Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0901-2015

for

IBM WebSphere DataPower Firmware Version 6.0.2.0

from

IBM Corporation

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-0901-2015 (*)

Application-Level Firewall Software

IBM WebSphere DataPower Firmware
Version 6.0.2.0

from	IBM Corporation
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

SOGIS
Recognition Agreement

Common Criteria

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

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 4.

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

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

Common Criteria
Recognition Arrangement

Bonn, 9 December 2015

For the Federal Office for Information Security

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

Bernd Kowalski
Head of Department

L.S.

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: Technical information on the IT security certification, Procedural Description (BSI 7138) [3]
- BSI certification: Requirements regarding the Evaluation Facility (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1[5] [1] also published as ISO/IEC 15408.
- Common Methodology for IT Security Evaluation (CEM), Version 3.1 [2] also published as ISO/IEC 18045.
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2. Recognition Agreements

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

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

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

---

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

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

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

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

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

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

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

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

2.2. International Recognition of CC – Certificates (CCRA)

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

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

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

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

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

As the product certified has been accepted into the certification process before 08 September 2014, this certificate is recognized according to the rules of CCRA-2000, i.e. for all assurance components selected.

3. Performance of Evaluation and Certification

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

The product IBM WebSphere DataPower Firmware, Version 6.0.2.0 has undergone the certification procedure at BSI.

The evaluation of the product IBM WebSphere DataPower Firmware, Version 6.0.2.0 was conducted by atsec information security GmbH. The evaluation was completed on 26 November 2015. 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: IBM Corporation.

The product was developed by: IBM Corporation.

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.

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 as outlined on the certificate. The certificate issued on 9 December 2015 is valid until 08. December 2020. The validity date can be extended by re-assessment or 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 and the Security Target and user guidance documentation mentioned herein to any applicant 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,

[6] Information Technology Security Evaluation Facility

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

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

5. Publication

The product IBM WebSphere DataPower Firmware, Version 6.0.2.0 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] IBM Corporation
550 King Street
Littleton, MA 01460
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 the 'IBM WebSphere DataPower Firmware, Version 6.0.2.0' and is, combined with its underlying operating system and hardware, a network appliance that provides application-level firewall functionality, web service proxy functionality, and message content transformation functionality.

The network appliance is used in the following scenarios:

- In the demilitarized zone (DMZ) between an enterprise and external partners, where the network appliance performs primarily security services (e.g. enforcement of security policies on incoming and outgoing traffic, message content transformation or multiprotocol bridging).
- Within the enterprise as an enterprise service bus (ESB), interconnecting disparate enterprise assets in a meaningful way (e.g message routing, multiprotocol bridging or message content transformation).

The TOE does not support clustering. In case several network appliances are used in the operational environment, each network appliance works independently from the other.

The flexibility of the configuration of the network appliance allows an enterprise to deploy a network appliance in scenarios requiring interoperability with a wide range of enterprise assets, such as

- Authentication systems,
- Databases,
- Mainframe applications,
- Diverse message transport systems,
- Web service applications,
- Web sites.

The network appliances are self-contained, rack mount units while the TOE is defined as the network appliance firmware and it contains an embedded operating system, an Secure Shell (SSH) daemon, an application called "Router", and a Watchdog application. The Router application and SSH daemon enforce all of the claimed security functionality.

The TOE consists of the Oversight subsystem (which includes the Watchdog application), the Router subsystem and the SSH daemon subsystem. All hardware and the remaining firmware are part of the Operational Environment.

There are three variations of the TOE (defined by the hardware it is hosted on) that are included in this Security Target (ST); each TOE provides similar security functionality and corresponds to the IBM products described below:

- The DataPower Service Gateway XG45 is a lightweight, level entry network appliance shipped in a 1U rack system that provides Web service proxy; Application level firewall based on information flow control policy based on protocol information, message content, and identity assertions (authentication); Message content transformation based on XML Path Language (XPath) and XML Stylesheet Language Tranformations (XSLT).
- The DataPower Integration Appliance XI52 offers all the functionality provided by the XG45 but in a more powerful 2U rack system. In addition, it provides support for more

message formats and more connectivity options (not included in the evaluated configuration).

