Federal Office
for Information Security

Certification Report

BSI-DSZ-CC-0902-2017

for

Dell™ EqualLogic® PS Series Storage Array Firmware Version 7.1.1 with a Broadcom® XLP® 416, XLR® 716, XLS® 608 or XLS® 616 Processor

from

Dell 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-0902-2017 (*)

Storage Area Network

Dell™ EqualLogic® PS Series Storage Array Firmware Version 7.1.1 with a Broadcom® XLP® 416, XLR® 716, XLS® 608 or XLS® 616 Processor

from	Dell Inc.
PP Conformance:	None
Functionality:	Product specific Security Target Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 2 augmented by ALC_FLR.1

SOGIS
Recognition Agreement

Common Criteria

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations 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, 7 February 2017

For the Federal Office for Information Security

Joachim Weber
Head of Devision

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 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 this certificate is a re-certification of a certificate issued according to CCRA-2000 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 Dell™ EqualLogic® PS Series Storage Array Firmware Version 7.1.1 with a Broadcom® XLP® 416, XLR® 716, XLS® 608 or XLS® 616 Processor has undergone the certification procedure at BSI. This is a re-certification based on BSI-DSZ-CC-0688-2013. Specific results from the evaluation process BSI-DSZ-CC-0688-2013 were re-used.

The evaluation of the product Dell™ EqualLogic® PS Series Storage Array Firmware Version 7.1.1 with a Broadcom® XLP® 416, XLR® 716, XLS® 608 or XLS® 616 Processor was conducted by atsec information security GmbH. The evaluation was completed on 25 January 2017. 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: Dell Inc.

The product was developed by: Dell 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 7 February 2017 is valid until 6 February 2022. Validity can be re-newed by re-certification.

[6] Information Technology Security Evaluation Facility

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 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 Dell™ EqualLogic® PS Series Storage Array Firmware Version 7.1.1 with a Broadcom® XLP® 416, XLR® 716, XLS® 608 or XLS® 616 Processor 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] Dell Inc.

300 Innovative Way
Nashua, NH 03062
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 Dell™ EqualLogic® PS Series Storage Array Firmware Version 7.1.1 with a Broadcom® XLP® 416, XLR® 716, XLS® 608 or XLS® 616 Processor.

The Dell EqualLogic PS Series Storage Array is a high performance, enterprise-level Storage Area Network (SAN) device. Each device, called an array, contains multiple, hot swappable drives for storing large quantities of data plus one to two controller cards. Multiple arrays can be connected together to function as a single array. One or more logical volumes can be created within a single array or that span across multiple arrays. Client computers connect to the volumes using the iSCSI protocol. A volume can be assigned to one or more iSCSI Clients (through the use of volume access control lists) and used by these clients as filesystems.

Each array supports multiple iSCSI connections for communicating with iSCSI Clients. The arrays support administrative interfaces on the same network as the iSCSI Clients. They also support separate connections for administrative consoles (physically separated from the iSCSI network). Multiple arrays can be logically linked together into a Group. Grouping allows volumes to be spread across multiple arrays and provides performance advantages as well.

Each array also supports IPsec to secure any network communication to the TOE. Administrative access can be secured via SSH.

The TOE is the firmware, the hardware processor that resides on the controller card within the device (a.k.a. array), and the supporting guidance documentation.

The Operational Environment for the TOE consists of the hardware models listed in the following table:

Model	Model suffixes	Broadcom processor (TOE)	SED support
PS4100	E, X, XV	XLS608 step B1	
PS4210	E, X, XV, XS	XLP416 step B2	
PS6000	E, X, XV, S	XLR716 step C4	
PS6010	E, X, XV, S	XLR716 step C4	
PS6100	E, X, XV, S, ES, XS, XVS	XLS616 step B1	X
PS6110	E, X, XV, S, ES, XS, XVS	XLR716 step C4	
PS6210	E, X, XV, S, XS	XLP416 step B2	X
PS6500	E, X	XLR716 step C4	
PS6510	E, X	XLR716 step C4	X
PS-M4110	E, X, XV, XS	XLS616 step B1	X

Table 1: Hardware models with processors

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

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

The TOE Security Functional Requirements (SFR) relevant for the TOE are outlined in the Security Target [6], chapter 6.1. They are selected from Common Criteria Part 2 and one of them is newly defined. Thus the TOE is CC Part 2 extended.

