National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

HP StoreOnce Generation 3 Version 3.6.6

Report Number: CCEVS-VR-VID10495-2013
Dated: December 17, 2013
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Table of Contents

List of Tables

1 Executive Summary

The evaluation of **HP StoreOnce Backup System** was performed by Leidos, in the United States and was completed in December 2013. The evaluation and validation were consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site www.niap-ccevs.org. The criteria against which the StoreOnce TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, revision 3. The evaluation methodology used by the evaluation team to conduct the evaluation was available in the Common Methodology for Information Technology Security Evaluation versions 3.1, revision 3. The Target of Evaluation (TOE) claims an Evaluation Assurance Level (EAL) of 2, augmented with ALC_FLR.3.

The TOE is a disk-based storage appliance for backing up host network servers or PCs to target devices on the appliance. These devices are configured as either Network-Attached Storage (NAS) or Virtual Tape Library (VTL) or StoreOnce Catalyst targets for backup applications.

Leidos determined that the product satisfies evaluation assurance level (EAL) 2 augmented with ALC_FLR.3 as defined within the Common Criteria (CC). The product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the *HP StoreOnce Backup System Generation 3 Version 3.6.6 Security Target*, version 0.6, December 13, 2013. This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is any of the StoreOnce models listed in the Security Target. This Validation Report is not an endorsement of HP StoreOnce by any agency of the US Government and no warranty of the product is either expressed or implied.

2 Identification

Evaluated Product:	HP StoreOnce Version 3.6.6
Sponsor & Developer:	Hewlett-Packard Long Down Avenue Stoke Gifford Bristol BS34 8QZ UK
CCTL:	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date:	December 2013
CC:	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, September 2009
Interpretations:	There were no applicable interpretations used for this evaluation.
CEM:	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 3, September 2009
PP:	None
Evaluation Class:	Evaluation Assurance Level (EAL) 2 Augmented with ALC_FLR.3
Description	The TOE is the HP StoreOnce network storage device.
Disclaimer	The information contained in this Validation Report is not an endorsement of the HP StoreOnce by any agency of the U.S. Government and no warranty of HP StoreOnce is either expressed or implied.
Evaluation Personnel:	Pascal Patin Greg Beaver
Validation Scheme:	NIAP Common Criteria Evaluation and Validation Scheme

2.1 Evaluation Details

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) using the Common Evaluation Methodology (CEM) for Evaluation Assurance Level (EAL) 1 through EAL 4 in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation. Note that assurance requirements outside the scope of EAL 1 through EAL 4 are addressed at the discretion of the CCEVS.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Validated Products List.

The following table serves to identify the evaluated Security Target and TOE.

Table 1 ST and TOE identification

ST Title:	HP StoreOnce Backup System Generation 3 Version 3.6.6 Security Target, December 13, 2013
TOE Identification:	HP StoreOnce Backup System, Generation 3 Version 3.6.6
Operating Platform:	The TOE includes the following single node appliances: HP StoreOnce 2610 iSCSI Backup HP StoreOnce 2620 iSCSI Backup HP StoreOnce 4210 iSCSI Backup HP StoreOnce 4210 FC Backup HP StoreOnce 4220 Backup HP StoreOnce 4420 Backup HP StoreOnce 4430 Backup The TOE also includes the HP StoreOnce B6200 multi-node appliance.

3 Security Policy

3.1 Summary

The HP StoreOnce Backup System is a disk-based storage appliance for backing up host network servers or PCs to target devices on the appliance. These devices are configured as either Network-Attached Storage (NAS) or Virtual Tape Library (VTL) or StoreOnce Catalyst targets for backup applications.

The total number of backup targets offered by an HP StoreOnce Backup System is split between VTL, NAS and StoreOnce Catalyst devices. The number of supported backup targets varies according to model (for single-node appliances) or number of nodes (for clusters). Each node in a cluster is capable of supporting 48 target devices. So as examples, a couplet can support 96 backup targets, while an 8 node (4 couplet) B6200 can support 384 (i.e., 48 x 8) backup targets. These devices may be all VTL, all NAS, all StoreOnce Catalyst or any combination of NAS and VTL devices. The HP StoreOnce Backup System supports both Common Internet File System (CIFS) and Network File System (NFS) protocols for connectivity to TOE provided NAS. This allows the TOE to provide backup targets for both Windows and UNIX/Linux hosts.

