Standard Protection Profile for Enterprise Security Management Access Control

October 24, 2013

Version 2.1

Document History

Version	Date	Comment
1.0	October 21, 2011	First complete version from the ESM Technical Community
1.*x*	November 2011 through February 2012	Updates to address CCEVS concerns and standardize with other CCEVS PPs.
2.0	February 22, 2012	First Public Release Version
2.1	October 24, 2013	Changes made based on consistency with ESM Authentication Server PP scope and formatting, ESM Technical Community feedback, and CCEVS input on cryptography.

Table of Contents

List of Figures

List of Tables

1 Protection Profile (PP) Introduction

1.1 Introduction

This section contains document management and overview information necessary to allow a Protection Profile (PP) to be registered through a Protection Profile Registry. The identification provides the labeling and descriptive information necessary to identify, catalogue, register, and cross-reference a PP. The overview summarizes the profile in narrative form and provides sufficient information for a potential user to determine whether the PP is of interest. The formal identification of the profile may be found in Appendix F - Identification.

1.2 ESM Protection Profile Suite Overview

Enterprise Security Management (ESM) refers to a suite of product/product components[1] used to provide centralized management of a set of IT assets within an organization.[2]

In the current ESM Protection Profile suite, profiles are defined that permit the definition of the following types of enterprise policies:

- **Access Control Polices:** Policies that authorize or deny specific actions of defined subjects (actors) against defined objects (IT assets or resources).
- **Identity and Credential Policies:** Policies that define and maintain attributes used for subject identification, authentication, authorization, and accountability.
- **Object Attribute Policies:** Policies that define and maintain attributes used for objects.
- **Authentication Policies:** Policies that define the circumstances under which users can authenticate to enterprise systems.
- **Secure Configuration Policies:** Polices that define baseline configurations for IT assets.

[1] Note: In a technical sense, the term "product" is inaccurate, but other terms (such as "system") are equally poor and overloaded. The various "products" within an ESM "system" may be distinct products, or they may simply be subproducts or functional capabilities within a larger product described in the ST. The use of the term "product" is solely because Security Targets describe *products*, as opposed to *systems* (which are integrated collections of products designed for a specific mission), and thus a PP typically describes a product (or a component of a product) in a manner independent from a specific vendor's implementation.

[2] In ESM usage, the term "enterprise" is often used instead of "organization", reflecting the fact that the overall enterprise might cross organizational boundaries.

- **Audit Policies:** Policies that define how audit data is collected, aggregated, reported, and maintained across the enterprise.

The ESM product/product components that consume and enforce the various policies provide the following types of security:

- **Preventative:** Actions performed against IT assets are prohibited if found to be a violation of an enterprise-defined central policy.
- **Detective:** The behavior of users and IT assets is audited and aggregated so that patterns of insecure, malicious, or otherwise inappropriate behavior across the enterprise can be detected.
- **Reactive:** IT assets are compared to a secure organizationally-defined central definition, and action is taken if discrepancies are identified.

There are three types of ESM capabilities. The first type, *policy definition*, is used to define a central organizational policy that will be used to govern the behavior of a set of IT assets. This is shown by the following examples:

- A Secure Configuration Management product may define a policy that governs the acceptable set of software assets that reside on a system or the configuration of one or more of that system's applications.
- A Policy Management product may define the operations that are and are not allowed against a specific system based on the subject requesting the operation and the object the request acts upon.

The second type, *policy consumption*, acquires a defined policy, stores it, and enforces it in a persistent manner. This is shown by the following examples:

- An Access Control product that resides on a system may receive a defined access control policy from Policy Management. It will then store it and persistently ensure that all subjects abide by it until instructed otherwise.
- An Access Control product that enforces data loss prevention access control on a system may receive a defined object attribute policy from Policy Management that associates certain types of objects with defined sensitivity levels. It will store this policy and will persistently block objects from leaving the system based on the sensitivity attributes assigned to the objects.

The third type, *policy enforcement*, acts upon a policy that is defined elsewhere as a result of a query to or command from the source of that policy. This is shown by the following

examples:

- An administrator attempts to log in to a Policy Management product to manage it. Their authentication request is submitted to an Authentication Server which applies a defined authentication policy to determine if the request should be authorized. The Policy Management product then enforces the Authentication Server's decision and allows or rejects access accordingly.
- A Secure Configuration Management product defines a policy to ensure that software deployed in the environment is up-to-date. An Access Control product is found to be an older version. The Secure Configuration Management product issues an instruction to the Access Control product to apply a patch. The secure configuration policy is subsequently enforced by the Access Control product acting on this instruction.

These three types of ESM capabilities are represented in the overall suite of ESM Protection Profiles.

The ESM PP Suite consists of 6 Protection Profiles that may be characterized as follows:

Table 1. Summary of the ESM Protection Profile Suite

Protection Profile	Access Control Policy	Identity and Credential Policy	Object Attribute Policy	Authentication Policy	Secure Configuration Policy	Audit Policy
ESM Access Control Protection Profile	C	C	C		E	$C_{(1)}$
ESM Policy Management Protection Profile	D	C/E	$D/C_{(2)}$	$E_{(3)}$	E	$C_{(1)}/D_{(5)}$
ESM Identity and Credential Management Protection Profile		D	$C/D_{(2)}$	$E_{(3)}$	E	$C_{(1)}$
ESM Authentication Server Protection Profile		$E/D_{(4)}$		$D/E_{(3)}$	E	$C_{(1)}$
ESM Audit Server Protection Profile		E		$E_{(3)}$	E	$C_{(1)}/D_{(1)}$
ESM Secure Configuration Management Protection Profile		E		$E_{(3)}$	D/E	$C_{(1)}/D$
C = Consume and Enforce; D = Define; E = Enforce						

Notes:

1) The audit policy is consumed as the TOE determines what events to audit. Alternatively, a de facto audit policy may be defined solely within an Audit Server TOE through it discarding an administratively-defined subset of the collected data.
2) Object attributes are defined either in the Identity and Credential Management PP or the Policy Management PP, but not both.
3) The authentication policy is enforced in the sense that the authentication server may mediate authentication requests to the TOE.

4) Specifically, it is conceivable that an authentication server may define a strength of secrets policy.
5) Specifically, the Policy Management TOE may define the access-control events audited by an Access Control TOE.

1.3 Overview of the ESM Access Control Protection Profile

This Protection Profile focuses on **access control decision and enforcement**. A product/product component[3] that conforms to this Protection Profile consumes a centrally-defined access control policy and enforces it. In doing so, it provides preventative security to the enterprise in a consistent manner. A product that conforms to this Protection Profile is expected to intercept requests against some type of defined resource (such as a file system object on a workstation or a web site on an organizational intranet) and determine if the request should be allowed. In an ESM environment, this capability is called a *Policy Decision Point*, or *PDP*. It will then enforce the results of this determination or pass the decision to a trusted entity that does the enforcement itself. In an ESM environment, this second capability is called a *Policy Enforcement Point*, or *PEP*. Products that are compliant with the profile defined in this document provide both Policy Decision and Policy Enforcement. Some ESM products only provide policy decision and defer enforcement to the operating environment; in such cases, the only way to evaluate such products against this Profile is to draw the TOE boundary such that the operational environment enforcement component is recategorized as a TOE component.

It is important to understand how ESM access control differs from the access control commonly found in an operating system:

- **ESM Access Control is centrally provisioned:** ESM Access Control enforces a *centrally-defined policy*, whereas an operating system enforces a *locally-defined* policy (i.e., a policy that is both local to and specific to that particular operating system). The ability to define a central access control policy and have it apply uniformly across the organization to a given set of users and/or IT assets allows for consistent application of organizational security policies.
- **ESM Access Control operates on organizationally defined objects:** ESM Access Control policies often operate on objects of different granularity than an operating system. Whereas an operating system focuses on fundamental objects such as files and IPC interfaces, an ESM product has the ability to operate on

[3] Henceforth, just "product".

higher-level abstractions that may be implemented as a combination of fundamental objects (for example, an "order", which might be a combination of multiple files). Thus ESM products provide the capability to mediate web transactions or prevent data exfiltration at a mail gateway. An ESM Access Control product that functions as an agent on an operating system will be deployed to perform a supplemental role to the native OS capabilities such as whitelisting applications that are created by trusted vendors (and more significantly, it can enforce a centrally-defined policy).

- **ESM Access Control is based on organizational identities:** ESM Access Control products operate using centralized identity data, as opposed to an operating system-specific user base. This permits access control to be configured using organizational attributes and contexts that the organization deems to be important instead of forcing policies to be broken down by legacy user and group distinctions.

As noted above, Access Control components are part of an overall suite of ESM components. An Access Control component will use the following capabilities provided by other ESM components:

- **Centralized policy definition:** A separate Policy Management capability is expected to define the set of rules that guide an Access Control product's policy decisions. These rules will include subject-object-operation tuples that define activities of interest and how the product should respond when these activities are detected. Subjects and objects are defined by organizationally-significant attributes (such as a user's username, their geographic location, the URL of a protected resource, and a time of day).
- **Centralized subject definition:** A separate Identity and Credential Management capability is expected to provide a central definition of users, and to associate users and possibly non-person entities (NPEs) such as programs and workstations with attributes that an organization considers security-relevant. The Access Control product will examine the security attributes of the subject performing an action in order to determine how the request should be handled.
- **Object definition:** In most cases, it is expected that the object attributes examined by an Access Control product will be an intrinsic part of the object's definition in the Operational Environment. For example, a web access manager

may examine the URL of a web page or the time of day that it is being accessed in order to determine if the access is appropriate. However, in some situations, a separate Attribute Management capability may be required in order to control access in the desired manner. For example, an operating system may have a third-party product associate its objects with security labels so that Mandatory Access Control (MAC) can be employed.

- **Centralized assurance of subject identity:** A separate Authentication Server product is expected to authenticate subjects in order to determine that their claimed identities are valid. Actions examined by the Access Control product are initiated by authenticated subjects.
- **Support for centralized auditing:** A separate Audit Server capability is expected to collect audit data for the purposes of centralized reporting and incident handling. An Access Control product must be able to write its audit data to a location that is either associated with this capability or can be queried by this capability so that subject accountability can be enforced. An Access Control product may also support the ability for access-control-relevant audit events of interest to be defined as part of the access control policy.
- **Support for secure configuration management:** a separate Secure Configuration Management is expected to examine the configuration of the Access Control product in order to ensure that it is operating in a manner that is consistent with organizational security policies. This may include various facets of the product's configuration such as ensuring it is fully patched, that it is using an up-to-date policy, or that its configuration settings are appropriate.

Figure 1 below provides a visual outline of how these dependencies may be deployed in relation to an Access Control product. These dependencies may either be satisfied by separate products or as additional facets of a complex product. If an ESM product provides multiple capabilities, it must be evaluated against all of the ESM Protection Profiles that it is capable of satisfying.