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

TOE Security Functions	Addressed issue
Auditing	Based on the Audit Policy the TOE monitor access of users and administrators the system. Administrators can review the audit logs.
Identification & Authentication	The TOE supports I&A of all client users (including administrators). Users are required to authenticate when connecting via the iSCSI protocol, the network administrative interfaces (i.e., GUI, SAN HQ, SSH/SCP), and the serial connection. No actions can be performed by a user until after the user has been successfully identified and authenticated. Access banners can be used to remind administrators about the responsibilities involved when using the TOE management interfaces.
User Data Protection	The TOE implements both access control lists (ACLs) and Access Policies to protect access to user data. The TOE also ensures that residual data from earlier storage allocations are not available upon reallocation. In addition does the TOE support the use of Self-Encrypting Drives to support the data protection at rest.
Security Management	The TOE implements a role-based management functionality to manage users and the TSF.
Reliable Time Stamps	The TOE uses an internal time source in the environment to provide reliable time stamps for audit records.
Trusted Channel	The TOE provides SSH-based access for securely accessing the TOE command-line management interface via the network. The TOE further implements IPsec which can be used to secure all TOE communication over the network.
Default Access Banners	The TOE displays an access banner to all users accessing the administrative interfaces to indicate that the system is trusted and no unauthorized personnel may use it.

Table 2: TOE Security Functions

For more details please refer to the Security Target [6], chapter 7.1.

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], chapters 3.1 – 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:

Dell™ EqualLogic® PS Series Storage Array Firmware Version 7.1.1 with a Broadcom® XLP® 416, XLR® 716, XLS® 608 or XLS® 616 Processor

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Dell EqualLogic PS Series Storage Array Firmware V7-1-1-R400572.zip That archive contains the 32-bit and 64-bit version: • kit_64_V7.1.1-R400572_548262610.tgz • kit_V7.1.1-R400572_351401522.tgz sha256(V7-1-1-R400572.zip): a6833f99a088f3e73f3db9eb021e45f81401b32c320513618a17a11c49b76f8d	7.1.1	Download
2	HW	Broadcom Processor XLP416	XLP416 step B2	Physical Delivery as part of the appliance
3	HW	Broadcom Processor XLR716	XLR716 step C4	Physical Delivery as part of the appliance
4	HW	Broadcom Processor XLS608	XLS608 step B1	Physical Delivery as part of the appliance
5	HW	Broadcom Processor XLS616	XLS616 step B1	Physical Delivery as part of the appliance
6	Doc	Updating Firmware for Dell EqualLogic PS Series Storage Arrays and FS Series Appliances sha256(110-6196-EN-R2_Updating_Firmware.pdf): ba4da120efaeebf5e88104d2589e1d050c09a9461f28df18cbbc25c28b678678	110-6196-EN-R2	Download
7	Doc	EqualLogic Master Glossary Version 7.0 sha256(110-6177-EN-R1_Master_Gloss_web.pdf): b90614d38abf9af02387feb927a4d38ef333eeb29314e9ae5a96f8e4115d5b23	110-6177-EN-R1	Download

No	Type	Identifier	Release	Form of Delivery
8	Doc	Dell EqualLogic PS Series Storage Arrays iSCSI Initiator and Operating System Considerations sha256(110-6176-EN_R4_Optimizing_SAN_Environment.pdf): f90afe9b7619bce43dbf045e637d76696a52eba56c47598bacb4d6d2665bc9ba	110-6176-EN-R4	Download
9	Doc	Dell EqualLogic PS Series Storage Arrays Release Notes and Fix List PS Series Firmware 7.1.1 sha256(110-6171-EN_R14_RelNotes_V7.1.1.pdf): bf1a410d4271a65e5b9ae0171dc94509db4c9f79b59366cbe5079e7f4b989be7	110-6171-EN-R14	Download
10	Doc	Dell EqualLogic Group Manager Administrator's Manual PS Series Firmware 7.0, FS Series Firmware 3.0 sha256(110-6152-EN-R1_Admin_web.pdf): 073a987d3af25b82db422145f0b81683b186d349693cf7dd6dc8770abdac2820	110-6152-EN-R1	Download
11	Doc	Dell EqualLogic Group Manager Online Help PS Series Firmware Version 7.0 FS Series Firmware Version 3.0 sha256(OLH-g11n-kit.zip): 731dd58de06091a8a3468f62c87d3b5789f1eabba4660789dacd273fbcdad303	7.0/3.0	Download
12	Doc	Dell EqualLogic Group Manager CLI Reference Guide PS Series Firmware 7.0, FS Series Firmware 3.0 sha256(110-6157-EN-R1_CLI_web.pdf): 789e1d75fa007bdf055b72c961d78d396fdbf60d0b5e3da59f707f79d15a7ba5	110-6157-EN-R1	Download
13	Doc	PS Series Storage Arrays Common Criteria Configuration Guide 7.1.1 sha256(110-6188-EN-R3_CommonCriteria.pdf): a2de1585b9cf7aaf9d78f4352bc1c3bab1eab85564f60b2105e96bf7a4822537	110-6188-EN-R3	Download
14	Doc	Dell EqualLogic Events Guide PS Series Firmware 7.0, FS Series Firmware 3.0 sha256(110-6158-EN-R1_Events_web.pdf): 14bcc4178910ca98be4f10cca6dc8f35fa50d36e2ad1af1d7c81edecf8f9c8ad	110-6158-EN-R1	Download

