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

Version 1.0
10/09/2012

Prepared for:
Hewlett-Packard Development Company, L.P.

11445 Compaq Center Drive West
Houston, Texas 77070

Prepared by:

Science Applications International Corporation

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive, Columbia, Maryland 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is Hewlett-Packard 3PAR InServ Storage Systems provided by Hewlett-Packard 3PAR. 3PAR InServ Storage Systems are physical appliances that primarily serve to host physical disk drives and provide a secure channels to configure the access policy that is enforced between content on the disks and attach storage area network (SAN) hosts. This evaluation includes the T-Class, F-Class and V-Class (also known as P10000) models.

The Security Target contains the following additional sections:

- TOE Description (Section 2)
- Security (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – Hewlett-Packard 3PAR® InServ® Storage Systems with Virtual Domains Security Target

ST Version – Version 1.0

ST Date – 10/09/2012

TOE Identification – The TOE consists of three basic components:

- Hewlett-Packard 3PAR InServ Storage Systems (specific models identified below) running InForm OS (version 3.1.1 .MU1+P16)
  - 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 V-Class or P10000[1] Storage System models V400 and V800
- 3PAR CLI client (version 3.1.1)
- InForm Management Console (version 4.2.1)

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.

The 3PAR Remote Copy feature involves network communication among instances of the TOE that is not protected by the TOE. As such, it is excluded from the scope of evaluation.

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 Security Target *'Hewlett-Packard 3PAR® InServ® Storage Systems Security Target'*.

[1] The terms V-Class and P10000 are synonymous.

Note also that there are a number of 3PAR host-based applications available for use with an InServ Storage System, but 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.

TOE Developer – Hewlett-Packard Company

Evaluation Sponsor – Hewlett-Packard Company

CC Identification – Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 3, July 2009

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- This ST does not conform to any Protection Profiles.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 3, July 2009.
    - Part 2 Extended
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 3, July 2009.
    - Part 3 Conformant
    - Assurance Level: EAL 2 augmented with ALC_FLR.2

Note that while this ST does not conform to any Protection Profile, some content from the Security Requirements for Network Devices, Version 1.0, 10 December 2010 (NDPP) have been adopted. However, the NDPP is primarily designed for network infrastructure devices that are both managed via a connected local area network (LAN) and also offer services related to instantiating a secure network infrastructure. The TOE represented in this ST are storage systems which primarily serve clients on a storage area network (SAN). While it is possible to have a far reaching IP-based SAN, SANs are typically limited in range and access and also require performance levels that are not generally conducive to added layers of transport security. As a result, the NDPP is not generally applicable to the TOE (or perhaps other SAN-based devices).

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that

'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.

- Other sections of the ST – Other sections of the ST use bolding to highlight text of special interest, such as captions.

2. TOE Description

The Target of Evaluation (TOE) is three classes of Hewlett-Packard 3PAR® InServ® Storage Systems along with the 3PAR CLI client and InForm Management Console applications. The storage systems in the evaluated configuration include the T-Class models T400 and T800, the F-Class models F200 and F400, and the V-Class/P10000 models V400 and V800. Each product consists of a set of distinct devices (as identified below) which vary primarily according to storage capacity, performance, and port type and number. The CLI client and Inform Management Console applications can be installed on host computers from which administrators will manage the storage systems and serve to provide access to the available security management functions.

Each appliance primarily consists of drive cages that can accept drive magazines that contain physical disk drives and a backplane that contains slots for controller nodes that provide and manage interfaces available to connect to client hosts and other network entities (e.g., management consoles). Note that each appliance is shipped with a service processor that occupies a physical slot, however it does not have access to any internal data storage resources in the appliance but rather connects to the management side. It is primarily designed to enable remote monitoring and trouble shooting of the appliance where remote monitoring and access (e.g., by 3PAR) are allowable. When configured, the feature effectively allows remote, third-party access to functions supporting problem solving, including access to the appliance configuration. Also, this feature is not part of the normal day-to-day operation of the TOE, souse of the service processor is excluded from the scope of the evaluation. More specifically, the service processor must be disabled (i.e., not configured) while operating the TOE in its evaluated configuration.

Furthermore, the backplane in each appliance is essentially a passive circuit that provides high-speed links between each pair of controller nodes, forming a full-mesh interconnect network within the appliance. This full-mesh interconnect is referred to as the 3PAR InSpire® Architecture with mesh-active controller technology, which effectively enables each installed controller node to directly communicate with every other installed controller node enabling, for example, hosts connected to one controller node to access storage resources connected to any of the controller nodes in the storage system (albeit only after being properly configured and exported as explained below).

	Model T400	Model T800	Model F200	Model F400	Model V400	Model V800
Controller Nodes	2 – 4	2 – 8	2	4	2-4	4-8
FC Host Ports iSCSI Host Ports Remote Copy Ports	0 – 64 0 – 16 2	0 – 128 0 – 32 2	0 – 12 0 – 8 0	0 – 24 0 – 16 0	0-96 0-16 0-8	0-192 0-32 0-8
GBs Control Cache GBs Data Cache	8 – 16 24 – 48	8 – 32 24 – 96	8 12	8 – 16 12 – 24	32-64 64-128	64-128 128-256
Drive Types SSD – Solid State Disk FC – Fiber Channel NL – Nearline	100/200GB SSD 300/600GB FC 1/2TB NL	100/200GB SSD 300/600GB FC 1/2TB NL	100/200GB SSD 300/600GB FC 1/2TB NL	100/200GB SSD 300/600GB FC 1/2TB NL	100/200GB SSD 300/600GB FC 1/2TB NL	100/200GB SSD 300/600GB FC 1/2TB NL
Disk Drives	16 – 640	16 – 1,280	16 – 192	16 – 384	16-960	16-1,920
Max Capacity	400TB	800TB	128TB	384TB	800TB	1,600TB

Table 1 TOE Series and Devices

2.1 TOE Overview

The HP 3PAR InServ Storage Systems are hardware appliances that offer network- and serial-port accessible administration interfaces. The primary service of a storage system is access to data storage resources (e.g., logical representations of physical disk drives) that are accessible via attached Fiber Channel (FC) or Internet SCSI (iSCSI) storage area networks (SANs). While the software employed in the TOE is common across the various TOE classes

and models and they share a common architecture and hence implement the same security functions and policies, they differ in CPUs, memory, disk drive capacity, access ports, and overall performance characteristics.

There are a number of optional features that can be individually licensed for use. Of these features, one – Virtual Domains – is required in the evaluated configuration. The configurations where Virtual Domains are not used are addressed in a separate evaluation. Also, Remote Copy is out of scope of the evaluation since it involves network communication between TOE peers that is not protected by the TOE. Each of the optional features is summarized as follows:

- **3PAR Virtual Domains** are used for access control. Virtual Domains facilitate limiting the privileges of users to only subsets of volumes and hosts in an InServ Storage System and ensures that Virtual Volumes (VVs) associated with a specific domain are not exported to hosts outside of that domain.
- **3PAR Thin Provisioning** supports the allocation of virtual volumes to application servers where only a fraction of the physical storage behind these volumes is provisioned. By enabling a true capacity-on-demand model, a storage administrator can use 3PAR Thin Provisioning to create Thinly-Provisioned Virtual Volumes (TPVVs) that maximize asset use.
- **3PAR Thin Conversion** converts a fully-provisioned volume to a TPVV. Virtual volumes with large amounts of allocated but unused space are converted to TPVVs that are much smaller than the original volume. To use the Thin Conversion feature, a 3PAR Thin Provisioning license and a 3PAR Thin Conversion license are required.
- **3PAR Thin Persistence** keeps InServ TPVVs small by detecting pages of zeros during data transfers and not allocating space for the zeros. This feature works in real-time and analyzes the data before it is written to the destination TPVV. It also allows a host OS to cause a TPVV to shrink (i.e., have real resources deallocated) by writing zeroes to previously allocated pages. To use the Thin Persistence feature, a 3PAR Thin Provisioning license, a 3PAR Thin Conversion license, and a 3PAR Thin Persistence license are required.
- **3PAR Thin Copy Reclamation** reclaims space when snapshots are deleted from an InServ Storage System. As snapshots are deleted, the snapshot space is reclaimed from a TPVV or fully-provisioned virtual volume and returned to the Common Provisioning Group (CPG) – see below – for reuse by other volumes.
- **3PAR Virtual Copy** allows instant virtual copy snapshots of existing volumes to be created. It uses copy-on-write technology so that virtual copies consume minimal capacity. Virtual copies are presentable to any host with read and write capabilities (as distinct virtual volumes). In addition, virtual copies can be made from other virtual copies, providing endless flexibility for test, backup, and business-intelligence applications.
- **3PAR Remote Copy** is a host-independent, array-based data mirroring solution that enables affordable data distribution and disaster recovery for applications. With this optional utility, virtual volumes can be copied from one InServ Storage Server to a second InServ Storage Server (i.e., from one TOE instance to another). Note that this feature involves copying VV data between clusters using dedicated Ethernet ports, however there is no security afforded for communication using those ports – as such the feature is not included in the scope of evaluation since the communication channel would need to be protected by the operational environment.
- **3PAR Dynamic Optimization** allows performance improvement of virtual volumes without interrupting access. Use this feature to avoid over provisioning for peak system usage by optimizing the layout of virtual volumes. With 3PAR Dynamic Optimization virtual volume parameters, RAID levels, set sizes, and disk filters can be changed by associating the virtual volume with a new CPG.
- **3PAR Adaptive Optimization** improves performance by automatically identifying over-used physical disks, and performing load balancing on those disks without interrupting access.
- **3PAR Virtual Lock** enforces the retention period of any volume or copy of a volume.

With the exception of Virtual Domains, each of these features can be optionally licensed and used in the evaluated configuration without any impact to any of the security claims in this Security Target. Virtual Domains, however, is required (i.e., not optional) in the evaluated configuration.

The T-Class, F-Class, and V-Class/P10000 InServ Storage Systems is summarized individually below.

T-Class Storage Systems

With the introduction of the HP 3PAR InServ® T400 and T800 Storage Systems with Thin Built In™, 3PAR incorporates thin capabilities into array hardware. Thin capabilities allow that data storage space can be logically allocated, but real space would be allocated only when they become necessary (i.e., a write operation occurs). Each T-Class Controller Node provides an efficient, silicon-based engine that drives on-the-fly storage optimizations to improve capacity utilization while delivering high service levels. The innovations of the T-Class more than double the performance of the previous generation of InServ arrays to make the T-Class an efficient single-system array. The following components are supported by the T-Class storage systems can be used in any combinations accommodated by the available controller node and drive cage magazine slots available on each appliance:

- HP 3PAR 2.33GHZ T-Class Controller Node
- HP 3PAR 2-Port iSCSI Adapter
- HP 3PAR 4-Port 4Gb Fibre Channel Adapter
- HP 3PAR 4x100GB 4Gb SSD Magazine
- HP 3PAR 4x200GB 4Gb SSD Magazine
- HP 3PAR 4x300GB 15K 4Gb FC LFF Drive Magazine
- HP 3PAR 4x600GB 15K 4Gb FC LFF Drive Magazine
- HP 3PAR 4x1TB 4Gb FC LFF Nearline Drive Magazine
- HP 3PAR 4x2TB 4Gb FC FC LFF Nearline Drive Magazine

F-Class Storage Systems

The 3PAR InServ F-Class offers the same 3PAR InSpire® Architecture, Mesh-Active controller technology, and features as the InServ T-Class—but in a scaled-down system. This means that the InServ F-Class shares the same 3PAR InForm® Operating System and supports all the same advanced software as the other InServ arrays—including 3PAR Thin Provisioning, 3PAR Virtual Domains, 3PAR Dynamic Optimization, 3PAR Virtual Copy, and 3PAR Remote Copy. The following components are supported by the F-Class storage systems can be used in any combinations accommodated by the available controller node and drive cage magazine slots available on each appliance:

- HP 3PAR 2-Port 4Gb F-Class Fibre Channel Adapter
- HP 3PAR 2-Port iSCSI F-Class Adapter
- HP 3PAR 2.33GHz F-Class Controller Node
- HP 3PAR 4x100GB 4Gb SSD Magazine
- HP 3PAR 4x200GB 4Gb SSD Magazine
- HP 3PAR 4x300GB 15K 4Gb FC LFF Single-Drive Magazine
- HP 3PAR 4x600GB 15K 4Gb FC LFF Single-Drive Magazine
- HP 3PAR 4x1TB 4Gb FC LFF Nearline Single-Drive Magazine
- HP 3PAR 4x2TB 4Gb FC FC LFF Nearline Single-Drive Magazine

V-Class/P10000 Storage Systems

The 3PAR InServ V-Class also offers the same 3PAR InSpire® Architecture, Mesh-Active controller technology, and features as the InServ T-Class—but in a scaled up system with more capacity, bandwidth, and FC host connections. It shares that same 3PAR InForm® Operating System and supports all the same advanced software as the other InServ arrays—including 3PAR Thin Provisioning, 3PAR Virtual Domains, 3PAR Dynamic Optimization, 3PAR Virtual Copy, and 3PAR Remote Copy. The following components are supported by the V-Class/P10000

storage systems can be used in any combinations accommodated by the available controller node and drive cage magazine slots available on each appliance:

- HP 3PAR 2.33GHZ V-Class Controller Node
- HP 3PAR 2-Port iSCSI Adapter
- HP 3PAR 4-Port 4Gb Fibre Channel Adapter
- HP 3PAR 4x100GB 4Gb SSD Magazine
- HP 3PAR 4x200GB 4Gb SSD Magazine
- HP 3PAR 4x300GB 15K 4Gb FC LFF Drive Magazine
- HP 3PAR 4x600GB 15K 4Gb FC LFF Drive Magazine
- HP 3PAR 4x1TB 4Gb FC LFF Nearline Drive Magazine
- HP 3PAR 4x2TB 4Gb FC FC LFF Nearline Drive Magazine
- HP 3PAR Upgrade 4x2TB 4Gb FC LFF Nearline Drive Magazine

2.1.1 TOE Architecture

The HP 3PAR InServ Storage System architecture consists of essentially three components – an array of disk units, managed by pairs of controller nodes (to which the disks are directly connected), clustered via a full-mesh backplane interconnect (see Figure 1 InSpire™ Full Mesh Architecture).