- The DataPower B2B Appliance XB62 runs in a 2U rack system and provides business to business (B2B) functionality in addition to the features included in the XG45 and XI52 models. It supports B2B messaging protocols such as AS1, AS2, AS3 and ebMS (not included in the evaluated configuration).

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. 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
1	Security audit
2	Cryptographic support (TLS version 1.2, SSH version 2, XML signature, XML encryption, Certificate validation, Random number generation)
3	User data protection
4	Identification and authentication
5	Security management
6	Protection of the TOE security functionality
7	Trusted channel

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

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

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

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

2. Identification of the TOE

The Target of Evaluation (TOE) is called:

IBM WebSphere DataPower Firmware

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Firmware for XB62 xb6020.CommonCriteria.scrypt3 SHA256: bf7b273b5dbc57e3a11ca655c10e3830d874a939aa7e83b50de216eb57041333	6.0.2	Download
2	SW	Firmware for XI52 xi6020.CommonCriteria.scrypt3 SHA256: 7035220ecee61a8c3d72e87f75565d79783e2405a14af01384f0db0c1e3ecc0c	6.0.2	Download
3	SW	Firmware for XG45 xg6020.CommonCriteria.scrypt3 SHA256: 8d6717c20eb36ccc9938be01d3d443a62ba72c3686941a186f9ebc0bc1a893fb	6.0.2	Download
4	DOC	Standalone Knowledge Center [9] dp602kc.zip SHA256: 6866c04169d35bfe9335c42198c2841c24466c3ed4420bdd7c5d5ed00b4436b8	6.0.2	Download
5	DOC	Secure Deployment Guide [8] DataPower_Secure_Deployment_Guide_6020.pdf SHA256: 5c024a819eff15c46b61170d7a38c0a623eef6e489cda835499e4e8abd879f79	6.0.2	Download

Table 2: Deliverables of the TOE

The firmware images and the images of the Standalone Knowledge Center [9] will be published on IBM's download website 'FixCentral'.

The delivery of the Secure Deployment Guide [8] will kicked off be by individually contacting IBM's level 2 support.

The TOE can be identified by the checksums as given in table 2. When being installed on the hardware, the administrator can issue the command show firmware upon wich the version of the firmware as well as the build number will be returned. The build number of the TOE is 256732.

3. Security Policy

The security policy for the TOE is defined by the security functional requirements and divided in two distinct groups: one for enforcing information flow control, and the other to enforce access control to objects and security management functions. The following is a list of the subjects and objects, and their security attributes, that are participating in the policy.

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 list of objectives which have to be met by the the environment can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The TOE is a set of applications in the firmware that provides application-level firewall functionality, web service proxy functionality and service integration functionality. The TOE consists of the following subsystems:

- Oversight subsystem,
- Router subsystem,
- SSH daemon subsystem.

The TOE runs on top of an embedded, optimized DataPower Operating System (IBM MCP 7, a variant of Red Hat Linux) that is included in the firmware package. The operating system, as well as the underlying hardware, are part of the Operational Environment.

The Oversight subsystem initializes processes and monitors the Router application to ensure that it is always running.

The Router subsystem performs the vast majority of the security functionality. It implements the firewall and enforces the firewall policies. It implements web service proxy features by enforcing information flow control policies, and it provides a command-line interface (CLI) administrative interface.

Administrators perform management tasks through a Command Line Interface (CLI). Administrators connect to the TOE either through the network appliance's Console connector (an RJ45 serial connector supporting RS-232c) or over the network appliance's Ethernet management connectors (MGT0 and MGT1) using TCP/IP. The Ethernet management connectors support the CLI over a SSH connection, which is provided through the SSH daemon subsystem. Secure Copy (SCP) is also supported via the SSH protocol.

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

Developer Testing

The developer used manual tests and a few automated tests. The test suite comprises 214 tests. Most of the tests were run manually, which by the nature of the TOE configuration requires several different steps to copying configuration files, configuration scripts, perform configuration commands, and running different types of external programs depending on which of the various protocols covered by the information flow was the subject in the respective test case.