Table 3: Deliverables of the TOE

The TOE firmware is to be downloaded from the Dell/Equalogic website on https://eqlsupport.dell.com/support/. The download is secured by the HTTPS protocol. In

order to access this site a user id and password are needed. The credentials can be obtained from Dell customer support by customers that have an active service plan with Dell.

The Broadcom processor is delivered together with the appliance using standard commercial shipping protection: cardboard boxes and sealing tape.

If the TOE is shipped in a "complete" fashion (i.e. the hardware parts and the software parts), the Common Criteria Configuration Guide [16] (section “Evaluated Versions”) contains instructions on how to verify that the installed software version and the Broadcom chips comprise in fact the TOE.

The TOE firmware version can be queried in the running system in the "Controllers" tab on the member display of the administrative UI. It shows information similar to the following:

Firmware: Storage Array Firmware V7.1.1 (R400572)

The same information can be queried in the CLI environment via the show subcommand.

The Broadcom processor version can be queried using the CLI environment via the cmv subcommand.

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: Auditing, identification & authentication, user data protection, security management, reliable time stamps, trusted channel and default access banners.

4. Assumptions and Clarification of Scope

The Assumptions defined in the Security Target and some aspects of Threats and Organisational Security Policies are not covered by the TOE itself. These aspects lead to specific security objectives to be fulfilled by the TOE-Environment. The following topics are of relevance: trained and trusted administrators, trusted administrative client software, protected authentication servers, trusted DNS, usage of anti-virus tools and firewalls, protected network (when in non-IPsec mode), secure generation of sufficiently complex security credentials, physical protection of underlying hardware, unaccessible SNMP interface, strong iSCSI client authentication, trained users, reliable NTP servers, reliable RTC, secure usage of SSH and cryptographic certificates and SEDset handling. Details can be found in the Security Target [6], chapter 4.2.

5. Architectural Information

The operating software (i.e. the firmware) of the array consists of two major parts, a network stack and a storage stack, which are executed in parallel. Memory protection is used for separation. Dedicated memory regions are used for the stacks to communicate. The network stack implements high speed network protocols (e.g., iSCSI) as well as the lower layers of the TCP/IP protocol. The storage stack implements the high speed storage algorithms and provides the execution environment for low speed background operations that are implemented as user mode processes. These user mode processes provide the administration algorithms and system monitoring functions.

The operating software interacts with the hardware specifically the Broadcom processor to use its the cryptographic services for providing IPsec functionality.

6. Documentation

The evaluated documentation as outlined in table 3 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 Tests

The majority of the developer tests were run on a model PS6010 and PS6210, configured according to Common Criteria Configuration Guide [16] with some exceptions but which did not cause any issues for the evaluation. One general functionality test has been performed on a PS4000 model.

The developer test configuration further included the XLP416 step B2 cryptographic processor (contained in the PS6210 model) and the XLR716 step C4 processor (contained in the PS6010 model).

The developer used automatic and manual tests. Manual tests have been used to verify functions on the admin GUI interface. Because the automatic test suites contain thousands of tests, these are only executed on the base product version (e.g. V7.1). For the evaluated TOE version 7.1.1, the developer filtered these and only choses a subset of the tests that where security-relevant for the claimed TOE security functions. The automatic test framework comes with the web interface that allows the tester to easily select subsets of tests to be executed. The test framework also shows the running status and results of each test.