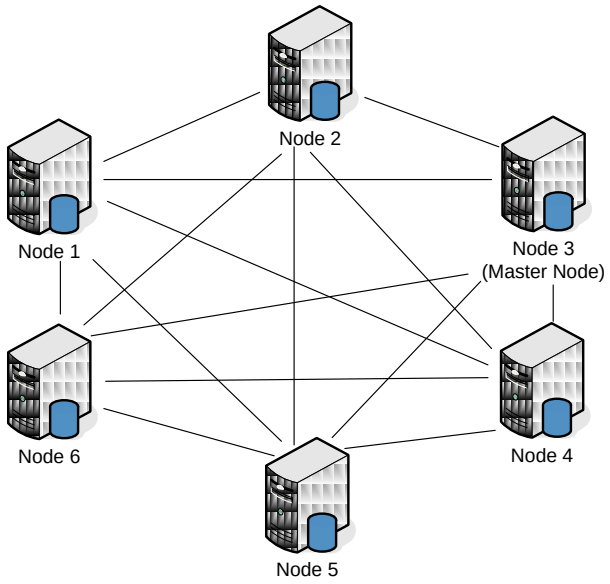

Figure 1 InSpire™ Full Mesh Architecture

The disks are standard Fiber Channel disk drives, Nearline disk drives, and/or Solid State Disks installed in hot-swappable magazines. Controller node pairs manage I/O operations between the installed disks and attached hosts and also facilitate the general operation of the server appliance including security management and logging. While each controller node can operate independently, the available nodes work in pairs to mitigate single node failures and are fully connected with a full-mesh backplane that is essentially a passive circuit board providing pair-wise point-to-point connections between all controller nodes in a given storage system for the purposes of load balancing and cache synchronization and consistency. I/O operations can be originated by any node, but is executed by the pair of nodes to which a given physical disk is connected. Note that some of the storage systems also have IP-based remote copy ports that are used to transfer (i.e., 3PAR Remote Copy) stored data between distinct storage system clusters (e.g., to have remote backups).

Each storage system appliance includes a number of Fiber Channel and Internet SCSI (iSCSI[2]) host ports. These ports can be used to directly connect a number of hosts, connect a number of storage area network (SAN) switches facilitating a very large network of SAN connected hosts, or a combination providing flexibility to support a wide variety of possible deployment environments. Hosts are logically defined and associated with Fiber Channel World Wide Names (WWNs) and/or iSCSI identifiers associated with the Fiber Channel or iSCSI adapters installed in the host.

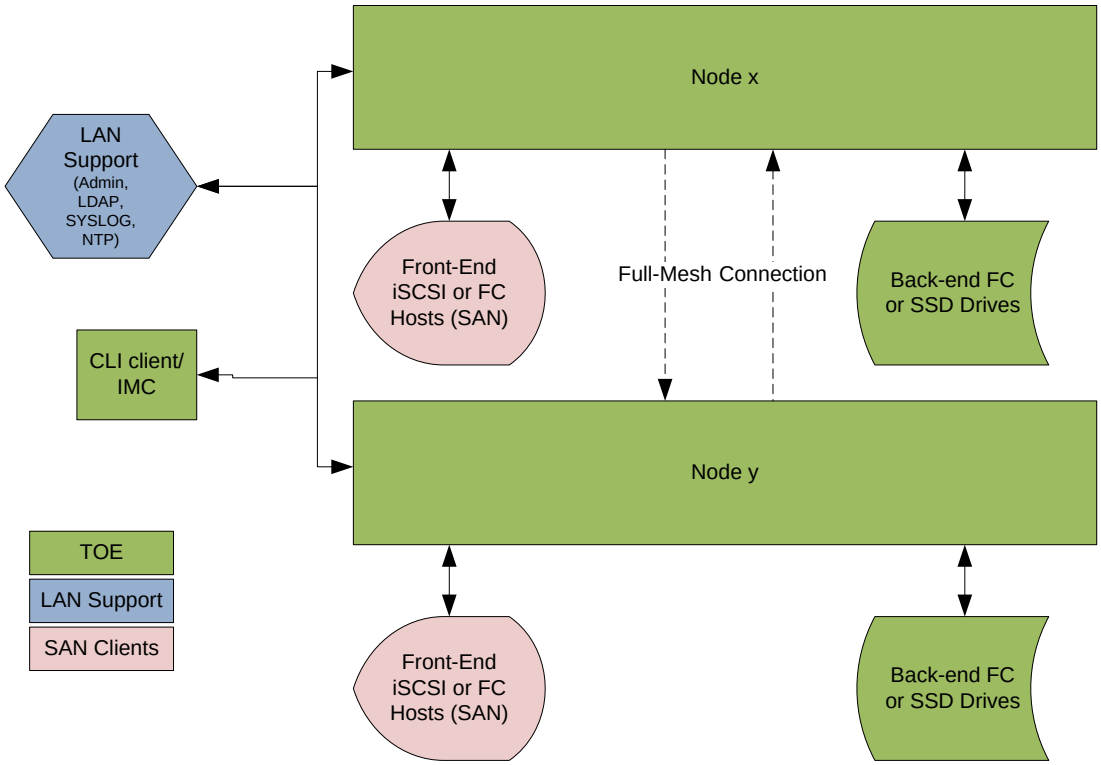

Figure 2 LAN and SAN Connections

It is important to understand that there are two distinct points of view in regard to accessing a storage system node and its resources. Client hosts attach to FC and iSCSI ports the Host Bus Adapters (HBAs) and can perceive only data storage resources that have been configured for host access. Client hosts cannot access or perform any security management of configuration type functions. On the other hand, administrators access storage system nodes via LAN and serial connections from which they can perform security and other manage and service operations, but while they can configure available disk resources for access by client hosts they cannot access the content of those disks. Moreover, even the operating system enabling storage system management doesn't have access to the disk resources that are made available to client hosts; rather, the operating system makes use of proprietary application-specific integrated circuits (ASICs) to move data between HBA data caches and physical disks so the operating system isn't directly involved. This architecture effectively separates the control and data sides of each storage system node.

From a client host point of view, the data resources are available in the form of Virtual Volumes (VVs) identified by Virtual Logical Units (VLUNs). Internally, the physical disks are installed in magazines which are in turn installed into cages of individual nodes and are logically divided into pools of 256MB (1GB in the case of the V-Class/P10000 storage systems) 'chunklets' that are assembled from across available disks into Logical Disks (LDs). Each VV is then built from all or part of a LD or spread across several LDs. Chunklets can be allocated from different cages, magazines, and physical disks to form RAID 0, RAID 10 (mirroring + striping), RAID 50 (RAID 5 + striping), and RAID Multi-parity (aka RAID 6) configurations to form LDs in order to achieve the required levels of availability and fault tolerance.

[2] The iSCSI ports are dedicated Gb Ethernet ports distinct from management Ethernet ports.

From an administrator point of view, in order to create a VV an administrator must first create a Common Provisioning Group (CPG). The CPG identifies an initial space allocation, a growth increment, and a RAID level. Additionally, each CPG includes growth warnings and growth limits. When the size of VVs associated with the CPG reaches the growth warning, an alert is generated so that an administrator can take action to avoid subsequent failure related to CPG exhaustion. When the size of VVs associated with the CPG reaches the growth limit, additional alerts will be generated and write operations that require additional space will fail.

When creating a VV, the administrator identifies the applicable CPG and also whether the VV is a Thinly-Provisioned Virtual Volume (TPVV) or fully provisioned virtual volume. Note that fully-provisioned VVs are allocated their entire space upon creation, while TPVVs are allocated no space upon creation, growing as write operations require more space. There is a third type of VV – administrative VV – which is automatically allocated by the server appliance for exclusive system usage.

Each VV has three data components: User Space, Snapshot Space, and Administrative Space. User Space is the area of the VV that corresponds to the logical disk regions available to configured hosts via the associated VLUN. Snapshot Space (aka Copy Space) is the area of the volume that corresponds to logical disk regions that contain a Virtual Copy or duplicate of a VV (including User Space and/or Snapshot Space, i.e., other copies) by recording changes that have occurred since the previous snapshot, if any, of the copied VV. This corresponds to the 3PAR Virtual Copy feature whereby virtual copies of VVs can be created and stored allowing the 'copied' data to be referenced and changes to be tracked to create a current view of the copied VV using minimal disk resources. These copies can be used for any client host purposes and any changes made to the copies are not reflected back into copied data repositories. Administration Space (aka Admin Space) is the area of the volume that corresponds to the logical disk regions that track changes since the last snapshot was created – it contains pointers to user data in the Snapshot Space. The Administration Space is used exclusively by the system, unlike User Space and Copy Space that can be accessed and populated as a result of host and user actions.

In addition to identifying whether the VV is fully- or thinly-provisioned, the administrator specifies the size of the VV and amount of User Space and Snapshot Space. TPVVs are also defined with warnings and limits. These limits work much the same as CPM warnings and limits, except that they work at the granularity of in individual TPVVs.

Once hosts and VVs are defined, an administrator can define associations so that hosts can access VVs. Access to a VV can be limited to a given host, a group of hosts (i.e., a host set), a given port (i.e., a Host Bus Adapter – HBA – through which hosts connect to the storage system), or a specific host-port combination. When hosts or host sets are identified, it doesn't matter which port the access comes from. When just a port is specified, then any host connected to that port can access the applicable VV. Note that multiple hosts could be connected to a single port when, for example, a SAN switch is connected to the port. However, when a host-port combination is specified then the VV can be access only via the identified host and via the identified port. Note that VV access can be configured to be read-only or read-write and it applies to an entire VV.

With the Virtual Domains feature enabled, up to 1024 domains can be defined in addition to the 'all' domain (which is the only domain when this feature is not present). Users can be assigned up to 32 domains (each with is own user class). CPGs and hosts are each assigned to a specific domain. Assignment to the 'all' domain effectively means they are unassigned and management is limited to users that are not restricted to a specific domain. VVs, LDs, and VLUNs are also implicitly associated with the domain of their associated CPG. When dealing with CPGs (and derived resources – VVs, LDs, and VLUNs) and hosts assigned to a domain, only adminsitrative users assigned to that specific domain or the 'all' domain or unrestricted administrative users can manage those hosts and CPG-derived data resources (such as creating or exporting VVs). Furthermore, VVs in a given domain can be exported only to hosts in the same domain regardless of user class or domain.

2.1.2 TOE Administration

While hosts access VVs via Fiber Channel and iSCSI interfaces, the storage systems also connect to a Local Area Network (LAN) through which administrators can connect and also through which supporting servers (e.g., LDAP, NTP) can be accessed when needed.

Administrators have four options for connecting to the storage system appliances in order to access available administration functions.

- **Maintenance Terminal**: A maintenance terminal can be directly connected to a storage system through an available serial port. This interface provides access to the available command-line (CLI) functions. The maintenance terminal port is intended only for use by authorized service personnel, and is not used by system administrators in the evaluated configuration.
- **SSHv2**: An administrator can connect to a storage system using SSH via a client with SSHv2 support. This interface provides access to the available CLI functions.
- **CLI Client**: 3PAR offers a CLI client that can be installed on a variety of operating systems, identified below. This interface provides a shell that enables an administrator to issue CLI commands on their host workstation and those commands are forwarded to the configured storage system for execution. Communication with storage systems is protected using SSL/TLS.
    - The CLI Client is supported on Sun Solaris 8, 9, and 10; Microsoft Windows XP Professional (SP1, SP2, and SP3), 2003 Server x86 and x64 (SP1 and SP2), Vista Business (SP1 and SP2), 2008 Server x86 and x64 (SP1 and SP2); Redhat Enterprise Linux 5; and, SuSE Enterprise Linux 10.
- **InForm Management Console (IMC)**: 3PAR also offers a graphical user interface (GUI) application that can be installed on a variety of operating systems, identified below. This interface provides a GUI that enables administrators to issue commands to configured storage systems for execution. Note that most management functions are available via this interface, but the CLI does offer some advanced capabilities not available through the IMC. Communication with storage systems is protected using SSL/TLS.
    - The IMC client is supported on Microsoft Windows XP Professional (SP1, SP2, and SP3), 2008 Server x64 (SP1 and SP2) and Windows 7 Professional and Redhat Enterprise Linux 5.

