



Certification Report

BSI-DSZ-CC-0688-2013

for

**Dell EqualLogic PS Series Storage Array Firmware
Version 5.1.1-H2**

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



Deutsches IT-Sicherheitszertifikat

erteilt vom



Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-0688-2013

Storage Area Network

Dell EqualLogic PS Series Storage Array Firmware
Version 5.1.1-H2

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



Common Criteria
Recognition
Arrangement



The IT product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1.

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

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

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

Bonn, 28 March 2013

For the Federal Office for Information Security

Bernd Kowalski
Head of Department

L.S.



This page is intentionally left blank.

Preliminary Remarks

Under the BSIG¹ 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.....	7
1 Specifications of the Certification Procedure.....	7
2 Recognition Agreements.....	7
3 Performance of Evaluation and Certification.....	8
4 Validity of the Certification Result.....	9
5 Publication.....	9
B Certification Results.....	11
1 Executive Summary.....	12
2 Identification of the TOE.....	13
3 Security Policy.....	13
4 Assumptions and Clarification of Scope.....	13
5 Architectural Information.....	13
6 Documentation.....	13
7 IT Product Testing.....	14
8 Evaluated Configuration.....	14
9 Results of the Evaluation.....	14
10 Obligations and Notes for the Usage of the TOE.....	17
11 Security Target.....	17
12 Definitions.....	18
13 Bibliography.....	20
C Excerpts from the Criteria.....	23
CC Part1:.....	23
CC Part 3:.....	24
D Annexes.....	33

A Certification

1 Specifications of the Certification Procedure

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

- BSIG²
- BSI Certification Ordinance³
- BSI Schedule of Costs⁴
- Special decrees issued by the Bundesministerium des Innern (Federal Ministry of the Interior)
- DIN EN 45011 standard
- BSI certification: Procedural Description (BSI 7125) [3]
- Common Criteria for IT Security Evaluation (CC), Version 3.1⁵ [1]
- Common Methodology for IT Security Evaluation, Version 3.1 [2]
- BSI certification: Application Notes and Interpretation of the Scheme (AIS) [4]

2 Recognition Agreements

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

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

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

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

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

³ Ordinance on the Procedure for Issuance of a Certificate by the Federal Office for Information Security (BSI-Zertifizierungsverordnung, BSIZertV) of 07 July 1992, Bundesgesetzblatt I p. 1230

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

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

As of September 2011 the new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. Details on recognition and the history of the agreement can be found at <https://www.bsi.bund.de/zertifizierung>.

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

2.2 International Recognition of CC – Certificates (CCRA)

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

As of September 2011 the arrangement has been signed by the national bodies of: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Republic of Korea, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Singapore, Spain, Sweden, Turkey, United Kingdom, United States of America. The current list of signatory nations and approved certification schemes can be seen on the website: <http://www.commoncriteriaportal.org>.

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

3 Performance of Evaluation and Certification

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

The product Dell EqualLogic PS Series Storage Array Firmware, Version 5.1.1-H2 has undergone the certification procedure at BSI.

The evaluation of the product Dell EqualLogic PS Series Storage Array Firmware, Version 5.1.1-H2 was conducted by atsec information security GmbH. The evaluation was completed on 25 March 2013. The 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.

⁶ Information Technology Security Evaluation Facility

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 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 5.1.1-H2 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 developer⁷ of the product. The Certification Report may also be obtained in electronic form at the internet address stated above.

⁷ Dell Inc.
One Dell Way
Round Rock, Texas 78682
United States

This page is intentionally left blank.

B Certification Results

The following results represent a summary of

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

1 Executive Summary

The Target of Evaluation (TOE) is the Dell EqualLogic PS Series Storage Array Firmware, Version 5.1.1-H2.

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 Internet Small Computer System Interface (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.

The TOE is the firmware that resides on the controller card(s) and the supporting guidance documentation.

The Operational Environment for the TOE consists of the following hardware models: PS4000 - E, X, XV; PS4100 - E, X, XV; PS6000 - E, X, XV, S; PS6010 - E, X, XV, S; PS6100 - E, X, XV, S, ES, XS, XVS; PS6500 - E, X; PS6510 – E, X.

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 SFRs are implemented by the following TOE security functions:

TOE security functions	Addressed issue
Auditing	Audit data generation, user identity association, audit review
Identification and authentication	I&A for iSCSI clients and administrators, I&A of arrays when joining a group
User data protection	Access control for iSCSI clients on the basis of access control lists (ACLs), residual information protection
Security management	Support of different administrator roles with different privileges
Reliable time stamps	Usage of internal time source to provide reliable time stamps
Trusted channel	Establishment of trusted channel for administrative communication

Table 1: TOE security functions

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

The assets to be protected by the TOE are defined in the Security Target [6], chapter 3.1. Based on these assets the TOE security problem is defined in terms of assumptions, threats and organisational security policies. This is outlined in the Security Target [6], chapter 3.1 to 3.3.