All security functions were tested by using only the external visible TOE interfaces. The tests mainly used the typical interfaces to the CLI (via SSH or telnet) in order to perform tests automatically. The tests themselves are feature-centric, that means that a specific functionality is tested rather than pursuing the test of specific type of interfaces. With this, a large number of functions are covered using CLI and which oftentimes involve identification and authentication functions.

All developer tests ran successfully.

7.2. Independent Evaluator Tests

The test configuration comprised of a group array configuration of two TOE instances. Both using a hardware model as underlying machine listed in the ST: PS6000 and PS4100. The PS4100 was configured using SED drives.

Testing on the PS4100 hardware-model also covered the XLS608 B1 processor.

All evaluator tests were performed on the TOE firmware version 7.1.1.

The independent functional evaluator test comprised 24 test cases including a variation of 9 developer test during test witnessing. The cryptographic tests included 16 valid and 7

invalid IPsec cipher combinations, as well as 7 valid and 6 invalid SSH cipher and protocol combinations.

The following security functions have been tested: I&A of user and administrators, cryptographic operations of IPsec and SSH, security management of audit, access control, communication channels, auditing, user data protection for SED drives and access banners.

The approach was to use normal external TOE interfaces for the tests. One exception is the SED test where the SED drive was attached to another computer, because SED functionality cannot be directly shown through external interfaces.

The tests where mainly manual tests with some scripting support.

The independent tests covered a broad range of TOE functions including tests from the previous evaluation. The focus lay on I&A and cryptographic tests. For the I&A tests different configurations with external authentication servers were tested to verify that the separation of users and administrators was not violated. For the cryptographic tests several supported ciphers and the lack of weak ciphers where tested. One test was an extension of a developer test that verified authorization of specific management commands tunneled through iSCSI.

All developer tests that were reran by the evaluator as well as the evaluator tests were executed successfully with all test actual results matching the expected results.

8. Evaluated Configuration

The TOE is the firmware, the hardware processor that resides on the controller card(s) within the device (a.k.a. array), and the supporting guidance documentation. The evaluated configuration is defined by the configuration laid out in the Common Criteria Configuration Guide [16].

The following main configuration changes compared to the factory default define the evaluated configuration:

- Strong passwords, conforming to a policy described in Common Criteria Configuration Guide [16] must be used for the accounts as well as the group and replication partners
- iSCSI target authentication must be used
- PSAPI and SNMPv3 must be turned off
- Administrative access is only allowed through SSH
- Only a specific set of cryptographic algorithms and protocols must be used. For IPsec, only the transport mode is allowed.
- Unencrypted access (FTP, telnet) must be turned off
- Certificates using the MD5 hash algorithm must not be used; certificates with SHA-1 or SHA-2 (SHA-256, SHA-384, SHA-512) hash algorithms should be used instead.
- Dell EqualLogic FS Series Network-Attached Storage (NAS) must not be used

9. Results of the Evaluation

9.1. CC specific results

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

The Evaluation Methodology CEM [2] was used.

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

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

- All components of the EAL 2 package including the class ASE as defined in the CC (see also part C of this report)
- The components ALC_FLR.1 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-0688-2013, re-use of specific evaluation tasks was possible. The focus of this re-evaluation was on the changed implemented cryptographic mechanisms and the SED support.

The evaluation has confirmed:

- PP Conformance: None
- for the Functionality: Product specific Security Target
  Common Criteria Part 2 extended
- for the Assurance: Common Criteria Part 3 conformant
  EAL 2 augmented by ALC_FLR.1

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

9.2. Results of cryptographic assessment

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

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

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
	IPsec				
1	Authenticity	RSA-signature verification RSASSA-PKCS1-v1_5 using	[RFC3447] (RSA), [FIPS180-4] (SHA)	Modulus length: 2048, 4096	no

