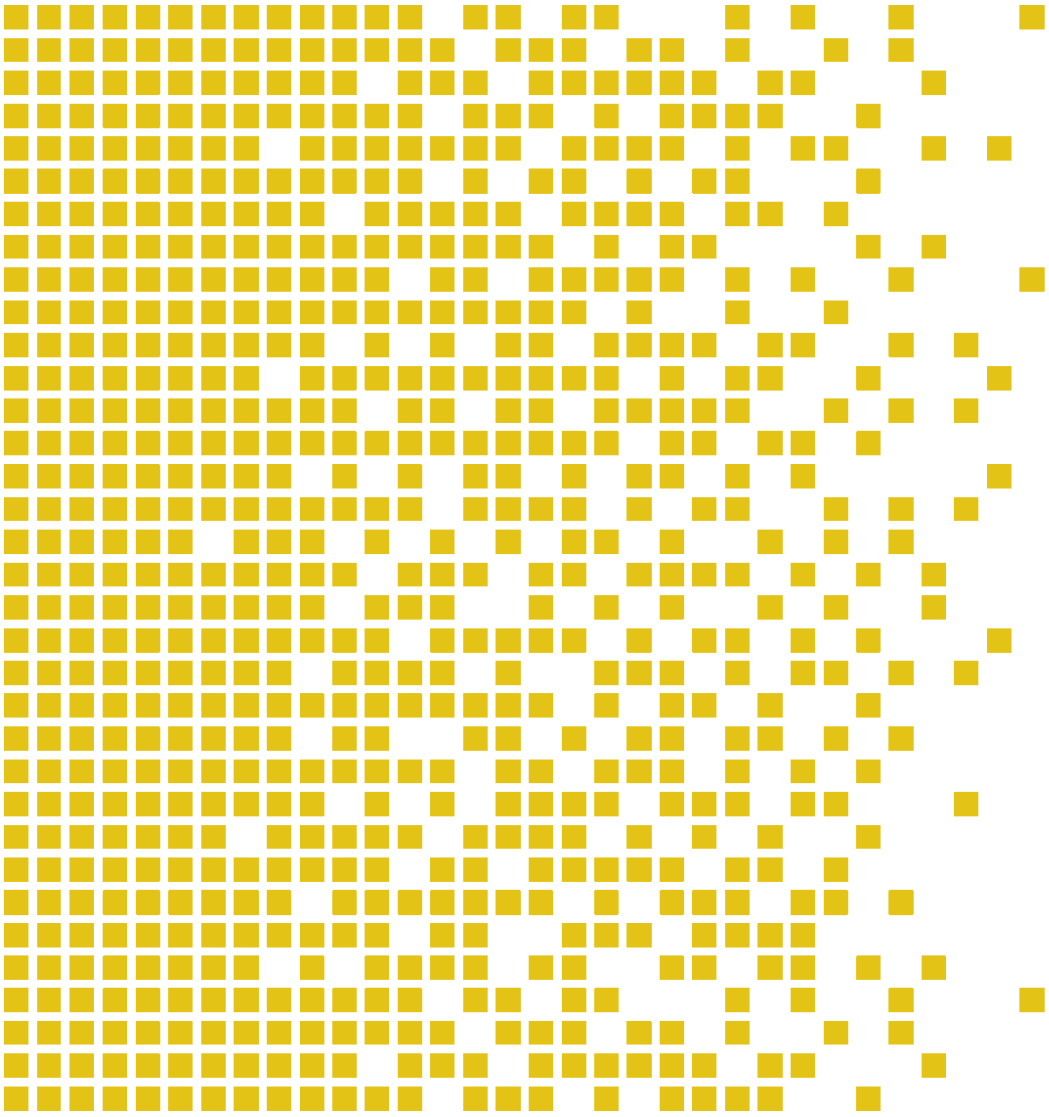
# SERTIT-070 CR Certification Report

Issue 1.0 23 November 2015

## Huawei AR Series Routers V200R006C10SPC030





SERTIT, Postboks 814, 1306 Sandvika, NORWAY
Phone: +47 67 86 40 00 Fax: +47 67 86 40 09 E-mail: post@sertit.no Internet: www.sertit.no

**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.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of the CCRA July 2nd 2014. The recognition under CCRA is limited to cPP related assurance packages or EAL 2 and ALC_FLR CC part 3 components.

**MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (SOGIS MRA)**

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

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

Huawei Technology Co. Ltd. Huawei AR Series Routers is a Huawei AR Series Routers (See Annex A for details) are the next-generation routing and gateway devices, which provide the routing, switching, wireless, voice, and security functions.

Huawei AR Series Routers version V200R006C10SPC030 have 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 EAL 3 augmented with ALC_FLR.2 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 | Kjartan Kvassnes<br>Certifier |
| Quality Assurance | Arne Høye Rage<br>Quality Assurance |
| Approved | Øystein Hole<br>Head of SERTIT |
| Date approved | 23 November 2015 |

# 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 |
| 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 |
| LMT | Local Maintenance Terminal |
| LPU | Line Process Unit |
| MCU | Main Control Unit |
| MPU | Main Processing Unit |
| 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 |
| SPM | Security Policy Model |
| SPU | Service Process Unit |
| SRU | Switch Router Unit |
| ST | Security Target |
| TOE | Target of Evaluation |
| TSF | TOE Security Functions |
| TSP | TOE Security Policy |
| VRP | Versatile Routing Platform |

# 3 References

[1] Huawei AR Series Service Routers V200R006C10 Security Target, Version 1.4, 15 June 2015.

[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-2012-09-004, Version 3.1 R4, September 2012.

[7] Evaluation Technical Report Common Criteria EAL3+ Evaluation of Huawei AR Series Routers V200R006C10SPC030, version 1.2, 28 July 2015.

[8] AR150&AR160&AR200&AR510&AR1200&AR2200&AR3200 Hardware Description, Issue 16, 15 Sep. 2014

[9] AR V200R006C10 Product Manual, v1.0

[10] Common Criteria Security Evaluation – Certification Configuration, v1.4, 23 April 2015

# 4 Executive Summary

## 4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Huawei AR Series Routers version V200R006C10SPC030 to the Sponsor, Huawei Technology Co. Ltd., 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 version of the product evaluated was Huawei AR Series Routers version V200R006C10SPC030.

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

Huawei AR Series Routers are the next-generation routing and gateway devices, which provide the routing, switching, wireless, voice, and security functions. Huawei AR provides a highly secure and reliable platform for scalable multiservice integration at enterprise and commercial branch offices of all sizes and small-to-medium sized businesses. It consists of both hardware and software.

At the core of each router is the VRP (Versatile Routing Platform) deployed on MPU (Main Processing Unit) or SRU (Switch Routing Unit), the software for managing and running the router's networking functionality. VRP provides security features including: 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.

MPU (Main Processing Unit) or SRU (Switch Routing Unit) are also providing network traffic processing capacity. Network traffic is processed and forwarded according to routing decisions downloaded from VRP.

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 1.4.2.1 and 1.4.2.2

## 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 EAL 3, augmented by ALC_FLR.2. 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

There are no Organizational Security Policies or rules with which the TOE must comply.

## 4.7 Security Claims

The Security Target[1] fully specifies the TOE's security objectives, the threats which these objectives counter 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 fails 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 of the TOE gains access to the TOE management interface.

- **T.UnauthorizedAccess**
  A user of the TOE 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) in the management network served by the TOE

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

It is assumed that the TOE (including any console attached, access of SD card) is protected against unauthorized physical access.

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.

It is assumed that the ETH interface in the TOE will be accessed only through sub-network where the TOE hosts. The sub-network is separate from the application (or, public) networks where the interfaces in the TOE are accessible.

The authorized administrators are not careless, will fully negligent or hostile, and will follow and abide by the instructions provided by the TOE documentation.

## 4.12 IT Security Objectives

The following objectives must be met by the TOE:

- O.Forwarding
  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, traffic should be isolated between VLANs. And TOE can find the loops in the network, and block certain interfaces to eliminate loops. TOE should supported stateful packet filtering, defend against network attacks.

- 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.

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

## 4.13 Non-IT Security Objectives

- 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, 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 SD card inserted in the Router) shall be protected against unauthorized physical access.