All devices (i.e., VTL, StoreOnce Catalyst and NAS) automatically include the TOE's data deduplication functionality. Data deduplication is a process in which the TOE compares blocks of data being written to a backup device with data blocks previously stored on the device. If duplicate data is found, a pointer is established to the original data, rather than storing the duplicate data. The TOE performs data deduplication at the block level and not at the file level, which reduces the amount of data actually stored on physical disks.

The HP StoreOnce Backup System products are hardware appliances that offer network accessible administration interfaces in the form of an HTTPS based Graphical User Interface or SSH protected Command Line Interface.

Remote administration sessions occurring through the management network are protected using cryptography (SSH and HTTPS). Network traffic between the product and NTP or LDAP servers occurs utilizing only protections inherent in the NTP and LDAP protocols. The HP StoreOnce Backup System allows a site to choose to combine the data and management networks. In single-node configurations, the data and management network must be combined. Both single-node and multi-node configurations utilize an Internal network for communication with storage devices.

The HP StoreOnce Backup Systems provides Ethernet network connections for use as a management network (i.e., used for all management traffic). All Ethernet-based networks support only IPv4 networking functionality. IPSec and IPv6 security features are not available, though some protection is supported for administrator network communications (e.g., SSH and HTTPS). The data network can be either Ethernet or Fibre Channel. The internal network will be Ethernet.

The HP StoreOnce Backup Systems include hardware-based RAID 5 or RAID 6 to reduce the risk of user data loss due to disk failure within a couplet.

3.2 TOE Threats

The following threats are identified in in the Security Target

T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms that may go undetected.
T.DATA_AVAILABILITY	User data may become unavailable due to isolated storage resource failures, node failures or due to resource exhaustion.
T.DATA_DISCLOSURE	A connected host might obtain access to user data for which they have no authorization.
T.UNAUTHORIZED_ACCESS	A user may gain unauthorized access to the TSF data and TSF executable code. A malicious user, process, or external IT entity may masquerade as an authorized entity in order to gain unauthorized access to TSF data or TSF resources. A malicious user, process, or external IT entity may misrepresent itself as the TSF to obtain identification and authentication data.
T.UNDETECTED_ACTIONS	Malicious remote users or external IT entities may take actions that adversely affect the security of the TOE. These actions may remain undetected and thus their effects cannot be effectively mitigated.
T.USER_DATA_REUSE	User data may be inadvertently sent to a destination not intended by the original sender.

3.3 Assumptions

The following assumptions are identified in the Security Target:

3.3.1. Assumptions

The following conditions are assumed to exist in the operational environment.

A.NO_GENERAL_PURPOSE	It is assumed that 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.
A.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment.
A.TRUSTED_ADMIN	TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
A.HOST_IDENTITY	It is assumed that iSCSI and Fiber Channel host identities properly reflect the adapters and hence the hosts to which they are associated such that authentication is not necessary.
A.MGMT_NET	It is assumed that a dedicated and protect “Management Network” exists between nodes of the TOE and hosts providing supporting services (e.g., AD and NTP).
A.DATA_NET	Clients on the “Data Network” do not have direct access to the Internal or Management networks that are used for managing, accessing, and supporting the TOE operations.
A.INTERNAL_NET	It is assumed that a dedicated and protected “Internal Network” exists that connects nodes of the TOE with network storage devices.
A.ETHERNET	It is assumed that network devices on the Internal Network do not intercept, impersonate or otherwise modify communications on the Internal network.

3.4 Clarification of Scope

This text covers some of the more important limitations and clarifications for this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (EAL 2 augmented with ALC_FLR.3 in this case).
2. This evaluation only covers the specific versions identified in this document, and not any earlier or later versions released or in process.
3. As with all EAL 2 evaluations, this evaluation did not specifically search for, nor seriously attempt to counter, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

4. The TOE relies on the operational environment in which it operates for the following security and other functionality:
   - The physical protection of the TOE
   - The physical protection of the Data Network, Management Network, and the Internal Network
   - That client hosts provide their correct identity (e.g., IP address, Fibre Channel port number), and that there is no attempt by client hosts to masquerade as other hosts.
5. The following product capabilities described in the guidance documentation were not included within the scope of the evaluation and no claims are made regarding them:
   a. The product includes a maintenance serial port that can be used for terminal access. This port can only be used by someone with direct physical access to the TOE.
   b. The product has an SNMP service that responds to GET, GETNEXT and GETBULK SNMP requests and generates notification messages (traps) for critical events (alerts) and alert state changes. It was not a part of the CC evaluated configuration.