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
		SHA-1			
2		RSA-signature verification RSASSA-PKCS1-v1_5 using SHA-256, SHA-384, SHA-512	[RFC3447] (RSA), [FIPS180-4] (SHA)	Modulus length: 2048, 4096	yes
3	IKE Authentication	RSA signature generation and verification for authentication (Auth. Method 1) IKEv1: RSAES-PKCS1-v1_5 encryption scheme with private key encryption for signing and public key decryption for signature verification.	[RFC2409] (IKEv1), [RFC3447] (RSA)	Modulus length: 2048, 4096	yes
4		RSA signature generation and verification for authentication (Auth. Method 1) IKEv2: RSASSA-PKCS1-v1_5) using SHA-1	[RFC5996] (IKEv2), [RFC3447] (RSA)	Modulus length: 2048, 4096	no
5		IKEv2: RSASSA-PKCS1-v1_5) using SH-256, SHA-384, SHA-512	[RFC5996] (IKEv2), [RFC3447] (RSA)	Modulus length: 2048, 4096	yes
6		PSK used as key PRF: HMAC-SHA1, PRF: HMAC-SHA-256, PRF: HMAC-SHA-384, PRF: HMAC-SHA-512 (Auth. Method 2)	[RFC2409] (IKEv1), [RFC5996] (IKEv2), [FIPS198-1] (HMAC), [FIPS180-4] (SHA)	Input: |Shared Key| >> 100	yes
7	Key Agreement	DH with DH group 14, 24	[RFC2409] (IKEv1), [RFC5996] (IKEv2), [DH] (DH as referenced in [RFC2409] & [RFC5996]), [RFC3526] (DH group 14), [RFC5114] (DH Group 24)	plength = 2048	yes
8		Key derivation: PRF: HMAC-SHA1 PRF: HMAC-SHA-256, PRF: HMAC-SHA-384, PRF:	[RFC2409] (IKEv1), [RFC5996] (IKEv2), [FIPS198-1] (HMAC), [FIPS180-4] (SHA),	|k| = variable	yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
		HMAC-SHA-512	[RFC4868] (HMAC -SHA2 with IPsec)		
9	IKE Confidentiality	AES in CBC mode	[RFC4109] (IKEv1), [RFC5996], [RFC4307] (IKEv2), Modeled after [RFC4303] ESP, [FIPS197] (AES), [SP800-38A] (CBC)	|k|= 128, 192, 256	yes
10		TDES in CBC mode, keying option 1 (three independent keys)	[RFC2409] (IKEv1), [RFC5996], [RFC4307] (IKEv2), Modeled after [RFC4303] ESP, [SP800-67] (TDES), [SP800-38A] (CBC)	|k|=168	yes
11	Integrity / authenticity IKE integrity	HMAC with SHA-1-96 HMAC with SHA-256-128 HMAC with SHA-384-192 HMAC with SHA-512-256	[FIPS180-4] (SHA), [FIPS198-1] (HMAC), [RFC4868] (HMAC -SHA2 with IPsec), [RFC2404] (HMAC using truncated SHA-1)	|k|=160, 256, 384, 512	yes
12	IPsec ESP encryption	IPsec ESP: AES in CBC mode	[FIPS-197] (AES), [SP 800-38A] (CBC), [RFC3602] (AESCBC with IPsec) [RFC2451] (ESP CBC)	|k|= 128,192, 256	yes
13	IPsec ESP integrity	HMAC with SHA-1- 96 HMAC with SHA- 256-128 HMAC with SHA- 384-192 HMAC with SHA- 512-256	[FIPS198-1] (HMAC), [FIPS180-4] (SHA) [RFC4868] (HMAC -SHA2 with IPsec	|k|=160, 256, 384, 512	yes
14	Trusted Channel	FTP_ITC.1-IPsec	[RFC4301] (IPsec), [RFC4303] (ESP) [RFC2409] (IKEv1), [RFC5996] (IKEv2)	See above	yes / no
	SSHv2				
15	Authentication	RSA signature generation (RSASSAPKCS1-v1_5 using SHA-1)	[RFC3447] (RSASSA-PKCS1-v1_5), [RFC4253] (SSH-2), [FIPS180-4] (SHA)	Modulus length = 2048	no
16	Key Agreement	DH with DH group14-sha1	[RFC4253] (SSH-2), DH is described in [RFC4253] refers to [RFC3526] for the	plength=2048	yes