Each interface has its pros and cons leaving administrators to choose which interfaces fit their specific circumstances. In general, a maintenance terminal is not required and is not recommended, but when present is used for initial setup and as a last resort when there is some problem preventing access to the other interfaces. The SSHv2 interface is useful when the administrator does not want to install a special client, for example when they might manage the storage systems from multiple workstations or alternately if they want the most secure network connection (i.e., SSHv2 as opposed to SSL/TLS used by the CLI client and IMC). Note that all of the SSH and SSL/TLS functions are implemented using current OpenSSL/OpenSSH distributions. The CLI client and IMC are useful for management of multiple storage systems as they retain state and local configuration information (e.g., basic information about the available storage systems). However, while the administrator needs to have confidence the SSHv2, CLI client, and IMC applications are trustworthy (e.g., do not include hidden functions that might exploit the administrator's privileges), none of these client applications actually perform any security functions directly.

In all cases, the administrator is required to provide an appropriate username and password (which can be between 6 and 8 characters) or credentials (when using public-key based authentication with SSH) that is verified by a storage system before a connection can be made and commands can be issued. Once logged on and connected, the user's assigned privilege level serves to limit access to the available management functions.

2.1.3 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 list of applicable device classes and models is provided in section 1.1 and additional optional components are identified in section 2.1.

Administrative access to an HP 3PAR InServ Storage System is achieved through use of CLI functions (via the maintenance terminal, SSHv2, or CLI client) or the IMC accessible functions (using the optional IMC client). Access to the administrative interfaces is obtained by either a SSHv2 connection, SSL connections (CLI client or IMC), or via a maintenance terminal attached to the serial connection.

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

- LDAP servers – The TOE can be configured to utilize Active Directory as an external authentication server.

- SYSLOG server – The TOE can be configured to export logs to an external SYSLOG server. However, the use of an external SYSLOG server is out of scope of the evaluation since SYSLOG is not a secure communication protocol and audit records might be disclosed as a result.
- Network Time Protocol (NTP) server – The TOE can be configured to utilize a NTP server to synchronize the internal clock of each individual node.
- FC and iSCSI client hosts – The TOE attaches to FC or iSCSI hosts, which access available storage resources, either directly through available ports or indirectly through a suitable SAN connected to available ports. Note that when connective via a SAN switch, the FC and iSCSI hosts are still individually identified on the TOE ports with their own respective identifiers.
- Management Workstation – An appropriate client (the CLI client or IMC provided by 3PAR or a third party client supporting SSHv2) operating on a suitable workstation is required to utilize the network-accessible administrative interfaces.

Note that communication with NTP and client hosts is not subject to cryptographic protection. Client hosts are attached via dedicated Storage Area Networks that are generally in close proximity and hence subject to the same physical protection assumption as the TOE. NTP communication does not natively support encryption options so it is expect that either that is not a concern in a given operational environment or alternately the servers will be place in close proximity with the TOE like client hosts. LDAP servers can be deployed with or without cryptographic protections depending on the needs of the operational environment.

There are a number of host-based applications available with the HP 3PAR InServ Storage System. These can be freely deployed as they do not perform security relevant operations in regard to the TOE. The most interesting of the available applications is the Host Explorer Agent. This application serves to inform the TOE about the association of Host Bus Adapter identifiers (for iSCSI and Fiber Channel) and hosts. Received information is stored by the TOE to assist in the definition of distinct hosts by authorized administrators.

2.1.4 Logical Boundaries

This section summarizes the security functions provided by HP 3PAR InServ Storage Systems:

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

2.1.4.1 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 can be configured to export audit records to store and protect audit records in local event logs. 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.

2.1.4.2 Cryptographic support

The TOE includes implementations of OpenSSH and OpenSSL to facilitate encrypted communication with remote administrators using SSHv2 clients or the CLI or IMC clients distributed as part of the TOE. The CLI client uses the same cryptography as the TOE (libcrypto.so, as supplied by OpenSSL, statically linked to the client code). The IMC client uses the Java™ Cryptography Extension (JCE) for cryptography.

2.1.4.3 User data protection

The TOE enforces an Access Control policy which controls access to the available Virtual Volume (VV) storage resources. Access to VVs can be limited to Fiber Channel (FC) or Internet SCSI (iSCSI) client hosts based on specific FC or iSCSI ports, specific hosts identified by World Wide Names (WWN) in the case of FC or iSCSI

identifiers, a defined set of hosts, or specific hosts on specific ports. In each case, access to a VV can be either read-write or read-only.

The associated between VVs and hosts and ports is configurable by a user with *super* or *edit* class for an appropriate domain (see section 2.1.4.5 below). Attached hosts cannot access or even perceive any VVs until access is explicitly granted (i.e., the VV is exported for access) by one of the methods identified above.

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

When VVs are thinly provisioned, resources are allocated to the VV as they are needed (e.g., as a result of write operations). Administrators must configure warning and limit levels so that they are notified when a VV is reaching its configured allocation limit. Administrators must also configure a limit level which will also result in a notification, but also at which time additional resources will no be allocated to the VV. These limits serve to bound the resources a given VV can consume, thereby protecting resources needed for other purposes.

2.1.4.4 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. In effect, administrative users can be assigned to the *browse*, *edit*, *service*, or *super* class individually for up to 32 specific domains (i.e., Virtual Domains). The TOE uses these attributes to determine access to available functions (see section 2.1.4.5 below). 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 (i.e., 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 retrieve the administrative user's groups from the LDAP server. The TOE maintains a database of group to user-class and domain mappings and will use these to determine an LDAP-authenticated administrative user's class and domain associations. If there is no mapping (i.e., the user doesn't belong to a mapped group), the TOE will not allow the administrative user to log in. Note that the TOE doesn't provide any functions to manage users defined in the LDAP server, with the exception of mapping groups to user classes and domains.

In addition to administrative users, the TOE identifies client host users using iSCSI identifiers and Fiber Channel World Wide Names (WWNs) but, except when iSCSI Challenge-Handshake Authentication protocol (CHAP) is configured client host users are only identified, are not authenticated.

2.1.4.5 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 assigned domain. Users in the *super* class can perform any functions (e.g., all security functions of the TOE including managing audit events, local user accounts, managing domains and their assignments, and access control) while other users have more limited access though still security relevant.

Administrative users can be assigned up to 32 domains (each with is own user class) utilizing the Virtual Domains licensed component. 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 resources in that domain.

When dealing with CPGs (and derived resources – VVs, LDs, and VLUNs) and client hosts assigned to a domain, only administrative users in the *browse* or *edit* class for that specific domain or the 'all' domain or users in the *super* class can manage those hosts and CPG-derived data resources (such as creating or exporting VVs). Furthermore, VVs in a given domain can be exported only to hosts in the same domain regardless of user class or domain. The resources (e.g., physical disk, chunklets, LDs) that underlay domain-assigned resources such as CPGs are implicitly part of the same domain. Similarly, VVs and VLUNs based on domain-assigned resources are implicitly in the same domain.

In effect virtual domains are used to organize users and resources and to limit the administrative functions users can perform (e.g., to resources within their assigned domains). Hosts do not perceive and are not directly subject to domain constraints, but rather are subject to domain constraints only indirectly in that administrators 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 CLI functions available via a maintenance console, SSHv2 sessions, or the CLI Client or alternately using the IMC client for GUI access to available functions.

Note that the HP 3PAR InServ Storage Systems support Simple Network Management Protocol (SNMP) and also Common Information Model (CIM) management capabilities. However, both are excluded from use in the evaluated configuration. In some cases SNMP is not a securable protocol and CIM is an application level management interface that, while configurable to use SSL/TLS, requires custom built user clients.

2.1.4.6 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 fore most, with the exception of some optional client software, the TOE is a stand alone physical device that 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 (e.g., for log accountability). The TOE can be configured to synchronize time with an external NTP server.

2.1.4.7 Trusted path/channels

The TOE protects interactive communication with remote administrators using SSHv2 (for user-provided SSH clients) or SSL/TLS (for 3PAR-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.

2.2 TOE Documentation

There are numerous documents that provide information and guidance for the deployment of 3PAR InServ Storage Severs. The following documents were specifically examined in the context of the evaluation:

- HP 3PAR InForm® OS 3.1.1 Concepts Guide
- HP 3PAR InForm OS 3.1.1 CLI Administrator's Manual
- HP 3PAR InForm OS 3.1.1 Messages and Operators Guide
- HP 3PAR InForm OS 3.1.1 Command Line Interface Reference
- HP 3PAR InForm Management Console 4.2.1 Software Users Guide
- HP 3PAR InForm OS Common Criteria Administrator’s Reference

3. Security Problem Definition

The Security Problem Definition is specified in this section to specifically identify the threats addressed by storage systems and the assumptions made in so doing.

3.1 Threats

T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms that may go undetected.
T.DATA_DISCLOSURE	A connected host might obtain access to user data for which they have no authorization.
T.DATA_AVAILABILITY	User data may become unavailable due to isolated storage resource failures or due to resource exhaustion.
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.

3.2 Assumptions

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. This also extends to supporting servers (e.g., NTP) and client hosts that are expected to be in close proximity to the TOE.
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. 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).

4. Security Objectives

Like the Security Problem Definition, the Security Objectives have been specified to represent the objectives necessary for a storage system TOE to address its corresponding threats as well as operational environment objectives necessary to fulfill the identified assumptions.

4.1 Security Objectives for the TOE

O.AVAILABILITY	The TOE will ensure that data can be stored in a manner that is protected from underlying resource failure and exhaustion.
O.LIMIT_ACCESS	The TOE will ensure that connected hosts can access only data resources for which they are authorized.
O.PROTECTED_COMMUNICATIONS	The TOE will provide protected communication channels for administrators.
O.RESIDUAL_INFORMATION_CLEARING	The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.
O.SYSTEM_MONITORING	The TOE will provide the capability to generate audit data and provide the means to store and review those data.
O.TOE_ADMINISTRATION	The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and restrict logged-in administrators to authorized functions and TSF data.

4.2 Security Objectives for the Environment

OE.NO_GENERAL_PURPOSE	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.
OE.PHYSICAL	Physical security, commensurate with the value of the TOE and the data it contains, is 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.
OE.TRUSTED_ADMIN	TOE Administrators will be carefully selected to ensure they are trusted and trained to follow and apply all administrator guidance in a trusted manner.

OE.HOST_IDENTITY	iSCSI and Fiber Channel hosts correctly reflect the iSCSI identifier or Fiber Channel World Wide Name (WWN) associated with their Host Bus Adapters (HBAs). Also, the SAN(s) connecting iSCSI and Fiber Channel must be controlled to mitigate potentially malicious attacks on the SAN(s).

5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

Note that while the *Security Requirements for Network Devices, Version 1.0, 10 December 2010* (NDPP) is not claimed and is not fully applicable to storage system type products operating primarily on Storage Area Networks (SANs), a number of SFRs have been adopted from that PP nonetheless. As a result, refinements and operations already performed in that PP are not identified (e.g., highlighted) here, rather the requirements have been copied from that PP and any residual operations have been completed herein. Of particular note, the NDPP made a number of refinements and completed some of the SFR operations defined in the CC and that PP should be consulted to identify those changes if necessary. The applicable NDPP-derived SFRs are italicized in Table 1. The rest of the SFRs are drawn from the Common Criteria (CC) part 2.

The SARs are drawn from the Common Criteria (CC) part 3.

5.1 Extended Requirements

All of the extended requirements in this ST, with the exception of FDP_AVL_EXT.1, have been drawn from the NDPP. The NDPP defines the following extended SFRs and since they are not redefined in this ST, the NDPP should be consulted for more information in regard to those CC extensions.

- FCS_CKM_EXT.4: Cryptographic Key Zeroization
- FCS_COMM_PROT_EXT.1: Communications Protection
- FCS_SSH_EXT.1: Explicit: SSH

  Note that the version of FCS_SSH_EXT.1 is refined in this ST to require additional ciphers and key exchange methods that are supported by the TOE.
- FCS_TLS_EXT.1: Explicit: TLS
- FPT_PTD.1: Management of TSF Data

Note that while the NDPP fails to include any dependency information for the SFRs identified above, applicable dependency information has been determined and identified in *Table 8 Requirement Dependencies* in this Security Target.