- OE.NetworkSegregation
  The operational environment shall provide segregation by deploying the management interface in TOE into a local sub-network, compared to the network interfaces in TOE serving the application (or public) 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

- 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_MD5 Cryptographic key generation
- FCS_CKM.4/RSA Cryptographic key destruction
- FDP_ACC.1 Subset access control
- FDP_ACF.1 Security attribute based access control
- FDP_DAU.1 Basic Data Authentication(for all series except AR1220-S/ AR1220W-S/AR2220-S/AR201-S/AR207-S/AR502G-L-D/AR502GR-L-D)
- FDP_DAU.1 Basic Data Authentication(for AR1220-S/ AR1220W-S/AR2220-S/AR201-S/AR207-S)
- FDP_DAU.1 Basic Data Authentication(for AR502G-L-D/AR502GR-L-D)
- FDP_IFC.1 Subset information flow control
- FDP_IFF.1 Simple security attributes (for all series except AR502G-L-D/AR502GR-L-D/AR511GW-LAV2M3/AR511GW-LM7/AR513W-V3M8)
- FDP_IFF.1 Simple security attributes (for AR502G-L-D/AR502GR-L-D/AR511GW-LAV2M3/AR511GW-LM7/AR513W-V3M8)
- FIA_AFL.1 Authentication failure handling
- FIA_ATD.1 User attribute definition
- FIA_SOS.1 Verification of secrets
- FIA_UAU.2 User authentication before any action
- FIA_UID.2 User identification before any action
- FMT_MOF.1 Management of security functions behaviour
- FMT_MSA.1 Management of security attributes
- FMT_MSA.3 Static attribute initialization
- FMT_SMF.1 Specification of Management Functions
- FMT_SMR.1 Security roles
- FPT_STM.1 Reliable time stamps
- FPT_FLS.1 Fail secure
- FRU_PRS.1 Limited priority of service
- FRU_RSA.1 Maximum quotas
- FRU_FLT.1 Degraded fault tolerance
- FTA_SSL.3 TSF-initiated termination
- FTA_TSE.1 TOE session establishment
- FTP_TRP.1 Trusted path

## 4.15 Security Function Policy

At the core of each router is the VRP (Versatile Routing Platform) deployed on MPU (Main Processing Unit) or SRU (Switch Routing Unit), the software for managing and running the router's networking functionality. VRP provides security features including: 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.

MPU (Main Processing Unit) or SRU (Switch Routing Unit) are also providing network traffic processing capacity. Network traffic is processed and forwarded according to routing decisions downloaded from VRP.

## 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 Senior Officials Group Information Systems Security (SOGIS) and the evaluation was conducted in accordance with the terms of these Arrangements.

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 Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the final Evaluation Technical Report (ETR)[7] to SERTIT in 28-07-2015. 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.3 | Authorisation controls |
| | ALC_CMS.3 | Implementation representation CM coverage |
| | ALC_DEL.1 | Delivery procedures |
| | ALC_DVS.1 | Identification of security measures |
| | ALC_LCD.1 | Developer defined life-cycle model |
| | ALC_FLR.2 | Flaw reporting procedures |
| Security Target evaluation | ASE_CCL.1 | Conformance claims |
| | ASE_ECD.1 | Extended components definition |
| | ASE_INT.1 | ST introduction |
| | ASE_REQ.2 | Derived security requirements |
| | ASE_SPD.1 | Security problem definition |
| | ASE_OBJ.2 | Security objectives |
| | 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 consistuent 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 listed in the ST[1] chapter 1.4.2.1 and Preparative Procedures documents [9] provided by the developer. The Common Criteria Security Evaluation – Certified Configuration [10] describes all necessary steps to configure the TOE in the certified configuration.

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. The readers are recommended to note the following two points:

- The AR160 series routers does not support MAC address limitation functionality, therefore the user must use ACL rules as per described in the guidance [10] to prevent relevant attacks.
- The correctness of the configuration file must be checked following the instructions given by the guidance [10] to prevent possible vulnerabilities.

## 5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user 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 two 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 Plan consists of 12 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 AR Series Routers version V200R006C10SPC030 meet the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL 3 augmented with ALC_FLR.2 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 AR Series Routers version V200R006C10SPC030 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 5 “Evaluation Findings”.

