# National Information Assurance Partnership

# Common Criteria Evaluation and Validation Scheme

# Validation Report

# Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains

**Report Number:** CCEVS-VR-VID10479-2012
**Dated:** October 30, 2012
**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**

# ACKNOWLEDGEMENTS

## Validation Team

**Mario Tinto**
*The Aerospace Corporation*
*Columbia, MD*

**Jean Petty**
*MITRE Corporation*
*McLean, VA*

## Common Criteria Testing Laboratory

*Science Applications International Corporation (SAIC)*
*Columbia, MD*

# Table of Contents

# 1 Executive Summary

The evaluation of Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains was performed by Science Applications International Corporation (SAIC), in the United States and was completed in October 2012. The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The criteria against which the Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. The evaluation methodology used by the evaluation team to conduct the evaluation was available in the Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009.

SAIC determined that the product satisfies evaluation assurance level "EAL 2 augmented with ALC_FLR.2" 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 *Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains Security Target*, Version 1.0, 10/09/2012.

This Validation Report applies only to the specific version of the TOE as evaluated. In this case the TOE is:

> Hewlett-Packard 3PAR InServ Storage Systems (specific models identified below) running InForm OS (version 3.1.1 .MU1+P16 with Virtual Domains)
>
> > HP 3PAR InServ T-Class Storage System models T400 and T800
> > HP 3PAR InServ F-Class Storage System models F200 and F400
> > HP 3PAR InServ P10000 (also known as V-Class) Storage System models V400 and V800
>
> 3PAR CLI client (version 3.1.1)
>
> InForm Management Console (version 4.2.1)

The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This Validation Report is not an endorsement of Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains by any agency of the US Government and no warranty of the product is either expressed or implied.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the individual work units and versions of the ETR. Also, at some discrete points during the evaluation, validators formed a Validation Oversight Review panel in order to review the Security Target and other evaluation evidence materials along with the corresponding evaluation findings in detail. The validation team found that the evaluation showed that the product satisfies all of the security functional and assurance requirements stated in the Security Target (ST). Therefore the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

The technical information included in this report was obtained from the *Evaluation Technical Report for Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains* Parts 1 and 2 and the *Evaluation Team Test Report for Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains* produced by SAIC.

## 1.1 Evaluation Details

**Evaluated Product:** Hewlett-Packard 3PAR InServ Storage Systems (specific models identified below) running InForm OS (version 3.1.1 .MU1+P16 with Virtual Domains)

HP 3PAR InServ T-Class Storage System models T400 and T800
HP 3PAR InServ F-Class Storage System models F200 and F400
HP 3PAR InServ P10000 (also known as V-Class) Storage System models V400 and V800

3PAR CLI client (version 3.1.1)

InForm Management Console (version 4.2.1)

**Sponsor:**
Hewlett-Packard Development Company, L.P.
4209 Technology Drive
Fremont, CA 84538

**Developer:**
Hewlett-Packard Development Company, L.P.
4209 Technology Drive
Fremont, CA 84538

**Evaluation Facility:**
Science Applications International Corporation
6841 Benjamin Franklin Drive
Columbia, MD 21046

**Kickoff Date:** 13 October 2011

**Completion Date:** October 2012

**CC:** Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 3, July 2009

Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 3, July 2009

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

**Interpretations:** None

**CEM:** Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 3, July 2009

**Evaluation Class:** EAL 2 augmented with ALC_FLR.2

**Description:** The Target of Evaluation (TOE) consists of three classes of Hewlett-Packard 3PAR® InServ® Storage Systems along with the 3PAR command line interface (CLI) client and InForm Management Console (IMC) applications. 3PAR InServ Storage Systems are physical appliances that primarily serve to host disk drives and provide secure channels to configure an access policy. The TOE enforces an access policy between content on the disks and attached storage area network (SAN) hosts. Hosts access the TOE via attached Fiber Channel (FC) or Internet SCSI (iSCSI) storage area networks. The TOE provides network-accessible administrative interfaces through CLI client, IMC, and Secure Shell (SSH). The Virtual Domains feature of the TOE provides the capability restrict an administrative user to a domain, which is a defined set of storage resources and client hosts.