4 Architectural Information

The HP StoreOnce Backup System product line is available in single-node or multi-node configurations. The Gen 3 architecture of a multi-node configuration is depicted in Figure 1. A single-node configuration would be identical to the architecture of a single node as shown in Figure 1. The multi-node architecture provides mechanisms for high availability support by offering the ability to continue operation in the event of the failure of one node within each couplet as well as by offering support of RAID levels to protect user and TSF data. Single-node configurations support availability of data through the support of RAID levels to protect user and TSF data store within the control of the TOE.

Figure 1 depicts a cluster composed of two couplets. Each couplet includes two nodes. This is an example of a multi-node StoreOnce configuration.

From the perspective of shared configuration data (i.e., TOE Data), there are two significant types of data depicted in Figure 1. The storage of TOE Security Function data is depicted by the box labeled “Fusion Manager Store”. This store of data is accessible to all of the nodes in the cluster. The second type of configuration data is labeled as “Ibrix FS” with N sets of node configuration data. This data is available within a couplet even after one node of that couplet fails.

The multi-node architecture includes distinct physical network ports that are used to isolate node-to-node communications from client-data backup operations. The ability to isolate internal TOE communications (which is not encrypted) to a dedicated network strengthens protection of TSF data. Administrative communication is cryptographically protected using SSHv2 and HTTPS/TLSv1.0. While the administrative communication would occur on the same network as client-data backup operations, they are protected cryptographically. The middle and lower end model single-node configuration, there would be no need for node-to-node communications, so no dedicated network would be employed. In a high end single node product, there is an internal network between the node and the storage devices.

The multi-node architecture supports up to four couplets of nodes in a cluster. Each cluster portrays a single management interface and one data interface per node. When a node in a couplet fails, the lost physical data interface is virtualized by the other node. Virtualization can occur for either an

Ethernet or Fibre Channel interface. When both nodes of a couplet fail, the data within that couplet is unavailable to users. Each time the active management node fails, reboots or is put in to a maintenance mode for repairs, a negotiation occurs between all remaining nodes in the cluster to elect a new active management node.

The single-node architecture makes use of RAID to provide availability of data stored by a node. In multi-node configurations, RAID of physical storage occurs inside a couplet with both nodes accessing the same RAID arrays. There is no RAID or other redundancy between couplets in a cluster.

Deduplication (a.k.a., deduping), allows data to be stored only once. When the same data occurs multiple times (as in the backup of data that has not changed) it is handled by reference as opposed to storing multiple copies. Remote copy (i.e., site replication) basically allows all the data to be copied to another cluster and makes use of the same deduping technology.

Remote administrator sessions are encrypted using SSHv2 or HTTPS/TLS. SNMPv2 is also supported. Internal cluster and client-host connections are not encrypted by the TOE.

A cluster can be configured to use NTP to synchronize time with an external server. When so configured, one node in the cluster becomes an NTP server. This NTP server node connects (as a client) to an external NTP server to obtain a time value from that external entity. The NTP server node then acts as a server to each of the other nodes within the cluster which are acting as NTP clients to the one node designated as the NTP server within the cluster.

