Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0992-2016

for

Huawei AR Series Service Router AR1220 software consisting of Versatile Routing Platform (VRP, V200R006), Concurrence Accelerate Platform (CAP) and underlying OS, V200R006C10SPC030

from

Huawei Technologies Co., Ltd.

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0992-2016 (*)

Router Software

Huawei AR Series Service Router AR1220 software consisting of Versatile Routing Platform (VRP, V200R006), Concurrence Accelerate Platform (CAP) and underlying OS, V200R006C10SPC030

from	Huawei Technologies Co., Ltd.
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) 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 and Notification. For details on the validity see Certification Report part A chapter 4

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Common Criteria
Recognition Arrangement

Bonn, 5 December 2016

For the Federal Office for Information Security

Thomas Gast
Head of Division

L.S.

DAkkS
Deutsche
Akkreditierungsstelle
D-ZE-19615-01-00

This page is intentionally left blank.

Preliminary Remarks

Under the BSIG[1] Act, the Federal Office for Information Security (BSI) has the task of issuing certificates for information technology products.

Certification of a product is carried out on the instigation of the vendor or a distributor, hereinafter called the sponsor.

A part of the procedure is the technical examination (evaluation) of the product according to the security criteria published by the BSI or generally recognised security criteria.

The evaluation is normally carried out by an evaluation facility recognised by the BSI or by BSI itself.

The result of the certification procedure is the present Certification Report. This report contains among others the certificate (summarised assessment) and the detailed Certification Results.

The Certification Results contain the technical description of the security functionality of the certified product, the details of the evaluation (strength and weaknesses) and instructions for the user.

[1] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

Contents

A. Certification

1. Specifications of the Certification Procedure

The certification body conducts the procedure according to the criteria laid down in the following:

- Act on the Federal Office for Information Security[2]
- BSI Certification and Approval Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN ISO/IEC 17065 standard
- BSI certification: Scheme documentation describing the certification process (CC-Produkte) [3]
- BSI certification: Scheme documentation on requirements for the Evaluation Facility, its approval and licencing process (CC-Stellen) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2. Recognition Agreements

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

2.1. European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

[2] Act on the Federal Office for Information Security (BSI-Gesetz - BSIG) of 14 August 2009, Bundesgesetzblatt I p. 2821

[3] Ordinance on the Procedure for Issuance of Security Certificates and approval by the Federal Office for Information Security (BSI-Zertifizierungs- und -Anerkennungsverordnung - BSIZertV) of 17 December 2014, Bundesgesetzblatt 2014, part I, no. 61, p. 2231

[4] Schedule of Cost for Official Procedures of the Bundesamt für Sicherheit in der Informationstechnik (BSI-Kostenverordnung, BSI-KostV) of 03 March 2005, Bundesgesetzblatt I p. 519

[5] Proclamation of the Bundesministerium des Innern of 12 February 2007 in the Bundesanzeiger dated 23 February 2007, p. 3730

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogisportal.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

This certificate is recognized under SOGIS-MRA for all assurance components selected.

2.2. International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

This certificate is recognized under CCRA-2014 for all assurance components selected.

3. Performance of Evaluation and Certification

The certification body monitors each individual evaluation to ensure a uniform procedure, a uniform interpretation of the criteria and uniform ratings.

The product Huawei AR Series Service Router AR1220 software consisting of Versatile Routing Platform (VRP, V200R006), Concurrence Accelerate Platform (CAP) and underlying OS, V200R006C10SPC030 has undergone the certification procedure at BSI.

The evaluation of the product Huawei AR Series Service Router AR1220 software consisting of Versatile Routing Platform (VRP, V200R006), Concurrence Accelerate Platform (CAP) and underlying OS, V200R006C10SPC030 was conducted by SRC Security Research & Consulting GmbH. The evaluation was completed on 16 November 2016. SRC Security Research & Consulting GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the applicant is: Huawei Technologies Co., Ltd..

The product was developed by: Huawei Technologies Co., Ltd..

The certification is concluded with the comparability check and the production of this Certification Report. This work was completed by the BSI.

4. Validity of the Certification Result

This Certification Report only applies to the version of the product as indicated. The confirmed assurance package is only valid on the condition that

- all stipulations regarding generation, configuration and operation, as given in the following report, are observed,
- the product is operated in the environment described, as specified in the following report and in the Security Target.

For the meaning of the assurance levels please refer to the excerpts from the criteria at the end of the Certification Report or in the CC itself.

The Certificate issued confirms the assurance of the product claimed in the Security Target at the date of certification. As attack methods evolve over time, the resistance of the certified version of the product against new attack methods needs to be re-assessed. Therefore, the sponsor should apply for the certified product being monitored within the assurance continuity program of the BSI Certification Scheme (e.g. by a re-certification). Specifically, if results of the certification are used in subsequent evaluation and certification procedures, in a system integration process or if a user's risk management needs regularly updated results, it is recommended to perform a re-assessment on a regular e.g. annual basis.