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

The above “Evaluation Findings” include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

# Annex A: Evaluated Configuration

## TOE Identification

The TOE consists of Huawei AR150 series, AR 160 series, AR200 series, AR1200 series, AR2200 series, AR3200 series, AR510 series, AR502 series, AR530 series, and AR550 series routers V200R006 build C10SPC030

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

- AR502/AR510 series do not support L2 forwarding
- AR1220-S/AR1220W-S/AR2220-S/AR201-S/AR207-S do not support BGP
- AR502G-L-D/AR502GR-L-D do not support OSPF/BGP

#### 6.2.1 Hardware

<table>
<tr><th>Model Types</th><th colspan="3">Typical System Configuration and Physical Parameters</th></tr>
<tr><td rowspan="9">AR1200<br>include(<br>AR1220V<br>AR1220W<br>AR1220VW<br>AR1220F<br>AR1220E<br>AR1220EV<br>AR1220EVW)</td><td>Item</td><td>Typical Configuration</td><td>Remark</td></tr>
<tr><td>Processing unit</td><td>AR1220F: 1GHz 2 Core<br>Others: 500MHz 2 Core</td><td>-</td></tr>
<tr><td>SDRAM</td><td>512M</td><td>-</td></tr>
<tr><td>Flash</td><td>AR1220F:512M<br>Others: 256M</td><td>-</td></tr>
<tr><td>SD card</td><td>0</td><td>-not supported</td></tr>
<tr><td>Forwarding Performance</td><td>AR 1220F:1Mpps<br>Others: 450K PPS</td><td></td></tr>
<tr><td>Fixed interface</td><td>FE/GE</td><td>8FE + 2GE</td></tr>
<tr><td>SIC Slot</td><td>2</td><td></td></tr>
<tr><td>WSIC Slot</td><td>0</td><td></td></tr>
<tr><td rowspan="5">AR2200<br>Include(<br>AR2220<br>AR2201-48FE<br>AR2202-48FE<br>AR2204<br>AR2220E<br>)</td><td>Item</td><td>Typical Configuration</td><td>Remark</td></tr>
<tr><td>Processing unit</td><td>AR2201-48FE: 2-core 533 MHz<br>AR2202-48FE: 2-core 533 MHz<br>AR2204: 2-core 800 MHz<br>AR2220: 4-core 600 MHz</td><td>-</td></tr>
<tr><td>SDRAM</td><td>AR2201-48FE: 512 MB<br>AR2202-48FE: 512 MB<br>AR2204: 1 GB<br>AR2220: 2 GB</td><td>-</td></tr>
<tr><td>Flash</td><td>AR 2220: 16M<br>Others: 512M</td><td>-</td></tr>
<tr><td>SD card</td><td>AR 2220: 2GB</td><td>MAX:</td></tr>
</table>

| | | | |
|---|---|---|---|
| | | Others: 0GB | AR2220: 4G<br>Others : 2G |
| | Forwarding Performance | AR2201-48FE: 350 kpps<br>AR2202-48FE: 350 kpps<br>AR2204: 450 kpps<br>AR2220: 1 Mpps | |
| | Fixed interface | GE | AR2201-48FE:<br>2GE+48FE<br>AR2202-48FE:<br>2GE+48FE<br>Others:3GE |
| | SIC Slot | 4 | |
| | WSIC Slot | 2 | |
| AR2240 | **Item** | **Typical Configuration** | **Remark** |
| | Processing unit | 600MHz 8 Core | -SRU40 main control board |
| | SDRAM | 2G | - |
| | Flash | 16M | - |
| | SD card | 2 GB | MAX:4G |
| | Forwarding Performance | 3M PPS | |
| | Fixed interface | GE | 3GE WAN |
| | SIC Slot | 4 | |
| | WSIC Slot | 2 | |
| | XSIC Slot | 2 | |
| AR3260 | **Item** | **Typical Configuration** | **Remark** |
| | Processing unit | 750MHz 12 Core | -SRU80 main control board |
| | SDRAM | 2G | - |
| | Flash | 16M | - |
| | SD card | 2 GB | MAX:4G |
| | Forwarding Performance | 5M PPS | |
| | Fixed interface | GE | 3GE WAN |
| | SIC Slot | 4 | |
| | WSIC Slot | 2 | |
| | XSIC Slot | 4 | |
| AR150<br>Include(<br>AR151 | **Item** | **Typical Configuration** | **Remark** |
| | Processing unit | 533MHz 2 Core | - |

