Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0975-2018

for

F5 Networks BIG-IP® Application Delivery Controller (ADC-AP) version 11.5.1 HF10 (build 10.123.180)

from

F5 Networks, 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-0975-2018 (*)

Network Device

F5 Networks BIG-IP® Application Delivery Controller (ADC-AP)
version 11.5.1 HF10 (build 10.123.180)

SOGIS IT SECURITY CERTIFIED
INFORMATION TECHNOLOGY SECURITY
MUTUAL RECOGNITION AGREEMENT

SOGIS
Recognition Agreement

from	F5 Networks, Inc.
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 4 augmented by ALC_FLR.3

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 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
for components up to
EAL 2 and ALC_FLR only

Bonn, 15 February 2018

For the Federal Office for Information Security

Joachim Weber
Head of Branch

L.S.

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

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:

- 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 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 related bodies of the signatory nations. A disclaimer beneath the logo indicates the specific scope of recognition.

This certificate is recognized according to the rules of CCRA-2014, i.e. up to and including CC part 3 EAL 2 components. The evaluation contained the SAR components above EAL 2 that are not mutually recognised in accordance with the provisions of the CCRA-2014, for mutual recognition the EAL 2 components of these assurance families are relevant.

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 F5 Networks BIG-IP® Application Delivery Controller (ADC-AP), version 11.5.1 HF10 (build 10.123.180) has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0856-2017. Specific results from the evaluation process BSI-DSZ-CC-0856-2017 were re-used.

The evaluation of the product F5 Networks BIG-IP® Application Delivery Controller (ADC-AP), version 11.5.1 HF10 (build 10.123.180) was conducted by atsec information security GmbH. The evaluation was initially completed on 26 October 2017 but a further delta evaluation task was performed to include a hotfix. This task was completed 15 February

2018. atsec information security GmbH is an evaluation facility (ITSEF)[6] recognised by the certification body of BSI.

For this certification procedure the sponsor and applicant is: F5 Networks, Inc.

The product was developed by: F5 Networks, 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

- 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 15 February 2018 is valid until 14 February 2023. 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,
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

[6] Information Technology Security Evaluation Facility

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 F5 Networks BIG-IP® Application Delivery Controller (ADC-AP), version 11.5.1 HF10 (build 10.123.180) 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] F5 Networks, Inc.
401 Elliott Ave West
Seattle, WA 98119
USA

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 called BIG-IP ADC-AP Version 11.5.1 HF10 (build10.123.180) (in the following named short as BIG-IP). The TOE provides the functionality of a reverse proxy and application gateway as well as a VPN endpoint with optional high availability failover. Its role based management functions can be accessed via a GUI, command line interface or an API.

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 4 augmented by ALC_FLR.3.

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:

Main Topic	TOE Security Functionality / Addressed Issue
Device management	Security Function Management Authentication Access Control Auditing Communications Security
Basic Traffic Management	Reply Detection Traffic Authentication TLS offloading
VPN Traffic	VPN Traffic
Cryptographic mechanisms	Key Generation Key Storage Certificate validation Cryptographic primitives in the TOE Random Number Generation Zeroization of Critical Security Parameters Crypto Statement (used cryptograhic functions)
TSF Protection and Support Functions	Failover of Redundant Systems Self-tests

Main Topic	TOE Security Functionality / Addressed Issue
	Update Verification Denial-of-Service Mitigation Protection of Sensitive Data Residual Information Protection

Table 1: TOE Security Functionalities

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

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. 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 3.1, 3.2 and 3.3.

