



COMMON CRITERIA CERTIFICATION REPORT

HPE StoreOnce Backup System Version 3.16

383-4-426

28 September 2017

Version 1.0





FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian CC Scheme, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

ITS Client Services

Telephone: (613) 991-7654

E-mail: itsclientservices@cse-cst.gc.ca



OVERVIEW

The Canadian Common Criteria Scheme provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories.

The CCEF that carried out this evaluation is CGI IT Security Evaluation & Test Facility.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme and to the Common Criteria portal (the official website of the International Common Criteria Project).



TABLE OF CONTENTS

Executive Summary	1
1 Identification of Target of Evaluation	2
1.1 Common Criteria Conformance.....	2
1.2 TOE description	2
1.3 TOE architecture.....	3
2 Security policy	4
2.1 Cryptographic functionality.....	4
3 Assumptions and Clarifications of Scope	5
3.1 Usage and Environmental assumptions	5
3.2 Clarification of Scope.....	5
4 Evaluated Configuration	6
4.1 Documentation.....	6
5 Evaluation Analysis Activities	8
5.1 Development.....	8
5.2 Guidance Documents	8
5.3 Life-cycle Support	8
6 Testing Activities	9
6.1 Assessment of Developer Tests.....	9
6.2 Conduct of Testing.....	9
6.3 Independent Functional Testing.....	9
6.4 Independent Penetration Testing	10
7 Results of the Evaluation	11
7.1 Recommendations/Comments.....	11
8 Supporting Content	12
8.1 List of Abbreviations.....	12
8.2 References	13



LIST OF FIGURES

Figure 1 TOE Architecture3

LIST OF TABLES

Table 1 TOE Identification2
Table 2 Cryptographic Algorithm(s)4



EXECUTIVE SUMMARY

HPE StoreOnce Backup System Version 3.16 (hereafter referred to as the Target of Evaluation, or TOE), from Hewlett Packard Enterprise, was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that the TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 28 September 2017 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the Canadian Certified Products list (CPL) and the Common Criteria portal (the official website of the International Common Criteria Project).



1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1 TOE Identification

TOE Name and Version	HPE StoreOnce Backup System Version 3.16
Developer	Hewlett Packard Enterprise
Conformance Claim	EAL 2+ (ALC_FLR.2)

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.

1.2 TOE DESCRIPTION

The TOE is a disk-based storage appliance used for backing up host network servers or PCs to target devices on the appliance. These devices are configured as Network-Attached Storage (NAS), Virtual Tape Library (VTL) or StoreOnce Catalyst stores. The TOE includes hardware-based RAID 5 or RAID 6 to reduce the risk of user data loss due to disk failure. The scope of the evaluation includes single-node appliances which operate as standalone devices and multi-node appliances which operate as a cluster. The TOE is managed in the form of a GUI or SSH protected Command Line Interface. Management sessions are protected using Cryptographic Algorithm Validation Program (CAVP) validated cryptography.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

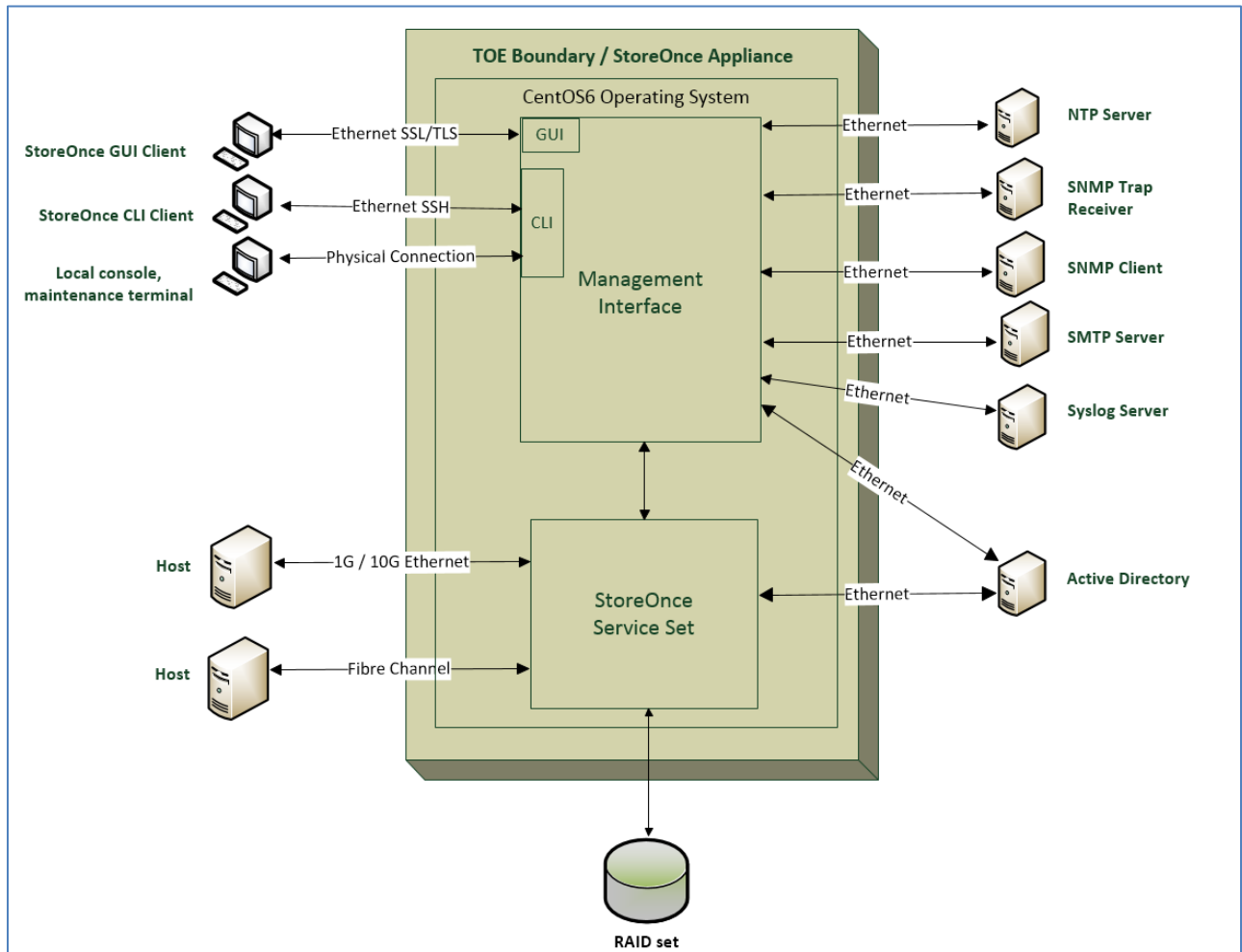


Figure 1 TOE Architecture



2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF
- TOE Access
- Trusted Paths/Channels

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following Government of Canada approved cryptographic algorithms were evaluated for correct implementation in the TOE:

Table 2 Cryptographic Algorithm(s)

Cryptographic Algorithm	Standard	Certificate Number
Triple-DES (3DES)	FIPS 46-3	2413
Advanced Encryption Standard (AES)	FIPS 197	4528, 4529
Rivest Shamir Adleman (RSA)	FIPS 186-4	2465
Secure Hash Algorithm (SHS)	FIPS 180-4	3709, 3710
Keyed-Hash Message Authentication Code (HMAC)	FIPS 198	2988



3 ASSUMPTIONS AND CLARIFICATIONS OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- There are no general-purpose computing capabilities (e.g., compilers or user applications) available on the TOE, other than those services necessary for the operation, administration and support of the TOE.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
- TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner. It is assumed that those assigned as Administrators of CIFS shares are trusted, competent and not careless.
- iSCSI and Fibre Channel host identities properly reflect the adapters and hence the hosts to which they are associated such that authentication is not necessary.
- A protected management network exists between nodes of the TOE and hosts providing supporting services (e.g., NTP, SNMP, SMTP, Syslog Server or AD).
- Confidentiality, integrity, and authenticity of the connection between the TOE and the host shall be protected by environment. The NAS clients shall authenticate NAS users (i.e. users who access NFS, and users who access CIFS with AD authentication mode) and managed user accounts properly.
- A dedicated and protected internal network exists that connects nodes of the TOE with network storage devices.
- Network devices on the internal network do not intercept, impersonate or otherwise modify communications on the Internal network.

3.2 CLARIFICATION OF SCOPE

The TOE incorporates CAVP-validated cryptography and was not subjected to CMVP (FIPS-140) validation.

The following physical/logical features and functions are not included in the scope of the evaluation:

- Third party applications that have the Catalyst Client plug-in software used to communicate directly with StoreOnce appliances;
- The connection between multiple StoreOnce appliances;
- Data at Rest Encryption, Data in Flight Encryption, and Secure Erase;
- Local/External Key Management; and
- Vulnerability Scanning.



4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises HPE StoreOnce Backup System, Version 3.16.2-1712.1 running on the following hardware appliances:

Gen 8 models:

- HPE StoreOnce 2700 (Single-node)
- HPE StoreOnce 2900 (Single-node)
- HPE StoreOnce 4500 (Single-node)
- HPE StoreOnce 4700 (Single-node)
- HPE StoreOnce 4900 (Single-node)
- HPE StoreOnce 6500 (Multi-node)

Gen 9 models:

- HPE StoreOnce 3100 (Single-node)
- HPE StoreOnce 3520 (Single-node)
- HPE StoreOnce 3540 (Single-node)
- HPE StoreOnce 5100 (Single-node)
- HPE StoreOnce 5500 (Single-node)
- HPE StoreOnce 6600 (Multi-node)

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

- a. Guidance Supplement HPE StoreOnce Backup System, Version 3.16, Version 0.1, May 31, 2017
- b. HP StoreOnce 6500 Backup System Installation Planning and Preparation Guide; Part Number: BB897-90951; Published: August 2015; Edition: 4
- c. HP StoreOnce 4900 Backup System Installation and Configuration Guide; Part Number: BB903-90945; Published: August 2015; Edition: 5
- d. HP StoreOnce 2700, 2900, 4500, and 4700 Backup System Installation and Configuration Guide; Part Number: BB877-90938; Published: August 2015; Edition: 5
- e. StoreOnce 3100, 3500, 5100 and 5500 System Installation and Configuration Guide; Part Number: BB913-90958; Published: March 2017; Edition: 4
- f. StoreOnce 6600 System Installation Planning and Preparation Guide; Part Number: BB918-90911; Published: September 2016; Edition: 2
- g. StoreOnce 6500 and 6600 Backup Systems User Guide For StoreOnce software version 3.16.x; Part Number: BB918-90913; Published: March 2017; Edition: 3



- h. StoreOnce 2xxx – 5xxx Backup Systems User Guide For StoreOnce software version 3.16.x; Part Number: BB913-90960; Published: March 2017; Edition: 4
- i. StoreOnce CLI Reference Guide (for software version 3.16.2); Part Number: BB913-90963; Published: March 2017
- j. StoreOnce Systems: Linux and UNIX Configuration Guide; Part Number: BB913-90945; Published: September 2016; Edition: 10
- k. StoreOnce 2700, 2900, 4500, 4700, and 4900 Service and Maintenance Guide; Part Number: BB877-90942; Published: March 2017; Edition: 8
- l. StoreOnce 3100, StoreOnce 3500 Series, and StoreOnce 5100 Systems Maintenance and Service Guide; Part Number: BB913-90959; Published: March 2017; Edition: 3
- m. StoreOnce 5500 Maintenance and Service Guide; Part Number: BB917-90911; Published: March 2017; Edition: 3



5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the TOE. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute the flaw information and corrections to consumers of the TOE.



6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT FUNCTIONAL TESTING

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

- a. Repeat of Developer's Tests: The evaluator repeated a subset of the developers tests;
- b. SNMP Agent: The objective of this test case is to demonstrate that Management Information Base objects can be accessed by recognized SNMP users;
- c. SNMP Trap: The objective of this test case is to demonstrate that the TOE can send SNMP trap messages to a SNMP trap receiver;
- d. SMTP: The objective of this test case is to demonstrate that the TOE is capable of sending email;
- e. NTP: The objective of this test case is to demonstrate that the TOE can make use of an NTP server;
- f. Access Control: The objective of this test case is to demonstrate controlled access to the VTL library, the Catalyst Store, NFS and CIFS shares;
- g. Secure Communication: The objective of this test case is to demonstrate that the web GUI is secured with TLS and the CLI is secured with SSH;
- h. Audit: The objective of this test case is to demonstrate the TOE's audit retention policy and that audit logs can be exported to a remote audit server; and
- i. Login Banner: The objective of this test case is to demonstrate that a login banner can be configured and is displayed during login on the GUI and the CLI.



6.3.1 FUNCTIONAL TEST RESULTS

The developer's tests and the independent functional tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 INDEPENDENT PENETRATION TESTING

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

- a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST; and
- b. Cookie Strength: The objective of this test is to determine whether the TOE is susceptible to weak session IDs;
- c. Session Fixation: The objective of this test is to determine whether the TOE is susceptible to session fixation;
- d. Weak Algorithms in SSH and TLS: The objective of this test is to determine whether the TOE offers weak algorithms for SSH and TLS; and
- e. Bypass: The objective of this test case is to determine whether the vulnerability scan interface could allow an unauthorized user to bypass TOE security features.

6.4.1 PENETRATION TEST RESULTS

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.



7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply 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 Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

7.1 RECOMMENDATIONS/COMMENTS

The TOE is a sophisticated storage system therefore the customer is well advised to follow the Guidance Supplement, HPE StoreOnce Backup System Version 3.16 as well as the documentation which is listed in the Section 1.5.1.1 of ST to configure the TOE in the evaluated configuration.



8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
AD	Active Directory
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CCS	Canadian Common Criteria Evaluation and Certification Scheme
CIFS	Common Internet File System
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
HPE	Hewlett Packard Enterprise
iSCSI	Internet Small Computer System Interface
IT	Information Technology
ITS	Information Technology Security
NAS	Network Attached Storage
NFS	Network File System
NTP	Network Time Protocol
PP	Protection Profile
RAID	Redundant Array of Independent Disks
SFR	Security Functional Requirement
SNMP	Simple Network Management Protocol
SMTP	Simple Mail Transfer Protocol



Term	Definition
SSH	Secure Shell
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VTL	Virtual Tape Library

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
Hewlett Packard Enterprise HPE StoreOnce Backup System Version 3.16 Security Target, Version 0.5, September 20, 2017.
Hewlett Packard Enterprise HPE StoreOnce Backup System Version 3.16 Common Criteria EAL 2+ Evaluation Technical Report, Version 0.4, September 28, 2017.