1.0 S9300&S9300E Terabit Routing Switch V200R003 Product Documentation, version 1.0 S9300&S9300E V200R003 Product Documentation, version 1.0 CC Huawei S Series Ethernet Switches V200R003 - AGD_OPE, version 1.0 CC Huawei S Series Ethernet Switches V200R003 - AGD_PRE, version 1.0
---------	---

Environmental Configuration

The TOE is tested in the following test set-up.



Certificate

The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of The Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced. Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown of this certificate. This certificate is not an endorsement of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.

Product Manufacturer: Huawei Technologies

Product Name: Huawei S2300, S2700, S5300, S5700, S6300, S6700, S7700, S9300, S9700 Ethernet Switches V200R003

Type of Product: Ethernet Switch

Version and Release Numbers: Version V200R003

Assurance Package: EAL 3 augmented with ALC_CMC.4

Evaluation Criteria: Common Criteria version 3.1R4 (ISO/IEC 15408)

Name of IT Security Evaluation Facility: Brightsight B.V.

Name of Certification Body: SERTIT

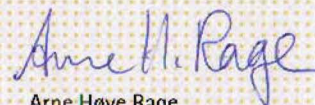
Certification Report Identifier: SERTIT-052 CR, issue 1.0, 21 August 2013

Certificate Identifier: SERTIT-052 C

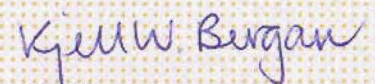
Date Issued: 21 August 2013



Kjartan Jæger Kvassnes
Certifier



Arne Høye Rage
Quality Assurance



Kjell Werner Bergan
Head of SERTIT



SERTIT

Norwegian Certification Authority for IT Security