<table>
<tr><td>AR151G-C<br>AR151G-HSPA+7<br>AR151W-P<br>AR156<br>AR156W<br>AR157<br>AR157G-HSPA+7<br>AR157VW<br>AR157W<br>AR158E<br>AR158EVW<br>)</td><td><table>
<tr><td>SDRAM</td><td>512 M</td><td>-</td></tr>
<tr><td>Flash</td><td>512M</td><td>-</td></tr>
<tr><td>SD card</td><td>0 MB</td><td>-not supported</td></tr>
<tr><td>Forwarding Performance</td><td>300K PPS</td><td>-</td></tr>
<tr><td>Fixed interface</td><td>FE/GE</td><td>AR151:<br>4FE+1FE<br>AR151W-P:<br>4FE+1FE<br>AR151G-HSPA+7:<br>4FE+1FE<br>AR151G-C:<br>4FE+1FE<br>Others<br>:4FE</td></tr>
</table></td></tr>
<tr><td>AR160<br>Include(<br>AR161FG-L<br>AR161FGW-L<br>AR162F<br>AR168F<br>AR169BF<br>AR169F<br>AR169FGVW-L<br>AR169FVW<br>AR161FW-P-M5<br>AR161<br>AR161G-L<br>AR169G-L<br>AR169-P-M9 )</td><td><table>
<tr><th>Item</th><th>Typical Configuration</th><th>Remark</th></tr>
<tr><td>Processing unit</td><td>533MHz 2 Core</td><td>-</td></tr>
<tr><td>SDRAM</td><td>AR169FVW: 1G<br>AR169FGVW-L: 1G<br>Others: 512 M</td><td>-</td></tr>
<tr><td>Flash</td><td>512M</td><td>-</td></tr>
<tr><td>SD card</td><td>0 MB</td><td>-not supported</td></tr>
<tr><td>Forwarding Performance</td><td>350K PPS</td><td>-</td></tr>
<tr><td>Fixed interface</td><td>FE/GE</td><td>5GE</td></tr>
</table></td></tr>
<tr><td>AR200<br>Include(<br>AR201<br>AR201VW-P<br>AR206<br>AR207<br>AR207G-HSPA+7<br>AR207V-P<br>AR207V<br>AR207VW<br>AR208E )</td><td><table>
<tr><th>Item</th><th>Typical Configuration</th><th>Remark</th></tr>
<tr><td>Processing unit</td><td>533MHz 2 Core</td><td>-</td></tr>
<tr><td>SDRAM</td><td>512 M</td><td>-</td></tr>
<tr><td>Flash</td><td>512M</td><td>-</td></tr>
<tr><td>SD card</td><td>0 MB</td><td>-not supported</td></tr>
<tr><td>Forwarding Performance</td><td>450K PPS</td><td>-</td></tr>
<tr><td>Fixed interface</td><td>FE/GE</td><td>8FE+1GE</td></tr>
</table></td></tr>
<tr><td>AR510</td><td><table>
<tr><th>Item</th><th>Typical Configuration</th><th>Remark</th></tr>
</table></td></tr>
</table>

| | | | |
|---|---|---|---|
| Include(<br>AR511GW-LAV2M3<br>AR511GW-LM7<br>AR513W-V3M8<br>) | Processing unit | 1.2GHz 4Core | - |
| | SDRAM | 2GB | - |
| | NAND Flash | 2GB | |
| | EMMC FLASH | 32GB | |
| | SD card | 0 MB | |
| | Forwarding Performance | 50K PPS | - |
| | Fixed interface | FE/GE | 2GE |
| AR502<br>Include(<br>AR502R-L-D<br>AR502GR-L-D<br>) | **Item** | **Typical Configuration** | **Remark** |
| | Processing unit | 600MHz 2Core | - |
| | SDRAM | 128M | - |
| | NAND Flash | 512M | |
| | SD card | 0 MB | |
| | Forwarding Performance | 50K PPS | - |
| | Fixed interface | FE/GE | 1GE |
| AR530<br>Include(<br>AR531G-U-D<br>AR531GR-U<br>AR531GPE-U<br>AR531-2C-H<br>AR531-F2C-H<br>) | **Item** | **Typical Configuration** | |
| | Processing unit | 533MHz 2 Core | - |
| | SDRAM | 512 M | - |
| | Flash | 512M | - |
| | SD card | 0 MB | -not supported |
| | Forwarding Performance | 350K PPS | - |
| | Fixed interface | FE/GE | AR531-2C-H:<br>8FE+2GE<br>AR531-F2C-H:<br>8FE+2GE<br>Others: 6FE+2GE |
| AR550<br>Include(<br>AR550-8FE-D<br>AR550-24FE-D<br>) | **Item** | **Typical Configuration** | **Remark** |
| | Processing unit | 533MHz 2 Core | - |
| | SDRAM | 512MB | - |
| | Flash | 128MB | - |
| | SD card | 0 MB | -not supported |
| | Forwarding | 450K PPS | - |