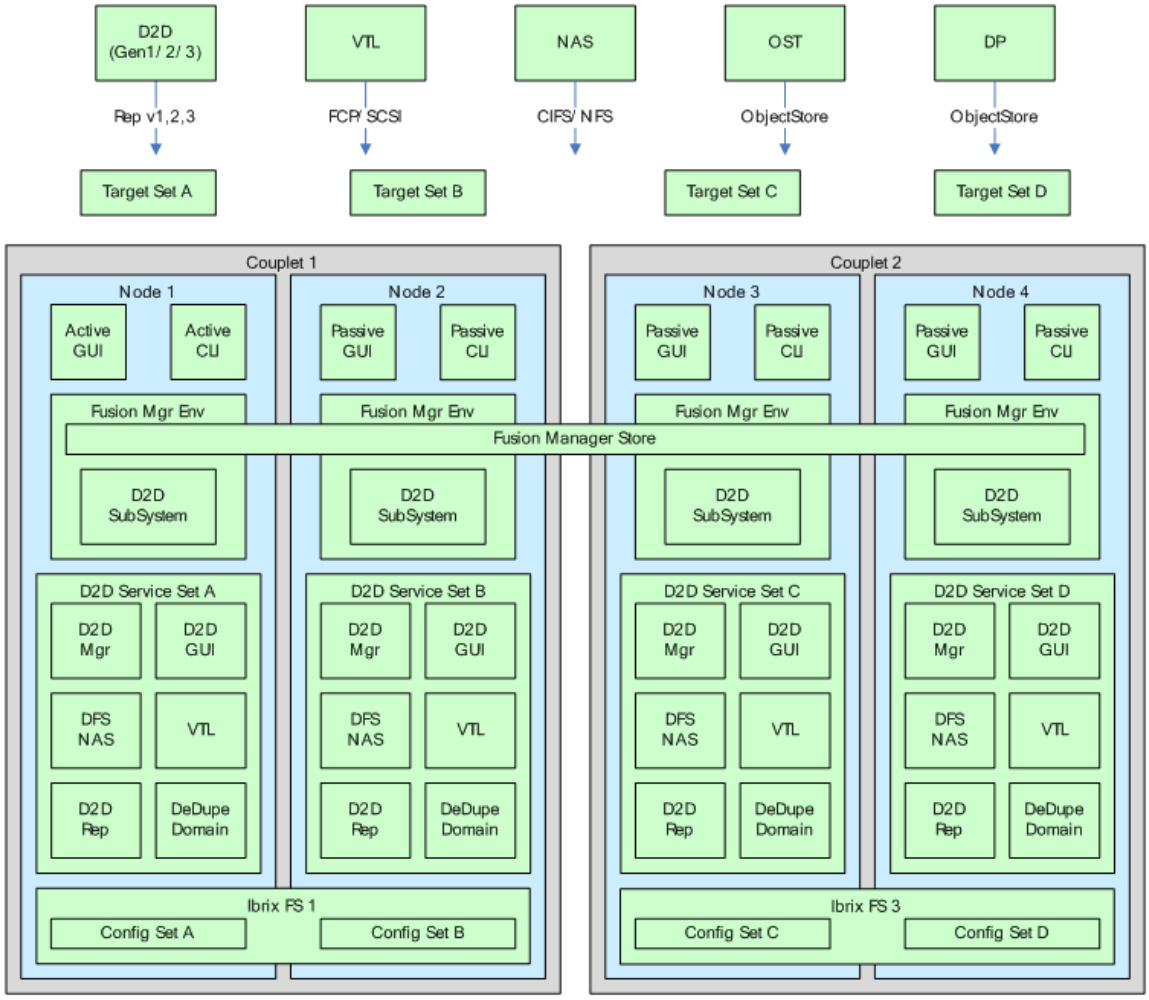

Figure 1 StoreOnce MultiNode Service Architecture

4.1 Physical Boundaries

The physical boundary of a HP StoreOnce Backup System is the physical boundary of the hardware of the cluster. Interfaces to this hardware include the following:

A per-node serial port which provides limited administrative access,

Fibre Channel ports for Fibre Channel host access to the data network,

Four (4) Ethernet connections for iSCSI host access to the data network,

Two (2) Ethernet connections for administrative device access to the management network, and

Two (2) Ethernet connections used for an internal network.

The TOE can be configured to rely on and utilize a number of other components in its operational environment.

Active Directory servers – The HP StoreOnce Backup System can be configured to utilize Active Directory as an external authentication server.

Network Time Protocol (NTP) server – The HP StoreOnce Backup System can be configured to act as an NTP client to synchronize the internal clock of the active node with an external source. The product can also be configured to offer NTP server functionality to each individual node in a cluster, to synchronize the clocks within the cluster.

iSCSI and Fibre Channel client hosts – The HP StoreOnce Backup System attaches to applicable ports which access available storage resources (SANs and VTLs).

Network Storage Devices – The HP StoreOnce Backup System is typically connected to a storage controller that manages the actual physical storage.

The TOE nodes, storage devices, and internal network must have physical protections that are consistent with the data being stored and transmitted. This internal network is expected to be dedicated such that communication between the TOE and either another TOE node or a storage device is not modified or disclosed.