In order to avoid an indefinite usage of the certificate when evolved attack methods require a re-assessment of the products resistance to state of the art attack methods, the maximum validity of the certificate has been limited. The certificate issued on 5 December 2016 is valid until 4 December 2021. Validity can be re-newed by re-certification.

The owner of the certificate is obliged:

1. when advertising the certificate or the fact of the product's certification, to refer to the Certification Report as well as to provide the Certification Report, the Security Target and user guidance documentation mentioned herein to any customer of the product for the application and usage of the certified product,

[6] Information Technology Security Evaluation Facility

2. to inform the Certification Body at BSI immediately about vulnerabilities of the product that have been identified by the developer or any third party after issuance of the certificate,
3. to inform the Certification Body at BSI immediately in the case that security relevant changes in the evaluated life cycle, e.g. related to development and production sites or processes, occur, or the confidentiality of documentation and information related to the Target of Evaluation (TOE) or resulting from the evaluation and certification procedure where the certification of the product has assumed this confidentiality being maintained, is not given any longer. In particular, prior to the dissemination of confidential documentation and information related to the TOE or resulting from the evaluation and certification procedure that do not belong to the deliverables according to the Certification Report part B, or for those where no dissemination rules have been agreed on, to third parties, the Certification Body at BSI has to be informed.

In case of changes to the certified version of the product, the validity can be extended to the new versions and releases, provided the sponsor applies for assurance continuity (i.e. re-certification or maintenance) of the modified product, in accordance with the procedural requirements, and the evaluation does not reveal any security deficiencies.

5. Publication

The product Huawei AR Series Service Router AR1220 software consisting of Versatile Routing Platform (VRP, V200R006), Concurrence Accelerate Platform (CAP) and underlying OS, V200R006C10SPC030 has been included in the BSI list of certified products, which is published regularly (see also Internet: https://www.bsi.bund.de and [5]). Further information can be obtained from BSI-Infoline +49 228 9582-111.

Further copies of this Certification Report can be requested from the developer[7] of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

[7] Huawei Technologies Co., Ltd.
Bantian Longgang
Shenzhen 518129
P.R. of China

B. Certification Results

The following results represent a summary of

- the Security Target of the sponsor for the Target of Evaluation,
- the relevant evaluation results from the evaluation facility, and
- complementary notes and stipulations of the certification body.

1. Executive Summary

The Target of Evaluation (TOE) is a software TOE consisting of Huawei’s Versatile Routing Platform (VRP, V200R006) supported by the Concurrence Accelerate Platform (CAP) and the underlying OS. The main purpose of the TOE is Layer 3 routing of incoming IP traffic. The software is part of the Service Router AR1220.

At the core of each router is the Versatile Routing Platform (VRP) deployed on Main Processing Unit (MPU), the software for managing and running the router’s networking functionality. VRP provides extensive security features. These features include different interfaces with associated 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 Main Processing Unit also provides network traffic processing capacity. Network traffic is processed and forwarded according to routing decisions.

The MPU consists of two CPU cores. On one core VRP is running. On the other core the Concurrence Accelerate Platform (CAP) is running. CAP is supporting VRP by directly forwarding L3 traffic, in case the route is already known to CAP and no decision by VRP is required. Both, VRP and CAP rely on the GLIBC library and the system call interface of the Linux kernel of the underlying OS.

There exists only one configuration of the TOE, referenced as indicated above.

The TOE in its certified version only runs on the specific HW platform AR1220. This type is referenced on a label on the bottom side of the casing. The identifier for the hardware used for testing for the VRP PCB Version is AR01BAK1A VER.A and for the MPU PCB Version is AR01SRU1B VER.C.

The Security Target [6] is the basis for this certification. It is not based on a certified Protection Profile.

The TOE Security Assurance Requirements (SAR) are based entirely on the assurance components defined in Part 3 of the Common Criteria (see part C or [1], Part 3 for details). The TOE meets the assurance requirements of the Evaluation Assurance Level EAL 2.

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6. They are selected from Common Criteria Part 2 and some of them are newly defined. Thus the TOE is CC Part 2 extended.

The TOE Security Functional Requirements are implemented by the following TOE Security Functionality:

TOE Security Functionality	Addressed issue
Authentication (AUTH)	This Security Function provides authentication of users by unique IDs. Access to any TSF management interface is only granted after successful authentication.
Access Control (AC)	This TSF regulates all access by external entities to operations of the TOE which are only executed after this TSF allowed access.
L3 Traffic Forwarding (L3TF)	This function provides network traffic forwarding which includes enforcing decisions about the

TOE Security Functionality	Addressed issue
	correct forwarding interface and assembling the outgoing network packets using correct IP addresses.
ACL (ACL)	This TSF provides Access Control Lists (ACLs) to filter traffic destined to the TOE to prevent internal traffic over-load and service interruption.
Cryptographic functions (CRYPTO)	This function provides an interface to cryptographic functions.
Communication Security (COMM)	This Security Function provides communication security.
Auditing (AUDIT)	This function provides audit abilities by receiving all types of logs and processing them according to user’s configuration.
Security Management (SM)	Provides management capabilities for the security functions through the local management terminal (LMT) or the remote management terminal (RMT).

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6], chapter 7.

The AR1220 is capable of L2 and L3 forwarding. Only Layer 3 forwarding is regarded as TOE functionality. Also, among others, Service of TELNET and FTP have to be disabled to use the TOE in the certified configuration. For more details on the certified configuration please see the Security Target [6], chapter 1.4.2.2, and especially the number of detailed product configuration settings that must be configured in the stated manner in [9] to achieve the certified TOE configuration.

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3. Based on these assets the TOE Security Problem is defined in terms of Assumptions, Threats and Organisational Security Policies. This is outlined in the Security Target [6], chapter 3.

This certification covers the configurations of the TOE as outlined in chapter 8.

The vulnerability assessment results as stated within this certificate do not include a rating for those cryptographic algorithms and their implementation suitable for encryption and decryption (see BSIG Section 9, Para. 4, Clause 2).

The certification results only apply to the version of the product indicated in the certificate and on the condition that all the stipulations are kept as detailed in this Certification Report. This certificate is not an endorsement of the IT product by the Federal Office for Information Security (BSI) or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by BSI or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

Huawei AR Series Service Router AR1220 software consisting of Versatile Routing Platform (VRP, V200R006), Concurrence Accelerate Platform (CAP) and underlying OS, V200R006C10SPC030

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	HW/ SW	Huawei AR Series Service Router AR1220 Software (VRP, CAP and OS) Software TOE already implemented as part of the router	Version V200R006C10SPC030 SHA-256 hash sum: ace4677fcf652423c35618974374e74c7f354cc50b669fe6152248eee8ad8526	SW included in HW. Physical goods delivered in a card-board box
2	DOC	CC Huawei AR Service Router AR1220 Software V200R006C10SPC030 - AGD_PRE_Production_V1.1	Version 1.1, 2016-09-14, [8] SHA-256 hash sum: e7cdf2ab785c7bd0be28dd2f003dd5cd764cd784e9031f4e1f337cb3668dbb5c	-
3	DOC	CC Huawei AR Service Router AR1220 Software V200R006C10SPC030 - AGD_PRE_User_V1.2	Version 1.2, 2016-09-23, [9] SHA-256 hash sum: d3bb9dd9154b8fcc00ebd808518f12d36fd4fba5c7ecc28ad309f025a906505c	CD
4	DOC	CC Huawei AR Service Router AR1220 Software V200R006C10SPC030 - AGD_OPE_V1.1	Version 1.1, 2016-09-14, [10] SHA-256 hash sum: 7d3a8c8f2a6b76c16bac671518b0a3b6a4089fa7d9ef2981335643b977cce3b2	CD
5	DOC	CC Huawei AR Service Router AR1220 Software V200R006C10SPC030 - Configuration and Reference V1.1	Version 1.1, 2016-09-14, [11] SHA-256 hash sum: c850e54d0a60896b7cf5b17fcfbcf75d9990a85c5bffb65290f8a36c28cfd6a6	CD
6	DOC	CC Huawei AR Service Router AR1220 Software V200R006C10SPC030 - Security Target Lite	Version 3.7, 21.10.2016 [6] SHA-256 hash sum: fdee5c2270784a174c5767d844da1e9f18eb2ebdcb5ef2d30aafd5d08c8b59ec	CD and Annex to this report

Table 2: Deliverables of the TOE

Please note that the end user cannot verify the hash value in item 1 of the table above since the software is already on the device and cannot be extracted for hashing. For the TOE user this hash value is irrelevant.

The TOE in its certified version only runs on the specific HW platform AR1220. This type is referenced on a label on the bottom side of the casing. The identifier for the hardware used for testing for the MPU PCB Version is AR01SRU1B VER.C.

The physical goods are delivered in a cardboard box and contain:

- Product AR1220 with implemented TOE software,
- CD with Guidance documentation that is relevant to the TOE consumer.

The CD excludes [8] which is dedicated only to production.

The TOE with the above mentioned items is packed into cardboard boxes and sealed with anti-tamper tags.

Physical goods are directly delivered using national delivery services. The box includes the product hardware with TOE firmware and CD containing guidance. Physical protection measures of the packaging include undamaged boxes and tamper evident measures. The customer shall validate the delivery chain and return the good if box or tamper evident measures has been broken. The administrator of the TOE is required to compare the reported firmware version with the version stated in the Security Target. The TOE is labelled with its reference "Huawei AR Series Service Router AR1220 software V200R006C10SPC030". After receipt the administrator is required to check the fingerprint of the documentation parts of the TOE on the CD against the reference hash values provided in the Security Target. The guidance [9] requires the administrator to compare the reported firmware version with the version stated in the Security Target by using the command "display version" on the command line interface. To identify the TOE the document [9] is providing the required information in chapter 2.

Documentation is provided on CD within sealed box and alternatively via web. The customer is required to validate the SHA-2 value against the values stated in the Security Target.

Please note that although the AR1220 product documentation can also be downloaded from Huawei's support website, that form of delivery has not been explicitely considered during the evaluation. The scope of the evaluation covers the delivery of the SW installed on the HW, and the documentation delivered on CD ROM together with the AR1220 in a sealed box.

3. Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the issues VRP access control and information control as described in the security target [6] chapter 6.2.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The topics as stated in the Security Target [6] chapter 3.2 are of relevance.

5. Architectural Information

The TOE is a software product consisting of Huawei's Versatile Routing Platform (VRP, V200R006) supported by the Concurrence Accelerate Platform (CAP) and the underlying OS. The TOE's software architecture consists of two logical planes to support centralized forwarding and control and distributed forwarding mechanism: Data plane and control management plane. The control and management plane is the core of the system. It controls and manages the system. The control and management unit processes protocols and signals, configures and maintains the system status, and reports and controls the system status. The data plane is responsible for high speed processing and non-blocking switching of data packets. It encapsulates or decapsulates packets, forwards them, completes inner high speed switching, and collects statistics.

The security functions of the TOE are enforced by the following subsystems:

- AM Subsystem (supports the TSFs Access Control, Authentication, Communication Security and Cryptographic Functions),
- CM Subsystem (supports the TSF Security Management),
- IM Subsystem (supports the TSF Auditing),
- TF Subsystem (supports the TSFs L3 Traffic Forwarding and ACL).

6. Documentation

The evaluated documentation as outlined in table 2 is being provided with the product to the customer. This documentation contains the required information for secure usage of the TOE in accordance with the Security Target.

Additional obligations and notes for secure usage of the TOE as outlined in chapter 10 of this report have to be followed.

7. IT Product Testing

There exists only one configuration of the TOE. The parameters and the commands are described in [11]. Details of the physical configuration of AR1220 are:

- Processing unit: 500MHz 2 Core
- SDRAM: 512MB
- 256MB internal NOR Flash
- No SD Card support
- 450K PPS Forwarding Performance
- Fixed interface Fast Ethernet (FE) / Gigabit Ethernet (GE) (8FE + 2GE)

The developer test plan structure corresponds to the TSF description. Each claimed security function is covered by a corresponding test. The tested TSFs are Authentication, Access Control, L3 Traffic Forwarding, ACL, Cryptographic functions, Communications, Auditing, Security Management.

For each security function the developer provides at least one test case. General approach of the developer's test cases is a positive / negative concept to demonstrate correctly implemented functionality.

For each test case the developer defined an expected result and were compared to the actual results.

All test cases were executed successfully and with the expected result.

The independent testing was partially performed using the developer’s testing environment, as well as using the test environment of the evaluation facility.

First the evaluator reproduced the developer test setup including the provided TOE and repeated each developer test.

Then the evaluator defined individual tests to cover the SFRs claimed in the Security Target [6].

Based on the knowledge of the TOE, his own experience and a public search of common design flaws and potential malfunction, the evaluator defined additional independent test cases to cover issues like design flaws and potential malfunction.

Test cases include:

- traffic routing and forwarding of the TOE by configuring different network address scenarios and sending and monitoring packets,
- accessibility of SSH service dependent to the configured Ethernet interface,
- establish SSH connection with cipher suites and parameters,
- examination of SSH including re-keying,
- possibilities to weaken TOE security by account password misconfiguration,
- bypass enforcement of client public key and invalid stored public keys,
- varying different CLI parameters,
- acquire RNG data and assess that the entropy of the RNG state is not diminished by implementation errors,
- verify reliability of timestamps in logs,
- examine that user passwords are not stored in plain text,
- erasing of temporary session keys from volatile memory after terminating SSH session.

Additionaly, the evaluator repeated every developer test without any deviations.

Vulnerability testing contained of tool-supported known vulnerability search and execution of vulnerability tests resulting from the analysis of potential vulnerabilities. In that context, the SSH interface to protect the TSFI was identified as a probable attack target. Therefore, the authentication by certificates to initialize an SSH session was tested by defining a probable attack scenario. In the defined scenario an attacker attempts to establish an SSH connection to the TOE without or with invalid or mismatching certificates. Also, the Cryptographic support (FCS) regarding to SSH (authentication) and RSA were penetration tested.

The overall test result is that no deviations were found between the expected and the actual test results.

8. Evaluated Configuration

There exists only one configuration of the TOE. The TOE is software only, that is delivered together with specific Hardware that it is running on. The Hardware itself is not part of the TOE.

Please see detailed information on the TOE identification in chapter 1.2 of the Security Target [6].

The TOE runs on a specific hardware platform AR1220 identified and specified in chapter 1.4.1 of the Security Target [6].

The 'display-version' command will identify the TOE. The result printout will include:

```
Huawei Versatile Routing Platform Software
VRP (R) software, Version 5.160 (AR1200 V200R006C10SPC030)
Copyright (C) 2011-2016 HUAWEI TECH CO., LTD
Huawei AR1220 Router uptime is 0 week, 0 day, 4 hours, 5 minutes
```

```
BKP 0 version information:
1. PCB      Version  : AR01BAK1A VER.A
2. If Supporting PoE : No
3. Board    Type     : AR1220
4. MPU Slot Quantity : 1
5. LPU Slot Quantity : 2

MPU 0(Master) : uptime is 0 week, 0 day, 4 hours, 3 minutes
SDRAM Memory Size    : 512     M bytes
Flash 1 Memory Size  : 256     M bytes
NVRAM Memory Size    : 512     K bytes
MPU version information :
1. PCB      Version  : AR01SRU1B VER.C
2. MAB      Version  : 0
3. Board    Type     : AR1220
4. CPLD0    Version  : 104
5. BootROM  Version  : 934
```

Note that not all displayed information are relevant to identify the correct version. The above example printout is from the actually tested TOE. For example, the SIC/WSIC extension slots are not relevant to the evaluation, as the SIC/WSIC cards represent additional network sockets. Also, the BKP version is not relevant, as it refers to the backplane board that is HW only and does not contain any software. The BootROM and CPLD0 versions however are fixed and will return exactly the version information as displayed above.

The printout 'Version 5.160' is not the version of the TOE in the CC-sense. The relevant TOE identification is represented by the string 'V200R006C10SPC030' because it is more specific.

9. Results of the Evaluation

9.1. CC specific results

The Evaluation Technical Report (ETR) [7] was provided by the ITSEF according to the Common Criteria [1], the Methodology [2], the requirements of the Scheme [3] and all interpretations and guidelines of the Scheme (AIS) [4] as relevant for the TOE.

The Evaluation Methodology CEM [2] was used.

For RNG assessment the scheme interpretations AIS 20 was used (see [4]).

As a result of the evaluation the verdict PASS is confirmed for the following assurance components:

- All components of the EAL 2 package including the class ASE as defined in the CC (see also part C of this report)

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 2

The results of the evaluation are only applicable to the TOE as defined in chapter 2 and the configuration as outlined in chapter 8 above.

9.2. Results of cryptographic assessment

The strength of the cryptographic algorithms was not rated in the course of this certification procedure (see BSIG Section 9, Para. 4, Clause 2). But Cryptographic Functionalities with a security level of lower than 100 bits can no longer be regarded as secure without considering the application context. Therefore, for these functionalities it shall be checked whether the related crypto operations are appropriate for the intended system. Some further hints and guidelines can be derived from the 'Technische Richtlinie BSI TR-02102' (https://www.bsi.bund.de).

Any Cryptographic Functionality that is marked in column '*Security Level above 100 Bits*' of the following table with '*no*' achieves a security level of lower than 100 Bits (in general context).

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Authentication	RSA signature	RSA: PKCS#1_V2.1, RSASSA-PKCS1-v1_5	modulus length = 2048	yes	Signing (FCS_COP.1/RSA), using SHA256, applied during server authentication for SSH Verifying (FCS_COP.1/RSA), using SHA256, applied during client authentication for SSH.
2	Key Generation	Diffie-hellman-group14-sha1	PKCS#3 RFC3526 (2048-bit MODP Group)	modulus length = 2048	yes	(FCS_CKM.1/DH), used in SSH V2.0. Generation of session keys for AES-128-CTR encryption and decryption as well as HMAC-SHA1 keys for generation and verification of integrity protection information are derived during DH key agreement according to RFC 4253, chap. 7.
3	Key Exchange	Diffie-hellman-group14-sha1	PKCS#3 RFC3526 (2048-bit MODP Group)	modulus length = 2048	yes	(FCS_CKM.2/DH), used in SSH V2.0. Exchange of session keys for AES-128-CTR encryption and decryption as well as HMAC-SHA1 keys for generation and verification of integrity protection information are derived during DH key agreement according to RFC 4253, chap. 7.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
4	Confidentiality	AES-128 in CTR mode	AES: FIPS 197 FIPS SP 800-38A	|k|=128	yes	Secure messaging for SSH V2.0 (FCS_COP.1/AES)
5	Integrity	HMAC-SHA1	FIPS 198-1	n/a	yes	Secure messaging for SSH V2.0 (FCS_COP.1.1/HMAC-SHA1)
6	Trusted Channel	SSH V2.0	RFC4344 RFC 4251 RFC 4252 RFC 4253 RFC 4254	n/a	yes	Trusted channel using SSH V2.0 using the crypto-graphic algorithms speci-fied in lines 1,2,3,4,6,7,8, (FTP_TRP.1) Client authentication mode is restricted to public key. Server authentication is supported according to chap. 6.6 of RFC 4253, ssh-rsa.
7	Cryptographic Primitive	Deterministic RNG DRG.2	ANSI X.9.31(aes-128)	n/a	n/a	Generation of the random number (FCS_RNG.1).
8	Cryptographic Primitive	Generation of prime numbers for RSA	None	n/a	n/a	Miller-Rabin-Test is used as primality test.
9	Cryptographic Primitive	SHA256	SHA256: FIPS 180-4	n/a	yes	FCS_COP.1/SHA256 Hashing for RSA signature for SSH Server authen-tication, Hashing for password storage

Table 3: TOE cryptographic functionality

10. Obligations and Notes for the Usage of the TOE

The documents as outlined in table 3 contain necessary information about the usage of the TOE and all security hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

The customer or user of the product shall consider the results of the certification within his system risk management process. In order for the evolution of attack methods and techniques to be covered, he should define the period of time until a re-assessment of the TOE is required and thus requested from the sponsor of the certificate.

If available, certified updates of the TOE should be used. If non-certified updates or patches are available the user of the TOE should request the sponsor to provide a re-certification. In the meantime a risk management process of the system using the TOE should investigate and decide on the usage of not yet certified updates and patches or take additional measures in order to maintain system security.

The limited validity for the usage of cryptographic algorithms as outlined in chapter 9 has to be considered by the user and his system risk management process.

The security measures may require special configuration of the product to obtain the evaluated configuration, including the Hardware and non TOE portions of the product. For this reason the TOE includes guidance documentation (see table 2) which contains obligations and guidelines for the administrator of the product on how to securely use the certified TOE and which measures have to be implemented in order to fulfil the security requirements of the Security Target of the TOE.

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report. It is a sanitised version of the complete Security Target used for the evaluation performed. Sanitisation was performed according to the rules as outlined in the relevant CCRA policy (see AIS 35 [4]).

12. Definitions

12.1. Acronyms

ACL	Access Control List
AIS	Application Notes and Interpretations of the Scheme
BKP	Backplane
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CAP	Concurrence Accelerate Platform
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETH	Ethernet
ETR	Evaluation Technical Report
FE	Fast Ethernet
FTP	File Transfer Protocol
GE	Gigabit Ethernet
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility

LMT	Local management terminal
LPU	Local Processing Unit
MPU	Main Processing Unit
OS	Operating System
PP	Protection Profile
PPS	Packets Per Second
RMT	Remote management terminal
RNG	Random Numer Generator
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SIC	Smart Interface Card
SSH	Secure shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
VRP	Versatile Routing Platform
WSIC	Double Width SIC

12.2. Glossary

Augmentation - The addition of one or more requirement(s) to a package.

Collaborative Protection Profile - A Protection Profile collaboratively developed by an International Technical Community endorsed by the Management Committee.

Extension - The addition to an ST or PP of functional requirements not contained in CC part 2 and/or assurance requirements not contained in CC part 3.

Formal - Expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts.

Informal - Expressed in natural language.

Object - A passive entity in the TOE, that contains or receives information, and upon which subjects perform operations.

Package - named set of either security functional or security assurance requirements

Protection Profile - A formal document defined in CC, expressing an implementation independent set of security requirements for a category of IT Products that meet specific consumer needs.

Security Target - An implementation-dependent statement of security needs for a specific identified TOE.

Semiformal - Expressed in a restricted syntax language with defined semantics.

Subject - An active entity in the TOE that performs operations on objects.

Target of Evaluation - An IT Product and its associated administrator and user guidance documentation that is the subject of an Evaluation.

TOE Security Functionality - Combined functionality of all hardware, software, and firmware of a TOE that must be relied upon for the correct enforcement of the SFRs.

13. Bibliography

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1,
Part 1: Introduction and general model, Revision 4, September 2012
Part 2: Security functional components, Revision 4, September 2012
Part 3: Security assurance components, Revision 4, September 2012
http://www.commoncriteriaportal.org

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012, http://www.commoncriteriaportal.org

[3] BSI certification: Scheme documentation describing the certification process (CC-Produkte) and Scheme documentation on requirements for the Evaluation Facility, approval and licencing (CC-Stellen), https://www.bsi.bund.de/zertifizierung

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8] https://www.bsi.bund.de/AIS

[5] German IT Security Certificates (BSI 7148), periodically updated list published also on the BSI Website, https://www.bsi.bund.de/zertifizierungsreporte

[6] Security Target BSI-DSZ-CC-0992-2016, Huawei AR Series Service Router AR1220 software consisting of Versatile Routing Platform (VRP, V200R006), Concurrence Accelerate Platform (CAP) and underlying OS, Version V3.7, Date: 2016-10-21, Huawei Technologies Co., Ltd. (confidential document)
Security Target Lite BSI-DSZ-CC-0992-2016, Huawei AR Series Service Router AR1220 software consisting of Versatile Routing Platform (VRP, V200R006), Concurrence Accelerate Platform (CAP) and underlying OS, Version 3.7, Date 2016-10-21, Huawei Technologies Co. (public sanitized document)

[7] Evaluation Technical Report (ETR) for Huawei AR Series Service Router AR1220 Software (VRP, CAP and OS), BSI-DSZ-CC-0992, Version 1.4, Date: 2016-10-17, SRC Security Research & Consulting GmbH, (confidential document)

[8] Preparative Procedures for Production, Huawei AR Service Router AR1220 Software V200R006C10SPC030, v1.1, 14.09.2016, Huawei Technologies Co., Ltd.

[9] Preparative Procedures for Users, Huawei AR Service Router AR1220 Software V200R006C10SPC030, v1.2, 23.09.2016, Huawei Technologies Co., Ltd.

[10] Operational User Guidance, Huawei AR Series Service Router AR1220 software consisting of Versatile Routing Platform (VRP,V200R006), Concurrence Accelerate Platform (CAP) and underlying OS V200R006C10SPC030, v1.1, 14.09.2016, Huawei Technologies Co., Ltd.

[11] Configuration and Reference, CC Huawei AR Series Service Router AR1220 V200R006, v1.1, 14.09.2016, Huawei Technologies Co., Ltd.

[8] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 35, Version 2, Öffentliche Fassung des Security Targets (ST-Lite) including JIL Document and CC Supporting Document and CCRA policies

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

“The conformance claim indicates the source of the collection of requirements that is met by a PP or ST that passes its evaluation. This conformance claim contains a CC conformance claim that:

- describes the version of the CC to which the PP or ST claims conformance.
- describes the conformance to CC Part 2 (security functional requirements) as either:
  - **CC Part 2 conformant** - A PP or ST is CC Part 2 conformant if all SFRs in that PP or ST are based only upon functional components in CC Part 2, or
  - **CC Part 2 extended** - A PP or ST is CC Part 2 extended if at least one SFR in that PP or ST is not based upon functional components in CC Part 2.
- describes the conformance to CC Part 3 (security assurance requirements) as either:
  - **CC Part 3 conformant** - A PP or ST is CC Part 3 conformant if all SARs in that PP or ST are based only upon assurance components in CC Part 3, or
  - **CC Part 3 extended** - A PP or ST is CC Part 3 extended if at least one SAR in that PP or ST is not based upon assurance components in CC Part 3.

Additionally, the conformance claim may include a statement made with respect to packages, in which case it consists of one of the following:

- Package name Conformant - A PP or ST is conformant to a pre-defined package (e.g. EAL) if:
  - the SFRs of that PP or ST are identical to the SFRs in the package, or
  - the SARs of that PP or ST are identical to the SARs in the package.
- Package name Augmented - A PP or ST is an augmentation of a predefined package if:
  - the SFRs of that PP or ST contain all SFRs in the package, but have at least one additional SFR or one SFR that is hierarchically higher than an SFR in the package.
  - the SARs of that PP or ST contain all SARs in the package, but have at least one additional SAR or one SAR that is hierarchically higher than an SAR in the package.

Note that when a TOE is successfully evaluated to a given ST, any conformance claims of the ST also hold for the TOE. A TOE can therefore also be e.g. CC Part 2 conformant.

Finally, the conformance claim may also include two statements with respect to Protection Profiles:

- PP Conformant - A PP or TOE meets specific PP(s), which are listed as part of the conformance result.
- Conformance Statement (Only for PPs) - This statement describes the manner in which PPs or STs must conform to this PP: strict or demonstrable. For more information on this Conformance Statement, see Annex D.”

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

“Evaluating a PP is required to demonstrate that the PP is sound and internally consistent, and, if the PP is based on one or more other PPs or on packages, that the PP is a correct instantiation of these PPs and packages. These properties are necessary for the PP to be suitable for use as the basis for writing an ST or another PP.

Assurance Class	Assurance Components
Class APE: Protection Profile evaluation	APE_INT.1 PP introduction
	APE_CCL.1 Conformance claims
	APE_SPD.1 Security problem definition
	APE_OBJ.1 Security objectives for the operational environment APE_OBJ.2 Security objectives
	APE_ECD.1 Extended components definition
	APE_REQ.1 Stated security requirements APE_REQ.2 Derived security requirements

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

“Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.”

Assurance Class	Assurance Components
Class ASE: Security Target evaluation	ASE_INT.1 ST introduction
	ASE_CCL.1 Conformance claims
	ASE_SPD.1 Security problem definition
	ASE_OBJ.1 Security objectives for the operational environment ASE_OBJ.2 Security objectives
	ASE_ECD.1 Extended components definition
	ASE_REQ.1 Stated security requirements ASE_REQ.2 Derived security requirements
	ASE_TSS.1 TOE summary specification ASE_TSS.2 TOE summary specification with architectural design summary

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.“
“Each assurance class contains at least one assurance family.”
“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	**Assurance Components**
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation
	ALC_LCD.1 Developer defined life-cycle model

Assurance Class	Assurance Components
	ALC_LCD.2 Measurable life-cycle model
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts
ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
	ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
	ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
	ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis

Assurance class decomposition

Evaluation assurance levels (chapter 8)

“The Evaluation Assurance Levels (EALs) provide an increasing scale that balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. The CC approach identifies the separate concepts of assurance in a TOE at the end of the evaluation, and of maintenance of that assurance during the operational use of the TOE.

It is important to note that not all families and components from CC Part 3 are included in the EALs. This is not to say that these do not provide meaningful and desirable assurances. Instead, it is expected that these families and components will be considered for augmentation of an EAL in those PPs and STs for which they provide utility.”

Evaluation assurance level (EAL) overview (chapter 8.1)

“Table 1 represents a summary of the EALs. The columns represent a hierarchically ordered set of EALs, while the rows represent assurance families. Each number in the resulting matrix identifies a specific assurance component where applicable.

As outlined in the next Section, seven hierarchically ordered evaluation assurance levels are defined in the CC for the rating of a TOE's assurance. They are hierarchically ordered inasmuch as each EAL represents more assurance than all lower EALs. The increase in assurance from EAL to EAL is accomplished by substitution of a hierarchically higher assurance component from the same assurance family (i.e. increasing rigour, scope, and/or depth) and from the addition of assurance components from other assurance families (i.e. adding new requirements).

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one component of each assurance family and all assurance dependencies of every component are addressed.

While the EALs are defined in the CC, it is possible to represent other combinations of assurance. Specifically, the notion of “augmentation” allows the addition of assurance components (from assurance families not already included in the EAL) or the substitution of assurance components (with another hierarchically higher assurance component in the same assurance family) to an EAL. Of the assurance constructs defined in the CC, only EALs may be augmented. The notion of an “EAL minus a constituent assurance component” is not recognised by the standard as a valid claim. Augmentation carries with it the obligation on the part of the claimant to justify the utility and added value of the added assurance component to the EAL. An EAL may also be augmented with extended assurance requirements.

Evaluation assurance level 1 (EAL 1) - functionally tested (chapter 8.3)

“Objectives

EAL 1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL 1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL 1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL 1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.”

Evaluation assurance level 2 (EAL 2) - structurally tested (chapter 8.4)

“Objectives

EAL 2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL 2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL 3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL 3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL 3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering."

Evaluation assurance level 4 (EAL 4) - methodically designed, tested, and reviewed (chapter 8.6)

"Objectives

EAL 4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL 4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL 4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs."

Evaluation assurance level 5 (EAL 5) - semiformally designed and tested (chapter 8.7)

"Objectives

EAL 5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL 5 assurance. It is likely that the additional costs attributable to the EAL 5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL 5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques."

Evaluation assurance level 6 (EAL 6) - semiformally verified design and tested (chapter 8.8)

"Objectives

EAL 6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL 6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs."

Evaluation assurance level 7 (EAL 7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL 7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL 7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Assurance Class	**Assurance Family**	**Assurance Components by Evaluation Assurance Level**						
		EAL 1	EAL 2	EAL 3	EAL 4	EAL 5	EAL 6	EAL 7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

“The AVA: Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.”

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

Vulnerability analysis is an assessment to determine whether potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses or quantitative or statistical analysis of the security behaviour of the underlying security mechanisms), could allow attackers to violate the SFRs.

Vulnerability analysis deals with the threats that an attacker will be able to discover flaws that will allow unauthorised access to data and functionality, allow the ability to interfere with or alter the TSF, or interfere with the authorised capabilities of other users.”

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.