FDP_AVL_EXP.1 has been crafted specifically to address availability properties applicable to SAN type TOEs. There are no SFRs in the CC that address the RAID-type reliability or simple warning and l,imit levels for the allocation of underlying resources to support those objects exported for use on a SAN. FDP_AVL_EXT.1 is defined as follows.

5.1.1 Data Availability (FDP_AVL_EXT)

Family Behaviour

This family defines the requirements for the TSF to be able to ensure certain availability properties that serve to address issues associated with failures and exhaustion of resources used to provide user data.

Management: FDP_ AVL_EXT.1

Configuration of available availability parameters could be considered for management functions.

Audit: FDP_ AVL_EXT.1

No audit records, beyond the alerts built into the requirements, are foreseen.

5.1.1.1 User data availability (FDP_AVL_EXT.1)

Hierarchical to: *No other components*
Dependencies: *None*

FDP_ AVL_EXT.1.1 The TSF shall implement the following RAID Disk Data Format levels [***selection: 0, 1, 5, 6, [assignment: other less common levels]***] that comply with the Common RAID Disk Data Format Specification, version 2.0.

Application Note: The intent is that a completed requirement would identify the supported RAID level and that the RAID design should conform to the current version of the Common RAID Disk Data Format Specification published by Storage Network Industry Association (SNIA).

FDP_ AVL_EXT.1.2 The TSF shall be able to generate an alert when a System Administrator configured warning threshold for user data storage is exceeded.

Application Note: The intent is that a warning level can be defined when an alert is generated that would potentially enable an administrator to take action to mitigate resource exhaustion.

FDP_ AVL_EXT.1.3 The TSF shall be able to generate an alert and prevent additional user data storage space allocation when a System Administrator configured limit for user data storage is exceeded.

Application Note: The intent is that an allocation limit can be defined and when that limit is reached an alert is generated and no further allocations are allowed.

5.2 TOE Security Functional Requirements

The following table describes the SFRs that are satisfied by Hewlett-Packard 3PAR® InServ® Storage Systems.

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_CKM_EXT.4: Cryptographic Key Zeroization
	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 signature)
	FCS_COP.1(3): Cryptographic Operation (for cryptographic hashing)
	FCS_COP.1(4): Cryptographic Operation (for keyed-hash message authentication)
	FCS_SSH_EXT.1: Explicit: SSH
	FCS_TLS_EXT.1: Explicit: TLS
FDP: User data protection	FDP_ACC.2 Complete access control
	FDP_ACF.1: Security attribute based access control
	FDP_AVL_EXT.1: User data availability
	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.5: Multiple authentication mechanisms
	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 (for general TSF data)
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Roles
FPT: Protection of the TSF	*FPT_PTD.1: Management of TSF Data (for reading of all symmetric keys)*
	FPT_STM.1: Reliable Time Stamps
FTP: Trusted path/channels	*FTP_TRP.1(1): Trusted Path*
	FTP_TRP.1(2): Trusted Path

Table 2 TOE Security Functional Components

5.2.1 Security audit (FAU)

5.2.1.1 Audit Data Generation (FAU_GEN.1)

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:
a) Start-up and shutdown of the audit functions;
b) All auditable events for the basic level of audit; and
c) All administrative actions;
d) [Specifically defined auditable events listed in **Table 3**].

Application Note: The concept of 'all administrative actions' in this SFR is not intended to include all actions taken by an administrative user, but rather to include only those actions associated with making configuration changes or reviewing potentially sensitive information (e.g., audit records). Otherwise, the concept of an administrator 'browsing' the configuration or non-sensitive TOE data is not necessarily subject to auditing.

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:
a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [information specified in column three of **Table 3**].

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1	None.	
FAU_GEN.2	None.	
FAU_SAR.1	Reading of information from the audit records.	No additional information.
FAU_SAR.3	None.	
FAU_STG.1	None.	
FAU_STG.4	None.	
FCS_CKM.1	Failure on invoking functionality.	No additional information.
FCS_CKM_EXT.4	Failure on invoking functionality.	No additional information.
FCS_COMM_PROT_EXT.1	None.	
FCS_COP.1(1)	Failure on invoking functionality.	No additional information.
FCS_COP.1(2)	Failure on invoking functionality.	No additional information.
FCS_COP.1(3)	Failure on invoking functionality.	No additional information.
FCS_COP.1(4)	Failure on invoking functionality.	No additional information.
FCS_SSH_EXT.1	Failure to establish an SSH session. [3] Establishment/Termination of an SSH session.	Reason for failure Non-TOE endpoint of connection (IP address) for both successes and failures.
FCS_TLS_EXT.1	Failure to establish a TLS Session.[3] Establishment/Termination of a TLS session.	Reason for failure. Non-TOE endpoint of connection (IP address) for both successes and failures.
FDP_ACC.2	None.	
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP.	The identity of the subject performing the operation.
FDP_AVL_EXT.1	None.	
FDP_RIP.2	None.	
FIA_ATD.1	None.	
FIA_UAU.1	All use of the authentication mechanism.	Provided user identity, origin of the attempt (e.g., IP address).
FIA_UAU.5	All use of the authentication mechanism.	Origin of the attempt (e.g., IP address).
FIA_UAU.7	None.	
FIA_UID.2	All use of the user identification mechanism.	The user identity provided.
FMT_MSA.1	All modifications of the values of security attributes.	No additional information.
FMT_MSA.3	Modifications of the default setting of permissive or restrictive rules.	No additional information.

[3] Auditing session establishment failures is highly dependent on the implementation and is currently not standardized in the industry. In this ST, no specific list or types of such failures is mandated as being auditable. More specifically in this case, only user-level authentication actions are necessarily associated with SSH and TLS session establishment failure.

Requirement	Auditable Events	Additional Audit Record Contents
	All modifications of the initial values of security attributes.	
FMT_MTD.1	None.	
FMT_SMF.1	None.	
FMT_SMR.1	None.	
FPT_PTD.1	None.	
FPT_STM.1	Changes to the time.	The old and new values for the time. Origin of the attempt (e.g., IP address).
FTP_TRP.1(1)	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.
FTP_TRP.1(2)	Initiation of the trusted channel. Termination of the trusted channel. Failures of the trusted path functions.	Identification of the claimed user identity.

Table 3 Auditable Events

5.2.1.2 User identity association (FAU_GEN.2)

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

5.2.1.3 Audit Review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**System Administrators**] with the capability to read [**all auditable information**] from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

5.2.1.4 Selectable audit review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to apply [***searching***] of audit data based on [**user identity**].

5.2.1.5 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [***prevent***] unauthorised modifications to the stored audit records in the audit trail.

5.2.1.6 Prevention of audit data loss (FAU_STG.4)

FAU_STG.4.1 The TSF shall [***overwrite the oldest stored audit records***] and [***no other actions***] if the audit trail is full.

5.2.2 Cryptographic support (FCS)

5.2.2.1 Cryptographic Key Generation (FCS_CKM.1)

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**Random Number Generation**] and specified cryptographic key sizes [**128 to 256 bits**] that meet the following: [**FIPS 140-2 Annex C (ANSI X9.31)**].

5.2.2.2 Cryptographic Key Zeroization (FCS_CKM_EXT.4)

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and CSPs when no longer required.

5.2.2.3 Communications Protection (FCS_COMM_PROT_EXT.1)

FCS_COMM_PROT_EXT.1.1 The TSF shall protect communications using [***SSH***] and [***TLS***].

5.2.2.4 Cryptographic Operation (for data encryption/decryption) (FCS_COP.1(1))

FCS_COP.1(1).1 Refinement: The TSF shall perform [encryption and decryption] in accordance with a specified cryptographic algorithm [AES operating in [**CTR and CBC modes**]] and cryptographic key sizes 128-bits, 256-bits, and [***192 bits***] that meets the following:

- FIPS PUB 197, 'Advanced Encryption Standard (AES)'
- [***NIST SP 800-38A***].

5.2.2.5 Cryptographic Operation (for cryptographic signature) (FCS_COP.1(2))

FCS_COP.1(2).1 Refinement: The TSF shall perform cryptographic signature services in accordance with a [***RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 1024bits or greater***] that meets the following:

- [***FIPS PUB 186-2, "Digital Signature Standard"***].

5.2.2.6 Cryptographic Operation (for cryptographic hashing) (FCS_COP.1(3))

FCS_COP.1(3).1 Refinement: The TSF shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm [***SHA-1, SHA-256,***] and message digest sizes [***160, 256***] bits that meet the following: FIPS Pub 180-3, 'Secure Hash Standard.'

5.2.2.7 Cryptographic Operation (for keyed-hash message authentication) (FCS_COP.1(4))

FCS_COP.1(4).1 Refinement: The TSF shall perform [keyed-hash message authentication] in accordance with a specified cryptographic algorithm HMAC-[***SHA-1***], key size [**160 bits**], and message digest sizes [***160***] bits that meet the following: FIPS Pub 198-1, 'The Keyed-Hash Message Authentication Code', and FIPS Pub 180-3, 'Secure Hash Standard.'

5.2.2.8 Explicit: SSH (FCS_SSH_EXT.1)

FCS_SSH_EXT.1.1 The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH connection be rekeyed after no more than 2^{28} packets have been transmitted using that key.

FCS_SSH_EXT.1.3 The TSF shall ensure that the SSH protocol implements a timeout period for authentication as defined in RFC 4252 of [**600 seconds**], and provide a limit to the number of failed authentication attempts a client may perform in a single session to [**6**] attempts.

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.5 The TSF shall ensure that, as described in RFC 4253, packets greater than [**35000**] bytes in an SSH transport connection are dropped.

FCS_SSH_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, **AES-CBC-192, AES-128-CTR, AES-192-CTR, and AES-256-CTR**.

FCS_SSH_EXT.1.7 The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [***no other public key algorithms***] as its public key algorithm(s).

FCS_SSH_EXT.1.8 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [***hmac-sha1, hmac-sha1-96***].

FCS_SSH_EXT.1.9 The TSF shall ensure that **diffie-hellman-group1-sha1,** diffie-hellman-group14-sha1**, diffie-hellman-group-exchange-sha1, and diffie-hellman-group-exchange-sha256 are** the only allowed key exchange methods used for the SSH protocol.

Application Note: Note that the TOE supports many more ciphers both for SSH and TLS, below, but they are not identified here since they are not FIPS approved. However, they are present in the TOE for compatibility reasons. In

general, administrators of the TOE should use clients that implement strong ciphers and key exchange methods so that those will be negotiated and used in practice. Note also that the implementation supports the use of DSA keys, while TOE guidance recommends the use of RSA keys for authentication.

5.2.2.9 Explicit: TLS (FCS_TLS_EXT.1)

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [***TLS 1.0 (RFC 2246)***] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA

Optional Ciphersuites:

[***none***].

Application Note: While multiple ciphers are supported by the server, in practice the CLI uses only TLS_RSA_WITH_AES_256_CBC_SHA and the IMC uses only TLS_RSA_WITH_AES_128_CBC_SHA.

5.2.3 User data protection (FDP)

5.2.3.1 Complete access control (FDP_ACC.2)

FDP_ACC.2.1 The TSF shall enforce the [**Access Control policy**] on [

- **subjects: Fiber Channel and iSCSI hosts,**
- **objects: Virtual Volumes]** and
- all operations among subjects and objects covered by the SFP.

FDP_ACC.2.2 The TSF shall ensure that all operations between any subject controlled by the TSF and any object controlled by the TSF are covered by an access control SFP.

5.2.3.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [**Access Control policy**] to objects based on the following:

- [**Subjects:**
  - **Fiber Channel and iSCSI hosts: host identifier and port identifier**
- **Objects:**
  - **Virtual Volume: Virtual Logical Unit (VLUN) and associated access (host sees, host set, port presents, or matched set)**].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a) if a VLUN is configured for 'host sees' access, only hosts with a matching host identifier can access the Virtual Volume as specified in the configuration;

b) if a VLUN is configured for 'host set' access, only hosts within the configured host set can access the Virtual Volume as specified in the configuration;

c) if a VLUN is configured for 'port presents' access, only hosts accessing the TOE via a port with a matching port identifier can access the Virtual Volume as specified in the configuration;

d) if a VLUN is configured for 'matched set' access, only hosts accessing the TOE via a port with a matching port identifier and with a matching host identifier can access the Virtual Volume as specified in the configuration].

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**no additional explicit allow rules**].

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the [**no additional explicit denial rules**].

5.2.3.3 User data availability (FDP_AVL_EXT.1)

FDP_ AVL_EXT.1.1 The TSF shall implement the following RAID Disk Data Format levels [***0, 1, 5, 6***] that comply with the Common RAID Disk Data Format Specification, version 2.0.

FDP_ AVL_EXT.1.2 The TSF shall be able to generate an alert when a System Administrator configured warning threshold for user data storage is exceeded.

FDP_ AVL_EXT.1.3 The TSF shall be able to generate an alert and prevent additional user data storage space allocation when a System Administrator configured limit for user data storage is exceeded.