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:

F5 Networks BIG-IP® Application Delivery Controller (ADC-AP), version 11.5.1 HF10 (build 10.123.180)

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	BIGIP-11.5.1.0.0.110.iso SHA256: bfca59ca1ec2606f24489dd52415bb8089f2f8b234bd82adbbc878111ac35888	11.05.01	Download
2	SW	Hotfix-BIGIP-11.5.1.10.123.180-HF10-ENG.iso SHA256: 1f505f4edd31ff0394207c6640f8dc8ec0923c24234fc7e61e21579ce4da573f	HF10	Download

No	Type	Identifier	Release	Form of Delivery
3	DOC	Documentation Supplement ISO (CommonCriteriaDocumentation-11.5.1.iso), containing [9] SHA256: 1f505f4edd31ff0394207c6640f8dc8ec0923c24234fc7e61e21579ce4da573f Note: Version 1.33 of [9] is the given version number of the main guigance document 'Guidance Supplement: AGD_PRE and AGD_OPE'. It is contained in the documentation supplement iso image, which is labeled as of version 11.5.1 like the TOE itself.	11.05.01	Download

Table 2: Deliverables of the TOE

The appliance on which the TOE will run may be shipped pre-installed with any version of the BIG-IP software. For the evaluated configuration, the user has to explicitly install and verify the evaluated release according to the instructions given in [9].

The software is downloaded from https://downloads.f5.com. The ISO images of the TOE as well as HF10 have to be downloaded individually and then need to be copied onto the appliance either via SSH or via an upload from the GUI. BIG-IP will perform an integrity check of the image. The TLS protected download page also provides the digital signatures of the ISO images for verification. The guidance is downloaded from https://askF5.com which resolves to https://support.f5.com and is provided as part of an ISO image. The guidance also instructs the user on how to verify the signatures of the TOE and HF10 ISO-images or checksums of the guidance ISO image.

Using the guidance and the SHA256 checksums provided in this certification report, the integrity of all images can be verified.

From the GUI, "System->Software Management: Image List" can be used to identify the currently running version of the TOE. Alternatively, the command string "tmsh show sys software status" can be used on the command line.

The output will be

'BIG-IP 11.5.1 10.123.180' and should be displayed as 'Active' and 'Complete'.

This corresponds to the major version 11, minor version 5, maintenance release 1, hotfix 10 and build 10.123.180.

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: The security policy enforced is defined by the selected set of Security Functional Requirements and implemented by the TOE. The TOE implements a role-based access control policy to control administrative access to the system.

In addition, the TOE implements policies pertaining to the following security functional classes: Security Audit, Cryptographic Support, User Data Protection, Identification and Authentication, Access Control, Traffic Management, VPN and Security Management. All of these functions are supported by TSF protection mechanisms including failover functions. Specific details concerning the above-mentioned security policies can be found in Section 7 of the Security Target [6].

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. Section 2.1 of [9] titled "Preparing for BIG-IP Installation and Configuration" lists expectations on the customer when preparing to use the TOE:

- Installed in a secure location
- No general purpose computing
- Trained administrators
- Trusted administrators
- Operational environment resources available and TOE attached to appropriate networks
- Keys and certificates used conform to the stated requirements

Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The TOE is an Application Delivery Controller (ADC) based on F5's Traffic Management Operating System (TMOS).

The TOE includes the Local Traffic Manager (LTM) and Access Policy Manager (APM) modules, providing network traffic management, and VPN gateway functionality.

BIG-IP runs on F5's TMOS (Linux: CentOS 5.4), either directly on appliance hardware or in a Virtual Clustered Multiprocessing (vCMP) environment. vCMP is a hypervisor that allows organizations to run multiple virtual Instances of the TOEs on the same hardware.

The relationships of TOE components in the evaluated configuration are shown in Figure 2 of the Security Target [6]. Virtual editions of the TOE running on third-party hypervisors are excluded from the certified scope.

BIG-IP can be connected in a redundant configuration to an identical (redundant) BIG-IP for failover purposes.

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. Developer Testing

Test Configuration

The test results provided by the developer were generated on the following systems: B4300, B4300+VCMP, 10000, 10000+VCMP, 7000, 10200, 5200, 5000.

The developer has performed his tests on the above listed hardware platforms. The software was installed and configured as defined in the document "Guidance Supplement: AGD_PRE and AGD_OPE" [9].