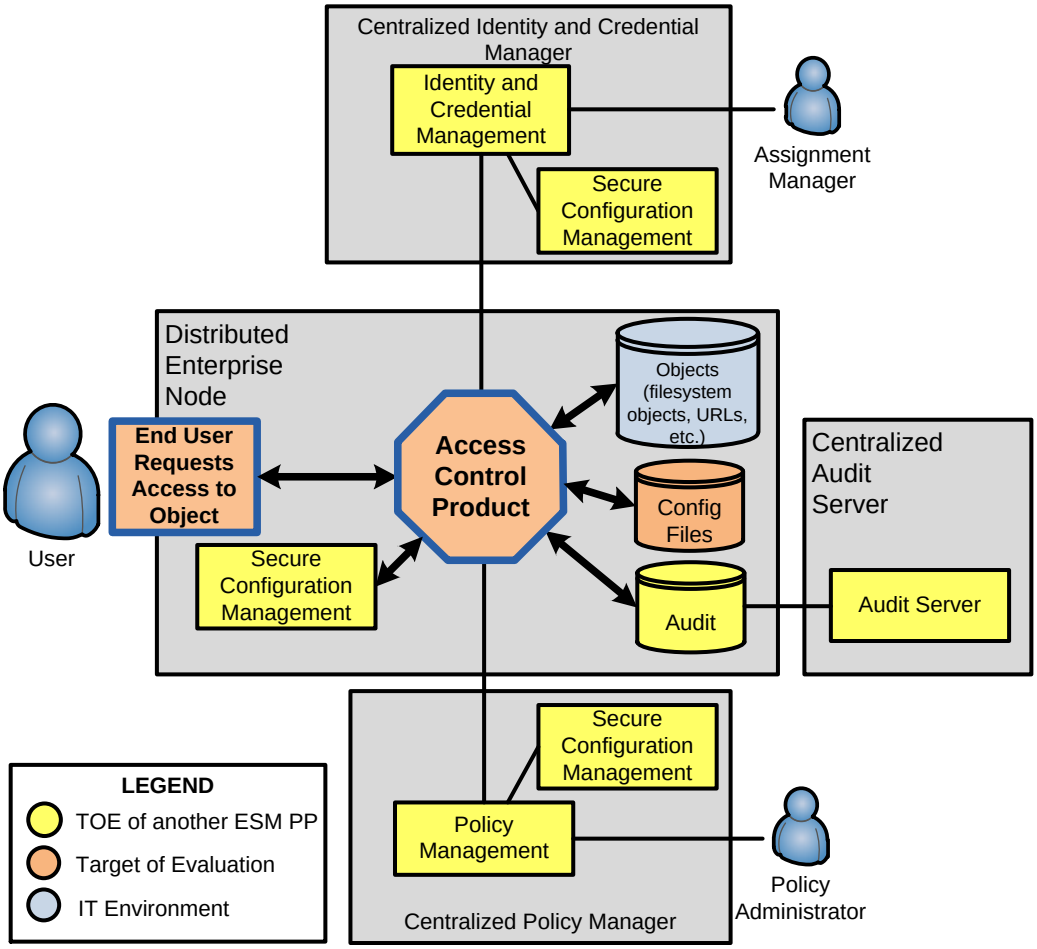

Figure 1. Context for Protection Profile

1.4 Compliant Targets of Evaluation

The purpose of an Access Control product is to consume trusted policies. These policies will determine what objects should be protected in the Operational Environment, what subjects are allowed to access these objects, and what set of operations this access is allowed to encompass. The PP does not prescribe any specific type of access control; Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), or other policies can be deployed if they are capable of enforcing the desired access control mechanism.

A TOE that conforms to this PP may be controlling access to any of a wide variety of resources. It is the responsibility of the Security Target (ST) author to clearly indicate the objects that are protected and the attributes that are used to determine how access is allowed or denied based on policy.

The TOE may be deployed as hardware or software, as a redundant distributed system, or as a single agent that resides on a server. The TSF must include all capabilities that are prescribed in section 6 of this Protection Profile. The TOE may claim any of the optional SFRs that are specified in Appendix C of this Protection Profile. If this is done, the Security Target for the TOE must make appropriate substitutions to the security problem definition as defined in section 7 of this Protection Profile. Inclusion of optional SFRs is not considered to violate strict conformance because specific instructions for handling these situations are provided to both the developer of the evidence and to the evaluation laboratory.

The TOE is expected be a subsystem within a larger ESM system. The entire ESM product is expected to be evaluated against all applicable ESM Protection Profiles.

1.5 Common Capabilities

This Protection Profile defines a set of requirements to be fulfilled by all products that can perform access control in an ESM setting. Because of the wide breadth of objects to which access can be controlled, devising a minimum set of objects that can be protected by the TOE Security Policy (TSP) is not possible. However, this poses the issue of TSPs claiming conformance to this Protection Profile by claiming the bare minimum of security functionality. The intent of this section is to provide an overview of types of access control technologies and to prescribe a baseline of minimum objects and operations that can be defined under the TSP for that technology.

When writing a Security Target to comply with this Protection Profile, the ST author must clearly identify the technology types that apply to the TOE. They must include appropriate corresponding information in the User Data Protection requirements to show that the TOE sufficiently meets the baseline for any applicable types. Note that as technology types become more clearly enumerated, it is expected that this section of the Protection Profile will be augmented in order to accommodate a wider variety of access control solutions.

Regardless of the technology type, it is essential for a product claiming conformance to an ESM Protection Profile to handle subjects and attributes that are **organizationally defined**. In other words, the TOE should make use of existing organizational repositories of users and user attributes whenever possible. The intent of ESM products is to provide **centralized definition** of subject and attribute data. The ST author must define the organizational data that the TOE will use, the trusted sources from which the data is

received, and the mechanism by which this data is interpreted (such as SAML assertions or X.509 certificates). It is expected that other ESM components will be responsible for maintaining these organizational attributes.

1.5.1 Host Access Control

Standard operating systems and applications are designed to provide access control to local operating system and application native resources. However, there are many potential capabilities that require access control to be enforced in terms of higher-level organizational abstractions that may consist of one or more native operating system or application resources. Host Access Control ESM products are designed to enforce access control in terms of these organizational abstractions. The following objects and operations are required, at minimum, for an ESM Host Access Control product to be sufficiently versatile to handle organizational demands:

- Read, write, modify, delete, and execute operations against files
- Read, write, modify, delete, and execute operations against executable processes
- Insertion and modification operations against system configuration parameters
- Shutdown and restart operations against the system of which the TOE is an element

Note that these objects are expected to be arbitrarily definable within a policy. The policy may be capable of controlling native objects directly, or may deal in abstractions that are a collection of objects. A product that provides access control to a single statically defined executable file (for example, a product that only exists to restrict access to Windows Solitaire) does not provide sufficient organizational value to be considered for evaluation.

A host access control TOE may be used to limit the permissions of a system administrator in the Operational Environment (e.g., operating system root account). For example, in Figure 2 below, a Linux “root” account user is trying to make a change to a configuration setting on the local operating system. Before the change is allowed to be made, the TOE will ensure the user has the proper authorizations to make a change to the local operating system configuration. If the policy enforced by the TOE does not allow that user to make the proposed changes to the Operating System, the TOE will prevent the change from occurring and audit the event.

In addition, a Host Access Control TOE may optionally enforce policy based on the day and time at which an operation was initiated.

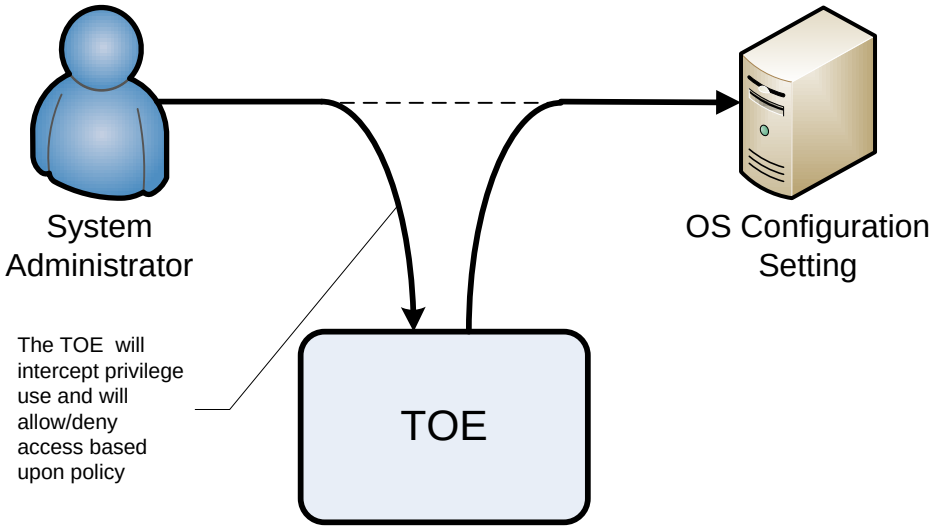

Figure 2. TOE Mediation of Administrator Access

Using the TOE as illustrated in Figure 2 above can help enforce separation of duties by imposing limitations on super users in the environment.

1.5.2 Web Access Control

A Web Access Control TOE is an application that examines subject requests to interact with web-based content and enforces a policy that determines whether these requests are allowed or denied. It typically resides on a central server through which subject requests will be routed. The following objects and operations are required, at minimum, for an ESM Web Access Control product to be sufficiently versatile to handle organizational demands:

- HTTP GET, HEAD, POST operations against web objects
- Execute operations against scripts that are embedded in web objects

Note that these objects are expected to be arbitrarily definable within a policy. A product that provides access control to a single statically defined HTTP object (for example, a single static URL) does not provide sufficient organizational value to be considered for evaluation.

In addition, a Web Access Control TOE may optionally enforce policy based on the day and time at which an operation was initiated.

1.5.3 Data Loss Prevention

The primary purpose of a Data Loss Prevention device is to identify the presence of and enforce access and release rights of sensitive information within an organization, reducing the risk of unauthorized disclosure. Today's Data Loss Prevention (DLP) solutions generally provide Network, Endpoint, and Enterprise Discovery protections. The key distinction with a Data Loss Prevention device is that the focus is on the information within the container (content), as opposed to access to the container itself. A good example of a data loss prevention device would be a "dirty word checker" commonly found within a cross-domain guard.

Network-based DLP solutions are positioned in networks in a manner similar to firewalls. Network DLP solutions are typically hardware, software-only or virtual machine appliances that detect and remediate exfiltration of data. Typical examples include e-mail, Web traffic and file transfer. Network content-aware DLP solutions can be deployed as either inline or attached to a span port on a router or network switch.

Endpoint DLP solutions are host agents that run locally within an OS to identify, audit and remediate sensitive information that is stored and operated on a user's computer or network server. Endpoint DLP solutions often control access and release of information through capabilities such as cut/paste, print, file operations (copy, save, delete and open), burn to CD/DVD and USB device control.