The test approach was to use mainly use manual tests (because of the restricted TOE interfaces) which requires a number management activities for most of the tests which can only be done via the admin CLI interface. All security functions with the exception of the DRNG tests were executed by using externally visible TOE interfaces. The DRNG was tested on a debug installation to enable the use of internal TOE interfaces to be used.

As the testing effort is quite high, the developer used an iterative test approach, where after an update of the TOE during the evaluation, he rerun all tests that were related to the changed functionality and also rerun tests that involve and verify the general functionality of the TOE.

The developer executed all tests on firmware level 249668. He then rerun all cryptographic tests, RNG tests, and audit tests on firmware level 256732 which is the final firmware version of the TOE. The firmware level difference was assessed by the evaluator who examined the source code differences. During that examination it became clear that the changes were of a nature that made it possible that the results for those executed tests are able to represent the final firmware level. The DRNG tests were executed on a debug firmware level based on 253964 which included the RNG design changes.

The TOE was configured according to the Secure Deployment Guide [8] with respect the test relevant settings for interfaces, cryptographic implementation, and Common Criteria mode.

All developer test results were consistent with the expected test results.

Independent Evaluator Testing

The independent functional evaluator tests comprised of 13 independent tests as well as 13 repeated developer tests witnessed by the evaluator.

The following security functions have been tested:

Authentication: FIA_UAU.2, FIA_UID.2, FIA_SOS.1, FIA_AFL.1, FIA_USB.1

Information Flow control: FDP_IFC.1, FDP_IFF.1

Security Management / Access control: FDP_ACC.2, FDP_ACF.1, FMT_MTD.1(DACP)

Cryptographic tests: FCS_CKM.1, FCS_CKM.2, FCS_COP.1 (ENC/MAC/MD/SGN)

The testing was performed on two configurations: the developer test were rerun on the final firmware level 256732, while the independent evaluator tests were executed on an earlier firmware level 255579 which the evaluator assessed by examining the source code

differences. During that examination it became clear that the change only affected the status output functionality and does not impact other functions.

The subset of developer tests was rerun on the platform XG45, XI52, and XB62, while all the independent evaluator tests were run on an XI52 platform which was setup in the ITSEF lab in Munich.

All tests were executed successfully with the actual results matching the expected results.

Penetration Testing

The penetration testing was performed on firmware level 255579. This firmware level differs from the final TOE firmware version in two aspects: one status output command has been corrected, and one potential buffer overflow vulnerability was corrected. By assessing the source code differences, the evaluator came to the conclusion that the penetration testing performed on 255579 was representative for the final TOE version.

For the collection of the RSA/DSA timing data, the developer supported the evaluator by providing a firmware version setup that allowed access to non-externally accessible functions.

The testing mainly covered the administrative SSH interface and the TLS/SSH-protected information flow control TSFI, and including on test on the JSON data payload TSFI. The total of 12 tests used only external interfaces with one exception: a program has developed that gets compiled on the underlying OS of the TOE in order to execute and measure the timing of DSA/RSA signature operations.

The evaluator used the information on potential vulnerabilities collected by the evaluators during the evaluation that should be considered in the vulnerability analysis. The evaluator took into account the ST, guidance documentation, functional specification, TOE design, security architecture description and implementation representation to identify possible potential vulnerabilities in the TOE mainly focusing on two aspects: the administrative login and management functionality, and the certificate validation mechanism. Specifically, the following areas were subject to penetration testing:

- Account Lockouts are forgotten over a reboot.
- Privilege Escalation
- Timing vulnerability for RSA and DSA signatures
- Incorrect JSON validation
- Acceptance of weak certificates
- Incomplete application of CRLs
- Use of weak SSH cipher
- Insufficient character classes applicable for user-selected passwords
- Insecure handling certificates not following ASN.1
- Unauthorized admin access with hard-coded password

Apart from standard tools to communicate with the TOE interfaces, the evaluator used self-written code as part of the penetration tests to verify the vulnerabilities. None of the penetration tests were successful.