This evaluation includes the T-Class, F-Class and P10000 (also known as V-Class) models. TOE software is common across the various TOE classes and models. The classes share a common architecture and hence implement the same security functions and policies. However, the classes and models differ in CPUs, memory, disk drive capacity, access ports, and overall performance characteristics.

**Disclaimer:** The information contained in this Validation Report is not an endorsement of the Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains by any agency of the U.S. Government and no warranty of Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains is either expressed or implied.

**PP:** None

**Validation Body:** National Information Assurance Partnership CCEVS

# 2 Identification

The evaluated product is as follows:

**Security Target:**

*Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains Security Target,* Version 1.0, 10/09/2012

**TOE Identification:**

Hewlett-Packard 3PAR InServ Storage Systems (specific models identified below) running InForm OS (version 3.1.1 .MU1+P16 with Virtual Domains)

HP 3PAR InServ T-Class Storage System models T400 and T800
HP 3PAR InServ F-Class Storage System models F200 and F400
HP 3PAR InServ P10000 (also known as V-Class) Storage System models V400 and V800

3PAR CLI client (version 3.1.1)

InForm Management Console (version 4.2.1)

**Evaluated Configuration:**

There are a number of software components that can be individually licensed for use with an InServ Storage System: 3PAR Virtual Domains, 3PAR Thin Provisioning, 3PAR Thin Conversion, 3PAR Thin Persistence, 3PAR Thin Copy Reclamation, 3PAR Virtual Copy, 3PAR Remote Copy, 3PAR Dynamic Optimization, 3PAR Adaptive Optimization, and 3PAR Virtual Lock. Any of these can be freely used in the evaluated configuration with the exception of 3PAR Remote Copy. Furthermore, the 3PAR Virtual Domains feature is required.

Note that the evaluated configuration specifically includes the use of 3PAR Virtual Domains because configurations excluding the use of the 3PAR Virtual Domains are addressed in an alternate evaluation; see *Hewlett-Packard 3PAR® InServ® Storage Systems Security Target.*

Note also that there are a number of 3PAR host-based applications available for use with an InServ Storage System. While these can be freely used, they do not have security ramifications and are excluded from the scope of evaluation since they run on client hosts rather that in the context of the InServ Storage System.

As explained in the Security Target, the following product features were not subject to evaluation:

- 3PAR Remote Copy,
- SNMP management of InServ Storage System,
- Common Information Model (CIM) management of the InServ Storage System,
- Export of audit records to an external Syslog server, and
- Use of the Maintenance Terminal and Service Processor.

The operational environment of the TOE does include a management workstation and may include time and authentication servers (Network Time Protocol and Lightweight Directory Access Protocol servers, respectively).

# 3 Security Policy

The TOE enforces the following security policies as described in the ST.

- Security audit
- Cryptographic support
- User data protection
- Identification and authentication
- Security management
- Protection of the TSF
- Trusted path/channels

***Note:*** *The ST should be consulted for more description of these and other security functions of the TOE.*

## 3.1 Security audit

The TOE generates audit records that include date and time of the event, responsible subject identity, and outcome for security events. The TOE provides an interface for authorized users to view locally stored event logs and provides the ability to search the auditable events based on user ID.

## 3.2 Cryptographic support

The TOE includes implementations of OpenSSH and OpenSSL to facilitate encrypted communication with remote administrators. An administrator may connect securely to the TOE using the CLI or IMC clients distributed as part of the TOE or an SSHv2 client.

## 3.3 User data protection

The TOE enforces a policy which controls access to the available storage resources, which the TOE presents as Virtual Volumes. Access to VVs can be limited to:

- Fiber Channel client hosts based on specific FC ports,
- Internet SCSI client hosts based on specific iSCSI ports,
- Specific FC hosts identified by World Wide Names (WWN),
- Specific iSCSI hosts identified by iSCSI name,
- A defined set of hosts, or
- Specific hosts on specified ports.

The association between VVs, hosts, and ports is configurable by an administrator subject to role and domain restrictions. Attached hosts cannot access or even perceive any VVs until access is explicitly granted by one of the methods identified above.

Note that the TOE enforces separation between its control functions and the data path (that is, control plane and data plane). Users logging in to manage the TOE have no access to the protected storage resources while client hosts connected to FC or iSCSI ports have no access to any TOE management functions.