Enterprise Discovery DLP solutions provide the capability to crawl data stores, such as databases, storage area network (SAN)/network-attached storage (NAS), SharePoint, document management systems, and even desktop endpoints to discover, catalog and remediate data objects that contain sensitive data. This is usually enabled as an appliance (hardware or virtual machine) or as agent-based software installed on the resource itself. As Enterprise Discovery DLP solutions are focused more on finding configurations, as opposed to enforcing policy, they are covered by the Secure Configuration Management ESM PP.

The TOE does not protect against disclosure by non-IT means, intentional obfuscation, or covert channels.

The following objects and operations are required, at minimum, for an ESM Data Loss Prevention product to be sufficiently versatile to handle organizational demands:

- Write operations against a print spool

- Read and write operations against removable devices
- Copy and paste operations within and between applications
- Send operations against a mail service
- HTTP POST operations against web content

In addition, the policies consumed by a Data Loss Prevention TOE must be able to define, identify, and catalog the types of data that should be protected from data loss. Note that these attributes are expected to be arbitrarily definable within a policy. A product that prevents loss of data that is defined to belong to one security domain based on a static sensitivity is of no benefit to an organization that does not employ the same sensitivity definition.

Finally, a Data Loss Prevention TOE must also be able to inspect data files such as databases, PDFs, and Word documents to determine if they contain sensitive information, including in hidden fields and metadata, to the level defined in the TSS. Furthermore, a DLP TOE should be able to also identify data objects based on patterns, signatures, or hashes for content that cannot be directly inspected. Finally, DLP solutions should be able to identify the existence of encrypted objects and allow or deny the transmission of them based on whether they are encrypted. This provides additional protection against data leakage by ensuring that documents or repositories that contain sensitive data cannot be transmitted to untrusted logical drives, posted to web forms, or sent as e-mail attachments.

Note that the intent of this type of access control is not to provide a comprehensive safeguard against malicious internal "leaks" entirely on its own. If mitigation of that threat is desired, sufficiently strong physical security, personnel security, and network boundary flow control devices also need to be employed to thwart a determined adversary.

1.6 Related Protection Profiles

This Protection Profile is one of a series of Protection Profiles written for Enterprise Security Management (ESM) products. The following Protection Profiles will complement this Protection Profile:

- Standard Protection Profile for ESM Policy Management

- Standard Protection Profile for ESM Identity and Credential Management
- Standard Protection Profile for ESM Authentication Server
- Standard Protection Profile for ESM Audit Server
- Standard Protection Profile for ESM Secure Configuration Management

Products claiming conformance to this protection profile are expected to identify compatible environmental products that conform to the other ESM Protection Profiles. However, because this Protection Profile suite is in its infancy, it is not yet possible to mandate that all dependent products will conform to a Protection Profile. Non-validated dependent products may be considered to be an acceptable part of the Operational Environment on a case-by-case basis as determined by the relevant national scheme.

1.7 Claiming Multiple Protection Profiles

The ESM family of Protection Profiles defines a number of similar and complementary capabilities. It is expected that many products will implement the capabilities of multiple PPs as part of the same TOE. The following guidelines have been developed along with examples to guide Security Target authors and evaluation laboratories in representing such products correctly and effectively:

- If the TOE performs functionality that is compatible with multiple PPs, then conformance to all applicable PPs must be claimed.

Example: a single product that provides both a mechanism to control access to environmental resources and the means to configure this mechanism is expected to claim conformance to both the Access Control and Policy Management PPs.

Example: a single product that can be used both to configure the security settings of systems or applications and to aggregate the log records of these entities could be expected to claim conformance to both the Audit Server and Secure Configuration Management PPs.

- If multiple PPs are claimed, duplicate SFRs may be combined as long as it’s clear that each individual copy of the SFR is satisfied on its own.

Example: a single product that claims conformance to both the Identity and Credential Management PP and the Authentication Server PP can represent FAU_GEN.1 as a single

iteration so long as the individual FAU_GEN.1 requirements for each PP are claimed and subsequently satisfied.

- If multiple PPs are claimed, different SFRs and security problem definition elements that have identical names must both be included with the original source clearly referenced for each.

Example: the threat T.FORGE has different wording in both the Access Control and Policy Management PPs. A product that claims conformance to both PPs must mitigate both of these threats. The ST must include both instances of this threat along with an identification of which instance came from which claimed PP.

- If a claim of multiple PPs defines two SFRs that are on "opposite ends" of a transaction, then both ends must be consistent and a single iteration of testing is satisfactory.

Example: a single product that claims conformance to both the Access Control and Policy Management PPs will have requirements both to define and to consume an access control policy. It is expected that in this case, the assignments for defining the policy data to be defined and the policy data to be consumed will be identical. Testing the ability of the TOE to both define and consume these policies is then performed simultaneously.

- If one claimed PP references the Operational Environment for a function that is part another claimed PP, it must be interpreted that this function is part of the TSF.

Example 1: the Access Control PP assumes that the TOE will receive access control policies from a Policy Management product in the Operational Environment. However, if a product claims conformance to both the Access Control and Policy Management PPs, these policies will be received from another part of the TOE and not actually the Operational Environment. This is because each PP is written from the perspective of that individual component. It is expected that in cases like this, it will be made clear when "the Operational Environment" actually refers to "the TSF of another claimed PP that is also part of the TOE".

Example 2: the extended requirement ESM_EAU.2 is entitled "Reliance on Enterprise Authentication". The intent of this requirement is for a TOE to allow an authentication server to handle administrator authentication on its behalf. If a product claims conformance to the Authentication Server PP in addition to the Identity and Credential Management PP, the "enterprise" authentication that the product relies on is actually its own authentication server component. It is expected that in cases like this, it will be made clear that the TOE is relying on itself to provide this capability because the TOE includes the specific component that is relied on.

- If a TOE that claims conformance to multiple PPs has remote network interfaces between components, these interfaces must be treated as external interfaces for the purposes of documentation and testing.

Example: a TOE that claims conformance both the Access Control and Policy Management PPs may have each component located on a different system. Even though the interface between the two TOE components is technically an internal interface, the ST author must discuss this interface with regards to FTP_ITC.1. The evaluator must subsequently test this interface as if it represented a connection between the TSF and the Operational Environment.

These combining rules – as well as any other guidance to the ST author – should be followed during ST development and checked as part of the ST evaluation process. As the ESM suite matures, a companion document will be developed to capture all of these ST development statements as ASE assurance activities to be checked.

1.8 Document Organization

Section 1 provides introductory material for the Protection Profile.

Section 2 states the applicable conformance claims for the Protection Profile.

Section 3 defines the types of threats that can be made against the TOE.

Section 4 defines the objectives that the TOE is expected to satisfy and lists the security functional requirements that will demonstrate compliance with these objectives.

Section 5 defines the extended components that are used in this Protection Profile.

Section 6 lists and explains the security functional requirements and security assurance

requirements that must be claimed in order for a TOE to be conformant with the Protection Profile.

Section 7 provides a mapping between the assumptions, threats, objectives, and requirements defined in the Protection Profile.

Section 8 defines the assumptions, threats, objectives, and organizational security policies that apply to the Protection Profile.

The document also contains the following appendices:

- Appendix A - This appendix provides a list of references and defines the acronyms used in this document.
- Appendix B - This appendix describes the Protection Profile's relationships with other standards so that the TOE's applicability to certification and accreditation efforts can be quickly identified.
- Appendix C - This appendix defines optional requirements that may be incorporated into compliant TOEs, the circumstances in which these optional requirements must be included, and the assurance activities to be performed by an evaluator in order to verify the requirements have been satisfied.
- Appendix D - This appendix describes the conventions used in the document.
- Appendix E - This appendix defines the terminology used in the document.
- Appendix F - This appendix provides the formal PP identification information.

2 Conformance Claims

2.1 CC Conformance Claims

This Protection Profile is compliant with *Common Criteria for Information Technology Security Evaluation*, CCMB-2012-09-001, Version 3.1 Revision 4 September 2012.

This Protection Profile is CC Part 2 extended and CC Part 3 conformant.

2.2 PP Conformance Claim

This Protection Profile does not claim conformance to any other Protection Profile.

2.3 Package Conformance Claim

This Protection Profile claims a package of EAL1 augmented.

2.4 ST Conformance Requirements

Security Targets that claim conformance to this Protection Profile must meet a minimum standard of strict conformance as defined by section D.2 of CC Part 1.

The ST must claim strict conformance to this PP by including all of the assurance requirements that are defined in section 6 of the PP. The ST may additionally claim one or more optional requirements as defined in Appendix C of the PP. The ST author must write the assumptions, TOE objectives, and environmental objectives in a manner that is consistent with the optional requirements that are claimed and the instructions provided in section 7 of the PP.

In this PP, application notes are provided to further clarify and explain the intent of the requirements specified and the expectation as to how the vendor will meet the requirements. It is expected that the evaluators of the ST will ensure strict conformance by determining that the ST and its described TOE not only contain all the statements within this PP but also met the expectations as stated by the application notes.

With respect to assurance, it is expected that the ST will contain assurance requirements equal to what is in the PP and that all assurance activities stated in the PP will be performed.

If the ST author believes the TOE exhibits a functionality that pertains to this PP but is

not described in the PP, it is recommended that the ST author consult with their national validation scheme and with the ESM Technical Community to discuss the possibility of adding optional capabilities to this document.

3 Threats

The following sections enumerate the threats that exist for the TOE.

3.1 Unauthorized Access to Environmental Resources

The primary purpose of deploying the TOE is to enforce access control against objects that reside in the Operational Environment. It does this by providing mechanisms to intercept subject requests to perform operations against objects and determine whether a defined access control policy should allow the request to occur. If these activities are subverted or bypassed, or if the TOE is incapable of controlling access to the expected level of granularity, then all or some of the Operational Environment will function as if the TOE did not exist. This situation allows for objects being accessed without proper authorization.

[T.UNAUTH]

3.2 Disabling the TOE

In order to enforce access control against objects, the TOE must reside in a logical location that will allow it to intercept requests. The types of resources to which access is being controlled may require the TOE to reside locally to these resources.

If the TOE is located on an endpoint system, the threat of the TOE being disabled is magnified. This is due to the fact that endpoint systems are less likely to perpetually remain in controlled access environments. When the assurance of physical access control is diminished, the risk of an attacker attempting to access the system is increased.

If the TOE runs as a process that can be terminated or if its files can be moved, altered, or removed from the operating system's startup sequence, a user will have the ability to circumvent access control enforcement.

[T.DISABLE]

3.3 Discontinuity of Policy Data Access

In cases where the TOE is located remotely from other ESM components, a risk may be present. If connections between the TOE and remote resources are disrupted, the TOE may not be able to properly enforce its security functions. Worse yet, the threat of discontinuity can be realized by denial of service or by simply unplugging physical

cables. It can also be very easily performed inadvertently and by individuals far removed from the operation of the TOE itself. Because of this, the TOE must have some way to maintain continuity of operations in the event of a virtually inevitable service outage.