No.	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
			DH group, [FIPS180-4] (SHA)		
17		Key derivation: PRF based on SHA-1	[RFC4253], sec. 7.2 (SSH), [FIPS180-4] (SHA)	|k| = variable	yes
18	Confidentiality	AES in CBC and CTR mode	[FIPS197] (AES), [SP800-38A] (CBC, CTR), [RFC4253] (SSH-2 using AES with CBC mode), [RFC4344] (SSH-2 using AES with CTR mode)	|k|=128, 192, 256	yes
19		TDES in CBC mode	[SP800-67] (TDES/TDEA), [SP800-38A] (CBC), [RFC4253] (SSH-2 using 3DES with CBC mode)	|k|=168	yes
20	Integrity	HMAC-SHA-1, HMAC-SHA-1-96	[FIPS180-4] (SHA), [FIPS198-1] (HMAC), [RFC4251] / [RFC4253] (SSH-2 general / detailed HMAC support), [RFC4253] (SSH-2 detailed HMAC support)	|k|=160	yes
21	Key generation	RSA key generation	[FIPS186-2], Miller Rabin primality tests.	n/a	
22	Trusted Channel	FTP_ITC.1-SSH: SSH v2.0	[RFC4253] (SSH v2.0)		yes / no
	SED				
23	Cryptographic Primitive Protection of SED Without Error Correction and Data Recovery	Robust Threshold Secret Sharing (RTSS) using SHA-1	[draft-mcgrew-tss-03]		no

Table 4: TOE cryptographic functionality

10. Obligations and Notes for the Usage of the TOE

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

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

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

11. Security Target

For the purpose of publishing, the Security Target [6] of the Target of Evaluation (TOE) is provided within a separate document as Annex A of this report.

12. Definitions

12.1. Acronyms

AIS	Application Notes and Interpretations of the Scheme
BSI	Bundesamt für Sicherheit in der Informationstechnik / Federal Office for Information Security, Bonn, Germany
BSIG	BSI-Gesetz / Act on the Federal Office for Information Security
CCRA	Common Criteria Recognition Arrangement
CC	Common Criteria for IT Security Evaluation
CEM	Common Methodology for Information Technology Security Evaluation
CLI	Command Line Interface
DNS	Domain Name Service
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
iSCSI	Internet Small Computer Systems Interface
IP	Internet Protocol
IPsec	Internet Protocol Security
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility

MD5	Message Digest 5 Algorithm
NAS	Network Attached Storage
NTP	Network Time Protocol
PP	Protection Profile
PSAPI	PS Application Programming Interface
RTC	Real Time Clock
SAN	Storage Area Network
SAR	Security Assurance Requirement
SED	Self Encrypting Drives
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
TCP	Transmission Control Protocol
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[8] https://www.bsi.bund.de/AIS

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

[6] Security Target BSI-DSZ-CC-0902-2017, Version 3.27, 2016-09-19, Dell EqualLogic PS Series Storage Array Firmware Version 7.1.1 with a Broadcom® XLP®, XLR®, or XLS® Processor Security Target, Dell Inc.

[7] Evaluation Technical Report, Version 4, 2017-01-19, atsec information security GmbH (confidential document)

[8] Configuration list for the TOE, Version 7.1.1, 2017-01-13, Configuration Collection including the Configuration List (7.1.1-cm-lists-2017-01-13.zip) (confidential document)

[9] Updating Firmware for Dell EqualLogic PS Series Storage Arrays and FS Series Appliances, 110-6196-EN-R2

[10] EqualLogic Master Glossary Version 7.0, 110-6177-EN-R1

[11] Dell EqualLogic PS Series Storage Arrays iSCSI Initiator and Operating System Considerations, 110-6176-EN-R4

[12] Dell EqualLogic PS Series Storage Arrays Release Notes and Fix List PS Series Firmware 7.1.1, 110-6171-EN-R14

[13] Dell EqualLogic Group Manager Administrator's Manual PS Series Firmware 7.0, FS Series Firmware 3.0, 110-6152-EN-R1

[14] Dell EqualLogic Group Manager Online Help PS Series Firmware Version 7.0/FS Series Firmware Version 3.0, Version 7.0/3.0

[8] specifically

- AIS 20, Version 3, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema
- AIS 38, Version 2, Reuse of evaluation results

[15] Dell EqualLogic Group Manager CLI Reference Guide PS Series Firmware 7.0, FS Series Firmware 3.0, 110-6157-EN-R1

[16] PS Series Storage Arrays Common Criteria Configuration Guide 7.1.1, 110-6188-EN_R3

[17] Dell EqualLogic Events Guide PS Series Firmware 7.0, FS Series Firmware 3.0, 110-6158-EN-R1

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.