5.2.3.4 Full Residual Information Protection (FDP_RIP.2)

FDP_RIP.2.1 The TSF shall ensure that any previous information content of a resource is made unavailable upon the [***allocation of the resource to***] all objects.

5.2.4 Identification and authentication (FIA)

5.2.4.1 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users: [**user identity, domain, class, password, and optionally a public key**].

Application Note: The term 'individual users' in this SFR is used to refer to administrative users as opposed to client hosts. The TOE maintains definitions only of administrative users while client host identities come from the hosts themselves and as such, though they are used, they are not defined within the TOE.

5.2.4.2 Timing of authentication (FIA_UAU.1)

FIA_UAU.1.1 The TSF shall allow [**host access to virtual volumes in accordance with the Access Control Policy**] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

5.2.4.3 Multiple authentication mechanisms (FIA_UAU.5)

FIA_UAU.5.1 The TSF shall provide [**local password-based and public key authentication mechanisms and access to an external LDAP server**] to support user authentication.

FIA_UAU.5.2 The TSF shall authenticate any user's claimed identity according to the [**local authentication mechanism – public key authentication when using SSHv2 and the user has a configured public key, otherwise via password authentication - if the user is defined there, otherwise the LDAP server will be consulted**].

5.2.4.4 Protected Authentication Feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only obscured feedback to the user while the authentication is in progress at the local console.

5.2.4.5 User identification before any action (FIA_UID.2)

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.2.5 Security management (FMT)

5.2.5.1 Management of security attributes (FMT_MSA.1)

FMT_MSA.1.1 The TSF shall enforce the [**Access Control policy**] to restrict the ability to [***manage***] **all** the security attributes to [**System Administrators in the domain of the protected object**].

5.2.5.2 Static attribute initialization (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the [**Access Control policy**] to provide [**restricted**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**System Administrators in the domain of the protected object**] to specify alternative initial values to override the default values when an object or information is created.

Application Note: The TOE does not support an explicit notion of default values, rather by implicit default when a new resource becomes available no access is possible until it is exported at which time explicit access rights to a host, set of hosts, port or some combination can be granted.

5.2.5.3 Management of TSF Data (for general TSF data) (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to manage the TSF data to the System Administrators.

5.2.5.4 Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [

- **Ability to review audit events;**
- **Ability to manage user accounts including domain assignments; and**
- **Ability to manage Virtual Volume access including management of associated hosts and Virtual Volume availability options and domain settings**].

5.2.5.5 Security Roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles: [System Administrator, [***[users assigned to user class of browse, edit, super, service, Create, Basic Edit, 3PAR AO, and 3PAR RM]***]].[4]

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.6 Protection of the TSF (FPT)

5.2.6.1 Management of TSF Data (for reading of all symmetric keys) (FPT_PTD.1)

FPT_PTD.1.1 Refinement: The TSF shall prevent reading of all pre-shared keys, symmetric key, and private keys.

5.2.6.2 Reliable Time Stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.2.7 Trusted path/channels (FTP)

5.2.7.1 Trusted Path (FTP_TRP.1(1))

FTP_TRP.1(1).1 Refinement: The TSF shall provide a communication path between itself and remote administrators using [**SSH or TLS**] that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from disclosure.

FTP_TRP.1(1).2 The TSF shall permit remote administrators to initiate communication via the trusted path.

FTP_TRP.1(1).3 Refinement: The TSF shall require the use of the trusted path for all remote administrative actions.

[4] Note that the 'System Administrator' role encompasses all users since users of each class can perform some set of security relevant management functions.

5.2.7.2 Trusted Path (FTP_TRP.1(2))

FTP_TRP.1(2).1	Refinement: The TSF shall provide a communication path between itself and remote administrators using [**SSH or TLS**] that is logically distinct from other communication paths and provides assured identification of its end points and detection of modification of the communicated data.
FTP_TRP.1(2).2	The TSF shall permit remote administrators to initiate communication via the trusted path.
FTP_TRP.1(2).3	Refinement: The TSF shall require the use of the trusted path for all remote administrative actions.

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are the EAL 2 augmented with ALC_FLR.2 components as specified in Part 3 of the Common Criteria.

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

Table 4 EAL 2 augmented with ALC_FLR.2 Assurance Components

5.3.1 Development (ADV)

5.3.1.1 Security architecture description (ADV_ARC.1)

ADV_ARC.1.1d The developer shall design and implement the TOE so that the security features of the TSF cannot be bypassed.

ADV_ARC.1.2d The developer shall design and implement the TSF so that it is able to protect itself from tampering by untrusted active entities.

ADV_ARC.1.3d The developer shall provide a security architecture description of the TSF.

ADV_ARC.1.1c The security architecture description shall be at a level of detail commensurate with the description of the SFR-enforcing abstractions described in the TOE design document.

ADV_ARC.1.2c The security architecture description shall describe the security domains maintained by the TSF consistently with the SFRs.

ADV_ARC.1.3c The security architecture description shall describe how the TSF initialisation process is secure.

ADV_ARC.1.4c The security architecture description shall demonstrate that the TSF protects itself from tampering.

ADV_ARC.1.5c The security architecture description shall demonstrate that the TSF prevents bypass of the SFR-enforcing functionality.

ADV_ARC.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.1.2 Security-enforcing functional specification (ADV_FSP.2)

ADV_FSP.2.1d The developer shall provide a functional specification.

ADV_FSP.2.2d The developer shall provide a tracing from the functional specification to the SFRs.

ADV_FSP.2.1c The functional specification shall completely represent the TSF.

ADV_FSP.2.2c The functional specification shall describe the purpose and method of use for all TSFI.

ADV_FSP.2.3c The functional specification shall identify and describe all parameters associated with each TSFI.

ADV_FSP.2.4c For each SFR-enforcing TSFI, the functional specification shall describe the SFR-enforcing actions associated with the TSFI.

ADV_FSP.2.5c For each SFR-enforcing TSFI, the functional specification shall describe direct error messages resulting from processing associated with the SFR-enforcing actions.

ADV_FSP.2.6c The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

ADV_FSP.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_FSP.2.2e The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

5.3.1.3 Basic design (ADV_TDS.1)

ADV_TDS.1.1d The developer shall provide the design of the TOE.
ADV_TDS.1.2d The developer shall provide a mapping from the TSFI of the functional specification to the lowest level of decomposition available in the TOE design.
ADV_TDS.1.1c The design shall describe the structure of the TOE in terms of subsystems.
ADV_TDS.1.2c The design shall identify all subsystems of the TSF.
ADV_TDS.1.3c The design shall describe the behaviour of each SFR-supporting or SFR-non-interfering TSF subsystem in sufficient detail to determine that it is not SFR-enforcing.
ADV_TDS.1.4c The design shall summarise the SFR-enforcing behaviour of the SFR-enforcing subsystems.
ADV_TDS.1.5c The design shall provide a description of the interactions among SFR-enforcing subsystems of the TSF, and between the SFR-enforcing subsystems of the TSF and other subsystems of the TSF.
ADV_TDS.1.6c The mapping shall demonstrate that all TSFIs trace to the behaviour described in the TOE design that they invoke.
ADV_TDS.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ADV_TDS.1.2e The evaluator shall determine that the design is an accurate and complete instantiation of all security functional requirements.

5.3.2 Guidance documents (AGD)

5.3.2.1 Operational user guidance (AGD_OPE.1)

AGD_OPE.1.1d The developer shall provide operational user guidance.
AGD_OPE.1.1c The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.
AGD_OPE.1.2c The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.
AGD_OPE.1.3c The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.
AGD_OPE.1.4c The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.
AGD_OPE.1.5c The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.
AGD_OPE.1.6c The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfil the security objectives for the operational environment as described in the ST.
AGD_OPE.1.7c The operational user guidance shall be clear and reasonable.
AGD_OPE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.2.2 Preparative procedures (AGD_PRE.1)

AGD_PRE.1.1d The developer shall provide the TOE including its preparative procedures.
AGD_PRE.1.1c The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_PRE.1.2c The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.
AGD_PRE.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AGD_PRE.1.2e The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

5.3.3 Life-cycle support (ALC)

5.3.3.1 Use of a CM system (ALC_CMC.2)

ALC_CMC.2.1d The developer shall provide the TOE and a reference for the TOE.
ALC_CMC.2.2d The developer shall provide the CM documentation.
ALC_CMC.2.3d The developer shall use a CM system.
ALC_CMC.2.1c The TOE shall be labeled with its unique reference.
ALC_CMC.2.2c The CM documentation shall describe the method used to uniquely identify the configuration items.
ALC_CMC.2.3c The CM system shall uniquely identify all configuration items.
ALC_CMC.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.2 Parts of the TOE CM coverage (ALC_CMS.2)

ALC_CMS.2.1d The developer shall provide a configuration list for the TOE.
ALC_CMS.2.1c The configuration list shall include the following: the TOE itself; the evaluation evidence required by the SARs; and the parts that comprise the TOE.
ALC_CMS.2.2c The configuration list shall uniquely identify the configuration items.
ALC_CMS.2.3c For each TSF relevant configuration item, the configuration list shall indicate the developer of the item.
ALC_CMS.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.3 Delivery procedures (ALC_DEL.1)

ALC_DEL.1.1d The developer shall document and provide procedures for delivery of the TOE or parts of it to the consumer.
ALC_DEL.1.2d The developer shall use the delivery procedures.
ALC_DEL.1.1c The delivery documentation shall describe all procedures that are necessary to maintain security when distributing versions of the TOE to the consumer.
ALC_DEL.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.3.4 Flaw reporting procedures (ALC_FLR.2)

ALC_FLR.2.1d The developer shall document and provide flaw remediation procedures addressed to TOE developers.
ALC_FLR.2.2d The developer shall establish a procedure for accepting and acting upon all reports of security flaws and requests for corrections to those flaws.
ALC_FLR.2.3d The developer shall provide flaw remediation guidance addressed to TOE users.
ALC_FLR.2.1c The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.2.2c The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.
ALC_FLR.2.3c The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.2.4c The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

ALC_FLR.2.5c The flaw remediation procedures shall describe a means by which the developer receives from TOE users reports and enquiries of suspected security flaws in the TOE.
ALC_FLR.2.6c The procedures for processing reported security flaws shall ensure that any reported flaws are remediated and the remediation procedures issued to TOE users.
ALC_FLR.2.7c The procedures for processing reported security flaws shall provide safeguards that any corrections to these security flaws do not introduce any new flaws.
ALC_FLR.2.8c The flaw remediation guidance shall describe a means by which TOE users report to the developer any suspected security flaws in the TOE.
ALC_FLR.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4 Tests (ATE)

5.3.4.1 Evidence of coverage (ATE_COV.1)

ATE_COV.1.1d The developer shall provide evidence of the test coverage.
ATE_COV.1.1c The evidence of the test coverage shall show the correspondence between the tests in the test documentation and the TSFIs in the functional specification.
ATE_COV.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.2 Functional testing (ATE_FUN.1)

ATE_FUN.1.1d The developer shall test the TSF and document the results.
ATE_FUN.1.2d The developer shall provide test documentation.
ATE_FUN.1.1c The test documentation shall consist of test plans, expected test results and actual test results.
ATE_FUN.1.2c The test plans shall identify the tests to be performed and describe the scenarios for performing each test. These scenarios shall include any ordering dependencies on the results of other tests.
ATE_FUN.1.3c The expected test results shall show the anticipated outputs from a successful execution of the tests.
ATE_FUN.1.4c The actual test results shall be consistent with the expected test results.
ATE_FUN.1.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

5.3.4.3 Independent testing - sample (ATE_IND.2)

ATE_IND.2.1d The developer shall provide the TOE for testing.
ATE_IND.2.1c The TOE shall be suitable for testing.
ATE_IND.2.2c The developer shall provide an equivalent set of resources to those that were used in the developer's functional testing of the TSF.
ATE_IND.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
ATE_IND.2.2e The evaluator shall execute a sample of tests in the test documentation to verify the developer test results.
ATE_IND.2.3e The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

5.3.5 Vulnerability assessment (AVA)

5.3.5.1 Vulnerability analysis (AVA_VAN.2)

AVA_VAN.2.1d The developer shall provide the TOE for testing.
AVA_VAN.2.1c The TOE shall be suitable for testing.
AVA_VAN.2.1e The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.
AVA_VAN.2.2e The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.2.3e The evaluator shall perform an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design and security architecture description to identify potential vulnerabilities in the TOE.

AVA_VAN.2.4e The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

6. TOE Summary Specification

This chapter describes the security functions:

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

6.1 Security audit

The TOE is designed to be able to generate log records for a wide range of security relevant and other events as they occur. The events that can cause an audit record to be logged include starting and stopping the audit function, any use of an administrator command (including review of audit records, but excluding general 'browsing' which is not considered security relevant when configuration changes are not made and sensitive TSF data is not access – see "Browse" in section 6.5) via the various CLI and IMC interfaces, as well as all of the events identified in Table 3.