The penetration testing was carried out using the source code, internal interfaces, and external interfaces of the TOE. The subsystems subject to penetration testing are all parts of the TOE. The TSF under examination were the following:

- Authentication
- Management and User Data Protection
- Cryptographic support
- Trusted channels

None of the evaluator's penetration tests were successful in the sense that they allowed the penetration of the TOE. In summary, no exploitable or residual vulnerabilities were identified within the claimed attack level.

8. Evaluated Configuration

The evaluated configuration consists of the firmware and guidance documentation specified in the ST [6], section 1.5.3.1 running on the hardware models specified in the ST [6] section 1.4.1. It includes the use of the optional IT products specified in the ST [6] section 1.4.1. The specifications for configuring the TOE in the evaluated configuration are located in the guidance documentation 'Secure Deployment Guide' [8]. The consumer must read, understand, and follow the guidance documentation provided as part of the TOE for the evaluated configuration. The following configuration information applies to the evaluated configuration:

- Audit must always be enabled.
- SSLv3.0 must be disabled. Only TLSv1.2 is allowed.
- The WebGUI for administrative management must be disabled.
- SNMP must be disabled.
- The XML Management Interface must be disabled.
- The USB port must be disabled.
- The Intelligent Platform Management Interface (IPMI) LAN channel must be disabled.
- A Web-based Graphical User Interface (WebGUI) is disabled by default and not allowed in the evaluated configuration.

Additional configuration information can be found in the 'Secure Deployment Guide' [8].

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 and guidance specific for the technology of the product [4] (AIS 34).

The following guidance specific for the technology was used:

(i) Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren (Functionality Classes and Evaluation Methodology for Deterministic RNGs)

(see [4], AIS 20).

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.

The evaluation has confirmed:

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

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
TLS						
1	Authenticity	RSA signature verification (RSASSA-PKCS1-v1-5) using SHA-1	RFC3447 [18] (PKCS#1 v2.1) FIPS180-4 [10] (SHA)	Modulus length: 1024, 2048, 4096	no	Verification of certificate signatures provided for authentication Server and client certificates (optional) are used. Algorithms used depending on the signature algorithm[8] / hash functions[9] used for
2		RSA signature verification (RSASSA-PKCS1-v1-5)	RFC3447 [18] (PKCS#1 v2.1) FIPS180-4 [10] (SHA)	Modulus length: 1024	no	

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
		using SHA-256		Modulus length: 2048, 4096	Yes	signing the certificates.
3	Authentication	RSA signature generation and verification (RSASSA-PKCS1-v1-5[10]) using SHA-1	RFC3447 [18] (PKCS#1 v2.1)	Modulus length: 1024, 2048, 4096	no	Client signs message (containing all previous handshake messages) with private key bound to his certificate. Server verifies signature of the message. algorithms[11] depending on the key used for signing, contained in the client certificate.
4		RSA signature generation and verification (RSASSA-PKCS1-v1-5[1]) using SHA-256	RFC3447 [18] (PKCS#1 v2.1)	Modulus length: 1024	no	
				Modulus length: 2048, 4096	yes	
5	Key establishment/ key transport	RSA encryption (client) and decryption (server) (RSAES-PKCS1-v1-5[12]) (TLS_RSA)	RFC3447 [18] (PKCS#1 v2.1)	Modulus length: 1024	no	Encrypted exchange of pre-master secret generated at client side[13]
				Modulus length: 2048, 4096	yes	

[8] Since the TOE in general also supports DSA signature generation and verification using SHA-1; authenticity may also be checked using DSA signature verification if the certificate itself is signed with DSA using SHA-1. Furthermore, if the signing key contained in the client certificate is stated to be used with DSA then DSA using SHA-1 signature generation and verification will be used by the TOE for authentication. However, this not claimed by the [ST] (please refer to FCS_COP.1) and as such not part of the TOE, and, therefore, is not listed above.

[9] In general, MD5 is also supported by the TOE as hash function. However, it is ensured by organizational controls that only certificates signed based on strong hash functions as claimed above are used within the TOE. Thus the weak hash function MD5 is never contained in a valid certificate installed/imported by the trained admin. Attacks that may take advantage of hash function weakness to obtain a forged signature are not feasible in the evaluated configuration.