[T.NOROUTE]

3.4 Policy and ESM Data Disclosure

The Operational Environment will almost certainly require data to be transmitted between remote devices in order to function. The TOE may receive policies to enforce from a remote source. It will receive user attributes or session data from elsewhere in the environment, and it will write audit data to a centralized repository that is located remotely. If this data is not protected by a sufficiently secure trusted channel when in transit, it may be subject to involuntary disclosure. An attacker with access to this data can use it for reconnaissance purposes or to replay known valid information in an attempt to impersonate a valid user or entity.

[T.EAVES]

3.5 False Enforcement Assurance

The Policy Management product must communicate with the TOE in order to distribute policies that the TOE will be responsible for enforcing. In order to provide assurance that a policy has been received and will be enforced, the TOE should be able to provide some evidence of policy receipt and consumption to the Policy Management product. However, if the format of this receipt is sufficiently generic or the communications channel is not sufficiently protected from disclosure, an attacker may intercept the distribution of the policy and return a false receipt to the Policy Management product. The result of this is that the TOE does not enforce the correct policy and nothing appears amiss from a management perspective, potentially making the security breach more difficult to detect.

[T.FALSIFY]

3.6 False Updates

When the TOE receives what appears to be updated policy information, the TOE must have some assurance of the authenticity of the policy and the identity of the sender. If the communications channel is not sufficiently protected or the mechanism by which the TOE validates the identity of the policy’s source is not sufficiently robust, an attacker

who is aware of the syntax used to transmit a policy may be able to forge an arbitrarily fake one and have the TOE consume it. If this occurs, the TOE may be configured to enforce a permissive fake policy that allows unauthorized access, to enforce a restrictive fake policy that prevents legitimate activities from being performed, or to consume an incorrectly formatted policy.

[T.FORGE]

3.7 Hidden Actions

Part of the reason for implementing an ESM solution within an organization is to provide transparency and accountability. Because of this, the TOE is expected to provide the capability to monitor and audit enforcement of its access control policies. If an attacker is able to confound audit data by exploiting previously-discussed attack vectors (impersonating Secure Configuration Management to reconfigure the TOE's audit ability, compromising a trusted channel to any remote audit repository to divert or rewrite data, disabling a part of the TOE responsible for auditing, or deleting or modifying local audit logs), then they can begin to probe a system for policy weaknesses with a reduced risk of discovery. Similarly, if the TOE does not identify and audit anomalous or malicious actions taken against itself, then the potential exists for its behavior to be altered without detection. If this were to occur, there would be no assurance that its access control enforcement was functioning properly.

[T.MASK]

3.8 Acceptance of Invalid Policy

The TOE is responsible for accepting input from potentially a variety of sources. If an attacker can replay policy data or modify legitimate policy data in transit, then the TSF may be enforcing an incorrect policy. This presents the attacker an opportunity to access data without authorization.

[T.OFLOWS]

4 Security Objectives

The following sections describe the security objectives that are expected to be satisfied by the TSF. If a TOE claims conformance to multiple Enterprise Security Management PPs, any references to other ESM products or components are to be interpreted as references to distributed components of the TOE. The TSF is expected to satisfy the objectives, regardless of whether the interface to which the objective applies is to the Operational Environment or to a distributed part of the TOE.

The inclusion or exclusion of optional SFRs (defined in Appendix C) will affect the objectives claimed by the TOE and the SFRs that satisfy them. Refer to section 7 for guidance on how the security problem definition is affected by the inclusion or exclusion of optional SFRs.

4.1 Data Protection

The purpose of an Access Control TOE is to prevent the execution of operations that would otherwise be allowed were the TOE not deployed. The result of this is the protection of assets or their assurance that they are being operated in an appropriate manner. In order to accomplish this result, the TOE should control access based on a comparison of the permissions of the entity seeking access (including attributes of the entity's operational environment) against the sensitivity of the object to which access is being sought in accordance with policy. This policy data will be distributed to the TOE by a compatible Policy Management product and can be queried by a compatible Secure Configuration Management product so that the TOE's security posture can be monitored and configured.

(O.DATAPROT: ESM_DSC.1, ESM_EID.2, FDP_ACC.1, FDP_ACF.1, FMT_MOF.1(1), FMT_MOF.1(2), FMT_MSA.1, FMT_MSA.3, FMT_SMF.1, FMT_SMR.1, FTA_TSE.1 (optional))

4.2 Rejection of Invalid Policies

The TOE must be capable of validating the integrity of any policy data it receives and rejecting any invalid or replayed data. If the TOE were able to accept invalid data, it could cause an incorrect policy to be implemented. It could also cause a buffer overflow by accepting an incorrectly formatted policy.

(O.OFLOWS: FPT_RPL.1, FTP_ITC.1)

4.3 Guaranteed Integrity

The TOE, to protect the integrity of locally held copies of policy, identity, credential, attribute, and other security information obtained from other ESM capabilities, must use sufficiently strong and trusted mechanisms to protect the local data at rest. Failure to do so would expose the TOE to the potential of compromise on many levels or ineffective policy management.

(O.INTEGRITY: FTP_ITC.1)

4.4 Self-Protection

As discussed in section 1.5.1, a Host-Based Access Control TOE may be deployed to control access to objects that reside on an operating system. In this case, there is an implicit assumption that users of that operating system do not require access to its complete suite of capabilities in order to accomplish their operational mission. Therefore, it is logically consistent to require the TSF to protect the objects that will impact the TOE's behavior. A user should be granted access only to those features of the operating system necessary to accomplish their designated role and must not be granted means to alter their own permissions.

(O.RESILIENT: FDP_ACC.1, FDP_ACF.1, FPT_FLS.1 (optional))

4.5 System Monitoring

In order to identify unauthorized TOE configuration changes and attempted malicious activity against protected objects, the TOE is expected to provide the ability to generate audit events. This audit trail should be able to provide administrative insight into system operations by identifying changes to subject data and, depending on the ESM architecture, usage of the authentication function. Depending on the architecture of the TOE, the audit data may be stored internally to the TOE or in an external repository.

This PP does not mandate any specific actions to be taken in the event that the audit repository is not accessible. The ST author must document the behavior that the TOE exhibits in this instance.

(O.MONITOR: FAU_GEN.1, FAU_SEL.1, FAU_STG.1, FAU_STG_EXT.1)

4.6 Continuity of Enforcement

Due to the distributed nature of ESM capabilities, situations such as network attacks, system attacks, or accidental maintenance errors may cause connections between systems to be severed. For this reason, the TOE should not fully rely on a remote Policy Management product to provide it with access control decision information. The capability must exist for the TOE to enforce some sort of policy in the event of a disruption of network service.

(O.MAINTAIN: FPT_FLS_EXT.1, FRU_FLT.1)

4.7 ESM Component Validation

In addition to the ability to validate policies, the TOE should have the ability to validate the identity of the policy's origin (whether this is another ESM product or a distributed part of the TOE). Similarly, the TOE should be able to identify itself to other ESM components (or distributed components of itself) so that policy, identity, and audit data is only sent to trusted entities. Failure to do so could allow a compromise of organizational security data that could provide a basis for subsequent attacks. The TOE is expected to implement a cryptographic protocol to protect these data in transit. However, the cryptographic primitives employed by the protocol can be implemented by the TOE or through a capability provided by the operational environment. Once a secure channel is established, it will subsequently be used to transmit ESM data throughout the enterprise as needed.

(O.MNGRID, O.PROTCOMMS, O.SELFID: FCO_NRR.2, FCS_IPSEC_EXT.1 (optional), FCS_SSH_EXT.1 (optional), FCS_TLS_EXT.1 (optional), FCS_HTTPS_EXT.1 (optional)), FPT_APW_EXT.1, FPT_SKP_EXT.1, FTP_ITC.1)

4.8 Cryptographic Services

The TOE must be able to use cryptographic primitives (encryption, decryption, random bit generation, etc.) in order to ensure the confidentiality and integrity of the policy data it receives and to provide trusted communications between itself and the Operational Environment where necessary. The services themselves may be part of the TOE (O.CRYPTO) or they may be implemented by the Operational Environment (OE.CRYPTO).

(O.CRYPTO (optional): FCS_CKM.1 (optional), FCS_CKM_EXT.4 (optional),

FCS_COP.1(1) (optional), FCS_COP.1(2) (optional), FCS_COP.1(3) (optional), FCS_COP.1(4) (optional), FCS_RBG_EXT.1 (optional))

5 Extended Components Definition

This section provides a definition for all the extended components described within this PP. This includes both the required components specified in Section 6.1 and the optional components specified in Appendix C.

Note that some extended classes and families refer to multiple extended requirements but only some of them are actually used in this PP. This is to give the reader a better awareness of the scope of the extended families and to consistently represent them between PPs. If the scope of the TOE is limited to this PP on its own, the extended components that are discussed here but are not included in section **Error! Reference ource not found.** are not to be included.

5.1 Class ESM: Enterprise Security Management

This ESM class specifies functional requirements that support the definition, consumption, and enforcement of centralized access control, authentication, secure configuration, and auditing policies. The functional requirements defined in this class differ from those defined in CC Part 2 by defining specific methods by which the TSF interacts with the Operational Environment to achieve the goals of Enterprise Security Management.

5.1.1 ESM_DSC Object Discovery

Family Behavior

The requirements of this family ensure that the TSF will have the ability to identify Operational Environment objects and take some action based on this identification.

Component Leveling

There is only one component in this family, ESM_DSC.1. ESM_DSC.1, Object Discovery, requires the TSF to search the Operational Environment for data that meets some criteria and take action based upon discovery of such data. The primary purpose of this requirement is for use in mandatory access control (MAC) or similar environments so that the TSF can identify data that is not in a location allowed by its associated attributes and subsequently take some form of corrective action based on this.

5.1.1.1 ESM_DSC.1 Object Discovery

The ESM_DSC family defines requirements for taking an inventory of objects in the Operational Environment that exhibit certain characteristics and acting upon those objects in some manner. This pertains to ESM because the ability of the TSF to perform this action supports the primary function of an ESM TOE (in this case, access control). The ESM_DSC.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to examine and act upon an observation made of the Operational Environment.

Hierarchical to: No other components.

Dependencies: No dependencies.

ESM_DSC.1.1 The TSF shall be able to discover objects in the Operational Environment that meet the following conditions: [selection: unencrypted data that policy requires to be encrypted, data that resides in a domain that is inconsistent with the data's defined sensitivity attributes, [***assignment: other condition(s) that indicate that data that resides in the Operational Environment should be catalogued by the TSF***]].

Application Note: *The specific purpose of object discovery in this Protection Profile is for the TSF to detect objects that are entering or residing a domain in which they should not be allowed to exist.*

ESM_DSC.1.2 The TSF shall take the following actions upon discovery of an object as defined by ESM_DSC.1.1: [selection: encrypt the object, move the object to a location consistent with its sensitivity attributes, delete the object, [***assignment: other action***]].