The management network is expected to provide connectivity for the TOE, administrative devices, and NTP servers. Active directory servers are accessed from the data network to manage NAS share permissions. Active Directory servers can be deployed with or without cryptographic protections depending on the needs of the operational environment. While physical security of this network is appropriate, TOE remote administrative sessions are protected from disclosure and modification using SSH and HTTPS/TLS,

The data network is used by clients to send data to the TOE for backup purposes. The data network is also expected to provide physical protections that are consistent with the data being stored and transmitted. Network devices on the Ethernet SAN are expected not to intercept, impersonate or otherwise modify communications on the SAN.

5 Documentation

The documentation for the TOE is:

- HP StoreOnce 4000 and 2000 Series Backup system user guide, Edition 4, November 2012
- HP B6000 StoreOnce Backup System Capacity Upgrade Kit Booklet, June 2012
- HP StoreOnce 4210, 4220/4420 and 4430 Upgrade Kit Installation Instructions, Edition 1, October 2012
- HP StoreOnce B6000 Backup System CLI Reference Guide, Edition 4, October 2012.
- HP StoreOnce Backup System Single-Node Products CLI Reference Guide, Edition 2, December 2012
- HP StoreOnce B6000 Series Backup System Installation Planning and Preparation Guide and Checklists (chapter 6), Edition 5, November 2012
- HP StoreOnce B6000 Series Backup System maintenance and service guide, Edition 1, August 2012
- HP StoreOnce B6000 Series Backup system user guide, Edition 4, November 2012
- HP StoreOnce Backup System Concepts Guide, Edition 2, September 2011
- HP StoreOnce Backup system service and maintenance guide for single node models that are running v3.4.0 (and later) software
- HP StoreOnce G3 Backup system Installation and Configuration Guide, Edition 1, December 2012

All of the listed documents were considered relevant and were used as a part of the evaluation. Any other customer documentation, either delivered with the product or available through other vendor sources, is not included in the scope of evaluation and should not be relied upon when using the product in its evaluated configuration.

6 IT Product Testing

The purpose of this activity was to determine whether the TOE behaves as specified in the design documentation and in accordance with the TOE security functional requirements specified in the ST for an EAL2 evaluation.

6.1 Developer Testing

The developer created test procedures specifically to fulfill the test requirements for an EAL2 evaluation. The tests were developed to provide good coverage of the security functions related to each of the security requirements in the Security Target. The developer has documented their tests in a test plan where the results of the tests are presented as prose conclusions, notes, screen shots, and summaries for each of the applicable test platforms.

6.2 Independent Testing

Independent testing took place at the developer's location in Fort Collins, Colorado in December 2013.

The evaluators received single and multi-node versions of the TOE installed and set up in a state that was consistent with the developer test plan. Both versions of the TOE were in a fully operational state without any errors or warning messages. Network configuration was consistent with what was described in the test plan.

Given the complete set of test results from test procedures exercised by the developer and the sample of tests directly exercised by the evaluators, the testing requirements for EAL2 are fulfilled.

7 Evaluated Configuration

The TOE is HP StoreOnce installed according to the Installation Planning and Preparation Guide and Checklists.

8 Results of the Evaluation

The Evaluation Team conducted the evaluation in accordance with the CC, the CEM, and the CCEVS. The Evaluation Team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each EAL2 assurance component. For Fail or Inconclusive work unit verdicts, the Evaluation Team advised the developer of the issue that needed to be resolved or the clarification that needed to be made to the particular evaluation evidence.

The Evaluation Team accomplished this by providing notes, comments, or vendor actions in the draft ETR sections for an evaluation activity (e.g., ASE, ADV) that recorded the Evaluation Team's evaluation results and that the Evaluation Team provided to the developer. The Evaluation Team also communicated with the developer by telephone and electronic mail. If applicable, the Evaluation Team re-performed the work unit or units affected. In this way, the Evaluation Team assigned an overall Pass verdict to the assurance component only when all of the work units for that component had been assigned a Pass verdict. Verdicts were not assigned to assurance classes. The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by Leidos.