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

[11] Since the TOE in general also supports DSA signature generation and verification using SHA-1; authenticity may also be checked using DSA signature verification if the certificate itself is signed with DSA using SHA-1. Furthermore, if the signing key contained in the client certificate is stated to be used with DSA then DSA using SHA-1 signature generation and verification will be used by the TOE for authentication. However, this not claimed by the [ST] (please refer to FCS_COP.1) and as such not part of the TOE, and, therefore, is not listed above.

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

[13] Client uses the enc key bound to the certificate as provided by the server to encrypt the pre-master secret. Server decrypts pre-master secret as indicator for possessing the respective private key

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
6	Key derivation	HMAC with SHA-256 (default: tls_prf_sha256)	RFC2104 [14] (HMAC) FIPS180-4 [10] (SHA)	256	yes	Symmetric keys and MAC keys for record layer[14]
7	Confidentiality	AES in CBC mode (AES_128_CBC, AES_256_CBC)	FIPS197 [11] (AES) SP800-38A [23] (CBC)	|k|=128, 256	yes	Bulk data encryption / decryption (record layer)
8		Three-key TDES in CBC mode (3DES_EDE_CBC)	FIPS46-3 [12] (DES) SP 800-67 [24] (TDES/TDEA), SP 800-38A [23] (CBC),	|k|=168	yes	
9	Integrity and authenticity	HMAC with SHA-1 or SHA-256 (SHA), (SHA256)	RFC2104 [14] (HMAC) FIPS180-4 [10] (SHA)	160 (SHA-1) 256 (SHA-256)	yes	Message authentication code (record layer)
10	Trusted Channel	FTP_ITC.1, ST [6] , sec. 6.1.8.1 for TLS	Cf. all lines above	See above	yes no	Depending on the sec. level of the used mechanisms above
SSHv2						
1	Authentication	RSA signature generation & verification RSASSAPKCS1-v1_5 using SHA-1 (ssh-rsa)	RFC3447 [18] (PKCS#1 v2.1) FIPS-180-4 [10] (SHA-1) RFC4253 [21] (SSH-TRANS) for host authentication RFC4252 [20], sec 7 (SSH-USERAUTH) for user authentication method: “publickey”	Modulus length: 1024, 2048 and 4096	no	Pubkeys are exchanged trustworthily out of band, e.g. checking fingerprints. Authenticity is not part of the TOE. (no certificates are used)
2		DSA signature generation & verification using SHA-1 (ssh-dss)	FIPS186-4 [27] (DSA) FIPS-180-4 [10] (SHA-1) RFC4253 [21] (SSH-TRANS) for host authentication RFC4252 [20], sec 7 (SSH-USERAUTH) for user authentication method: “publickey”	plength= 1024 qlength= 160	no	
3		UserID & password	RFC4252 [20], sec. 5	Guess	yes	ST [6]

[14] pre-master secret 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

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
			(SSH-USERAUTH) method; “password”	success prob. ε ≤ 3 10^-4		FIA_SOS.1 & FIA_AFL.1: SSH (CLI): Blocking after x attempts (1≤x≤64) – lock-out duration 120 min or explicit re-enabling by admin SFTP: Blocking after x attempts (1≤x≤64) – lock-out until explicit re-enabling by admin.
4	Key agreement	DH with DH group1-sha1	RFC4253 [21] (SSH-TRANS) supported by RFC2409 [16] (DH groups IKE) FIPS-180-4 [10] (SHA-1)	plength=1024	no	
5		DH with DH group14-sha1	RFC4253 [21] (SSH-TRANS) supported by RFC3526 [28] (DH groups IKE) FIPS-180-4 [10] (SHA-1)	plength=2048	yes	
6		DH with diffie-hellman-group-exchange-sha1	RFC4253 [21] (SSH-TRANS) supported by RFC4419 [29] (DH-Group Exchange) FIPS-180-4 [10] (SHA-1)	plength=1024	no	
				plength= 2K, 3K, 4K,	yes	
7	Confidentiality	AES in CBC mode, and CTR mode (aes128-cbc, aes192-cbc, aes256-cbc) (aes128-ctr, aes192-ctr, aes256-ctr);	FIPS197 [11] (AES), SP 800-38A [23] (CBC, CTR), RFC 4253 [21] (SSH using AES with CBC mode), RFC4344 [22] (SSH using AES with CTR mode)	|k|=128, 192, 256	yes	Binary packet protocol: encryption
8		Three-key TDES in CBC mode	FIPS46-3 [12] (DES) SP 800-67 [24] (TDES/TDEA),	|k|=168	yes	