The TOE supports thinly-provisioned VVs. When a VV is thinly provisioned, the TOE allocates physical storage resources to the VV as the storage is needed (for example, as a result of write operations). Administrators may configure warning and limit levels for a VV and its underlying physical storage resources. The TOE will notify an administrator when storage allocated to a VV reaches the configured allocation warning level. When storage allocated to VV reaches the configured limit level, the TOE will both notify administrators and prevent any further allocation of physical storage to the VV. These limits serve to bound the resources a given VV can consume, thereby protecting resources needed for other purposes.

## 3.4 Identification and authentication

The TOE requires administrative users to provide unique identification and authentication data before any access to the system is granted, to include access to administrative functions. The TOE maintains the following security attributes belonging to locally-defined, individual administrative users: user identity, domain, class (permissions), password, and optionally a public key. An administrative user can be assigned to the browse, edit, service, or super class. Browse and edit users may be assigned to specific Virtual Domains. The TOE uses these attributes to determine access to available functions. The TOE protects the locally stored user authentication attributes using MD5 hashes. The TOE also provides obscured feedback when the password is entered.

In addition, the TOE can be configured to use an external LDAP server (for example, Active Directory) for authentication. If an administrative user is not defined locally, the provided user identity and password are forwarded to the configured LDAP server. If the LDAP authentication is successful, the TOE will determine an administrative user's class and domain associations using information retrieved from the LDAP server. Note that the TOE does not provide functions to manage users defined in an LDAP server.

In addition to administrative users, the TOE identifies client host users using iSCSI names and Fiber Channel WWNs. Client host users are only identified and are not authenticated, except when an administrator configures iSCSI Challenge-Handshake Authentication protocol.

## 3.5 Security management

As identified above, the TOE supports four user classes (browse, edit, service, and super) that can be assigned to individual users for each domain defined. Users in the super class can perform any functions (that is, all security functions of the TOE including managing audit events, local user accounts, managing domains, and access control) while other users have more limited access, although still security relevant, to security management functions.

Administrator can assign users to domains (with browse or edit user class in each domain) using the Virtual Domains feature. Domains are not directly relevant to users in the service or super classes since those classes transcend domains. However, users in the browse or edit class in a given domain are limited to managing client hosts and storage resources in that domain.

Virtual domains are used to organize users, storage resources, and client hosts. A virtual domain limits the administrative functions a user can perform. For example, an edit user in a domain can only export Virtual Volumes that belong to the domain and can only export them to client hosts in the same domain. Hosts do not perceive and are not directly subject to domain constraints, but rather are subject to domain constraints only indirectly. An administrator cannot configure host accessible resources in violation of the domain constraints. As such, this enforcement is not considered access control since none of the access checks involve domain-related checks.

The security functions of the TOE are managed by authorized users using either command line or graphical user interfaces. The command line interface is accessible via SSHv2 sessions or the CLI client HP provides with the TOE. The graphical user interface is accessible using the IMC client.

## 3.6 Protection of the TSF

The TOE implements a number of features design to protect itself to ensure the reliability and integrity of its security features. First and foremost, the TOE is a stand-alone physical device, with the exception of some optional client software. The TOE does not host or execute untrusted applications. The TOE appliance is designed with separate physical connections so that administrative and supporting service network communications are physically isolated from client host communications. Each of the physical interfaces is associated with a well-defined set of standards-based services that have been carefully design to comply with the applicable standards and to implement and enforce the security and other access policies of the TOE without offering any functions that might serve to bypass or allow any of those policies to be subverted in some way. The TOE clients are applications designed to provide administrative interfaces. They are carefully designed to provide functions to administrators correctly, but necessarily must be used in conjunction with hosts that will protect them from potential tampering.

Internally, the TOE protects particularly sensitive data such as stored passwords and cryptographic keys so that they are not accessible even by an administrator. It also provides an internal real-time clock in each node to ensure that reliable time information is available (for example, for log accountability). The TOE can be configured to synchronize time with an external NTP server.

## 3.7 Trusted path/channels

The TOE protects interactive communication with remote administrators using SSHv2 (for user-provided SSH clients) or SSL/TLS (for HP-provided CLI and IMC clients). In each case, both integrity and disclosure protection is ensured. Note that communication with a configured LDAP server can also be protected using TLS.