Application Note: *If the assignment is selected, the specific action taken must relate to corrective action taken against the discovered object.*

Management: ESM_DSC.1

The following actions could be considered for the management functions in FMT:

a) Specification of detection criteria.

b) Specification of actions taken upon discovery of object that meets detection criteria.

Audit: ESM_DSC.1

The following actions should be auditable if ESM_DSC.1 Object discovery is included in the PP/ST:

a) Minimal: Discovery of objects that meet detection criteria.
b) Minimal: Action taken against discovered object.

5.1.2 ESM_EID Enterprise Identification

Family Behavior

The requirements of this family ensure that the TSF will have the ability to interact with external entities for the purpose of identifying administrators, users, or other subjects.

Component Leveling

There are two non-hierarchical components in this family, ESM_EID.1 and ESM_EID.2.

ESM_EID.1, Enterprise Identification, requires the TSF to be able to receive identification requests from a defined set of external entities. These identification requests are then used as inputs for enterprise authentication. ESM_EID.1 is specific to the capability of an authentication server. Therefore, it is only discussed further in the ESM Authentication Server Protection Profile.

ESM_EID.2, Reliance on Enterprise Identification, is the opposite of ESM_EID.1. This allows the TSF to accept the validity of an identity that was asserted in the Operational Environment.

5.1.2.1 ESM_EID.2 Reliance on Enterprise Identification

The ESM_EID family defines requirements for facilitating enterprise user identification. This allows for the subsequent execution of enterprise user authentication. This differs from FIA_UID.1 and FIA_UID.2 specified in CC Part 2 because these requirements specifically apply to a user presenting identification to the TSF in order to perform activities that are mediated by the TSF. ESM_EID.2 applies to the ability of the TSF to be presented identification from the Operational Environment and to treat this as valid rather than performing its own identification request.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
ESM_EID.2.1	The TSF shall rely on [selection: [***assignment: identified TOE component(s) responsible for subject identification***], [***assignment: identified Operational Environment component(s) responsible for subject identification]***] for subject identification.
Application Note:	*If the subjects being identified in this manner are users or administrators of the TSF, it is expected that the assignment(s) will be completed with one or more authentication servers. Future versions of this Protection Profile may require the entities named in this assignment to be compliant with the Standard Protection Profile for Enterprise Security Management Authentication Server.* *If this SFR is claimed for a TOE that performs host-based access control, it is also acceptable to complete the second assignment with the operating system(s) on which the TOE resides. This prevents a malicious user from attempting to bypass the TSF by creating a new local user on a host system that may not be subject to the TOE's access control policy enforcement.*
ESM_EID.2.2	The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.
Application Note:	*If the TSF uses two different methods for identifying two distinct sets of subjects, the ST author must represent this by creating a different iteration of this SFR for each method.*

Management: ESM_EID.2

There are no management activities foreseen.

Audit: ESM_EID.2

There are no auditable events foreseen.

5.2 Class FAU: Security Audit

5.2.1 FAU_STG_EXT.1 External Audit Trail Storage

The FAU_STG_EXT family defines requirements for recording audit data to an external IT entity. Audit data refers to the information created as a result of satisfying FAU_GEN.1. This pertains to security audit because it discusses how audit data should be handled. The FAU_STG_EXT.1 requirement has been added because CC Part 2 lacks an audit storage requirement that demonstrates the ability of the TSF to write audit data to one or more specific external repository in a specific secure manner, as well as supporting the potential for local temporary storage.[4]

Hierarchical to:	No other components.
Dependencies:	FAU_GEN.1 Audit Data Generation FTP_ITC.1 Inter-TSF Trusted Channel
FAU_STG_EXT.1.1	The TSF shall be able to transmit the generated audit data to [***assignment: non-empty list of external IT entities and/or "TOE-internal storage"***].
Application Note:	*The term "transmit" is intended to both TOE-initiation of the transfer of information, as well as the TOE transferring information in response to a request from an external IT entity.* *Examples of external IT entities could be an Audit Server ESM component on an external machine, an evaluated operating system sharing the platform with the TOE, or a centralized logging component. Transmission to multiple sources is permitted.*

[4] FAU_STG.1 could have been treated as an optional requirement in Appendix C -. However, as there might be systems that had only local storage, that would have meant FAU_STG_EXT.1 would also need to be optional. Combining both into a single non-optional SFR mandates protected audit storage and transmission, while still supporting an "all-in-one" product that combines ESM capabilities.

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

a) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and

b) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

Management: FAU_STG_EXT.1

The following actions could be considered for the management functions in FMT:

a) Specification of the external IT entities that will receive generated audit data.

Audit: FAU_STG_EXT.1

The following actions should be auditable if FAU_STG_EXT.1 External audit trail storage is included in the PP/ST:

a) Basic: Establishment and disestablishment of communications with the external IT entities that are used to receive generated audit data.

5.3 Class FCS: Cryptographic Support

5.3.1 FCS_CKM_EXT.4 Cryptographic Key Zeroization

The FCS_CKM_EXT family defines requirements for deletion of cryptographic keys. The FCS_CKM_EXT.4 requirement has been added to provide a higher degree of specificity for key generation than the corresponding requirements in CC Part 2.

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Management: FCS_CKM_EXT.4

There are no management actions foreseen.

Audit: FCS_CKM_EXT.4

The following actions should be auditable if FCS_CKM_EXT.4 Cryptographic Key Zeroization is included in the PP/ST:

a) Basic: Failure of the key zeroization process.

5.3.2 FCS_HTTPS_EXT HTTPS

Family Behavior

The requirements of this family ensure that the TSF will implement the HTTPS protocol in accordance with an approved cryptographic standard.

Component Leveling

There is only one component in this family, FCS_HTTPS_EXT.1. FCS_HTTPS_EXT.1, HTTPS, requires the TOE to implement HTTPS in accordance with a defined standard.

5.3.2.1 FCS_HTTPS_EXT.1 HTTPS

Hierarchical to:	No other components.
Dependencies:	FCS_TLS_EXT.1 TLS
FCS_HTTPS_EXT.1.1	The TSF shall implement the HTTPS protocol that complies with RFC 2818.
Application Note:	*The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done by adding additional detail in the TSS.*
FCS_HTTPS_EXT.1.2	The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

Management: FCS_HTTPS_EXT.1

There are no management actions foreseen.

Audit: FCS_HTTPS_EXT.1

The following actions should be auditable if FCS_HTTPS_EXT.1 HTTPS is included in

the PP/ST:

a) Basic: Failure to establish a session.
b) Basic: Establishment/termination of a session.

5.3.3 FCS_IPSEC_EXT IPsec

Family Behavior

The requirements of this family ensure that the TSF will implement the IPsec protocol in accordance with an approved cryptographic standard.

Component Leveling

There is only one component in this family, FCS_IPSEC_EXT.1. FCS_ IPSEC_EXT.1, IPsec, requires the TOE to implement IPsec in accordance with a defined standard.

5.3.3.1 FCS_IPSEC_EXT.1 IPsec

Hierarchical to:	No other components.
Dependencies:	FCS_COP.1 Cryptographic Operation
FCS_IPSEC_EXT.1.1	The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), [selection: no other algorithms, AES-GCM-128, AES-GCM-256 as specified in RFC 4106], and using [selection, choose at least one of: IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]].
Application Note:	*The first selection is used to identify additional cryptographic algorithms supported. Either IKEv1 or IKEv2 support must be provided, although conformant TOES can provide both; the second selection is used to*

make this choice. For IKEv1, the requirement is to be interpreted as requiring the IKE implementation conforming to RFC 2409 with the additions/modifications as described in RFC 4109. RFC 4868 identifies additional hash functions for use with both IKEv1 and IKEv2; if these functions are implemented, the third (for IKEv1) and fourth (for IKEv2) selection can be used. IKEv2 will be required after January 1st, 2014.

FCS_IPSEC_EXT.1.2 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.3 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.

Application Note: *The above requirement can be accomplished either by providing Security Administrator-configurable lifetimes (with appropriate FMT requirements and instructions in documents mandated by AGD_OPE, as necessary), or by "hard coding" the limits in the implementation.*

FCS_IPSEC_EXT.1.4 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to [***assignment: number between 100 - 200***] MB of traffic for Phase 2 SAs.

Application Note: *The above requirement can be accomplished either by providing Security Administrator-configurable lifetimes (with appropriate FMT requirements and instructions in documents mandated by AGD_OPE), or by "hard coding" the limits in the implementation. The ST author selects the amount of data in the range specified by the requirement.*

FCS_IPSEC_EXT.1.5 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: 24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP),

[***assignment: other DH groups that are implemented by the TOE***], no other DH groups].

Application Note: *The above requires that the TOE support DH Group 14. If other groups are supported, then those should be selected (for groups 24, 19, and 20) or specified in the assignment above; otherwise "no other DH groups" should be selected. This applies to IKEv1 and (if implemented) IKEv2 exchanges. In future publications of this PP DH Groups 19 (256-bit Random ECP) and 20 (384-bit RandomECP) will be required.*

FCS_IPSEC_EXT.1.6 The TSF shall ensure that all IKE protocols implement Peer Authentication using the [selection: DSA, rDSA, ECDSA] algorithm.

Application Note: *The selected algorithm should correspond to an appropriate selection for FCS_COP.1(2).*

FCS_IPSEC_EXT.1.7 The TSF shall support the use of pre-shared keys (as referenced in the RFCs) for use in authenticating its IPsec connections.

FCS_IPSEC_EXT.1.8 The TSF shall support the following:

1. Pre-shared keys shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters: [selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [***assignment: other characters***];
2. Pre-shared keys of 22 characters and [selection: [***assignment: other supported lengths***], no other lengths].

Application Note: *The ST author selects the special characters that are supported by TOE; they may optionally list additional special characters supported using the assignment. For the length of the pre-shared keys, a common length (22 characters) is required to help promote*

interoperability. If other lengths are supported they should be listed in the assignment; this assignment can also specify a range of values (e.g., "lengths from 5 to 55 characters") as well.

Management: FCS_IPSEC_EXT.1

There are no management actions foreseen.

Audit: FCS_ IPSEC _EXT.1

The following actions should be auditable if FCS_ IPSEC _EXT.1 IPsec is included in the PP/ST:

a) Basic: Failure to establish an SA.
b) Basic: Establishment/termination of an SA.

5.3.4 FCS_RBG_EXT Random Bit Generation

Family Behavior

The requirements of this family ensure that the TSF will generate random numbers in accordance with an approved cryptographic standard.

Component Leveling

There is only one component in this family, FCS_RBG_EXT.1. FCS_RBG_EXT.1, Cryptographic Operation (Random Bit Generation), requires the TOE to perform random bit generation in accordance with a defined standard.

5.3.4.1 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: NIST Special Publication 800-90 using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES), Dual_EC_DRBG (any)]; FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES] seeded by an entropy source that accumulates entropy from [selection: choose one of: (1)

one or more independent hardware-based noise sources, (2) one or more independent software-based noise sources, (3) a combination of hardware-based and software-based noise sources.].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [selection, choose one of: 128 bits, 256 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors that it will generate.