In general, the logged audit records identify the date and time, the nature or type of the triggering event, an indication of whether the event succeeded, failed or had some other outcome, and the identity of the agent (e.g., user or network host) responsible for the event. The logged audit records also include event-specific content that includes at least all of the content required in Table 3.

The TOE includes an internal log implementation that can be used to store and review audit records locally.

Locally stored audit records can be viewed and searched using regular expressions by a user with the *super* or *browse* class via both the CLI and IMC interfaces. There are no interfaces/functions that facilitate the clearing or modification of stored records.

Should the available space for audit logs become exhausted, the oldest log file will be overwritten as necessary to accommodate recording new records.

The Security audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: The TOE can generate audit records for events include starting and stopping the audit function, administrator commands, and all other events identified in **Table 3**. Furthermore, each audit record identifies the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in **Table 3**.
- FAU_GEN.2: The TOE identifies the responsible user for each event based on the specific administrator or host (identified by host identifier) that caused the event.
- FAU_SAR.1: The TOE provides CLI and IMC interfaces to review its internal audit log.
- FAU_SAR.3: The TOE audit review functions include the ability to search the stored audit logs using regular expressions so that, for example, records resulting from specific user actions can be readily identified.
- FAU_STG.1: The TOE doesn't provide the ability to clear the audit log and similarly doesn't provide any functions that allow modification of stored audit records.
- FAU_STG.4: The TOE will automatically overwrite the oldest audit log records with new records as necessary.

6.2 Cryptographic support

The TOE utilizes an implementation of OpenSSL and OpenSSH to perform its cryptographic operations. These operations include creating symmetric encryption session keys between 128 and 256 bits as well as the zeroization of secret and private keys when they are no longer required by the TOE. The cryptographic operations have been subject to FIPS algorithm verification as follows:

Function	Standard	Certificate
Encryption/Decryption		
• AES CTR and CBC (128-256 bits)	FIPS PUB 197 NIST SP 800-38A	#1929 (libgcrypt) #2147 (libcrypto) #2145 (Java JCE)
Cryptographic signature services		
• RSA Digital Signature Algorithm (rDSA) (modulus 1024 and 2048)	FIPS PUB 186-2	#995 (libgcrypt) #1104 (libcrypto) #1103 (Java JCE)
Cryptographic hashing		
• SHA-1 and SHA-256 (digest sizes 160, 256)	FIPS Pub 180-3	#1694 (libgcrypt) #1868 (libcrypto) #1867 (Java JCE)
Keyed-hash message authentication		
• HMAC-SHA-1 (digest size 160 bits)	FIPS Pub 198-1 FIPS Pub 180-3	#1163 (libcgrypt) #1314 (libcrypto) #1312 (Java JCE)

Table 5 Cryptographic Functions

Random numbers used to create cryptographic keys are generated using two libraries *librcypto (*the OpenSSL Pseudo Random Number Generator) as well as *libgcrypt* (an open source Continuously Seeded Pseudo Random Number Generator implementation), both of which use the debian */dev/urandom* entropy source. Random number generation in both cases is done in accordance with ANSI X9.31.

Similarly, key zeroization occurs within the *libcrypto* and *libgcrypt* libraries. *libcrypto* zeroizes keys used as session keys in securing SSL channels using the OPENSSL_cleanse() routine, which does a single-pass overwrite of the data area using pseudo random data based on the memory address of the storage area prior to freeing the storage. Keys are destroyed when no longer used and the storage is freed at that time. gnuTLS uses the libcrypt secure memory pool for session keys. *libgcrypt* uses a four-pass overwite with a pattern of 0xff, 0xaa, 0x55, 0x00, on each byte of secure memory area prior to releasing it back into the secure memory pool. Keys are destroyed/freed when no longer needed. Note that the *libcrypto* and *libgcrypt* implementations are unmodified by HP.

The primary cryptographic functions are related to SSH and SSL/TLS which are used to encrypt remote administrator sessions. Those operations involve AES encryption and decryption using CTR and CBC modes with 128, 192, and 256 bit keys as well as SHA-1, SHA-256, and HMAC-SHA-1 hashing and keyed hashing.

These supporting cryptographic functions are included to support the SSHv2 (RFCs 4251, 4252, 4253, and 4254) and TLSv1 (RFC 2246) secure communication protocols. *Note that SSHv1and SSLv1ares not enabled, but the TOE supports SSLv2 and SSLv3 and will connect to clients requesting those protocols, but they are not recommended since they are not as secure.*

The TOE supports TLSv1 with AES (CBC and CTR) 128, 192, or 256 bit ciphers, in conjunction with SHA-1, and RSA. The following cipher suites are implemented by the TOE:

- TLS_RSA_WITH_AES_128_CBC_SHA,
- TLS_RSA_WITH_AES_256_CBC_SHA,
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA, and
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA.

Note that while multiple ciphers are supported by the server, in practice the CLI uses only TLS_RSA_WITH_AES_256_CBC_SHA and the IMC uses only TLS_RSA_WITH_AES_128_CBC_SHA.

The TOE supports SSHv2 with AES (CBC and CTR) 128, 192, or 256 bit ciphers, in conjunction with HMAC-SHA-1 or HMAC-SHA-1-96, and RSA (with diffie-hellman-group1-sha1, diffie-hellman-group14-sha1, diffie-hellman-group-exchange-sha1, or diffie-hellman-group-exchange-sha256 for the key exchange method). SSHv2 connections are rekeyed prior to reaching 2^{28} packets; the authentication timeout period is 600 seconds allowing clients to retry only 6 times; both public-key and password based authentication can be configured; and packets are limited to 35000 bytes.

Note that the TOE supports many other ciphersuites for both SSH and TLS as provided by the OpenSSL and OpenSSH libraries for compatibility reasons. However, they are not identified here since they are not FIPS approved algorithms.

The Cryptographic support function is designed to satisfy the following security functional requirements:

- FCS_CKM.1: The TOE uses random number generation to create keys between 128 and 256 b its in length.
- FCS_CKM_EXT.4: The TOE performs immediate (i.e., when no longer needed) and complete (i.e., the entire key or parameter) zeroization of plaintext cryptographic keys and security parameters.
- FCS_COMM_PROT_EXT.1: The TOE provides SSH, and TLS in support of secure administrator session protection.
- FCS_COP.1(1): The TOE implements AES with CTR and CBC modes and 128, 192, and 256 bit keys sizes.
- FCS_COP.1(2): The TOE implements the RSA Digital Signature Algorithm with a key size (modulus) including 1024 and greater bits.
- FCS_COP.1(3): The TOE implements SHA-1 cryptographic hashes.
- FCS_COP.1(4): The TOE implements HMAC-SHA-1 keyed-hash message authentication.
- FCS_SSH_EXT.1: The TOE supports SSHv2 interactive command-line secure administrator sessions as indicated above.
- FCS_TLS_EXT.1: The TOE supports TLSv1secure administrator sessions.

6.3 User data protection

As summarized in section 2.1.1 the TOE implements Virtual Volumes based on underlying logical and physical resources. Virtual Volumes are identified by Virtual Logical Units (VLUNs) used by hosts to identify Virtual Volumes to which they have access.

Hosts are defined within the TOE and are associated with host identifiers – World Wide Names (WWNs) in the case of Fiber Channel hosts and iSCSI identifiers for iSCSI hosts. To assist administrators in defining hosts, the TOE can report host identifiers that have been encountered but are not associated with a current host definition and also there is a host-based application – the Host Explorer Agent – that reports information to the TOE corresponding a given actual host and the identifiers associated with its Host Bus Adapters (HBAs).

Hosts can be grouped into host sets associated with a given VLUN. Additionally, hosts access the TOE through specific Fiber Channel or iSCSI ports.

Users with the *super* or *edit* class can define access to Virtual Volumes identified by VLUN in the following four ways:

- **Host Sees**: The TOE makes the Virtual Volume visible via its VLUN to specifically identified hosts. The port used by the host is irrelevant.
- **Host Set**: The TOE makes the Virtual Volume visible via its VLUN to all members of an identified host set. Any hosts added to the host set would automatically obtain access to the associated Virtual Volume. Similarly, a removed host loses access. The port used by the host is irrelevant.
- **Port Presents**: The TOE makes the Virtual Volume visible via its VLUN to all hosts connected to a particular port. The host identifier and any host sets are irrelevant.

- **Matched Set**: The TOE makes the Virtual Volume visible via its VLUN to a particular host on a particular port.

In each case, when a Virtual Volume is visible to a host, it will be accessible though in some cases the access is further restricted to read-only access (e.g., when a read-only snapshot is exported). Also, Virtual Volumes that are not 'visible' to hosts cannot be accessed in any way. Hence, other than attempting to violate a read-only restriction, a given host cannot attempt to access an unauthorized Virtual Volume – there are simply no mechanics for that. However, a given host can query the available Virtual Volumes and the result will be consistent with these access rules.

As summarized in section 2.1.1, physical disks are divided into chunklets which form the basis of Logical Disks, Common Provisioning Groups (CPGs), and ultimately Virtual Volumes. Internally, if a chunklet is returned to the available chunklet pool is it zeroed by the TOE. When a chunklet is allocated for a new use – either when a fully provisions Virtual Volume is created or a thinly-provisioned Virtual Volume requires more space – that newly allocated space is also zeroed prior to any read or write operation. The TOE also makes use of data caches and implements a strict write-before-read policy for access to the cache and the TOE is designed to ensure that cache requests correspond to their represented media before allowing read access to the data therein. When a disk is marked as failed the TOE attempts to write zeroes to all the chunklets. Obviously, that might not be 100% effective. HP offers customers the option of disposing of failed media, as opposed to returning it to mitigate data disclosure concerns.

When CPGs are created by a user with the super or edit class, that user can identify whether the CPG should utilize a RAID 0, 1, 5, or 6 fault tolerance configuration as well as whether fault tolerance (i.e., parity) should be on the granularity of a disk drive, drive magazine, drive cage, or controller node. Additionally, the user must define warning and limit levels for the CPG. As the CPG resources are allocated to one or more VVs, if the configured warning level is reached an alert is generated in the form of a log indicating that the level has been reached and perhaps some remedial action should be taken. Furthermore, if CPG resources are allocated to its limit level an alert will be generated and no more resources can be allocated and applicable write operations will fail.

In addition, when a Thinly Provisioned VV (TPVV) is created by a user with the super or edit class, warning and limit levels must also be configured for the TPVV. As with CPGs, when the resources allocated to the TPVV reach the warning level, an alert is issued and when resources allocated to the TPVV reach the limit level an alert is issued and write operations will fail since no further resources will be allocated to the TPVV.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.2: The TOE controls all operations between attached host clients and Virtual Volumes.
- FDP_ACF.1: The TOE enforces access control rules to determine whether attached hosts can access (read-only or read-write) configured Virtual Volumes as described above.
- FDP_AVL_EXT.1: The TOE allows CPGs to be configured in RAID 0, 1, 5, and 6 configurations and both CPGs and VVs are configured with warning and limit levels as described above.
- FDP_RIP.2: The TOE is designed to ensure that residual information will be cleared prior to any potential access when underlying resources are reallocated between user accessible objects (i.e., Virtual Volumes).

6.4 Identification and authentication

The TOE includes an internal data base where administrative users can be defined with a user name, domain, class, and password. Additionally, administrative users can provide a public-key-based authentication credentials to the TOE, which will be stored and used to support public-key based authentication (using 1024-bit (or higher) RSA or DSA and limited to verification that does not involve access to an external public-key infrastructure) when using SSH. The TOE can also be configured to utilize the services of an external LDAP server (i.e., Active Directory) to authenticate administrative users and determine their assigned class.

All interactive user interfaces (maintenance terminal, SSHv2 client, CLI Client, or IMC) require administrative users to log in with a user name and valid password (or optionally public-key-based authentication credentials when using SSHv2) prior to successfully being connected to the TOE enabling access to security management functions. If the

administrative user is defined in the internal user database, that information will be used. If the administrative user is not defined internally, the configured LDAP server will be consulted. In each case, the administrative user authentication will either succeed or not. Administrative users not defined internally will not be able to successfully log in. Note that passwords are not echoed or otherwise displayed when logging into any of the available interactive user interfaces. In the case of public-key authentication, applicable credentials are not exposed to users.

In the case of locally defined administrative users, they have an assigned user class. In the case of LDAP-defined administrative users, the LDAP server is consulted to query the administrative user's groups. The TOE maintains a mapping between LDAP groups and administrative user classes and domains. Once the administrative user's groups are queried, the TOE mapping is consulted to determine the user's domains and classes. If the user doesn't belong to a mapped group, the login attempt will fail.

Once an administrative user is successfully logged in, their user domains and classes will be used to limit the set of functions the user can successfully exercise. Note that a user can be assigned to up to 32 domains (of the 1024 that can be defined in the TOE) by virtue of associated groups and each domain assignment includes its own user class assignment. As such, a user could be in the *browse* class for one domain and the *edit* class for another. However, the *service* and *super* classes transcend domains and assignment to one of these classes, regardless of domain, provides access to the associated functions (see section 6.5) regardless of any domain assignments.

Client host users are identified using iSCSI identifiers and Fiber Channel World Wide Names (WWNs). In general the client host identifiers are not authenticated by the TOE. The iSCSI and Fibre Channel WWNs are well defined in their respective standards. The TOE administrator needs to ensure the assumed authenticity of host identifiers in their operational environment. This likely would require physical protection of the applicable storage area networks as well as some suitable knowledge about (they are appropriately evaluated) or control over the respective hosts. Note that while not specifically claimed or otherwise addressed, it should be understood that the TOE can be configured to require iSCSI hosts to use Challenge-Handshake Authentication protocol (CHAP) authentication, but that is not claimed herein since it is not a default behavior and there is no subsequent use of cryptographic functions, for example, that would serve to protect the integrity of traffic to and from authenticated hosts limiting any assurance that may have been gained.

The Identification and authentication function is designed to satisfy the following security functional requirements:

- FIA_ATD.1: The TOE defines users in terms of user identity (i.e., name), domain, class and password.
- FIA_UAU.1: With the exception of hosts identified by iSCSI identifiers and Fiber Channel WWNs accessing virtual volumes on designated ports, the TOE doesn't offer any services to users until they are successfully authenticated with their user name and password or public key.
- FIA_UAU.5: The TOE can be configured to automatically utilize an external LDAP server for authentication of users not internally defined.
- FIA_UAU.7: The TOE is designed to not echo passwords when users are logging in.
- FIA_UID.2: The TOE doesn't offer any services to users, including client hosts, until they are successfully identified with either their user name and password or public-key credentials in the case of administrative users or iSCSI identifier or Fiber Channel WWN in the case of client hosts.

6.5 Security management

The TOE supports four standard user classes that can be assigned to individual users. Users in the *super* class can perform any functions (e.g., all security functions of the TOE including managing audit events, user accounts, and access control). While other users have more limited access they each can perform security-relevant security management functions nonetheless. Users are assigned to domains and each domain assignment is associated with a class. However, the *super* and *service* classes transcend domains, so if a user is assigned one of these user classes their domain assignments are irrelevant in regard to functions associated with those classes. Similarly, the 'all' domain is effectively a superset of all domains, providing access based on the user class (i.e., *browse* or *edit*) to all system resources.

The four standard classes can generally perform the following operations:

- **Super**: Allows access to all system functions. This class can review and otherwise manage the audit events in the local audit log, manage (define users accounts with specific domains and user classes) user accounts, manage domain definitions, define hosts (by associating specific WWNs or iSCSI identifiers with them), manage LDAP group association with user classes and domains, and manage (i.e., define and specify the exported VLUN attributes) access to Virtual Volumes.

  This class is not limited by domain, so a user in this class can perform the associated functions on all TOE resource, though there are restrictions as described below

- **Service**: Allows access to limited system functions to service the storage server; allows limited access to user information and user group resources. Note that this class doesn't provide the ability to perform any of the identified security management functions.

  This class is not limited by domain, so a user in this class can perform the associated functions on all TOE resources.

- **Edit**: Allows access to most system functions, such as defining hosts, creating and editing Virtual Volumes (including selecting availability options and assigning domains), and managing access to Virtual Volumes. The edit class allows access to all identified security management functions, but does not offer access to some non-security related service functions.

  This class is limited by domain, so a user in this class can perform the associated functions only on TOE resources in the same domain. In other words, a user with the edit class can only create VVs using CPGs in the same domain and can export VVs to hosts in the same domain. Users in the 'all' domain are not limited in terms of resources they can manage, except as explained below.

- **Browse**: Allows read-only accessibility, including review of the audit events and alerts.

  This class is limited by domain, so a user in this class can perform the associated functions only on TOE resources in the same domain (where applicable). In other words, a user with the edit class can only browse, for example, CPGs, VVS, hosts, and users in the same domain. Users in the 'all' domain are not limited in this regard.

In addition to the four standard user classes are four extended roles (listed below). There is no functional difference between standard and extended roles except they involve different sets of allowable functions and as such should generally be considered subsets of the Super role, above, and also are assigned to the 'all' domain and cannot be restricted in that regard. The extended roles define a set of rights optimized for CLI users with specialized or restricted tasks. In general, the minimum set of rights should be assigned to each user.

- **Create:** Rights are limited to creating objects. For example, virtual volumes, CPGs, hosts, and schedules.
- **Basic Edit:** Rights are similar to the Edit role. For example, creating and editing virtual volumes and other objects. The rights to remove objects are more restricted for the Basic Edit role than the Edit role. On the other hand, this role can create domains, configure authentication parameters, and create users.
- **3PAR AO:** Rights are limited to internal use by HP for Adaptive Optimization operations. T
- **3PAR RM:** Rights are limited to internal use by HP for Recovery Manager operations.

When configuring and exporting storage resources, users cannot normally export resources from one domain to hosts of another domain regardless of their user class. The exception is that a Super user can create domain sets and assign hosts and individual domains to those domain sets such that ultimately volumes exported to hosts within a domain set can be accessible by other hosts in the domain set which can facilitate cross-domain access to the volume exported in this manner.

The security functions of the TOE are managed by authorized users using either CLI functions available via a maintenance console, SSHv2 sessions, or the CLI Client or alternately using the IMC client for GUI access to available functions.

The Security management function is designed to satisfy the following security functional requirements:

- FMT_MSA.1: The TOE restricts the ability to manage the access settings for Virtual Volumes to users with the super user or that are in the applicable domain with the edit class (aka System Administrators in the domain of the protected object). Note that VVs (in a given domains) can be defined and exported to defined hosts (in the same domain) and/or ports (which are not associated with domains); in turn hosts are associated with specific iSCSI or WWN identifiers. iSCSI and WWN identifiers are properties of hosts that are not configurable or alterable within the TOE.
- FMT_MSA.3: The TOE restricts the ability to manage the access settings for Virtual Volumes to users with the super user or that are in the applicable domain with the edit class (aka System Administrators in the domain of the protected object). Note that there aren't actually any defaults beyond the fact that access can only be obtained after access is specifically configured in accordance with the access control rules.
- FMT_MTD.1: The TOE restricts the ability to manage security relevant TOE data (i.e., TSF data) to users with any user class (aka System Administrators).
- FMT_SMF.1: The TOE provides a full range of functions that can be used to manage the TOE and its security functions including reviewing audit events, managing user accounts, and managing access to Virtual Volumes.
- FMT_SMR.1: The TOE implements browse, edit, service, and super user classes. The user classes are collectively referred to as System Administrator in this Security Target.

6.6 Protection of the TSF

The TOE is a series of hardware appliance Controller Nodes each of which includes a hardware-based real-time clock. The TOE's embedded OS manages the clock and exposes administrator clock-related functions. The TOE can also be configured to use a network time server in order to automatically synchronize the time of its internal clock.

Each TOE appliance is a stand alone physical device that 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. While the administrative interface is function rich, the TOE is designed specifically to provide access only to hashed (and not plain text) passwords and also, while cryptographic keys can be entered, the TOE does not disclose any keys stored in the TOE.

The Protection of the TSF function is designed to satisfy the following security functional requirements:

- FPT_PTD.1: The TOE does not offer any functions that will disclose to any users a stored cryptographic key.
- FPT_STM.1: The TOE includes its own hardware clock and is capable of being configured to use a network time server for synchronization.

6.7 Trusted path/channels

In the cases of SSHv2 and TLS, the TOE offers both a secure command line interface (CLI) and a graphical user interface (GUI), i.e., the InForm Management Console (IMC), interactive administrator sessions. An administrator with an appropriate SSHv2 client or the HP 3PAR CLI Client or IMC can establish secure remote connections with the TOE. However, to successfully establish such an interactive session, the administrator must be able to provide acceptable user credentials (e.g., user id and password), after which they will be able to issue commands within their assigned authorizations.

Additionally, the TOE can be configured to protect communication with a configured LDAP server using TLSv1.

The Trusted path/channels function is designed to satisfy the following security functional requirements:

- FTP_TRP.1(1): The TOE provides SSH and TLS, based on its embedded OpenSSL/OpenSSH libraries, to support secure remote administration. In each case, the administrator can initiate the remote session, the remote session is secured (disclosure and modification) using cryptographic operations, and all remote security management functions require the use of one of these secure channels.
- FTP_TRP.1(2): The TOE provides SSH and TLS, based on its embedded OpenSSL/OpenSSH libraries, to support secure remote administration. In each case, the administrator can initiate the remote session, the remote session is secured (disclosure and modification) using cryptographic operations, and all remote security management functions require the use of one of these secure channels.

7. Protection Profile Claims

This ST does to conform to any Protection Profile.

8. Rationale

This section provides the rationale for completeness and consistency of the Security Target. The rationale addresses the following areas:

- Security Objectives;
- Security Functional Requirements;
- Security Assurance Requirements;
- Requirement Dependencies;
- TOE Summary Specification.

8.1 Security Objectives Rationale

This section shows that all secure usage assumptions, organizational security policies, and threats are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

8.1.1 Security Objectives Rationale for the TOE and Environment

This section provides evidence demonstrating the coverage of organizational policies and usage assumptions by the security objectives. Note that the NDPP does not explicitly or clearly correspond or rationale correspondence between its Security Problem Definition and Security Objectives, so the mapping had to be inferred and correspondence rationale has been devised to complete this ST appropriately.

	T.ADMIN_ERROR	T.DATA_DISCLOSURE	T.DATA_AVAILABILITY	T.UNAUTHORIZED_ACCESS	T.UNDETECTED_ACTIONS	T.USER_DATA_REUSE	A.NO_GENERAL_PURPOSE	A.PHYSICAL	A.TRUSTED_ADMIN	A.HOST_IDENTITY
O.AVAILABILITY			X							
O.LIMIT_ACCESS		X								
O.PROTECTED_COMMUNICATIONS				X						
O.RESIDUAL_INFORMATION_CLEARING		X				X				
O.SYSTEM_MONITORING	X			X	X					
O.TOE_ADMINISTRATION				X						
OE.NO_GENERAL_PURPOSE							X			
OE.PHYSICAL								X		
OE.TRUSTED_ADMIN									X	
OE.HOST_IDENTITY										X

Table 6 Environment to Objective Correspondence

8.1.1.1 T.ADMIN_ERROR

An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms that may go undetected.

This Threat is satisfied by ensuring that:

- O.SYSTEM_MONITORING: To reduce the potential of an administrative error might be unnoticed or untraceable, the TOE is expected to log security relevant events and export those logs to an external log server.

8.1.1.2 T.DATA_DISCLOSURE

A connected host might obtain access to user data for which they have no authorization.

This Threat is satisfied by ensuring that:

- O.LIMIT_ACCESS: To ensure that connect client hosts cannot access data for which they are not authorized, the TOE is expected to enforce an access policy limiting connected hosts to access only authorized resources.
- O.RESIDUAL_INFORMATION_CLEARING: To reduce the potential of data being erroneously disclosed through resource reallocation, the TOE is expected to ensure that residual data is appropriately managed.

8.1.1.3 T.DATA_AVAILABILITY

User data may become unavailable due to isolated storage resource failures or due to resource exhaustion.

This Threat is satisfied by ensuring that:

- O.AVAILABILITY: To reduce the threat of lack of data access due to resource failure or exhaustion, the TOE is expected to ensure that data can be stored in a manner alleviating failure situations and also to allow administrators to configure limits so that user accessible resources are limited and warnings are issued when limits are reached.

8.1.1.4 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.

This Threat is satisfied by ensuring that:

- O.PROTECTED_COMMUNICATIONS: To reduce the potential that an attacker might gain unauthorized access to the TOE or its data via data transmitted across a network, the TOE is expected to protect its administrator communication channels from disclosure, modification, and also to ensure the identity of the TSF.
- O.SYSTEM_MONITORING: To reduce the potential of unauthorized access attempts that might go unnoticed, the TOE is expected to log security relevant events and export those logs to an external log server.
- O.TOE_ADMINISTRATION: To reduce the potential of unauthorized access to TOE security functions and data, the TOE is expected to be designed to ensure that only presumably authorized administrators can log in and access security management functions. Note that the TOE is expected to restrict access to security functions and TSF data so that only authorized administrators can access it and in some cases TSF data is not accessible at all.

8.1.1.5 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.

This Threat is satisfied by ensuring that:

- O.SYSTEM_MONITORING: To reduce the potential of security relevant actions occurring without notice, the TOE is expected to log security relevant events and export those logs to an external log server.

8.1.1.6 T.USER_DATA_REUSE

User data may be inadvertently sent to a destination not intended by the original sender.

This Threat is satisfied by ensuring that:

- O.RESIDUAL_INFORMATION_CLEARING: To reduce the potential of data being erroneously sent to an unintended recipient, the TOE is expected to ensure that residual data is appropriately managed.

8.1.1.7 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.

This Assumption is satisfied by ensuring that:

- OE.NO_GENERAL_PURPOSE: 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.

8.1.1.8 A.PHYSICAL

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.