| | | | |
|---|---|---|---|
| | Performance | | |
| | Fixed interface | FE/GE | AR550-8FE-H: 4GE+8FE<br>AR550-24FE-H: 4GE+24FE |

**Table 1: Hardware Scope**

#### 6.2.2 Software

| Type | Name | Version |
|---|---|---|
| Software | Product software | V200R006C10 |
| | VRP | V500R016C30 |
| | Linux | WRlinux4.3(AR150/AR160/AR200/AR530/AR550/AR1200/AR2200/AR3200)<br>ANDROID4.1.2(AR510)<br>WRLinux 4.3 with Linux kernel 3.4.5(AR502) |

**Table 2: Software Scope**

#### 6.2.3 Guidance

| Type | Name | Version |
|---|---|---|
| Guidance | AR150&AR160&AR200&AR510&AR1200&AR2200&AR3200 Hardware Description | Issue 16 / 2014-09-15 |
| | AR V200R006C10 Product Manual | V1.0 |
| | Common Criteria Security Evaluation – Certification Configuration | Version:1.4 / 2015-04-23 |

## TOE Documentation

The supporting guidance documents evaluated were:

[a] AR150&AR160&AR200&AR510&AR1200&AR2200&AR3200 Hardware Description, Issue 16, 15 Sep. 2014

[b] AR V200R006C10 Product Manual, v1.0

[c] Common Criteria Security Evaluation – Certification Configuration, v1.4, 23 April 2015

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

## TOE Configuration

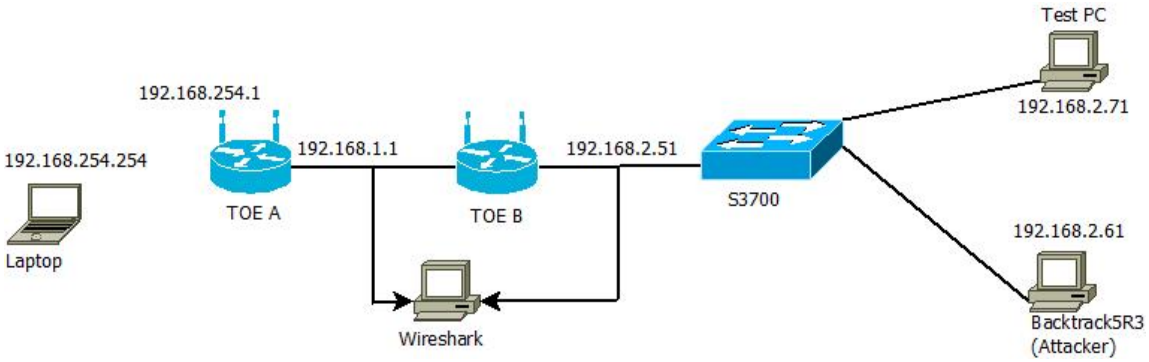
The following configuration was used for testing:

| ITEM | IDENTIFIER |
|---|---|
| HARDWARE | One of the hardware models from each series listed in section TOE Identification |
| SOFTWARE | Product software version V200R006, VRP V500R016, WRLinux 4.3 / Android 4.1.2 / WRLinux 4.3 with Linux kernel 3.4.5, configured according to [10]. |
| MANUALS | AR150&AR160&AR200&AR510&AR1200&AR2200&AR3200 Hardware Description, Issue 16, 2014-09-15<br><br>AR V200R006C10 Product Manual, v1.0<br><br>Common Criteria Security Evaluation – Certification Configuration, v1.4, 23 April 2015 |

## Environmental Configuration

The TOE is tested in the following test setups:

Network diagram 1:




Network diagram 2: