Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0937-2014

for

Cisco Catalyst 6500-E Series Switches - Cisco IOS Software, Version 15.1(1)SY1, RELEASE SOFTWARE (fc5)

from

Cisco Systems, Inc.

BSI - Bundesamt für Sicherheit in der Informationstechnik, Postfach 20 03 63, D-53133 Bonn
Phone +49 (0)228 99 9582-0, Fax +49 (0)228 9582-5477, Infoline +49 (0)228 99 9582-111

Bundesamt
für Sicherheit in der
Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0937-2014

Network Device

Cisco Catalyst 6500-E Series Switches
Cisco IOS Software, Version 15.1(1)SY1, RELEASE SOFTWARE (fc5)

from	Cisco Systems, Inc.
PP Conformance:	U.S. Government Approved Protection Profile - Protection Profile for Network Devices Version 1.0
Functionality:	PP conformant Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ALC_CMC.1, ALC_CMS.1, AGD_OPE.1, AGD_PRE.1, ADV_FSP.1, ATE_IND.1, AVA_VAN.1

Common Criteria Recognition Arrangement

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 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report.

The evaluation has been conducted in accordance with the provisions of the 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.

Bonn, 20 February 2014
For the Federal Office for Information Security

Bernd Kowalski L.S.
Head of Department

SOGIS Recognition Agreement

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

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:

- BSIG[2]
- BSI Certification Ordinance[3]
- BSI Schedule of Costs[4]
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- 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 technical domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL1 to EAL4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For higher recognition levels the technical domain Smart card and similar Devices has been defined. It includes assurance levels beyond EAL4 resp. E3 (basic). In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

---

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 a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

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

As of September 2011 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. Details on recognition and the history of the agreement can be found at https://www.bsi.bund.de/zertifizierung.

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

2.2 International Recognition of CC – Certificates (CCRA)

An arrangement (Common Criteria Recognition Arrangement) on the mutual recognition of certificates based on the CC Evaluation Assurance Levels up to and including EAL 4 has been signed in May 2000 (CCRA). It includes also the recognition of Protection Profiles based on the CC.

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. 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.

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 Cisco Catalyst 6500-E Series Switches, Cisco IOS Software, Version 15.1(1)SY1, RELEASE SOFTWARE (fc5) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0838-2014. Specific results from the evaluation process BSI-DSZ-CC-0838-2014 were re-used.

The evaluation of the product Cisco Catalyst 6500-E Series Switches, Cisco IOS Software, Version 15.1(1)SY1, RELEASE SOFTWARE (fc5) was conducted by media transfer AG. The evaluation was completed on 20 February 2014. media transfer AG is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: Cisco Systems, Inc.

The product was developed by: Cisco Systems, Inc.

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

[6] Information Technology Security Evaluation Facility

- 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.

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 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 Cisco Catalyst 6500-E Series Switches, Cisco IOS Software, Version 15.1(1)SY1, RELEASE SOFTWARE (fc5) 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] Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA

This page is intentionally left blank.

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 TOE is the “Cisco Catalyst 6500-E Series” switching and routing platform, i.e. a network device composed of hardware and software that is connected to the network and has an infrastructure role in the overall enterprise.

The TOE is used to construct IP networks by interconnecting multiple smaller networks or network segments. As a Layer2 switch, it performs analysis of incoming frames, makes forwarding decisions based on information contained in the frames, and forwards the frames toward the destination. As a Layer3 switch/router, it supports routing of traffic based on tables identifying available routes, conditions, distance, and costs to determine the best route for a given packet.

The Security Target [6] is the basis for this certification. It is based on the U.S. Government Approved Protection Profile - Protection Profile for Network Devices Version 1.0 [7].

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 Protection Profile for Network Devices Version 1.0 [7]: ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ALC_CMC.1, ALC_CMS.1, AGD_OPE.1, AGD_PRE.1, ADV_FSP.1, ATE_IND.1 and AVA_VAN.1

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. 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
Security Audit	The TOE generates a comprehensive set of audit logs that identify specific TOE operations. For each event, the TOE records the date and time of each event, the type of event, the subject identity, and the outcome of the event.
Cryptographic Support	The TOE provides cryptography support for secure communications and protection of information.
User Data Protection	The TOE supports three mechanisms to filter traffic and enforce flow control: VLANs, ACLs and VACLs.
Identification and Authentication	All users wanting to use TOE services are identified and authenticated prior to being allowed to access any of the services. The TOE performs authentication, using Cisco IOS platform authentication mechanisms, to authenticate access to user EXEC and privileged EXEC command modes.
Security Management	The TOE provides secure administrative services for management of general TOE configuration and the security functionality provided by the TOE. All TOE administration occurs either

TOE Security Functionality	Addressed issue
	through a secure IPSec tunnel, or a local console connection (serial port).
Protection of the TSF	The TOE provides secure transmission when TSF data is transmitted between separate parts of the TOE.
Resource Utilization	The TOE provides the capability of controlling and managing resources so that a denial of service will not occur. The resource allocations are configured to limit the number of concurrent administrator sessions.
TOE Access	The TOE can terminate inactive sessions after an authorized administrator configurable time period. Once a session has been terminated the TOE requires the user to re-authenticate to establish a new session.
Trusted Path/channels	The TOE establishes a trusted path between the appliance and the CLI and the syslog server using IPSec encrypted connection. The TOE can also establish trusted paths of peer-to-peer VPN tunnels.

Table 1: TOE Security Functionalities

For more details please refer to the Security Target [6] , chapter 6.1.

The assets to be protected by the TOE are defined in the Security Target [6] , chapter 3.3 . 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 3.4, 3.5 and 3.6.

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 cryptographic algorithms 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:

Cisco Catalyst 6500-E Series Switches, Cisco IOS Software, Version 15.1(1)SY1, RELEASE SOFTWARE (fc5)

The following table outlines the TOE deliverables:

No	Type	Identifier	Form of Delivery
1	SW	Software version id: IOS 15.1(1)SY1 TOE Image name: s2t54-adventerprisek9-mz.SPA.151-1.SY1.bin SHA-256 hash value of TOE image file: 67951355B24F7E8EF26FA0A19635748CAD5EC57BEB713C4BEE976EF042971574	Download from Cisco website.
2	DOC	Guidance documentation, Cisco Catalyst 6500-E Series Switches, Common Criteria Operational User Guidance and Preparative Procedures, Cisco Systems, Inc., EDCS 1182242, Version 1.0 SHA-256 value of PDF file: C815F1B3F730CD83DE321AA8C83D8628F1E838C0CD70A749404E9385AB64A59F	Download from Cisco website.
3	HW	One or more WS-C6503-E, WS-C6504-E, WS-C6506-E, WS-C6509-E, or WS-C6513-E Switch Chassis One or more Supervisor 2T (Sup2T) Cards (VS-S2T-10G or VS-S2T-10G-XL) per chassis Each Sup2T running IOS 15.1(1)SY1 With one or more of the following Line Cards installed to one or more chassis: • WS-X6908-10G-2TXL / WS-X6908-10G-2T • WS-X6848-SFP-2TXL / WS-X6848-SFP-2T • WS-X6824-SFP-2TXL / WS-X6824-SFP-2T • WS-X6848-TX-2TXL / WS-X6848-TX-2T • WS-X6816-10G-2TXL / WS-X6816-10G-2T • WS-X6816-10T-2TXL / WS-X6816-10T-2T • WS-x6904 Estelle-4x40 GE / 16x10 GE (Lite or XL)	Package delivered by trusted delivery firm. Perform acceptance procedures.

Table 2: Deliverables of the TOE

The following non-TOE parts are necessary to operate the TOE:

No	Identification	Version	Required by the TOE
1	Management Workstation with IPSec Client	Any server that supports the IPSec protocol may be used.	YES
2	NTP Server	Any server that supports NTPv1 (RFC 1059), NTPv2 (RFC 1119), or NTP v3 (RFC 1305) may be used.	NO
3	Syslog server	Any server that supports the syslog functionality according to RFC 5424.	YES
4	Authentication Server	RADIUS RFC 2865, 2866, 2869 and RFC 3162 (IPv6) and TACACS+ RFC 1492)	YES

Table 3: Components in the TOE Environment

2.1 Ordering of TOEs by customers:

TOEs can be ordered by customers with support contracts via the Cisco Connection Online (CCO) procedures.

All orders are transferred electronically to Cisco manufacturing for processing. TOEs are assembled from TOE parts.

TOE parts are TOE image and TOE hardware:

- The TOE image consists of TOE software and TOE documentation. The TOE software in turn consists of the operating system IOS 15.1(1)SY1. The TOE documentation in turn consists of guidance documentation, release notes and/or defect reports.
- The TOE hardware consists of a set of chassis, supervisor engines, and line cards according to the configuration list.

TOE images can be ordered separately, independent of TOE hardware.

2.2 Delivery of TOEs to customers:

The final packaged TOE product (TOE image and TOE hardware) is distributed together with its shipping documents (traveller paperwork, license pack). Cisco uses trusted delivery firms for the delivery of TOEs to their customers.

2.3 Acceptance of TOEs by customers:

The customer has to follow the procedures for “Secure acceptance of the TOE” when receiving the shipped TOE product. Procedures for “Secure acceptance of the TOE” are described in the guidance documentation [9], section 2.

Particularly, the customer has to check:

- Before unpacking, inspect the physical packaging of the equipment and verify that the external cardboard packing is printed with Cisco logo and motifs.
- Verify that the packaging has not been opened and re-sealed.
- Verify that the packaging has white tamper-resistant Cisco bar coded labels applied.
- Compare the serial number of the TOE on the shipping documentation with the serial number on the separately mailed invoice for the equipment.
- Verify that the box is indeed shipped from the expected delivery firm.
- Unpack the TOE package and inspect the contents.
- Verify the serial numbers on the components match the serial numbers of the shipping documentation and the serial numbers of the invoice.
- Install the TOE hardware.
- Inspect the TOE documentation.
- If a TOE image has been downloaded, check the cryptographic SHA-256 checksum of the image (e.g. Table 2, No. 1) and install the TOE image onto the TOE hardware.
- Start the TOE as described in the guidance documentation [9] and verify the correct (evaluated) version of the TOE is running.

If any of these checks fails, the customer has to inform the developer about it.

The TOE hardware components can be identified by the part number printed on the tamper-resistant Cisco labels applied to each hardware component. See Table 2 for the list of allowed part numbers with respect to chassis, supervisor engine cards and line cards.

Additionally, with a running TOE all hardware components can be listed using the following IOS command “*show inventory*”. The printed part numbers can be checked against Table 2, No 3.

The TOE firmware can be identified using the IOS command “*show version*”. The IOS version must match with the following information taken from the Guidance Documentation [9]: The TOE displays "Cisco IOS Software, s2t54 Software (s2t54-ADVIPSERVICESK9-M), Version 15.1(1)SY1, RELEASE SOFTWARE (fc5)

The TOE documentation can be identified by the document title, the version, and EDCS number as well as by a cryptographic SHA-256 checksum (e.g. Table 2, No. 2).

3 Security Policy

The Security Policy is expressed by the set of Security Functional Requirements and implemented by the TOE. It covers the following issues: Security Audit, Cryptographic Support, User Data Protection, Identification and Authentication, Security Management, Protection of the TSF, Resource Utilization, TOE Access and Trusted Path/channels.

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 following topics are of relevance: OE.NO_GENERAL_PURPOSE, OE.PHYSICAL, OE.TRUSTED_ADMIN. Details can be found in the Security Target [6], chapter 4.2.

5 Architectural Information

The Switch subsystem architecture is composed of the following functional blocks:

- Runtime Functionality:
  The runtime functionality is the core/kernel operating system functionality for the switch subsystem as well as the system runtime clock. It encompasses resource management operations (e.g., device control), and operations creating the process context in which other functionality operates.
- Crypto Engine Functionality:
  The crypto engine functionality implements support for cryptographic operations used by other parts of the subsystem. These functions include key generation, key destruction, encryption, decryption, signature services, hashing and keyed-hash authentication.
- IPsec Functionality and IPsec Internet Key Exchange (IKE) Functionality:
  The IPsec functionality and IKE functionality cooperate to allow the TOE to use authentication and encryption services to prevent unauthorized viewing or modification of data as it travels over the connected networks.

- Firewall Functionality:
  The firewall functionality monitors packets flowing through the switch subsystem. This function of the switch subsystem can permit or deny traffic flows through the TOE based on TOE security policies.
- CLI Functionality:
  The CLI (Command Line Interface) functionality accepts administrative user input from an external terminal connected via the serial line or via an IPsec secured remote terminal connection.
- Logging Functionality:
  The logging functionality receives system event messages that are generated as normal part of TOE operation and stores them in an internal or external buffer so they can be retrieved and reviewed by an authorized administrative user.
- AAA Functionality:
  The AAA functionality is used primarily for local or remote authentication as well as local authorization.

Using the functionality provided by the components listed above the TOE subsystem implements the following logical interfaces:

- TSFI_1.1 Management Commands,
- TSFI_1.2 Security Audit Commands,
- TSFI_2.1 Network Traffic (External) Interface,
- TSFI_2.2 Network Traffic (Internal) Interface,
- TSFI_2.3 IPsec Network Interface,
- TSFI_3.2 Time Server Interface,
- TSFI_3.3 AAA Interface, and
- TSFI_3.4 Syslog Interface.

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

7.1 Description of the test configuration

The independent testing was performed in the test environment that has been installed and configured at the evaluator’s lab using the hardware and software components delivered by the developer.

The most advanced and complex TOE configuration, the Virtual Switching System (VSS) configuration, was selected for independent testing, though any other configuration with only one Supervisor Module could have been selected.

In the VSS configuration, the TOE consists of two Supervisor Modules in two switch chassis building a highly available switch cluster. Nevertheless, at any time only one Supervisor Module is active while the other module is in a hot-stand-by mode. All TSF is provided by the active Supervisor Module.

The TOE consists of a 6503-E and a 6509-E chassis each equipped with the Sup2T supervisor engine which constitute the VSS Domain 10. A laptop as test client is connected to the TOE via the External Network 192.168.217.0/24.

A Linux server located on the Internal Network (10.1.1.0/24) provides the Syslog, NTP and RADIUS service for the TOE. The SSH client on this server is used for remote admin access, too. The Internal Network connects to the TOE via the IPsec (transfer) Network (10.2.2.0/24). This IPsec network has been configured between the TOE and the dedicated IPsec C2911 router.

A second Linux server with a Open Source IPsec implementation and a Open Source SSH implementation is located on the Internal Network (199.99.99.0/24) and connects through an IPsec tunnel (10.3.3.0/24) to the TOE. This server is used to test the IPsec SFRs claimed in the ST and to provide a remote admin console using SSH within the IPsec tunnel for connecting to the command line interface (CLI) of the TOE.

All mentioned networks (Internal, External, IPsec) are realised through the configuration of separate VLANs on an auxiliary switch.

7.2 Independent testing approach:

For independent testing, the evaluators specified test cases with the intention of covering all SFRs defined in the ST. For that purpose, some of the developer's tests have been chosen and additional evaluator tests have been specified.

For test case specification and test case execution documentation the evaluators used the Open Source based test management tool "testlink".

Independent test subset chosen, including a short justification:

The evaluators specified 107 individual test cases. A subset of 21 test cases are developer provided tests that have been repeated to verify the developer test results. Another approximately 60 test cases are motivated and derived from assurance activities required by the NDPP. The remainder of the test cases are focused on testing boundary conditions not tested by the developer.

7.3 Penetration testing approach

The penetration testing was performed in the test environment that has been installed and configured at the evaluator's lab using the hardware and software components delivered by the developer.

The approach chosen by the evaluators is appropriate for the assurance component AVA_VAN.2, requiring the resistance of the TOE to an attack with the Basic attack potential. First the evaluators used publicly available sources to identify potential vulnerabilities in the TOE, e.g.:

- Search with Internet Search Engines (e.g. Google) for vulnerabilities
- Search in CVE Repository for registered IOS vulnerabilities
- Search in OVAL Repository for registered IOS vulnerabilities

- Search the Cisco Security Intelligence Operations Portal
- Run the Cisco IOS Software Checker for known security advisories
- Search in Cisco Manuals and Cisco Whitepapers for the Catalyst 6500-E Switches

In addition the evaluators applied an “unstructured analysis” while evaluating the developer provided Common Criteria evidence documentation to identify potential vulnerabilities applicable to the TOE.

The evaluators analysed which of the potential vulnerabilities identified in the steps above are not applicable to the TOE in its operational environment. For the remaining potential vulnerabilities, the evaluators devised the attack scenarios where these potential vulnerabilities could be exploited.

For each identified attack scenario they first performed a theoretical analysis on the related attack potential. Where the attack potential was Basic, the evaluators conducted penetration tests. They analyzed the results of these tests to determine, whether at least one of the attack scenarios with the attack potential Basic was successful.

The overall test result is that no deviations were found between the expected and the actual penetration test results. No attack scenario with the attack potential Basic was actually successful in the TOE’s operational environment as defined in the Security Target [6], provided that all configurations and measures as required by the developer in the Guidance Documentation [9] are being applied.

8 Evaluated Configuration

The TOE is composed of hardware, software and documentation. To use the TOE in the evaluated configuration, the TOE must be configured as specified in the “Cisco Catalyst 6500-E Series Switches, Common Criteria Operational User Guidance and Preparative Procedures”.

The hardware of the evaluated configuration of the TOE consists of two chassis, one supervisor engine per chassis, and one line card per chassis.

The software of the evaluated configuration of the TOE consists of an image for Cisco IOS version 15.1(1)SY1, to be run identically on each supervisor engine.

The evaluated configuration of the TOE is uniquely referenced by labels found at different locations of the components. The labels are both physically available as printed text on hardware components, and they are electronically available as output text from the configuration command line of the TOE.

See Table 2 for the precise description of the evaluated configuration of the TOE.

9 Results of the Evaluation

9.1 CC specific results

The Evaluation Technical Report (ETR) [8] 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 interpretation AIS 20 was used (see [4]).

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

- All components claimed in the Security Target [6], chapter 6.1.2 and defined in the CC (see also part C of this report).

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-838-2014, re-use of specific evaluation tasks was possible.

The evaluation has confirmed:

- PP Conformance: U.S. Government Approved Protection Profile - Protection Profile for Network Devices Version 1.0 [7]
- for the Functionality: PP conformant plus product specific extensions
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  ASE_CCL.1, ASE_ECD.1, ASE_INT.1, ASE_OBJ.2, ASE_REQ.2, ASE_SPD.1, ASE_TSS.1, ALC_CMC.1, ALC_CMS.1, AGD_OPE.1, AGD_PRE.1, ADV_FSP.1, ATE_IND.1, AVA_VAN.1

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	Random bit generation	AES-ECB AES-CBC	FIPS PUB 197, NIST SP 800-38A, NIST SP 800-38D NIST SP 800-90A	|k| = 256	n/a	FCS_RBG_EXT.1
2	Authentication	IPsec: RSA signature generation and verification for mutual authentication using SHA-1	FIPS PUB 186-3	Modulus length = 2048	No	FCS_IPSEC_EXT.1
3		IPsec: RSA signature	FIPS PUB 186-3	Modulus length = 2048	Yes	FCS_IPSEC_EXT.1

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
		generation and verification for mutual authentication using SHA-265, SHA-384				
4		IPsec: Pre-shared keys:	n/a	PSK of >= 22 characters e.g. Security Target [6]	Yes	FCS_IPSEC_EXT.1
5	Key Agreement	IPsec: DH with diffie-hellman group 14	RFC 2409 RFC 3526	plength = 2048	Yes	FCS_IPSEC_EXT.1
6	Confidentiality	IPsec: AES-CBC	FIPS PUB 197, NIST SP 800-38A, NIST SP 800-38D	|k| = 128 |k| = 256	Yes	FCS_IPSEC_EXT.1
7	Integrity	IPsec: HMAC-SHA-1 HMAC-SHA-256 HMAC-SHA-512	FIPS PUB 180-3 FIPS PUB 198-1	|k| = 160 |k| = 256 |k| = 512	Yes	FCS_IPSEC_EXT.1

Table 4: TOE cryptographic functionality

10 Obligations and Notes for the Usage of the TOE

The documents as outlined in table 2 contain necessary information about the usage of the TOE and all security advisories 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.

To repeat the most important information from the user guidance:

- Administrators must pay particular attention to the functionality excluded from the evaluated configuration. Features such as HTTP/HTTPS, telnet, and SNMP are not to be enabled in the Common Criteria compliant operational configuration.

- To be in the evaluated configuration, the TOE must be operated in “FIPS mode” of operation to fulfill some cryptographic functional requirements.
- To be in the evaluated configuration, the system clock must be set to UTC time for correct password timeout calculations.
- To be in the evaluated configuration, remote administration can only be done using an IPsec secured connection between the admin console and the TOE. This is even true if SSH is used as the protocol for accessing the command line interface.

  If an IPsec secured connection between the admin console and the TOE cannot be established, local administration via the console line must be used to operate the TOE in its evaluated configuration.
- CMP (Connectivity Management Processor) interface provides a backup network interface to the supervisor engine when the main Route Processor (RP) is unreachable. To be in the evaluated configuration, the CMP must not be used.

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.

12 Definitions

12.1 Acronyms

AIS Application Notes and Interpretations of the Scheme

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

CCRA Common Criteria Recognition Arrangement

CC Common Criteria for IT Security Evaluation

CEM Common Methodology for Information Technology Security Evaluation

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

IT Information Technology

ITSEF Information Technology Security Evaluation Facility

PP Protection Profile

SAR Security Assurance Requirement

SFP Security Function Policy

SFR Security Functional Requirement

ST Security Target

TOE Target of Evaluation

TSF TOE Security Functionality

VLAN Virtual Local Area Network

12.2 Glossary

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

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

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.

Protection Profile - An implementation-independent statement of security needs for a TOE type.

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 - A set of software, firmware and/or hardware possibly accompanied by guidance.

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 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Revision 3, July 2009

[3] BSI certification: Procedural Description (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[8].

[5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website

[6] Security Target BSI-DSZ-CC-0937-2014, Version: 1.0, 2014-02-14, ST for Cisco Catalyst 6500-E Series Switches, EDCS 1252106, Cisco Systems, Inc.

[7] U.S. Government Approved Protection Profile - Protection Profile for Network Devices Version 1.0, Version 1.0, December 10, 2010, National Information Assurance Partnership (NIAP)

[8] Evaluation Technical Report, Version 1.5, Date 2014-2-19, ETR Part Summary, media transfer AG, (confidential document)

[9] Guidance documentation, Cisco Catalyst 6500-E Series Switches, Common Criteria Operational User Guidance and Preparative Procedures, Cisco Systems, Inc., EDCS 1182242, Version 1.0, 20 February 2014

[8] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

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

Assurance Class	Assurance Components
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 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.

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
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”

Evaluation assurance level 1 (EAL1) - functionally tested (chapter 8.3)

“Objectives

EAL1 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.

EAL1 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.

EAL1 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 EAL1 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 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 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.

EAL2 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 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

EAL3 permits a conscientious developer to gain maximum assurance from positive security engineering at the design stage without substantial alteration of existing sound development practises.

EAL3 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 (EAL4) - methodically designed, tested, and reviewed (chapter 8.6)

“Objectives

EAL4 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. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 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 (EAL5) - semiformally designed and tested (chapter 8.7)

“Objectives

EAL5 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 EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 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 (EAL6) - semiformally verified design and tested (chapter 8.8)

“Objectives

EAL6 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.

EAL6 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 (EAL7) - formally verified design and tested (chapter 8.9)

“Objectives

EAL7 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 EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.”

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.”

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.