#	Purpose	Cryptographic Mechanisms	Standard of Implementation	Key Size [Bits]	Sec. Level ≧ 100 Bits	Comments
		(3des-cbc)	SP 800-38A [23] (CBC), RFC4253 [21] (SSH using 3DES with CBC mode)			
9	Integrity and authenticity	HMAC-SHA-1	FIPS180-4 [10] (SHA), RFC2104 [14] (HMAC), RFC4251 [19] / RFC4253 [21] (SSH general / detailed HMAC support), RFC4253 [21] (SSH detailed HMAC support)	|k|=160	yes	Binary packet protocol: message authentication
10	Trusted channel	FTP_ITC.1, ST [6] , sec. 6.1.8.1 for SFTP			yes no	Depending on the sec. Level of the used mechanisms above
11	Trusted path	FTP_TRP.1, ST [6] , sec. 6.1.8.2 for SSH			yes no	Depending on the sec. level of the used mechanisms above
XML						
1	Authenticity	RSA signature verification (RSASSA-PKCS1-v1-5) using SHA-1	RFC3447 [18] (PKCS#1 v2.1) FIPS180-4 [10] (SHA)	Modulus length: 1024, 2048, 4096	no	Verification of certificate signatures provided as part of the XML blob (e.g. as reference). Key usage of certificates signing, encryption Algorithms used depending on the signature algorithm / hash algorithm used for signing the certificates.
2		RSA signature verification (RSASSA-PKCS1-v1-5) using SHA-256	RFC3447 [18] (PKCS#1 v2.1) FIPS180-4 [10] (SHA)	Modulus length: 1024 Modulus length: 2048, 4096	no yes	
3		DSA signature verification using SHA-1	FIPS186-4 [27] (DSA) FIPS-180-4 [10] (SHA-1)	plength= 1024 qlength= 160	no	
4	Authentication	RSA signature generation and verification RSASSAPKCS1-v1_5 using SHA-1	XML Signature Syntax and Processing (Second Edition) [26] RFC3447 [18]	Modulus length: 1024, 2048, 4096	no	

XML						
		(xmldsig#rsa-sha-1) (xmldsig#sha-1)	(PKCS#1 v2.1) FIPS-180-4 [10] (SHA)			
5		RSA signature generation and verification RSASSAPKCS1-v1_5 using SHA-256, SHA-384, SHA-512 (xmldsig-more#rsa-sha256, sha384, sha512)	XML Signature Syntax and Processing (Second Edition) [26] RFC3447 [18] (PKCS#1 v2.1) FIPS-180-4 [10] (SHA)	Modulus length: 1024	no	
				Modulus length: 2048, 4096	yes	
6		DSA signature generation and verification using SHA-1 (xmldsig#dsa-sha-1)	XML Signature Syntax and Processing (Second Edition) [26] FIPS186-4 [27] (DSA) FIPS-180-4 [10] (SHA)	plength= 1024 qlength= 160	no	
7	Integrity and authenticity	HMAC-SHA-1 possibly truncated, minimum to 80 bits (xmldsig#hmac-sha-1)	XML Signature Syntax and Processing (Second Edition) [26] FIPS180-4 [10] (SHA), RFC2104 [14] (HMAC) RFC2404 [15] (HMAC using truncated SHA-1)	|k|=160 no trunc or trunc to 96, 128	yes	Message authentication code XML Signature is also supported for XML encryption. It is the recommended way to provide key based authentication
				|k|=160 trunc 80	no	
8	Key transport (public key)	RSA encryption and decryption RSAES-PKCS1-v1_5 (xmlenc#rsa-1_5)	XML Encryption Syntax and Processing [25] RFC3447 [18] (PKCS#1 v2.1)	Modulus length: 1024	no	The symmetric key gets encrypted by a pub key and transported within the XML structure
				Modulus length: 2048, 4096	yes	
9		RSA encryption and decryption RSAES-OAEP (including MGF1 with SHA1 mask generation function i.e. EME-OAEP is used with SHA1) (xmlenc#rsa-oaep-mgf1p) (xmldsig#sha1)	XML Encryption Syntax and Processing [25] RFC3447 [18] (PKCS#1 v2.1)	Modulus length: 1024	no	
				Modulus length: 2048, 4096	yes	
10	Key transport (key wrapping)	AES key wrapping (xmlenc#kw-aes128, kw-aes256, kw aes192)	XML Encryption Syntax and Processing [25] RFC3394 [30]	|k|=128, 192, 256	yes	The symmetric key gets wrapped with a shared secret (KEK) &