Listed below are the security function requirements (SFRs) imposed on the TOE to be evaluated and pass at Evaluation Assurance Level 2 augmented with ALC_FLR.3. These components are taken from CC Part 2:

Requirement Class	Requirement Component
FAU: Security Audit	FAU_GEN.1: Audit data generation
	FAU_GEN.2: User identity association
	FAU_SAR.1: Audit review
	FAU_SAR.3: Selectable audit review
	FAU_STG.1: Protected audit trail storage
	FAU_STG.4: Prevention of audit data loss
FCS: Cryptographic support	FCS_CKM.1: Cryptographic key generation
	FCS_COMM_PROT_EXT.1: Communications Protection
	FCS_COP.1(1): Cryptographic Operation (for data encryption/decryption)
	FCS_COP.1(2): Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(3): Cryptographic Operation (for keyed-hash message authentication)
	FCS_HTTPS_EXT.1: HTTPS Protocol
	FCS_SSH_EXT.1: Secure Shell Protocol
	FCS_TLS_EXT.1: Transport Layer Security Protocol
FDP: User data protection	FDP_ACC.2: Complete access control
	FDP_ACF.1: Security attribute based access control
	FDP_AVL_EXT.1(1): Data Availability (User Data)
	FDP_AVL_EXT.1(2): Data Availability (TSF Data)
	FDP_AVL_EXT.1(3): Data Availability (Couplet)
	FDP_AVL_EXT.3(1): Failure Alerts (User Data)
	FDP_AVL_EXT.3(2): Failure Alerts (TSF Data)
	FDP_AVL_EXT.3(3): Failure Alerts (Couplet)
	FDP_RIP.2: Full residual information protection
FIA: Identification and authentication	FIA_ATD.1: User attribute definition
	FIA_UAU.1: Timing of authentication
	FIA_UAU.7: Protected authentication feedback
	FIA_UID.2: User identification before any action
FMT: Security management	FMT_MSA.1: Management of security attributes
	FMT_MSA.3: Static attribute initialization
	FMT_MTD.1: Management of TSF data
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security roles
FPT: Protection of the TSF	FPT_PTD_EXT.1(1): Protection of TSF Data (authentication data)
	FPT_PTD_EXT.1(2): Protection of TSF Data (symmetric key data)
	FPT_STM.1: Reliable time stamps
TOE Access	FTA_SSL.3: TSF-initiated Termination
FTP: Trusted path/channels	FTP_TRP.1(1): Trusted Path (Disclosure)
	FTP_TRP.1(2): Trusted Path (Modification)

The evaluators concluded that the overall evaluation result for the target of evaluation is Pass. The evaluation team reached Pass verdicts for all applicable evaluator action elements and consequently all applicable assurance components.

- The TOE is CC Part 2 Extended
- The TOE is CC Part 3 Conformant.

The validators reviewed the findings of the evaluation team, and have concurred that the evidence and documentation of the work performed support the assigned rating.

9 Validator Comments/Recommendations

It is important that the implications of the assumption A.HOST_IDENTITY (Section 3.3.1, above) be understood. The TOE assumes that it is in a relatively benign environment and that client hosts are essentially co-located and are afforded the same physical security protections as that of the TOE. Further, the client hosts are trusted to present accurate host identifiers; that they do not lie about their identities. Thus, the TOE accepts the host identifier (e.g., IP Address, Fibre Channel port number) as given, does not authenticate the claimed host identity, and provides access to TOE resources based upon the claimed identity.

If the assumption A.HOST_IDENTITY cannot be guaranteed then, at a minimum, the environment must be augmented with an authentication mechanism in order to provide the proper protection from a client host masquerading as another host and thereby obtaining unauthorized access to data and resources.

10 Annexes

Not applicable.

11 Security Target

HP StoreOnce Backup System Generation 3 Version 3.6.6 Security Target, December 13, 2013

12 Acronym List

CC	Common Criteria
CCTL	CC Testing Laboratory
CI	Configuration Item
CM	Configuration Management
CMP	Configuration Management Plan
CVE	Common Vulnerabilities and Exposures
CVS	Concurrent Versioning System
DoD	Department of Defense
EAL	Evaluation Assurance Level
FSP	Functional Specification
GUI	Graphical User Interface
HLD	High-level Design
ID	Identity/Identification
IP	Internet Protocol
IT	Information Technology
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OS	Operating System
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSS	TOE Summary Specification

13 **Bibliography**

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 3, July 2009.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 3, July 2009.

[3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009.

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009.

[5] HP StoreOnce Backup System Generation 3 Version 3.6.6 Security Target, December 13, 2013

[6] Common Criteria Evaluation and Validation Scheme - Guidance to CCEVS Approved Common Criteria Testing Laboratories, Version 2.0, 8 Sep 2008.