Management: FCS_RBG_EXT.1

There are no management actions foreseen.

Audit: FCS_RBG_EXT.1

The following actions should be auditable if FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation) is included in the PP/ST:

a) Basic: Failure of the randomization process.

5.3.5 FCS_SSH_EXT SSH

Family Behavior

The requirements of this family ensure that the TSF will implement the SSH protocol in accordance with an approved cryptographic standard.

Component Leveling

There is only one component in this family, FCS_SSH_EXT.1. FCS_SSH_EXT.1, SSH, requires the TOE to implement SSH in accordance with a defined standard.

5.3.5.1 FCS_SSH_EXT.1 SSH

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

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

Application Note: The ST author must provide enough detail to determine how the implementation is complying with the standard(s)

identified; this can be done by adding additional detail in the TSS. In a future version of this PP, a requirement will be added regarding rekeying. The requirement will read "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.1.2 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.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [***assignment: number of bytes***] bytes in an SSH transport connection are dropped.

Application Note: *RFC 4253 provides for the acceptance of "large packets" with the caveat that the packets should be of "reasonable length" or dropped. The assignment should be filled in by the ST author with the maximum packet size accepted, thus defining "reasonable length" for the TOE.*

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [selection: AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other algorithms].

Application Note: *In the assignment, the ST author can select the AES-GCM algorithms, or "no other algorithms" if AES-GCM is not supported. If AES-GCM is selected, there should be corresponding FCS_COP entries in the ST. Since the Dec. 2010 publication of NDPP v1.0, there has been considerable progress with respect to the prevalence of AES-GCM support in commercial network devices. It is likely that an updated version of this PP will be published in the future which will require AES-GCM and AES-CBC will become optional.*

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport

implementation uses SSH_RSA and [selection: PGP-SIGN-RSA, PGP-SIGN-DSS, no other public key algorithms] as its public key algorithm(s).

Application Note: *RFC 4253 specifies required and allowable public key algorithms. This requirement makes SSH-RSA "required" and allows two others to be claimed in the ST. The ST author should make the appropriate selection, selecting "no other public key algorithms" if only SSH_RSA is implemented.*

FCS_SSH_EXT.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [selection: hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96].

FCS_SSH_EXT.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

Management: FCS_SSH_EXT.1

There are no management actions foreseen.

Audit: FCS_SSH_EXT.1

The following actions should be auditable if FCS_SSH_EXT.1 SSH is included in the PP/ST:

a) Basic: Failure to establish a session.
b) Basic: Establishment/termination of a session.

5.3.6 FCS_TLS_EXT TLS

Family Behavior

The requirements of this family ensure that the TSF will implement the TLS protocol in accordance with an approved cryptographic standard.

Component Leveling

There is only one component in this family, FCS_TLS_EXT.1. FCS_TLS_EXT.1, TLS, requires the TOE to implement TLS in accordance with a defined standard.

5.3.6.1 FCS_TLS_EXT.1 TLS

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[selection:
None
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
].

Application Note: *The ST author must make the appropriate selections and assignments to reflect the TLS implementation. The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to this component, or by additional detail in the TSS.*

The ciphersuites to be used in the evaluated configuration

are limited by this requirement. The ST author should select the optional ciphersuites that are supported; if there are no ciphersuites supported other than the mandatory suites, then "None" should be selected. If administrative steps need to be taken so that the suites negotiated by the implementation are limited to those in this requirement, the appropriate instructions need to be contained in the guidance called for by AGD_OPE. The Suite B algorithms (RFC 5430) listed above are the preferred algorithms for implementation. Since the Dec. 2010 publication of this requirement in NDPP v1.0, there has been limited progress with respect to extending the prevalence of TLS 1.2 support in commercial products. Future publications of this PP will require support for TLS 1.2 (RFC 5246); however, it is likely the next version of this PP will not include a requirement for TLS 1.2 support, but will require that the TOE offer a means to deny all connection attempts using SSL 2.0 or SSL 3.0.

Management: FCS_TLS_EXT.1

There are no management actions foreseen.

Audit: FCS_TLS_EXT.1

The following actions should be auditable if FCS_TLS_EXT.1 TLS is included in the PP/ST:

a) Basic: Failure to establish a session.
b) Basic: Establishment/termination of a session.

5.4 Class FPT: Protection of the TSF

5.4.1 FPT_APW_EXT Protection of Stored Credentials

Family Behavior

The requirements of this family ensure that the TSF will protect credential data from disclosure.

Component Leveling

There is only one component in this family, FPT_APW_EXT.1. FPT_APW_EXT.1, Protection of Stored Credentials, requires the TOE to store credentials in non-plaintext form and to prevent the reading of plaintext credentials.

5.4.1.1 FPT_APW_EXT.1 Protection of Stored Credentials

This SFR describes the behavior of the TOE when it must store credentials – either credentials for administrative users or credentials for enterprise users. An explicit requirement was required as there is no equivalent requirement in the Common Criteria. It was based on the requirement defined in the Network Device Protection Profile.

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

Management: FPT_APW_EXT.1

There are no management actions foreseen.

Audit: FPT_APW_EXT.1

There are no auditable actions foreseen.

5.4.2 FPT_FLS_EXT.1 Failure of Communication

This SFR describes the behavior of the TOE in the event there is a failure of the Policy Management product and TOE to communicate with one another.

Hierarchical to: No other components

Dependencies: No dependencies

FPT_FLS_EXT.1.1 The TSF shall maintain policy enforcement in the following manner when the communication between the TSF and the Policy Management product encounters a failure state: [selection: deny all requests, enforce the last policy received, [***assignment: failure policy***]].

Application Note: *The extended requirement above is used by the ST author to describe the behavior of the TOE in the event there is a failure of the Policy Management product and TOE to communicate with one another. This requirement was refined to show that the notion of a "secure state" is defined for the TOE to be continued enforcement of some sort of policy. The specific nature of the policy to be enforced in this situation is to be completed by the ST author.*

Management: FPT_FLS_EXT.1

The following actions could be considered for the management functions in FMT:

a) Definition of the behavior to take when a communications failure occurs.

Audit: FPT_FLS_EXT.1

The following actions should be auditable if FPT_FLS_EXT.1 Failure of Communications is included in the PP/ST:

a) Basic: Failure of communication between the TOE and Policy Management product.

5.4.3 FPT_SKP_EXT Protection of Secret Key Parameters

Family Behavior

The requirements of this family ensure that the TSF will protect credential data from disclosure.

Component Leveling

There is only one component in this family, FPT_SKP_EXT.1. FPT_SKP_EXT.1, Protection of Secret Key Parameters, requires the TOE to ensure that there is no mechanism for reading secret cryptographic data.

5.4.3.1 FPT_SKP_EXT.1 Protection of Secret Key Parameters

This SFR describes the behavior of the TOE when handling pre-shared, symmetric, and private keys, collectively referred to here as secret key parameters. An explicit requirement was required as there is no equivalent requirement in the Common Criteria. It was based on the requirement defined in the Network Device Protection Profile.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
FPT_SKP_EXT.1.1	The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Management: FPT_SKP_EXT.1

There are no management actions foreseen.

Audit: FPT_SKP_EXT.1

There are no auditable actions foreseen.

6 Security Requirements

The requirements in this document are divided into two sets of functional and assurance requirements. The first set of functional requirements is drawn from the Common Criteria and is designed to address the core requirements for auditing and policy enforcement. Functional requirements in this PP were drawn from Part 2 of the CC and are a formal instantiation of the Security Objectives. These requirements are relevant to supporting the secure operation of the TOE.

The Security Assurance Requirements (SARs) are typically inserted into a PP and listed separately from the SFRs; the CEM is then consulted during the evaluation based on the SARs chosen. Because of the nature of the Common Criteria Security Assurance Requirements and the specific technology identified as the TOE, a more tailored approach is taken in this PP. While the SARs are still listed for context and completeness in Section 6.2, the majority of the activities that an evaluator needs to perform for this TOE with respect to each SFR and SAR are detailed in "***Assurance Activities***" paragraphs. Assurance Activities are normative descriptions of activities that must take place in order for the evaluation to be complete. Assurance Activities are located in two places in this PP; those that are associated with specific SFRs are located with those SFRs, while those that are independent of the SFRs are detailed in Section 6.2. Note that the Assurance Activities are in fact a tailored evaluation methodology, presented in-line for readability, comprehension, and convenience.

For the activities associated directly with SFRs, after each SFR one or more Assurance Activities is listed detailing the activities that need to be performed to achieve the assurance required for conformant devices.

For the SARs that require activities that are independent of the SFRs, Section 6.2 indicates the additional Assurance Activities that need to be accomplished, along with pointers to the SFRs for which specific Assurance Activities associated with the SAR have been written.

Future iterations of the Protection Profile may provide more detailed Assurance Activities based on lessons learned from actual product evaluations.

6.1 Security Functional Requirements

The security functional requirements for the PP consist of the following components, summarized in Table 2. The formatting used for these requirements is defined in

Appendix D.1 – Operations.

Table 2. TOE Functional Components

Functional Component	
ESM_DSC.1 (optional)	Object Discovery *(optional – defined in Appendix C.2.1)*
ESM_EID.2	Reliance on Enterprise Identification
FAU_GEN.1	Audit Data Generation
FAU_SEL.1	Selective Audit
FAU_STG.1	Protected Audit Trail Storage (Local Storage)
FAU_STG_EXT.1	External Audit Trail Storage
FCO_NRR.2	Enforced Proof of Receipt
FCS_CKM.1 (optional)	Cryptographic Key Generation (for Asymmetric Keys) *(optional – defined in Appendix C.5.1)*
FCS_CKM_EXT.4 (optional)	Cryptographic Key Zeroization *(optional – defined in Appendix C.5.2)*
FCS_COP.1(1) (optional)	Cryptographic Operation (for Data Encryption/Decryption) *(optional – defined in Appendix C.5.3)*
FCS_COP.1(2) (optional)	Cryptographic Operation (for Cryptographic Signature) *(optional – defined in Appendix C.5.4)*
FCS_COP.1(3) (optional)	Cryptographic Operation (for Cryptographic Hashing) *(optional – defined in Appendix C.5.5)*
FCS_COP.1(4) (optional)	Cryptographic Operation (for Keyed-Hash Message Authentication) *(optional – defined in Appendix C.5.6)*
FCS_HTTPS_EXT.1 (optional)	HTTPS *(optional – defined in Appendix C.5.7)*
FCS_IPSEC_EXT.1 (optional)	IPsec *(optional – defined in Appendix C.5.8)*
FCS_RBG_EXT.1 (optional)	Extended: Cryptographic operation (Random Bit Generation) *(optional – defined in Appendix C.5.9)*
FCS_SSH_EXT.1 (optional)	SSH *(optional – defined in Appendix C.5.10)*
FCS_TLS_EXT.1 (optional)	TLS *(optional – defined in Appendix C.5.11)*
FDP_ACC.1 FDP_ACC.1(1) FDP_ACC.1(2)	Access Control Policy *(as defined for specific technology types in Appendix C.1.1 through C.1.4)*
FDP_ACF.1 FDP_ACF.1(1)	Access Control Functions *(as defined for specific technology types in Appendix C.1.1 through C.1.4)*

Functional Component	
FDP_ACF.1(2)	
FMT_MOF.1(1)	Management of Functions Behavior
FMT_MOF.1(2)	Management of Functions Behavior
FMT_MSA.1	Management of Security Attributes
FMT_MSA.3	Static attribute initialization
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_APW_EXT.1	Protection of Stored Credentials
FPT_FLS.1 (optional)	Failure with Preservation of Secure State *(optional – defined in Appendix C.3.1)*
FPT_FLS_EXT.1	Failure of Communications
FPT_SKP_EXT.1	Protection of Secret Key Parameters
FPT_RPL.1	Replay Detection
FRU_FLT.1	Degraded Fault Tolerance
FTA_TSE.1 (optional)	TOE Session Establishment *(optional – defined in Appendix C.4.1)*
FTP_ITC.1	Inter-TSF Trusted Channel (Prevention of Disclosure)

6.1.1 PP Application Notes

6.1.1.1 Usage

Application notes are provided after many requirements in the PP in order for the reader to identify the intent behind each requirement. The ST author must not reproduce any of these application notes in the ST.