Test Approach

The developer did not perform all tests on all platforms. The tests where performed on the platforms defined in the Security Target [6]. Only hardware-specific tests where executed on the specific hardware i.e. on the 5000 and 7000 series although they use the same chip-set. The vCMP platform was used for just two of the test runs as it does not have an impact on the actual results. In general, the TOE does not have any hardware dependencies apart from the Cavium chip for entropy, which was available on all tests.

The developer devised manual tests for testing specific functionality. Protocol compliance testing was performed via standard tools TAHI for IPv6 compliance tests and IxANVL for all other protocol compliance tests.

Test Results

The test results provided by the developer were generated on the hardware platforms listed above. The developer uses the tool 'ap test manager' to track the tests and records the verdict with the test runs.

All test results from all tested environments show that the expected test results are identical to the actual test results.

The developer did not test all machines of all families mentioned in the Security Target [6] but only once for each CPU and co-processor. Differences between the machines are related to the provided hardware environment that has no impact on the security of the TOE.

Test Coverage

The functional specification has identified the following different TSFI:

CLI: The command-line shell (tmsh) accessed via SSH.

Configuration Utility (GUI): The web GUI accessed via HTTPS/TLS.

iControl API: A SOAP based API.

Network Protocols: The network protocols supported for administrative tasks as well as the protocols supported by the proxy functions.

The test mapping provided by the developer shows that the tests cover all individual TSFI identified for the TOE. An extension to this mapping by the evaluator also shows that the TSFI have been covered with the developer's test suite.

Test Depth

In addition to the mapping to the functional specification, the developer provided a mapping of test cases to subsystems of the high-level design. This mapping shows that all subsystems and the internal interfaces are covered by test cases. To show evidence that the internal interfaces have been called, the developer provided the description of the internal interfaces as part of the design.

Conclusion

The evaluator has verified that developer testing was performed on hardware conformant to the Security Target [6].

The evaluator was able to follow and fully understand the developer testing approach by using the information provided by the developer.

The evaluator analysed the developer testing coverage and the depth of the testing by reviewing all test cases. The evaluator found the testing of the TSF to be extensive and covering the TSFI as identified in the functional specification as well as the subsystem internal interfaces identified in the design documentation.

The evaluator reviewed the test results provided by the developer and found them to be consistent with the expected test results according to the test plan.

7.2. Evaluator Testing Effort

Test Configuration

The evaluator verified the test systems according to the documentation in the 'Evaluated Configuration Guide [9]' and the test plan.

Evaluator Tests Performed

In addition to running a random sample of the developer tests, the evaluator devised tests for a subset of the TOE.

The evaluator has chosen these tests for the following reasons:

- The test cases examine some of the security functions of the TOE in more detail than the developer-supplied test cases.
- The test cases cover security aspects not included in the developer testing

The evaluator created several test cases for testing a few functional aspects where the developer test cases were not considered by the evaluator to be broad enough. During the evaluator's review of the test cases provided by the developer, the evaluator gained confidence in the developer testing effort and the depth of test coverage in the developer supplied test cases. The analysis has shown a very wide coverage of the TSF, therefore the evaluator devised only a small number of test cases.

Summary of Evaluator Test Results

The tests were performed remotely at the developer's data center via VPN as well as on-site. Only one test configuration was used as the SFRs are not dependent on the hardware platform.

SSH was used for console access and HTTPS connections for the GUI and iControl. The TOE was installed on the test machine by the evaluator according to the instructions in [9] and verified by the evaluator. The configuration triggered by the ccmode script[8] ensured the evaluation-compliant system configuration. After running the automated configuration, no further system configuration was performed and only the specifics for the test cases were set up. The test systems were therefore configured according to the Security Target [6] and the instructions in [9]. The developer provided manual test cases. The evaluator verified the configuration against [9] before conducting the independent tests. The test results were analysed for completeness and failures.

All the test results conformed to the expected test results from the test plan.

[8] The ccmode command is the first step in configuring the BIG-IP to be compliant with specific Common Criteria requirements. It performs functions such as setting the required password policy, the allowed ciphersuites for SSL, logging options, etc.

In addition to repeating a subset of developer tests, the evaluator decided to run some additional test cases on the provided test systems:

- Verification of the firewall via nmap scans.
- SSLv3 and SSLv2 handshake attempts to verify that they are not supported.
- TLS with disallowed ciphers to verify that they are not supported (no downgrade).
- Code analysis of the iControl python test scripts.

Finally, a test suite related to specifics of the TOE's cryptographic functions was devised and run. All tests passed successfully.

7.3. Evaluator Penetration Testing

The evaluator took the following approach to derive penetration tests for the TOE:

The evaluator decided to not generate simple penetration tests, but instead to perform a source code analysis for some of the identified potential vulnerabilities.

The evaluator has performed his analysis on the TOE source code that was available via the developer's source browsing tool as well as via shell access to a complete source tree.

The analysis addressed the following security functions because they were considered to be the most important parts of the code where the TOE's security policy was enforced, and where the evaluator could assess whether the enforcement could be bypassed or not:

- Network interfaces: General TSF protection.
- User data handling interfaces: General TSF protection.
- Privilege escalation for administrative roles: Separation of roles.
- Issues reported from CPPCheck: General source code analysis.

No residual vulnerabilities for the TOE were identified.

In addition, some of the testing conducted as part of the evaluators independent testing can be considered penetration testing. It is shown in the chapter on the evaluator testing above.

8. Evaluated Configuration

This certification covers the evaluated configuration which consists of BIG-IP ADC-AP Version 11.5.1 HF10 (build10.123.180).

The following configuration specifics apply to the evaluated configuration of the TOE:

- Appliance mode is licensed. This results, amongst other effects, in root access to the underlying system being disabled, and Always-On Management not being able to access the host.
- A physical network port is dedicated on each device for the exchange of management traffic with the mirrored device (configuration synchronization, failover monitoring).
- Dynamic routing is excluded from the evaluated configuration.

The following interfaces are disabled:

- Shells other than tmsh (e.g. bash and other user-serviceable shells).
- Management of the TOE via SNMP.

- Management of the TOE via the appliance's LCD display.
- Remote (i.e., SSH) access to the Lights-Out / Always-On Management capabilities of the system.
- Serial port console.

The evaluated configuration is limited to the physical and logical boundaries as mentioned in the Security Target [6], chapter 1.5.5, especially is it limited to the listed Hardware configurations.

Virtual editions of the TOE running on third-party hypervisors are excluded from the certified scope.

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 4 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.3 augmented for this TOE evaluation.

As the evaluation work performed for this certification procedure was carried out as a re-evaluation based on the certificate BSI-DSZ-CC-0856-2017, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the licensed functionality and the inclusion of a hotfix as compared to the TOE of BSI-DSZ-CC-0856-2017. The base evaluation included the Advanced Firewall Manager module, whereas the current evaluation does not include this firewall functionality, but instead the Access Policy Manager module for VPN and web gateway functionality. The TOE for this evaluation is therefore a different instantiation of the same BIG-IP base product, with only the availability of the above named functionality being different. No other changes have been made to the TOE.

The evaluation has confirmed:

- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 4 augmented by ALC_FLR.3

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	Authenticity	RSA signature verification (RSASSA-PKCS1-v1_5) using SHA-1	FIPSPUB186-3[9] (RSA) referring to RFC3447 (PKCS#1 v2.1) FIPSPUB180-3[10] (SHA)	Modulus length: 2048, 3072, 4096	no	Algorithms used depending on the signature algorithm / hash algorithm used for signing the certificates and the accepted signature algorithms / hash algorithms by the peers. Server certificates required and client certificates optional. Verification of certificate signatures provided for authentication of peers. The certificates are not generated by the TOE[11]
2		RSA signature verification (RSASSA-PKCS1-v1_5) using SHA-256, SHA-384	RFC3447 (PKCS#1 v2.1) FIPSPUB180-3 (SHA)	Modulus length: 2048, 3072 4096	yes	
3		ECDSA signature generation and verification using SHA-1	FIPSPUB186-3 (ECDSA), FIPSPUB180-3 (SHA),	secp256r1 NIST P-256	no	
4		ECDSA signature generation and verification using SHA-256, SHA-384	FIPSPUB186-3 (ECDSA), FIPSPUB180-3 (SHA)	secp256r1 NIST P-256	yes	

[9] Note, that FIPSPUB186-3 is obsoleted by FIPSPUB186-4.

[10] Note, that FIPSPUB180-3 is obsoleted by FIPSPUB180-4.

[11] Please note that the TOE in general can handle signature algorithms with smaller key sizes than those listed above and using weak hash functions (e.g. MD5). However, the administrator is advised not to import certificates with such signatures. The same holds true for signing algorithms and respective hash functions as contained in the certificate itself.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
						(imported into the TOE).
5	Authentication Client Depending on client's certificate if any (subject public key info and key usage).	RSA signature generation (client) and verification (server). (RSASSA-PKCS1-v1_5[12]) using SHA-1	RFC3447 (PKCS#1 v2.1) RFC5246 (TLSv1.2)	Modulus length: 2048, 3072, 4096	no	Certificates with signing capability. Client cert type: rsa_sign. CertificateVerify: Client provides signature over the whole handshake message Only for TLSv1.1.
6		RSA signature generation (client) and verification (server). (RSASSA-PKCS1-v1_5) using SHA-256, SHA-384	RFC3447 (PKCS#1 v2.1) RFC5246 (TLSv1.2)	Modulus length: 2048, 3072 4096	yes	
7		RSA signature generation (client) and verification (server). (RSASSA-PKCS1-v1_5) using MD5 / SHA-1 combination	RFC3447 (PKCS#1 v2.1) RFC4346 (TLSv1.1)	Modulus length: 2048, 3072 4096	no	
8		ECDSA signature generation and verification using SHA-1	FIPSPUB186-3 (ECDSA), FIPSPUB180-3 (SHA), RFC4492 (ECC for TLS)	secp256r1 NIST P-256	no	Client cert Type: ecdsa_sign. The public key of the certificate MUST use a curve and point format supported by the server.
9		ECDSA signature generation and verification using SHA-256, SHA-384	FIPSPUB186-3 (ECDSA), FIPSPUB180-3 (SHA), RFC4492 (ECC for TLS)	secp256r1 NIST P-256	yes	
10	Authentication Server (static)[13]	Generating and verifying the PRF contained in the “Finished message”. (TLS_RSA, TLS_ECDH)	RFC5246 (TLSv1.2) RFC4346 (TLSv1.1)			Please refer to PRF within key derivation below.

[12] Implicitly EMSA-PKCS1-v1_5 encoding method is required based on block type 1 (PS= FF).

[13] Static keys / parameter contained in the certificate. Server Certificate must contain the RSA key or the ECDH parameters pub key. Key usage encipherment (RSA) and key exchange for (ECDH params). By successfully decoding the premaster secret (RSA) or computing / agree upon the premaster secret ECDH shared secret) and producing a correct “Finished message” with the master secret derived from the premaster secret as key, the server demonstrates that it knows the private key corresponding to the certificate. For TLS >= 1.1 it is only historical to list the key authentication key within the cipher since cert signing is not any longer bound to the key contained in the cipher provided for key authentication.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
11	Authentication Server (ephemeral)	RSA signature generation and verification (RSASSA-PKCS1-v1_5) using SHA-1 (TLS_ECDHE_RSA)	RFC3447 (PKCS#1 v2.1) FIPSPUB180-3 (SHA) RFC5246 (TLSv1.2)	Modulus length: 2048, 3072 4096	no	ServerKeyExchange: RSA signature over the ephemeral
12		RSA signature generation and verification (RSASSA-PKCS1-v1_5) using SHA-256, SHA-384 (TLS_ECDHE_RSA)	RFC3447 (PKCS#1 v2.1 FIPSPUB180-3 (SHA) RFC5246 (TLSv1.2)	Modulus length: 2048, 3072 4096	yes	
13		RSA signature generation (client) and verification (server). (RSASSA-PKCS1-v1_5) using MD5 / SHA-1 combination	RFC3447 (PKCS#1 v2.1 RFC4346 (TLSv1.1)	Modulus length: 2048, 3072 4096	no	For TLSv1.1
14		ECDSA signature generation and verification using SHA-1 (TLS_ECDHE_ECDSA)	ANSI X9.62 (ECDSA), FIPSPUB180-3 (SHA), RFC4492 (ECC for TLS)	secp256r1 NIST P-256	no	See above however with ECDSA as signature algorithm.
15		ECDSA signature generation and verification using SHA-256, SHA-384 (TLS_ECDHE_ECDSA)	ANSI X9.62 (ECDSA), FIPSPUB180-3 (SHA), RFC4492 (ECC for TLS),	secp256r1 NIST P-256	yes	
16	Key establishment: Key transport	RSA encryption (client) and decryption (server) (RSAES-PKCS1-v1_5[14]) (TLS_RSA)	RFC3447 (PKCS#1 v2.1) SP800-56B (IFC key establishment)	Modulus length: 2048, 3072 4096	yes	Server certificate is used for key exchange. Encrypted exchange of pre-master secret generated at client side. Server authentication (#14).

[14] Implicitly EME-PKCS1-v1_5 encoding method is required based on block type 2 (PS= random data).

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
17	Key establishment: Key agreement Ephemeral	ECDHE	RFC4492 (ECC for TLS) TR-03111 (ECC) SP800-56-A (ECC DH)	secp256r1 NIST P-256	yes	Unauthenticated ephemeral ECDH key / parameters provided by the server in the ServerKeyExchange. This is the only curve that is hard coded in the TOE.
18	Static	ECDH	RFC4492 (ECC for TLS) TR-03111 (ECC) SP800-56-A (ECC DH)	secp256r1 NIST P-256	yes	The ECDH-parameters contained in the certificate (static). Since NIST P-256 is the only curve hard coded in the TOE – only certificates with ECDH parameters based on NIST P-256 will work. Server authentication (#14)
19	Key derivation	PRF: HMAC with SHA-256, 384 (default: prf_sha256 for TLSv1.2, also prf_sha384 possible)	FIPSPUB198-1 (HMAC) FIPSPUB180-3 (SHA) RFC5246 (TLSv1.2)	variable	yes	Symmetric keys and MAC keys for record layer. Pre-master secret / (DH / ECDH shared secret) is converted into the master secret, the keys of the record layer are generated by expanding the master secret using the security parameters of the handshake protocol.
20		PRF: HMAC with MD5 and SHA-1 in combination (default: prf for TLSv1.1)	FIPSPUB198-1 (HMAC) RFC1321, RFC6151 (MD5) FIPSPUB180-3 (SHA) RFC4346 (TLSv1. 1)	variable	no	

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
21	Integrity and authenticity	HMAC with SHA-1 or SHA-256 or SHA-384 (SHA), (SHA256), (SHA384)	FIPSPUB198-1 (HMAC) FIPSPUB180-3 (SHA)	160 (SHA-1) 256 (SHA-256) 384 (SHA-384)	yes	Message authentication code (record layer)
22	Trusted Channel	FTP_ITC.1 [6], sec. 6.1. 10.1 for HTTPS, syslog	Cf. all lines above	See above	no[15]	Confidentiality is provided by AES-CBC with key size 256 bits using non-TSF (AES-NI).

Table 3: TOE cryptographic functionality (TLS)

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
1	Authentication	RSA signature generation & verification RSASSAPKCS1-v1_5 using SHA-1 (ssh-rsa)	RFC3447 (PKCS#1 v2.1) FIPSPUB180-3 (SHA-1) RFC4253 (SSH-TRANS) for host authentication RFC4252, sec 7 (SSH-USERAUTH) for user authentication method: “publickey”	Modulus length: 1024	no	Pubkeys are exchanged trustworthy out of band. Authenticity is not part of the TOE. (no certificates used, server lists are in general possible at the client side – however client is not part of the TOE).

[15] Security properties of TLS are diminished by incomplete verification of the verify_data field in the Finished message, see section 10.

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits	Comments
2		UserID & password	RFC4252, sec. (SSH-USERAUTH) method; “password”	Guess success prob.	yes	[6] FIA_AFL.1: Recommendation as of [9] not to change the default setting where the blocking after 3 attempts is configured. Min 15 characters. No FIA_SOS claimed.
3	Key establishment: Key agreement	DH with DH group14-sha1	RFC4253 (SSH-TRANS) supported by RFC3526 (DH groups IKE) FIPSPUB180-3 (SHA-1)	plength= 2048	yes	Hard coded in the TOE code.
4	Integrity and authenticity	HMAC-SHA-1	FIPSPUB180-3 (SHA), RFC2104 (HMAC), RFC4251 / RFC4253 (SSH general / detailed HMAC support), RFC4253 (SSH detailed HMAC support)	|k|=160	yes	Binary packet protocol: message authentication
5	Key generation	RSA key generation	FIPSPUB186-3, B.3.3 and C.3 for Miller Rabin primality tests.	n/a	n/a	FCS_CKM.1 Host key generation using FCS_RBG_EXT.1
6	Trusted path	FTP_TRP.1, [6] section 6.1.10.2 for SSH			yes/no[16]	Confidentiality is provided by AES-CBC with key size 256 bits using non-TSF (AES-NI).

Table 4: TOE cryptographic functionality (SSH)

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 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.

[16] Depending on the sec. level of the used mechanisms above.

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.

Please note that upon detecting a block cipher CBC padding error, the record decryption aborts with a masked error (the same error code as for a MAC error) without unconditionally computing a MAC as countermeasure against information leakage. In addition, the padding check itself is not implemented in constant time. Consequently, no constant time unpadding and no constant time MAC verification is implemented in the TOE. Thus, the TOE is vulnerable to all variants of CBC padding attacks based on timing side channels. This vulnerability was registered as CVE-2013-0169 with a CVSS base score of 2.6 LOW.

Please also note that the TOE does not verify every byte in the Finished Message (Finished.verify_data) of a TLS handshake as required by the TLS protocol. Specifically, only the first and the last four bytes of the 12 Byte Finished.verify_data message are checked, while the middle four bytes are being ignored. Incomplete validation of the Finish Message increases the probability not to detect modifications of the handshake.

These vulnerabilities, however, are not considered to be exploitable by an attacker at the Enhanced Basic attack potential for EAL4.

In addition, the following aspects need to be fulfilled when using the TOE:

- MD2: The TOE includes code that potentially allows the TOE to successfully validate certificates signed with the md2WithRSAEncryption algorithm. MD2 is no longer considered a valid and secure hash algorithm. It is thus required to hook into the TOE's processing of certificates and reject certificates with the undesired algorithm using so called iRules. See [9], section 2.3.8.3 for more information.

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

ADC	Application Delivery Controller
AIS	Application Notes and Interpretations of the Scheme
APM	Access Policy Manager

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
cPP	Collaborative Protection Profile
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
HF	Hot Fix
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
LTM	Local Traffic Manager
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

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[17] 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-0975-2018, Version 1.6, 2018-02-12, BIG-IP 11.5.1 HF 10 (build 10.123.180) ADC-AP Security Target, F5 Networks, Inc.

[7] Evaluation Technical Report, Version 7, 2018-02-15, Final Evaluation Technical Report, atsec information security GmbH (confidential document)

[8] Configuration list for the TOE, 2017-09-26, CI list for documentation in Perforce (confidential document)

[9] Documentation Supplement ISO (CommonCriteriaDocumentation-11.5.1.iso), containing 'Guidance Supplement: AGD_PRE and AGD_OPE', Version 1.33, 2017-07-05

[17] specifically

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

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
	ASE_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.”

This page is intentionally left blank.

C. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.