XML						
11		CMS TDES key wrap[15] (xmlenc#kw-tripledes)	XML Encryption Syntax and Processing [25] RFC3217 [17]	|k|=168	yes	transported within the XML structure
12	Confidentiality	AES in CBC mode (xmlenc# (aes128-cbc, aes192-cbc, aes256-cbc))	XML Encryption Syntax and Processing [25] FIPS197 [11] (AES), SP 800-38A [23] (CBC)	|k|=128, 192, 256	yes	Block encryption
13		TDES in CBC mode (xmlenc#tripledes-cbc)	XML Encryption Syntax and Processing [25] SP 800-67 [24] (TDES/TDEA), SP 800-38A [23] (CBC),	|k|=168	yes	
14	Key generation	AES key generation based on RNG as defined in FCS_RNG.1 |k|=128, 192, 256 TDES key generation 3x56 =|k|=168		n/a	n/a	Symmetric key for block encryption, FCS_CKM.1

Table 3: 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 hints therein have to be considered. In addition all aspects of Assumptions, Threats and OSPs as outlined in the Security Target not covered by the TOE itself need to be fulfilled by the operational environment of the TOE.

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

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

[15]CMS TDES key wrap specifies the TripleDES key wrap algorithm for wrapping TripleDES content encryption keys with TripleDES key encryption keys when using the CMS KeyAgreeRecipientInfo or KEKRecipientInfo choice for providing recipient specific information when encrypting data using the CMS EnvelopedData type.

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

AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
ASN	Abstract Syntax Notation
B2B	Business to Business
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
CBC	Cipher Block Chaining
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
cPP	Collaborative Protection Profile
CRL	Certificate Revocation List
DMZ	Demilitarized Zone
DRNG	Deterministic Random Number Generator
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ESB	Enterprise Service Bus
ETR	Evaluation Technical Report
GUI	Graphical User Interface
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
JSON	JavaScript Object Notation
LAN	Local Area Network
PP	Protection Profile
RNG	Random Number Generator
RSA	Ron Rivest, Adi Shamir, and Leonard Adleman
SAR	Security Assurance Requirement
SFP	Security Function Policy

SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
USB	Intelligent Platform Management Interface (IPMI
USB	Universal Serial Bus
XML	Extensible Markup Language

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

[2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 4, September 2012

[3] BSI certification: Technical information on the IT security certification of products, protection profiles and sites (BSI 7138) and Requirements regarding the Evaluation Facility for the Evaluation of Products, Protection Profiles and Sites under the CC and ITSEC (BSI 7125)

[4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE[16].