# 4 Assumptions

The ST identifies the following assumptions about the use of the product:

- 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.
- Physical security, commensurate with the value of the TOE and the data it contains, is assumed to be provided by the environment. This also extends to supporting servers (e.g., NTP) and client hosts that are expected to be in close proximity to the TOE.
- Administrators are trusted to follow and apply all administrator guidance in a trusted manner.
- 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. Implicit in this assumption is the SAN(s) connecting iSCSI and Fiber Channel must be controlled to mitigate potentially malicious attacks on the SAN(s).

# 5 Architectural Information

The TOE is a stand-alone storage system appliance with two management clients that run on a management workstation. Figure 1 below shows the TOE within its operational environment[1]. The TOE storage system is divided into a control plane and a data plane. The control plane provides secure channels for administrator communication, enforces administrator roles, enforces Virtual Domain restrictions, and provides security management functions including access policy management. The data plane provides client hosts with access to storage resources subject to the access policy. The control / data plane separation prevents an administrator from accessing storage resources through a management interface.

[1] The ST excludes product features (for example, Remote Copy, SNMP server, CIM server) and operational environment components (for example, maintenance terminal and syslog server). Figure 1 does not show excluded features and components.

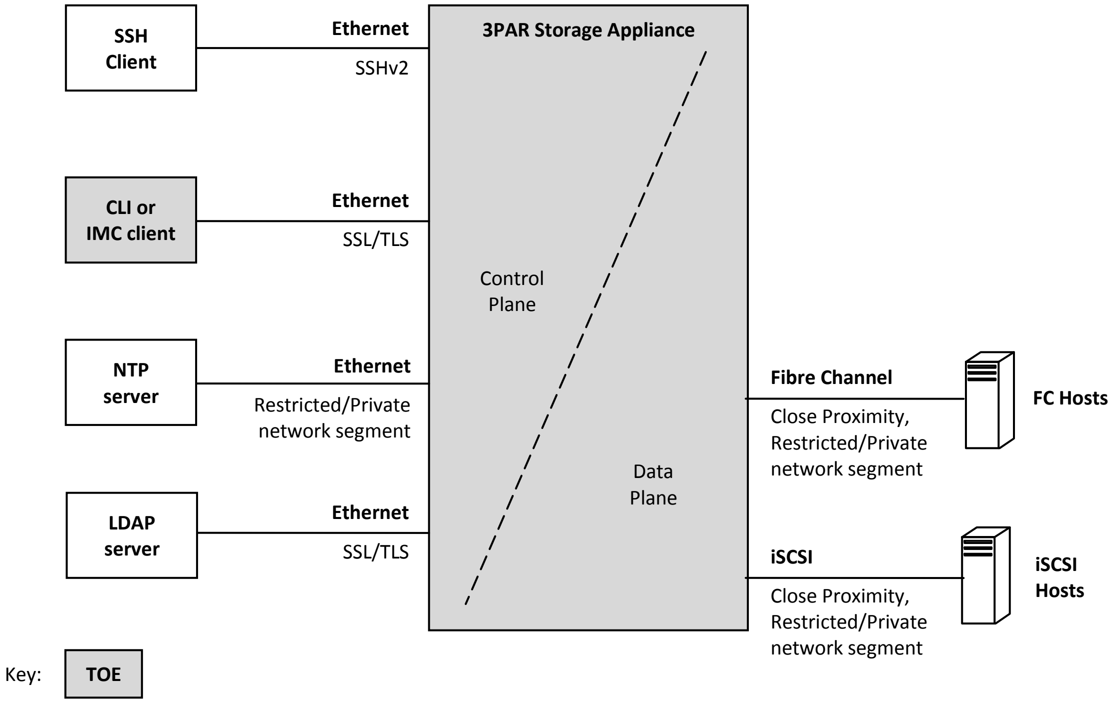

**Figure 1 TOE Architecture**

## 5.1 Physical Boundaries

The physical boundary of an HP 3PAR InServ Storage System is the physical boundary of the hardware. Interfaces to this hardware include iSCSI and Fibre Channel ports for data connections, Ethernet ports for server administration, and a serial port which provides limited administrative access. The following components are included in the TOE:

- InServ Storage Server appliances,
- CLI client, and
- IMC client.