The evaluated configuration covered by this certification is defined by the configuration laid out in the EqualLogic PS Series Storage Arrays Common Criteria Configuration Guide [11] (for more details see chapter 8 of this report).

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 5.1.1-H2

The following table outlines the TOE deliverables:

No	Type	Identifier	Release	Form of Delivery
1	SW	Dell EqualLogic PS Series Storage Array Firmware	5.1.1-H2	Download
2	DOC	EqualLogic PS Series Group Administration, PS Series Firmware Version 5.1 [9]	110-6056-EN-R1	Download
3	DOC	EqualLogic PS Series Firmware Command Line Reference Version 5.1 [10]	110-6057-EN-R1	Download
4	DOC	EqualLogic PS Series Storage Arrays Common Criteria Configuration Guide [11]	110-6074-EN Rev. 2	Download
5	DOC	EqualLogic Updating PS Series Storage Array Firmware, Firmware Version 5.1 [12]	110-0025-EN Rev.18	Download
6	DOC	EqualLogic PS Series Storage Arrays Release Notes, PS Series Firmware Version 5.1 [13]	110-6055-EN Rev. 4	Download
7	DOC	EqualLogic Master Glossary, PS Series Firmware Version 5.1 [14]	110-6026-EN-R2	Download

Table 2: Deliverables of the TOE

The TOE is to be downloaded from the Dell/Equallogic website on <https://support.equallogic.com/support/>. The download is secured by the HTTPS protocol.

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

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

Firmware: Storage Array Firmware V5.1.1 (R189834 H2)

The same information can be queried in the CLI environment via the show subcommand (for example member show) which would report:

Version: V5.1.1 (R189834 H2)

3 Security Policy

The security policy is expressed by the set of security functional requirements and implemented by the TOE. It covers the following issues:

The TOE uses the Challenge Handshake Authentication Protocol (CHAP) to authenticate iSCSI users. All iSCSI communication is performed in the clear over the network (i.e., the iSCSI communication, including authentication via CHAP, is not protected from disclosure or modification). Therefore this network traffic is assumed to be protected by the TOE environment.

The TOE controls access to the volumes through the use of access control lists (ACLs). Each volume has its own ACL.

For network-based administrative connections, the TOE provides both a graphical user interface (GUI) over TLS and a command line interface (CLI) via Secure Shell (SSH). Both the GUI and CLI protect the communication from disclosure and modification.

The TOE supports local and remote authentication databases. A local authentication database is stored on the local storage drives of the array by the TOE. RADIUS is a remote authentication database server and is part of the operational environment of the TOE.

Multiple arrays can be logically linked together (grouped) to act as a single array. This is called a group. Grouping allows volumes to be spread across multiple arrays.

Within a group, one array acts as the initial contact point, called the group leader, for the entire group. Each group member must successfully authenticate to the group leader using the correct group name and group membership password in order to join the group. The TOE performs the group member identification and authentication.

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: protection of network traffic (except administrative communication), physical protection of underlying hardware, trained and trusted administrators as well as trained users. Details can be found in the Security Target [6], chapter 3.2.

5 Architectural Information

The operating software 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 in addition 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.

6 Documentation

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

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

7 IT Product Testing

7.1 Test Configuration

The developer tests were run on a model PS6100, configured according to the Common Criteria Configuration Guide [11].

The evaluator tests were run on a model PS6000, configured according to the Common Criteria Configuration Guide [11].

Both developer tests and evaluator test were run on the TOE, in the evaluated configuration on a supported hardware platform.

7.2 Developer Tests

The developer used automatic and manual tests. Because the automatic test suites contain thousands of tests, these are only executed on the base product version (i.e. V5.0). For exact the evaluated TOE version, the developer filtered these and only chooses 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.

Manual tests have been used to verify functions on the administrator GUI. All tests (manual and automatic) are independent from each other as they define the necessary test setup solely from this test case.

All security functions were tested by using only the external visible TOE interfaces. The test focused on the identification and authentication functionality.

All results of the developer tests were as expected.

7.3 Independent Evaluator Tests

The evaluator remotely witnessed a small subset of developer tests via a web meeting. Furthermore the evaluator performed a small subset of 3 developer tests and 17 evaluator tests within the premises of the ITSEF.

The evaluator performed tests in all areas of the TSF (audit, I&A, access control, management), also exercising different variants of I&A with respect to local and RADIUS authentication. A subset of these test activities were dedicated to verify that the various settings (disabling of services) necessary for the evaluated configuration are actually enforced by the TOE. All type of TSFIs were tested.

All independent tests results were as expected.

7.4 Evaluator Penetration Testing

The evaluator focused on the authentication functions accessible via the SSH, GUI interfaces, and iSCSI.

The tests consisted of 8 manual test and one tool-driven test and considered the following topics: RADIUS interaction, concurrent sessions, available network services, SNMP restriction enforcement, client-side permission checks, system commands and password guessing attacks.

The penetration tests showed that the TOE in its evaluated configuration is not vulnerable to attacks with basic attack potential.

8 Evaluated Configuration

The evaluated configuration covered by this certification is defined by the configuration laid out in the EqualLogic PS Series Storage Arrays Common Criteria Configuration Guide [11].

The following main configuration changes define the evaluated configuration:

- Strong passwords, conforming to a policy described in [11] must be used for the accounts as well as the group and replication partners.
- iSCSI target authentication must be used.
- PS series API and SNMPv3 must be turned off.
- The volume creation process ensures that residual data is deleted.
- Administrative access is only allowed through encrypted channels (TLS/SSH).
- Non encrypted access (FTP, Telnet) must be turned off.
- Only a specific set of cryptographic algorithms and protocols must be enabled.

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 component ALC_FLR.1 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 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 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).

This holds for the cryptographic algorithms listed in the following table and used for the establishment of a trusted channel.

Algorithm	Key length	Intended purpose	Implementation standard
RSA	1024	Generation and verification of digital signatures	PKCS#1 v1.5
DSA	L=1024, N=160	Generation and verification of digital signatures	FIPS 186-3
DH	1024, 2048	Key agreement	RFC4253, RFC4419
TDES in CBC mode	168	TLSv1	FIPS PUB 46-3, SP800-38A
AES in CBC and CTR mode	128, 192, 256	SSH, TLSv1	FIPS PUB 197, SP800-38A
HMAC-SHA-1	160	SSH, TLSv1	FIPS 180-4,
HMAC-SHA-1-96	96		RFC2140

Table 3: Cryptographic algorithms implemented by the TOE

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, the customer should define the period of time until a re-assessment for the TOE is required and thus requested from the sponsor of the certificate.

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

ACL	Access Control List
AES	Advanced Encryption Standard
AIS	Application Notes and Interpretations of the Scheme
API	Application Programming Interface
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
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface
CTR	Counter
DH	Diffie-Hellman
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standard
FIPS PUB	Federal Information Processing Standard Publications
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
iSCSI	Internet Small Computer System Interface
IT	Information Technology
ITSEF	Information Technology Security Evaluation Facility
PKCS	public-key cryptography standard
PP	Protection Profile
RADIUS	Remote Authentication Dial-In User Service
RFC	Request for Comments
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman

SAN	Storage Area Network
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SNMP	Simple Network Management Protocol
SSH	Secure Shell
ST	Security Target
TCP	Transport Control Protocol
TDES	Triple Data Encryption Standard
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality

12.2 Glossary

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

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

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

Informal - Expressed in natural language.

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

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

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

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

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

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

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

13 Bibliography

- [1] Common Criteria for Information Technology Security Evaluation, Version 3.1, Part 1: Introduction and general model, Revision 3, July 2009
Part 2: Security functional components, Revision 3, July 2009
Part 3: Security assurance components, Revision 3, July 2009
- [2] Common Methodology for Information Technology Security Evaluation (CEM), Evaluation Methodology, Version 3.1, Rev. 3, July 2009
- [3] BSI certification: Procedural Description (BSI 7125)
- [4] Application Notes and Interpretations of the Scheme (AIS) as relevant for the TOE⁸.
- [5] German IT Security Certificates (BSI 7148), periodically updated list published also in the BSI Website
- [6] Security Target BSI-DSZ-CC-0688-2013, Version 2.5, 21 January 2013, Dell EqualLogic PS Series Storage Array Firmware Version 5.1.1-H2 Security Target, Dell Inc.
- [7] Evaluation Technical Report, Version 3, 26 February 2013, atsec information security GmbH (confidential document)
- [8] Configuration list for the TOE, Version 1, 5.1.1-H2-cm-lists-v1.sh (confidential document)
- [9] EqualLogic PS Series Group Administration, PS Series Firmware Version 5.1, 110-6056-EN-R1, Dell Inc.
- [10] EqualLogic PS Series Firmware Command Line Reference Version 5.1, 110-6057-EN-R1, Dell Inc.
- [11] EqualLogic PS Series Storage Arrays Common Criteria Configuration Guide, 110-6074-EN Rev. 2, Dell Inc.
- [12] EqualLogic Updating PS Series Storage Array Firmware, Firmware Version 5.1, 110-0025-EN Rev.18, Dell Inc.
- [13] EqualLogic PS Series Storage Arrays Release Notes, PS Series Firmware Version 5.1, 110-6055-EN Rev. 4, Dell Inc.
- [14] EqualLogic Master Glossary, PS Series Firmware Version 5.1, 110-6026-EN-R2, Dell Inc.

⁸specifically

- AIS 20, Version 2, Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren
- AIS 32, Version 7, CC-Interpretationen im deutschen Zertifizierungsschema

This page is intentionally left blank.

C Excerpts from the Criteria

CC Part1:

Conformance Claim (chapter 10.4)

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

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

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

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

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

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

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

CC Part 3:

Class APE: Protection Profile evaluation (chapter 10)

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

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

APE: Protection Profile evaluation class decomposition”

Class ASE: Security Target evaluation (chapter 11)

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

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

ASE: Security Target evaluation class decomposition

Security assurance components (chapter 7)

“The following Sections describe the constructs used in representing the assurance classes, families, and components.”

“Each assurance class contains at least one assurance family.”

“Each assurance family contains one or more assurance components.”

The following table shows the assurance class decomposition.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.1 Basic functional specification ADV_FSP.2 Security-enforcing functional specification ADV_FSP.3 Functional specification with complete summary ADV_FSP.4 Complete functional specification ADV_FSP.5 Complete semi-formal functional specification with additional error information ADV_FSP.6 Complete semi-formal functional specification with additional formal specification
	ADV_IMP.1 Implementation representation of the TSF ADV_IMP.2 Implementation of the TSF
	ADV_INT.1 Well-structured subset of TSF internals ADV_INT.2 Well-structured internals ADV_INT.3 Minimally complex internals
	ADV_SPM.1 Formal TOE security policy model
	ADV_TDS.1 Basic design ADV_TDS.2 Architectural design ADV_TDS.3 Basic modular design ADV_TDS.4 Semiformal modular design ADV_TDS.5 Complete semiformal modular design ADV_TDS.6 Complete semiformal modular design with formal high-level design presentation

Assurance Class	Assurance Components	
AGD:	AGD_OPE.1 Operational user guidance	
Guidance documents	AGD_PRE.1 Preparative procedures	
ALC: Life cycle support	ALC_CMC.1 Labelling of the TOE ALC_CMC.2 Use of a CM system ALC_CMC.3 Authorisation controls ALC_CMC.4 Production support, acceptance procedures and automation ALC_CMC.5 Advanced support	
	ALC_CMS.1 TOE CM coverage ALC_CMS.2 Parts of the TOE CM coverage ALC_CMS.3 Implementation representation CM coverage ALC_CMS.4 Problem tracking CM coverage ALC_CMS.5 Development tools CM coverage	
	ALC_DEL.1 Delivery procedures	
	ALC_DVS.1 Identification of security measures ALC_DVS.2 Sufficiency of security measures	
	ALC_FLR.1 Basic flaw remediation ALC_FLR.2 Flaw reporting procedures ALC_FLR.3 Systematic flaw remediation	
	ALC_LCD.1 Developer defined life-cycle model ALC_LCD.2 Measurable life-cycle model	
	ALC_TAT.1 Well-defined development tools ALC_TAT.2 Compliance with implementation standards ALC_TAT.3 Compliance with implementation standards - all parts	
	ATE: Tests	ATE_COV.1 Evidence of coverage ATE_COV.2 Analysis of coverage ATE_COV.3 Rigorous analysis of coverage
		ATE_DPT.1 Testing: basic design ATE_DPT.2 Testing: security enforcing modules ATE_DPT.3 Testing: modular design ATE_DPT.4 Testing: implementation representation
		ATE_FUN.1 Functional testing ATE_FUN.2 Ordered functional testing
ATE_IND.1 Independent testing – conformance ATE_IND.2 Independent testing – sample ATE_IND.3 Independent testing – complete		
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey AVA_VAN.2 Vulnerability analysis AVA_VAN.3 Focused vulnerability analysis AVA_VAN.4 Methodical vulnerability analysis AVA_VAN.5 Advanced methodical vulnerability analysis	

Assurance class decomposition

Evaluation assurance levels (chapter 8)

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

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

Evaluation assurance level (EAL) overview (chapter 8.1)

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

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

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

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

Assurance Class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		1	1	1	1	1	1
	ADV_FSP	1	2	3	4	5	5	6
	ADV_IMP				1	1	2	2
	ADV_INT					2	3	3
	ADV_SPM						1	1
	ADV_TDS		1	2	3	4	5	6
Guidance Documents	AGD_OPE	1	1	1	1	1	1	1
	AGD_PRE	1	1	1	1	1	1	1
Life cycle Support	ALC_CMC	1	2	3	4	4	5	5
	ALC_CMS	1	2	3	4	5	5	5
	ALC_DEL		1	1	1	1	1	1
	ALC_DVS			1	1	1	2	2
	ALC_FLR							
	ALC_LCD			1	1	1	1	2
	ALC_TAT				1	2	3	3
Security Target Evaluation	ASE_CCL	1	1	1	1	1	1	1
	ASE_ECD	1	1	1	1	1	1	1
	ASE_INT	1	1	1	1	1	1	1
	ASE_OBJ	1	2	2	2	2	2	2
	ASR_REQ	1	2	2	2	2	2	2
	ASE_SPD		1	1	1	1	1	1
	ASE_TSS	1	1	1	1	1	1	1
Tests	ATE_COV		1	2	2	2	3	3
	ATE_DPT			1	1	3	3	4
	ATE_FUN		1	1	1	1	2	2
	ATE_IND	1	2	2	2	2	2	3
Vulnerability assessment	AVA_VAN	1	2	2	3	4	5	5

Table 1: Evaluation assurance level summary”

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

“Objectives

EAL1 is applicable where some confidence in correct operation is required, but the threats to security are not viewed as serious. It will be of value where independent assurance is required to support the contention that due care has been exercised with respect to the protection of personal or similar information.

EAL1 requires only a limited security target. It is sufficient to simply state the SFRs that the TOE must meet, rather than deriving them from threats, OSPs and assumptions through security objectives.

EAL1 provides an evaluation of the TOE as made available to the customer, including independent testing against a specification, and an examination of the guidance documentation provided. It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.

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

Evaluation assurance level 2 (EAL2) - structurally tested (chapter 8.4)

“Objectives

EAL2 requires the co-operation of the developer in terms of the delivery of design information and test results, but should not demand more effort on the part of the developer than is consistent with good commercial practise. As such it should not require a substantially increased investment of cost or time.

EAL2 is therefore applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record. Such a situation may arise when securing legacy systems, or where access to the developer may be limited.”

Evaluation assurance level 3 (EAL3) - methodically tested and checked (chapter 8.5)

“Objectives

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

EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.”

Evaluation assurance level 4 (EAL4) - methodically designed, tested, and reviewed
(chapter 8.6)**“Objectives**

EAL4 permits a developer to gain maximum assurance from positive security engineering based on good commercial development practises which, though rigorous, do not require substantial specialist knowledge, skills, and other resources. EAL4 is the highest level at which it is likely to be economically feasible to retrofit to an existing product line.

EAL4 is therefore applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and are prepared to incur additional security-specific engineering costs.”

Evaluation assurance level 5 (EAL5) - semiformally designed and tested (chapter 8.7)**“Objectives**

EAL5 permits a developer to gain maximum assurance from security engineering based upon rigorous commercial development practises supported by moderate application of specialist security engineering techniques. Such a TOE will probably be designed and developed with the intent of achieving EAL5 assurance. It is likely that the additional costs attributable to the EAL5 requirements, relative to rigorous development without the application of specialised techniques, will not be large.

EAL5 is therefore applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.”

Evaluation assurance level 6 (EAL6) - semiformally verified design and tested
(chapter 8.8)**“Objectives**

EAL6 permits developers to gain high assurance from application of security engineering techniques to a rigorous development environment in order to produce a premium TOE for protecting high value assets against significant risks.

EAL6 is therefore applicable to the development of security TOEs for application in high risk situations where the value of the protected assets justifies the additional costs.”

Evaluation assurance level 7 (EAL7) - formally verified design and tested (chapter 8.9)

"Objectives

EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs. Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis."

Class AVA: Vulnerability assessment (chapter 16)

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

Vulnerability analysis (AVA_VAN) (chapter 16.1)

"Objectives

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

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

This page is intentionally left blank

D Annexes

List of annexes of this certification report

Annex A: Security Target provided within a separate document.

This page is intentionally left blank.