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

[6] Security Target BSI-DSZ-CC-0901-2015, Version 1.42, Date 13.03.2015, IBM WebSphere DataPower Firmware, Version 6.0.2.0 Security Target, IBM Corporation

[7] Evaluation Technical Report BSI-DSZ-CC-0901 for IBM WebSphere DataPower Firmware, Version 6.0.2.0, Version 7, Date 26.11.2015, atsec information security GmbH, (confidential document)

[8] WebSphere DataPower Version 6.0.2 Secure Deployment Guide, Revision 2, Date 08.10.2015, IBM Corporation

[9] Standalone Infocenter for the TOE Version 6.0.2, Date 27.03.2015, File name agd/dp602kc-2015-03-27.zip, IBM Corporation

[10] SECURE HASH STANDARD (SHS), Version FIPS 180-4, Date March 2012

[11] FIPS PUB 197: Advanced Encryption Standard (AES), Author(s) National Institute of Standards and Technology, Date 2001-11-26

[12] FIPS PUB 46-3: Data Encryption Standard (DES), Author(s) National Institute of Standards and Technology, Date 1999-10-25

[13] RFC 4253, The Secure Shell (SSH) Transport Layer Protocol, Author(s) T. Ylonen, C. Lonvick, Date 2006-01-01

[14] RFC2104, HMAC: Keyed-Hashing for Message Authentication, Author(s) H. Krawczyk, M. Bellare, R. Canetti, Date 1997-02-01

[15] RFC2404, The Use of HMAC-SHA-1-96 within ESP and AH, Author(s) C. Madson, R. Glenn, Date 1998-11-01

[16] RFC2409, The Internet Key Exchange (IKE), Author(s) D. Harkins, D. Carrel, Date 1998-11-01

---

[16] specifically

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

[17] RFC3217, Triple-DES and RC2 Key Wrapping, Author(s) R. Housley, Date 2001-12-01

[18] RFC3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, Author(s) J. Jonsson, B. Kaliski, Date 2003-02-01

[19] RFC4251, The Secure Shell (SSH) Protocol Architecture, Author(s) T. Ylonen, C. Lonvick, Date 2006-01-01

[20] RFC4252, The Secure Shell (SSH) Authentication Protocol, Author(s) T. Ylonen, C. Lonvick, Date 2006-01-01

[21] RFC4253, The Secure Shell (SSH) Transport Layer Protocol, Author(s) T. Ylonen, C. Lonvick, Date 2006-01-01

[22] RFC4344, The Secure Shell (SSH) Transport Layer Encryption Modes, Author(s) M. Bellare, T. Kohno, C. Namprempre, Date 2006-01-01

[23] SP 800-38A, Recommendation for Block Cipher Modes of Operation: Methods and Techniques, Version NIST Special Publication 800-38A 2001 Edition, Date December 2001

[24] SP 800-67, Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Version Revision 1, Date January 2012

[25] XML Encryption Syntax and Processing, Date December 10, 2002

[26] XML Signature Syntax and Processing (Second Edition), Date 10 June 2008

[27] DIGITAL SIGNATURE STANDARD (DSS), Version FIPS PUB 186-4, Date July 2013

[28] RFC3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), Author(s) T. Kivinen, M. Kojo, Date 2003-05-01

[29] RFC4419, Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol, Author(s) M. Friedl, N. Provos, W. Simpson, Date 2006-03-01

[30] RFC3394, Advanced Encryption Standard (AES) Key Wrap Algorithm, Author(s) J. Schaad, R. Housley, Date 2002-09-01

This page is intentionally left blank.

C. Excerpts from the Criteria

CC Part 1:

Conformance Claim (chapter 10.4)

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

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

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

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

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

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

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

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

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

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

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

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

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

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

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

The following table shows the assurance class decomposition.

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

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

Assurance class decomposition

Evaluation assurance levels (chapter 8)

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

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

Evaluation assurance level (EAL) overview (chapter 8.1)

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

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

These EALs consist of an appropriate combination of assurance components as described in Chapter 7 of this CC Part 3. More precisely, each EAL includes no more than one

component of each assurance family and all assurance dependencies of every component are addressed.

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

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

“Objectives

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

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

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

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

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

“Objectives

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

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

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

“Objectives

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

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

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

"Objectives

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

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

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

"Objectives

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

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

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

"Objectives

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

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

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

"Objectives

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

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

Table 1: Evaluation assurance level summary”

Class AVA: Vulnerability assessment (chapter 16)

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

Vulnerability analysis (AVA_VAN) (chapter 16.1)

“Objectives

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

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

D. Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.