This Assumption is satisfied by ensuring that:

- OE.PHYSICAL: Physical security, commensurate with the value of the TOE and the data it contains, is 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.

8.1.1.9 A.TRUSTED_ADMIN

TOE Administrators are trusted to follow and apply all administrator guidance in a trusted manner.

This Assumption is satisfied by ensuring that:

- OE.TRUSTED_ADMIN: TOE Administrators will be carefully selected to ensure they are trusted and trained to follow and apply all administrator guidance in a trusted manner.

8.1.1.10 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. 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).

This Assumption is satisfied by ensuring that:

- OE. HOST_IDENTITY: iSCSI and Fiber Channel hosts correctly reflect the iSCSI identifier or Fiber Channel World Wide Name (WWN) associated with their Host Bus Adapters (HBAs). Also, the SAN(s) connecting iSCSI and Fiber Channel must be controlled to mitigate potentially malicious attacks on the SAN(s).

8.2 Security Requirements Rationale

This section provides evidence supporting the internal consistency and completeness of the components (requirements) in the Security Target. Note that **Table 7** indicates the requirements that effectively satisfy the individual objectives. .

8.2.1 Security Functional Requirements Rationale

All Security Functional Requirements (SFR) identified in this Security Target are fully addressed in this section and each SFR is mapped to the objective for which it is intended to satisfy. Note that the NDPP identifies the correspondence between Security Objectives and SFRs, but fails to provide any rationale for the correspondence. As such, correspondence rationale has been devised to complete this ST appropriately.

	O.AVAILABILITY	O.LIMIT_ACCESS	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEARING	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION
FAU_GEN.1					X	
FAU_GEN.2					X	
FAU_SAR.1					X	
FAU_SAR.3					X	
FAU_STG.1					X	
FAU_STG.4					X	
FCS_CKM.1			X			
FCS_CKM_EXT.4			X			
FCS_COMM_PROT_EXT.1			X			
FCS_COP.1(1)			X			
FCS_COP.1(2)			X			
FCS_COP.1(3)			X			
FCS_COP.1(4)			X			
FCS_SSH_EXT.1			X			
FCS_TLS_EXT.1			X			
FDP_ACC.2		X				
FDP_ACF.1		X				
FDP_AVL_EXT.1	X					
FDP_RIP.2		X		X		
FIA_ATD.1						X
FIA_UAU.1						X
FIA_UAU.5						X
FIA_UAU.7						X
FIA_UID.2						X
FMT_MSA.1						X
FMT_MSA.3						X

	O.AVAILABILITY	O.LIMIT_ACCESS	O.PROTECTED_COMMUNICATIONS	O.RESIDUAL_INFORMATION_CLEARING	O.SYSTEM_MONITORING	O.TOE_ADMINISTRATION
FMT_MTD.1						X
FMT_SMF.1						X
FMT_SMR.1						X
FPT_PTD.1			X			
FPT_STM.1					X	
FTP_TRP.1(1)			X			
FTP_TRP.1(2)			X			

Table 7 Objective to Requirement Correspondence

8.2.1.1 O.AVAILABILITY

The TOE will ensure that data can be stored in a manner that is protected from underlying resource failure and exhaustion.

This TOE Security Objective is satisfied by ensuring that:

- FDP_AVL_EXT.1: The TOE is required to implement selected RAID levels to defend against resource failures and also to implement warning and limit levels so that administrators can define maximum resource allocation and also when to receive alerts about impending resource exhaustion.

8.2.1.2 O.LIMIT_ACCESS

The TOE will ensure that connected hosts can access only data resources for which they are authorized.

This TOE Security Objective is satisfied by ensuring that:

- FDP_ACC.2: The TOE is required to implement an access policy controlling all operations between attached hosts and virtual volumes managed by the TOE.
- FDP_ACF.1: The TOE is required to implement an effective set of rules to enforce the access control policy between hosts and virtual volumes.
- FDP_RIP.2: The TOE is required to clear all information when allocating storage resources for subsequent activities.

8.2.1.3 O.PROTECTED_COMMUNICATIONS

The TOE will provide protected communication channels for administrators.

This TOE Security Objective is satisfied by ensuring that:

- FCS_CKM.1: The TOE is required to be able to generate encryption keys to support other cryptographic operations.

- FCS_CKM_EXT.4: The TOE is required to zeroize keys when no longer need to prevent subsequent disclosure.
- FCS_COMM_PROT_EXT.1: The TOE is required to implement SSH or IPSEC and optionally TLS to protect its network communication channels.
- FCS_COP.1(1): The TOE is required to implement FIPS-conformant AES in support of cryptographic protocols.
- FCS_COP.1(2): The TOE is required to implement FIPS-conformant RSA cryptographic digital signatures.
- FCS_COP.1(3): The TOE is required to implement FIPS-conformant SHA-1 and SHA-256 in support of cryptographic protocols.
- FCS_COP.1(4): The TOE is required to implement FIPS-conformant HMAC SHA-1 in support of cryptographic protocols.
- FCS_SSH_EXT.1: The TOE is required to implement SSH properly to protect applicable network communication channels.
- FCS_TLS_EXT.1: The TOE is required to implement TLS properly to protect applicable network communication channels.
- FPT_PTD.1: The TOE is required to prevent even administrators from readily accessing sensitive user and TSF data such as cryptographic keys.
- FTP_TRP.1(1): The TOE is required to protect communication between itself and its administrators from disclosure and modification.
- FTP_TRP.1(2): The TOE is required to protect communication between itself and its administrators from disclosure and modification.

8.2.1.4 O.RESIDUAL_INFORMATION_CLEARING

The TOE will ensure that any data contained in a protected resource is not available when the resource is reallocated.

This TOE Security Objective is satisfied by ensuring that:

- FDP_RIP.2: The TOE is required to clear all information when allocating storage resources for subsequent activities.

8.2.1.5 O.SYSTEM_MONITORING

The TOE will provide the capability to generate audit data and provide the means to store and review those data.

This TOE Security Objective is satisfied by ensuring that:

- FAU_GEN.1: The TOE is required to be able to generate audit events for security relevant activities on the TOE.
- FAU_GEN.2: The TOE is required to associate audit events to users to ensure proper accountability.
- FAU_SAR.1: The TOE is required to provide the means for a user to review recorded audit records.
- FAU_SAR.3: The TOE is required to provide functions to sort audit records to make their review more effective.
- FAU_STG.1: The TOE is required to protect stored audit records so they cannot be inappropriately modified.
- FAU_STG.4: The TOE is required to have well-defined behavior when the available audit storage space becomes exhausted so that appropriate procedures can be in place to mitigate that possibility.
- FPT_STM.1: The TOE is required to generate reliable time stamps to be used in its audit records for proper accounting.

8.2.1.6 O.TOE_ADMINISTRATION

The TOE will provide mechanisms to ensure that only administrators are able to log in and configure the TOE, and restrict logged-in administrators to authorized functions and TSF data.

This TOE Security Objective is satisfied by ensuring that:

- FIA_ATD.1: The TOE is required to facilitate the definition of users with appropriate user attributes.
- FIA_UAU.1: The TOE is required to ensure that users must be authenticated in order to access functions, other than those specifically intended to be accessed without authentication (i.e., user data resources available to client hosts).
- FIA_UAU.5: The TOE is required to implement a local authentication mechanism and can support additional authentication mechanisms.
- FIA_UAU.7: The TOE is required to not echo passwords when being entered to mitigate the chance of an accidental password disclosure.
- FIA_UID.2: The TOE is required to ensure that users must be identified in order to access functions of the TOE.
- FMT_MSA.1: The TOE is required limit the ability to manage the access control functions to authorized administrators.
- FMT_MSA.3: The TOE is required to implement default secure values and limit the management of default values to authorized administrators.
- FMT_MTD.1: The TOE is required to restrict access to security relevant data to administrators.
- FMT_SMF.1: The TOE is required to provide a minimum set of security functions to ensure the TOE security features can be properly managed.
- FMT_SMR.1: The TOE is required to implement a minimum of a System Administrator role and can implement additional roles where necessary.

8.3 Security Assurance Requirements Rationale

The Security Assurance Requirements (SARs), which correspond to EAL2 augmented with ALC_FLR.2. They have been chosen as the de facto minimum standard for commercial product evaluation assurance as found in most available Protection Profiles.

8.4 Requirement Dependency Rationale

As can be seen in the following table all of the SFR and SAR dependencies are satisfied in this ST.

ST Requirement	CC Dependencies	ST Dependencies
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1 and FIA_UID.1	FAU_GEN.1 and FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FCS_CKM.1	(FCS_CKM.2 or FCS_COP.1) and FCS_CKM.4	FCS_COP.1(*) and FCS_CKM_EXT.4
FCS_CKM_EXT.4	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1)	FCS_CKM.1
FCS_COMM_PROT_EXT.1	(FCS_IPSEC_EXT.1 or FCS_SSH_EXT.1 or FCS_TLS_EXT.1)	FCS_SSH_EXT.1 and FCS_TLS_EXT.1
FCS_COP.1(1)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(2)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(3)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_COP.1(4)	(FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1) and FCS_CKM.4	FCS_CKM.1 and FCS_CKM_EXT.4
FCS_SSH_EXT.1	FCS_COP.1	FCS_COP.1(*)
FCS_TLS_EXT.1	FCS_COP.1	FCS_COP.1(*)

ST Requirement	CC Dependencies	ST Dependencies
FDP_ACC.2	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 and FMT_MSA.3	FDP_ACC.2 and FMT_MSA.3
FDP_AVL_EXT.1	none	none
FDP_RIP.2	none	none
FIA_ATD.1	none	none
FIA_UAU.1	FIA_UID.1	FIA_UID.2
FIA_UAU.5	none	none
FIA_UAU.7	FIA_UAU.1	FIA_UAU.1
FIA_UID.2	none	none
FMT_MSA.1	(FDP_ACC.1 or FDP_IFC.1) and FMT_SMR.1 and FMT_SMF.1	FDP_ACC.2 and FMT_SMR.1 and FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 and FMT_SMR.1	FMT_MSA.1 and FMT_SMR.1
FMT_MTD.1	FMT_SMR.1 and FMT_SMF.1	FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	none	none
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_PTD.1	none	none
FPT_STM.1	none	none
FTP_TRP.1(1)	none	none
FTP_TRP.1(2)	none	none
ADV_ARC.1	ADV_FSP.1 and ADV_TDS.1	ADV_FSP.2 and ADV_TDS.1
ADV_FSP.2	ADV_TDS.1	ADV_TDS.1
ADV_TDS.1	ADV_FSP.2	ADV_FSP.2
AGD_OPE.1	ADV_FSP.1	ADV_FSP.2
AGD_PRE.1	none	none
ALC_CMC.2	ALC_CMS.1	ALC_CMS.2
ALC_CMS.2	none	none
ALC_DEL.1	none	none
ALC_FLR.2	none	none
ATE_COV.1	ADV_FSP.2 and ATE_FUN.1	ADV_FSP.2 and ATE_FUN.1
ATE_FUN.1	ATE_COV.1	ATE_COV.1
ATE_IND.2	ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1	ADV_FSP.2 and AGD_OPE.1 and AGD_PRE.1 and ATE_COV.1 and ATE_FUN.1
AVA_VAN.2	ADV_ARC.1 and ADV_FSP.2 and ADV_TDS.1 and AGD_OPE.1 and AGD_PRE.1	ADV_ARC.1 and ADV_FSP.2 and ADV_TDS.1 and AGD_OPE.1 and AGD_PRE.1

Table 8 Requirement Dependencies

8.5 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 9 Security Functions vs. Requirements Mapping** demonstrates the relationship between security requirements and security functions.

	Security audit	Cryptographic support	User data protection	Identification and authentication	Security management	Protection of the TSF	Trusted path/channels
FAU_GEN.1	X						
FAU_GEN.2	X						
FAU_SAR.1	X						
FAU_SAR.3	X						
FAU_STG.1	X						
FAU_STG.4	X						
FCS_CKM.1		X					
FCS_CKM_EXT.4		X					
FCS_COMM_PROT_EXT.1		X					
FCS_COP.1(1)		X					
FCS_COP.1(2)		X					
FCS_COP.1(3)		X					
FCS_COP.1(4)		X					
FCS_SSH_EXT.1		X					
FCS_TLS_EXT.1		X					
FDP_ACC.2			X				
FDP_ACF.1			X				
FDP_AVL_EXT.1			X				
FDP_RIP.2			X				
FIA_ATD.1				X			
FIA_UAU.1				X			
FIA_UAU.5				X			
FIA_UAU.7				X			
FIA_UID.2				X			
FMT_MSA.1					X		
FMT_MSA.3					X		
FMT_MTD.1					X		
FMT_SMF.1					X		
FMT_SMR.1					X		
FPT_PTD.1						X	
FPT_STM.1						X	
FTP_TRP.1(1)							X
FTP_TRP.1(2)							X

Table 9 Security Functions vs. Requirements Mapping