6.1.1.2 Composition Philosophy

The ESM PPs represent a family of related Protection Profiles written to encompass the variable capabilities of ESM products. For an ST that claims conformance to multiple PPs within the ESM PP family, it is recommended that the ST author clarify how the ESM components relate to one another through usage of application notes. This will assist the reader in determining how the parts of the product that are to be evaluated correspond with the CC's notion of different ESM capabilities.

For example, multiple parts of the ESM may be deployed as a single appliance, as a series of redundant servers that also contain policy enforcement mechanisms, or as a client-server deployment in which enforcement points reside on individual client systems

that report to a single server. Usage of application notes makes it easy to determine the requirements that are unnecessary to claim based on the architecture of the ESM system.

6.1.2 Class ESM: Enterprise Security Management

ESM_EID.2 Reliance on Enterprise Identification

Hierarchical to: No other components.

ESM_EID.2.1 The TSF shall rely on [selection: [***assignment: identified TOE component(s) responsible for subject identification***], [***assignment: identified Operational Environment component(s) responsible for subject identification]***] for subject identification.

Application Note: *If the subjects being identified in this manner are users or administrators of the TSF, it is expected that the assignment(s) will be completed with one or more authentication servers. Future versions of this Protection Profile may require the entities named in this assignment to be compliant with the Standard Protection Profile for Enterprise Security Management Authentication Server.*

If this SFR is claimed for a TOE that performs host-based access control, it is also acceptable to complete the second assignment with the operating system(s) on which the TOE resides. This prevents a malicious user from attempting to bypass the TSF by creating a new local user on a host system that may not be subject to the TOE's access control policy enforcement.

ESM_EID.2.2 The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

Dependencies: No dependencies.

Application Note: *If the TSF uses two different methods for identifying two distinct sets of subjects, the ST author must represent this by creating a different iteration of this SFR for each*

method.

Assurance Activity:

The evaluator shall check the TSS and ensure that it describes where the subject identity data that the TOE uses to make access control decisions comes from. The evaluator shall also check to ensure that this information is appropriately represented by iterating the SFR for each identification mechanism that is used by the TSF.

There are no Operational Guidance activities for this SFR.

This SFR is not separately tested; appropriate behavior of the access control SFP is sufficient to assert that accurate subject identity data is received by the TOE.

6.1.3 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

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; and

b) All auditable events identified in Table 3 for the [not specified] level of audit; *and*

c) [***assignment: other auditable events***].

Table 3. Auditable Events

Component	Event	Additional Information
FAU_SEL.1	All modifications to audit configuration	None
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
FCO_NRR.2	The invocation of the non-repudiation service	Identification of the information, the destination, and a copy of the evidence provided
FCS_CKM.1 (optional)	Failure of the key generation activity	None
FCS_CKM_EXT.4 (optional)	Failure of the key zeroization process	Identity of subject requesting or causing zeroization, identity of object or entity being cleared

Component	Event	Additional Information
FCS_COP.1(1) (optional)	Failure of encryption or decryption	Cryptographic mode of operation, name/identifier of object being encrypted/decrypted
FCS_COP.1(2) (optional)	Failure of cryptographic signature	Cryptographic mode of operation, name/identifier of object being signed/verified
FCS_COP.1(3) (optional)	Failure of hashing function	Cryptographic mode of operation, name/identifier of object being hashed
FCS_COP.1(4) (optional)	Failure in Cryptographic Hashing for Non-Data Integrity	Cryptographic mode of operation, name/identifier of object being hashed
FCS_HTTPS_EXT.1 (optional)	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FCS_IPSEC_EXT.1 (optional)	Failure to establish an SA, establishment/termination of an SA	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FCS_RBG_EXT.1 (optional)	Failure of the randomization process	None
FCS_SSH_EXT.1 (optional)	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FCS_TLS_EXT.1 (optional)	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FDP_ACC.1	Any changes to the enforced policy or policies	Identification of Policy Management product making the change
FDP_ACF.1	All requests to perform an operation on an object covered by the SFP	Subject identity, object identity, requested operation
FMT_MOF.1	All modifications to TSF behavior	None
FPT_FLS_EXT.1	Failure of communication between the TOE and Policy Management product	Identity of the Policy Management product, reason for the failure
FPT_RPL.1	Detection of replay	Action to be taken based on the specific actions
FTA_TSE.1 (optional)	Denial of session establishment	None
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel

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 (if applicable), 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, [***assignment: other audit relevant information***].

Application Note: *The "other audit relevant information" must include sufficient information to identify the responsible individual and the specific action taken by the individual.*

Dependencies: FPT_STM.1 Reliable Time Stamps

Assurance Activity:

The evaluator shall check the TSS and ensure that it summarizes the auditable events and describes the contents of the audit records.

The evaluator shall check the operational guidance and ensure that it lists all of the auditable events and provides description of the content of each type of audit record. Each audit record format type shall be covered, and shall include a brief description of each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN 1.2, and the additional information specified in Table 3.

The evaluator shall review the operational guidance, and any available interface documentation, in order to determine the administrative interfaces (including subcommands, scripts, and configuration files) that permit configuration (including enabling or disabling) of the mechanisms implemented in the TOE that are necessary to enforce the requirements specified in the PP. The evaluator shall document the methodology or approach taken to do this. The evaluator may perform this activity as part of the activities associated with ensuring the AGD_OPE guidance satisfies the requirements. Using this list, the evaluation shall confirm that each security relevant administrative interface has a corresponding audit event that records the information appropriate for the event.

The evaluator shall test the TOE's audit function by having the TOE generate audit records for all events that are defined in the ST and/or have been identified in the

previous two activities. The evaluator shall then check the audit repository defined by the ST, operational guidance, or developmental evidence (if available) in order to determine that the audit records were written to the repository and contain the attributes as defined by the ST.

This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an incorrect authentication secret is entered, then audit records will be expected to be generated as a result of testing identification and authentication. The evaluator shall also check to ensure that the content of the logs are consistent with the activity performed on the TOE. For example, if a test is performed such that a policy is defined, the corresponding audit record should correctly identify the policy that was defined.

FAU_SEL.1 Selective Audit

Hierarchical to:	No other components.
FAU_SEL.1.1	The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes: a) [selection: object identity, user identity, subject identity, host identity, event type] b) [***assignment: list of additional attributes that audit selectivity is based upon***]
Application Note:	*The selective audit capability is expected to be exercised by a compatible Policy Management or Secure Configuration Management product, not by a user directly accessing the TOE.*
Dependencies:	FAU_GEN.1 Audit Data Generation FMT_MTD.1 Management of TSF Data

Assurance Activity:

The evaluator shall check the TSS in order to determine that it discusses the TSF's ability to have selective auditing and that it summarizes the mechanism(s) by which auditable events are selected for auditing.

The evaluator shall check the operational guidance in order to determine the selections that are capable of being made to the set of auditable events, and shall confirm that it contains all of the selections identified in the Security Target.

The evaluator shall test this capability by using a compatible ESM Policy Management or ESM Secure Configuration Management product to configure the TOE in the following manners:

- *All selectable auditable events enabled*
- *All selectable auditable events disabled*
- *Some selectable auditable events enabled*

For each of these configurations, the evaluator shall perform all selectable auditable events and determine by review of the audit data that in each configuration, only the enabled events are recorded.

FAU_STG.1 Protected Audit Trail Storage (Local Storage)

Hierarchical to:	No other components.
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.
FAU_STG.1.2	The TSF shall be able to prevent unauthorized modifications to the stored audit records in the audit trail.
Application Note:	*In addition to the capability to export the audit information, the TOE is required to have some amount of local storage. The ST writer must specify the amount of local storage available for the audit records; this can be in megabytes, average number of audit records, etc.*
Dependencies:	FAU_GEN.1 Audit Data Generation

Assurance Activity:

The evaluator shall examine the TSS to ensure it describes the amount of audit data that are stored locally, what happens when the local audit data store is full, and how these records are protected against unauthorized access.

The evaluator shall examine the operational guidance to determine that it describes the relationship between the local audit data and the audit data that are sent to the audit log

server. For example, when an audit event is generated, is it simultaneously sent to the external server and the local store, or is the local store used as a buffer and "cleared" periodically by sending the data to the audit server.

The evaluator shall test this capability by attempting to access locally-stored audit data without authorization and observe that the attempts fail. They shall also observe that the space allocated for audit storage is consistent with the TSF's capabilities.

FAU_STG_EXT.1 External Audit Trail Storage

Hierarchical to: No other components.

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [***assignment: non-empty list of external IT entities and/or "TOE-internal storage"***].

Application Note: *The term "transmit" is intended to both TOE-initiation of the transfer of information, as well as the TOE transferring information in response to a request from an external IT entity.*

Examples of external IT entities could be an Audit Server ESM component on an external machine, an evaluated operating system sharing the platform with the TOE, or a centralized logging component. Transmission to multiple sources is permitted.

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

a) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and

b) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

Dependencies: FAU_GEN.1 Audit Data Generation

FTP_ITC.1 Inter-TSF Trusted Channel

Application Note: *This requirement provides the ability to transmit generated audit data to one or more external IT entities or products; it also supports local storage and protection of generated audit data (presumably, as a temporary measure when communications with the external IT entity are unavailable). The ST author must indicate how audit data is recorded when the external IT entity specified in this requirement is unavailable and how synchronization is achieved when communications are re-established.*

Assurance Activity:

The evaluator shall check the TSS in order to determine that it describes the location where the TOE stores its audit data, and if this location is remote, the trusted channel that is used to protect the data in transit.