The following additional components are supported in the operational environment:

- Management workstation (supporting SSH, CLI, or IMC client),
- SSH client,
- Network Time Protocol server, and
- Lightweight Directory Access Protocol server.

Please refer to the Security Target for more technical details about the product and its associated security claims and functions.

# 6 Documentation

The following documentation was used as evidence for the evaluation of the HP 3PAR InServ Storage System.

## 6.1 Design Documentation

1. *Hewlett-Packard 3PAR® InServ® Common Criteria Evaluation Development Documentation,* Hewlett-Packard, Revision F, 20 August 2012

## 6.2 Guidance Documentation

1. *HP 3PAR InForm OS Common Criteria Administrator's Reference,* Hewlett-Packard, Part number QL226-96586, August 2012. (Delivered 24 August 2012)
2. *HP 3PAR InForm OS 3.1.1 Concepts Guide,* Hewlett-Packard, Part Number QL226-96555, May 2012
3. *HP 3PAR InForm OS 3.1.1 CLI Administrator's Manual,* Hewlett-Packard, Part Number QL226-96553, May 2012
4. *HP 3PAR InForm OS 3.1.1 Command Line Interface Reference,* Hewlett-Packard, Part Number QL226-96554, June 2012
5. *HP 3PAR InForm Management Console 4.2.1 Software: Users Guide,* Hewlett-Packard, Part Number QL226-96251, November 2011
6. *HP 3PAR Host Explorer 1.1.0 MU1 Software User Guide,* Hewlett-Packard, Part Number QL226-96142, August 2011
7. *HP 3PAR InForm OS 3.1.1 Messages and Operators Guide,* Hewlett-Packard, Part Number QL226-96245, March 2012
8. *HP 3PAR E-Class/F-Class Storage System Physical Planning Manual,* Hewlett-Packard, Part Number QL226-96551, June 2012
9. *HP 3PAR S-Class/T-Class Storage System Physical Planning Manual,* Hewlett-Packard, Part Number QL226-96559, June 2012
10. *HP P10000 3PAR Storage System Physical Planning Manual,* Hewlett-Packard, Part Number QL226-96562, June 2012
11. *HP 3PAR InForm OS 3.1.1 GA/MU1 Release Notes,* Hewlett-Packard, Part Number QL226-96556, June 2012
12. *HP 3PAR InForm OS 3.1.1 GA/MU1 Service Notes,* Hewlett-Packard, Part Number QL226-96557, June 2012

## 6.3 Life-Cycle Documentation

1. *Hewlett-Packard 3PAR® InServ® Life-Cycle Management,* Hewlett-Packard, Revision E, 30 August 2012
2. *Hewlett-Packard 3PAR® InServ® Flaw Remediation Process for Security Defects,* Hewlett-Packard, Revision B, 27 April 2012

## 6.4 Test Documentation

1. *Hewlett-Packard 3PAR InServ Common Criteria Test Overview,* Hewlett-Packard, Version C, 22 June 2012
2. *Test Plan HP 3PAR InServ Storage Systems Common Criteria InForm OS 3.1.1 MU1 CLI; F-Class, T-Class, and V-Class Storage Systems,* Hewlett-Packard, Part Number 245-200045, Version v1.3, 9 August 2012
3. *Raw Test Results HP 3PAR InServ Storage Systems Common Criteria InForm OS 3.1.1 MU1: CLI; F-Class, T-Class, and V-Class Storage Systems,* Hewlett-Packard, Part Number 2045-200047, Version v1.2, 5 August 2012
4. *Test Plan HP 3PAR InServ Storage Systems Common Criteria IMC 4.2.1; InForm OS 3.1.1 MU1 IMC; F-Class, T-Class, and V-Class Storage Systems,* Hewlett-Packard, Part Number 245-200046, Version v3.0, 11 June 2012

# 7 Product Testing

This section describes the testing efforts of the developer and the Evaluation Team. It is derived from information contained in the *Evaluation Technical Report for Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains Part 1*, 1.1, 09/04/2012.

Evaluation team testing was conducted at the vendor’s development site in HP offices in Fremont, CA during the week of 6 August 2012.

## 7.1 Developer Testing

The developer created test procedures specifically to fulfill the test requirements for an EAL 2 augmented with ALC_FLR.2 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.

## 7.2 Evaluation Team Independent Testing

The evaluators received the TOE in the form that normal customers would receive it. HP installed TOE hardware and software. The evaluation team configured the TOE in accordance with the CC Administrator’s Reference. The team exercised a representative subset of the developers test plan on equipment configured in the testing laboratory. Note that the final subset of developer tests exercised during independent testing consisted of manual tests (representing about 20% of the developer tests).

Also, the evaluators devised independent tests. The independent tests were intended to confirm that the TSF correctly enforces it access control policy when duplicate VLUN are defined in distinct domains and to confirm the TSF identifies and authenticates users accessing the TOE via the Maintenance Terminal serial port.

## 7.3 Penetration Testing

In addition to the use of developer provided and independently devised security functional tests, the evaluators also explored the possibility to penetrate or bypass the security mechanisms. Much of this work was based on analysis of the design and actual configuration information derived from the installed and configured products. However, the evaluators also performed scans of the installed products for open ports. The team attempted to use Remote Copy features, which confirmed the features were disabled appropriately in the test configuration.

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 EAL 2 augmented with ALC_FLR.2 are fulfilled.

# 8 Results of the Evaluation

The evaluation was conducted based upon Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009. A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation team assigned a Pass, Fail, or Inconclusive verdict to each work unit of each assurance component. For Fail or Inconclusive work unit verdicts, the evaluation team advised the developer of issues requiring resolution or clarification within the evaluation evidence. 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.

The validation team agreed with the conclusion of the evaluation team, and recommended to CCEVS management that an "EAL 2 augmented with ALC_FLR.2" certificate rating be issued for Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains.

The details of the evaluation are recorded in the *Evaluation Technical Report for Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains* Parts 1 and 2 and the *Evaluation Team Test Report for Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains*, which are controlled by the SAIC CCTL. The security assurance requirements are listed in the following table.

**TOE Security Assurance Requirements**

| Requirement Class | Requirement Component |
|---|---|
| **ADV: Development** | ADV_ARC.1: Security architecture description |
| | ADV_FSP.2: Security-enforcing functional specification |
| | ADV_TDS.1: Basic design |
| **AGD: Guidance documents** | AGD_OPE.1: Operational user guidance |
| | AGD_PRE.1: Preparative procedures |
| **ALC: Life-cycle support** | ALC_CMC.2: Use of a CM system |
| | ALC_CMS.2: Parts of the TOE CM coverage |
| | ALC_DEL.1: Delivery procedures |
| | ALC_FLR.2: Flaw reporting procedures |
| **ATE: Tests** | ATE_COV.1: Evidence of coverage |
| | ATE_FUN.1: Functional testing |
| | ATE_IND.2: Independent testing - sample |
| **AVA: Vulnerability assessment** | AVA_VAN.2: Vulnerability analysis |

# 9 Validator Comments/Recommendations

The TOE was successfully evaluated in the defined evaluated configuration and scope described in sections 9 and 10 of this Validation Report. The validation team recommends certification of the TOE at EAL 2 augmented with ALC_FLR.2.

The following information should be considered by potential consumers or buyers of this product:

- The product consumer or buyer must be aware that the product presumes that the client hosts are non-malicious. The product does not authenticate the client hosts; the client host identity is assumed to be correct. In essence, this is an assumption that the TOE operates in a benign environment; that client hosts do not misrepresent their identities and otherwise act maliciously. If the customer's environment is not consistent with this assumption, then additional protections would need to be implemented to mitigate the risks presented by a potentially malicious client host.

- In the current product, administrators are not warned prior to audit records being overwritten. Based on feedback provided during the evaluation, HP added guidance to administrator documentation that the audit log should be archived on a daily basis. Although the vendor's solution is considered acceptable relative to satisfying the stated requirement, the Validators consider it to be a minimally acceptable solution.

# 10 Annexes

Not applicable.

# 11 Security Target

The ST for this product's evaluation is Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains Security Target, Version 1.0, 10/09/2012.

# 12 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] *Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains Security Target*, Version 1.0, 10/09/2012.

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

[7] *Evaluation Technical Report for Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains Part 1*, version 1.1, 09/04/2012.

[8] *Evaluation Technical Report for Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains Part 2*, version 1.1, 09/04/2012.

[9] *Evaluation Team Test Report for Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains*, version 1.0, 09/04/2012.