The evaluator shall check the operational guidance in order to determine that it lists any configuration steps required to set up audit storage. If audit data is stored in a remote repository, the evaluator shall also check the operational guidance in order to determine that a discussion on the interface to this repository is provided, including how the connection to it is established, how data is passed to it, and what happens when a connection to the repository is lost and subsequently re-established.

The evaluator shall test this function by configuring this capability, performing auditable events, and verifying that the local audit storage and external audit storage contain identical data. The evaluator shall also make the connection to the external audit storage unavailable, perform audited events on the TOE, re-establish the connection, and observe that the external audit trail storage is synchronized with the local storage. Similar to the testing for FAU_GEN.1, this testing can be done in conjunction with the exercise of other functionality. Finally, since the requirement specifically calls for the audit records to be transmitted over the trusted channel established by FTP_ITC.1, verification of that requirement is sufficient to demonstrate this part of this one.

6.1.4 Class FCO: Communication

FCO_NRR.2 Enforced proof of receipt

Hierarchical to:	FCO_NRR.1 Selective proof of receipt
FCO_NRR.2.1	The TSF shall enforce the generation of evidence of receipt for received [policies] at all times.
FCO_NRR.2.2	The TSF shall be able to relate the [***assignment: list of attributes***] of the recipient of the information, and the [***assignment: list of information fields***] of the information to which the evidence applies.
Application Note:	*The ST author must complete the first assignment with the information that the TOE uses to identify itself as a valid recipient of a policy (such as a hostname, IP address, and digital certificate).* *The ST author must complete the second assignment with the information that is used to uniquely identify a policy (such as policy name and version) so that an accurate receipt can be sent to the Policy Management product.*
FCO_NRR.2.3	The TSF shall provide a capability to verify the evidence of receipt of information to [originator] given [***assignment: limitations on the evidence of receipt***].
Application Note:	*The ST author must complete the assignment with the time interval in which the TOE sends policy receipt and implementation status to the Policy Management product.*
Dependencies:	FIA_UID.1 Timing of Identification

Assurance Activity:

The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it discusses how the TOE identifies itself to the Policy Management product and how it provides evidence of the policy's consumption to the Policy Management product.

The evaluator shall check the operational guidance in order to determine how the TOE confirms evidence of received policy data back to the Policy Management product that originally sent it that policy data. This should include the contents and formatting of the receipt such that the data that it contains is verifiable.

The evaluator shall test this capability by configuring an environment such that the TOE is allowed to accept a policy from a certain source, sending it a policy from that source, observing that the policy is subsequently consumed, and that an accurate receipt is transmitted back to the Policy Management product within the time interval specified in the ST. The evaluator confirms accuracy by using the Policy Management product to view the receipt and ensure that its contents are consistent with known data.

6.1.5 Class FCS: Cryptographic Support

The cryptographic requirements for the TOE can either be implemented by the TSF or by reliance on non-ESM Operational Environment components. The expectation is that the TSF is able to use a suite of cryptographic algorithms that have been previously validated rather than forcing vendors to implement their own unique and redundant cryptographic capabilities. The ST author must clearly indicate what cryptographic capabilities are used by the TSF. Regardless of where the cryptographic capabilities reside, the expected capabilities are the same.

Refer to Appendix C.5C.5 for the cryptographic requirements for the TOE.

6.1.6 Class FDP: User Data Protection

The PP has included three types of data protection mechanisms that relate to different situations in which access control is necessary. The list of such mechanisms is expected to be amended over time to include additional means of access control as necessary.

There are currently three distinct sets of FDP_ACC.1 and FDP_ACF.1 requirements within this Protection Profile. Depending on the data protection mechanism that applies to the TOE claimed within the evaluation, the Security Target author must choose the corresponding FDP requirements for the Security Target. Each set of FDP requirements claims specific functionality that relates to the mechanism chosen. The FDP requirements can be found within Appendix C.1. The three current mechanisms for TOEs to conform to are as follows: Host-based Access Control, Web-based Access Control, and Data Loss Prevention Access Control.

FDP_ACC.1 Access Control Policy

Refer to Appendix C.1.

Application Note: *If the TSF is able to enforce multiple different types of access control policies simultaneously (host-based, data loss prevention, etc.), it may be necessary to iterate this requirement for each distinct policy type that is enforced. In this situation, it is acceptable to refine the names of the policies being enforced so that the overloaded term "access control SFP" does not create ambiguity.*

Assurance Activity:

Specific assurance activities are defined for each technology type in Appendix C.1.

If the TSF enforces multiple distinct types of access control policies, the evaluator shall also ensure that the SFRs for each policy are properly iterated in the ST and that all of the assurance activities for each individual iteration are satisfied.

FDP_ACF.1 Access Control Functions

Refer to Appendix C.1.

Application Note: *If the TSF is able to enforce multiple different types of access control policies simultaneously (host-based, data loss prevention, etc.), it may be necessary to iterate this requirement for each distinct policy type that is enforced. In this situation, it is acceptable to refine the names of the policies being enforced so that the overloaded term "access control SFP" does not create ambiguity.*

Assurance Activity:

Refer to FDP_ACC.1 above.

6.1.7 Class FMT: Security Management

FMT_MOF.1(1) Management of Functions Behavior

Hierarchical to: No other components.

FMT_MOF.1.1(1) The TSF shall restrict the ability to [selection: determine

the behavior of, disable, enable, modify the behavior of] the functions[: audited events, repository for trusted audit storage, access control SFP, policy being implemented by the TSF, access control SFP behavior to enforce in the event of communications outage, [***assignment: other functions***]] to [an authorized and compatible Policy Management product].

Application Note: *The ST author must define how the TSF is able to trust the Policy Management product. For example, the TSF may internally associate certain keys with its Policy Management product such that if a trusted channel is established using those keys, then the TSF knows that it should trust policy data that originates from the other end of that channel.*

With respect to the ability to determine the behavior of the policy being implemented by the TSF, this can be a query as to the version of a policy, or a query as to the details of the policy. This must be made clear in the TSS.

Dependencies: FMT_SMF.1 Specification of Management Functions

FMT_SMR.1 Security Roles

Assurance Activity:

The evaluator shall check the TSS in order to determine that it summarizes how the management functions described in the SFR are performed (or, if their behavior is fixed, why this is the case) and how the TSF determines that the management request is authorized.

The evaluator shall check the operational guidance in order to determine that it describes the process by which the TOE can be associated with a Policy Management product and how that product is subsequently used to manage the TOE.

The evaluator shall test this capability by deploying the TOE in an environment where there is a Policy Management product that is able to communicate with it. The evaluator shall configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator shall use the

Policy Management product to modify the behavior of the functions specified in the requirement above. For each function, the evaluator shall verify that the modification applied appropriately by using the Policy Management product to query the behavior for and after the modification.

The evaluator shall also perform activities that cause the TOE to react in a manner that the modification prescribes. These actions include, for each function, the following activities:

- *Audited events: perform an event that was previously audited (or not audited) prior to the modification of the function's behavior and observe that the audit repository now logs (or doesn't log) this event based on the modified behavior*
- *Repository for trusted audit storage: observe that audited events are written to a particular repository, modify the repository to which the TOE should write audited events, perform auditable events, and observe that they are no longer written to the original repository*
- *Access Control SFP: perform an action that is allowed (or disallowed) by the current Access Control SFP, modify the implemented SFP such that that action is now disallowed (or allowed), perform the same action, and observe that the authorization differs from the original iteration of the SFP.*
- *Policy being implemented by the TSF: perform an action that is allowed (or disallowed) by a specific access control policy, provide a TSF policy that now disallows (or allows) that action, perform the same action, and observe that the authorization differs from the original iteration of the FSP.*
- *Access Control SFP behavior to implement in the event of communications outage: perform an action that is handled in a certain manner in the event of a communications outage (if applicable), re-establish communications between the TOE and the Policy Management product, change the SFP behavior that the TOE should implement in the event of a communications outage, sever the connection between the TOE and the Policy Management product, perform the same action that was originally performed, and observe that the modified way of handling the action is correctly applied.*

Once this has been done, the evaluator shall reconfigure the TOE and Policy Management product such that the Policy Management product is no longer authorized to configure the TOE. The evaluator shall then attempt to use the Policy Management product to configure the TOE and observe that it is either disallowed or that the option is

not even present.

FMT_MOF.1(2) Management of Functions Behavior

Hierarchical to:	No other components.
FMT_MOF.1.1(2)	The TSF shall restrict the ability to [determine the behavior of] the functions[: policy being implemented by the TSF, [***assignment: other functions***]] to [an authorized and compatible Enterprise Security Management product].
Dependencies:	FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security Roles

Assurance Activity:

The evaluator shall check the TSS in order to determine that it indicates the ESM products (or distributed TOE components if multiple ESM PPs are claimed) that are authorized to query the TOE and that this includes, at minimum, a Policy Management component.

The evaluator shall check the operational guidance in order to determine that it describes the process by which the TOE can be associated with other ESM products and why these other products are used to interface with the TSF.

The evaluator shall test this capability by deploying the TOE in an environment where there is a Policy Management product that is able to communicate with it. The evaluator shall configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator shall use the Policy Management product to query the policy being implemented by the TOE.

Once this has been done, the evaluator shall reconfigure the TOE and Policy Management product such that the Policy Management product is no longer authorized to configure the TOE. The evaluator shall then attempt to use the Policy Management product to configure the TOE and observe that it is either disallowed or that the option is not even present.

FMT_MSA.1 Management of Security Attributes

Hierarchical to:	No other components.

FMT_MSA.1.1	The TSF shall enforce the [access control SFP] to restrict the ability to [selection: change_default, query, modify, delete, [***assignment: other operations***]] the security attributes [access control policies, access control policy attributes, implementation status of access control policies] to [an authorized and compatible Policy Management product].
Dependencies:	FDP_ACC.1 Subset Access Control FMT_SMF.1 Specification of Management Functions FMT_SMR.1 Security Roles

Assurance Activity:

The evaluator shall review the TSS and the operational guidance to confirm that the indicated attributes are maintained by the TOE.

The evaluator shall also confirm that the operational guidance defines how authorizations to manage the defined security attributes are derived so that an administrator will know how to configure separation of duties.

The evaluator shall test this capability by using the associated Policy Management product to confirm that each identified operation against the indicated attributes may be performed, and that the TOE interfaces do not provide the ability for any other roles to perform operations against the indicated attributes.

FMT_MSA.3 Static Attribute Initialization

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [access control SFP] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow the [authorized and compatible Policy Management product] to specify alternative initial values to override the default values when an object or information is created.
Application Note:	*The intent of this SFR is to define the ability of the TSF to*

operate in a default deny posture if configured to do so.

Dependencies: FMT_MSA.1 Management of Security Attributes

FMT_SMR.1 Security Roles

Assurance Activity:

The evaluator shall review the TSS in order to determine how the TSF puts restrictive default values into place (for example, access control policies should operate in deny-by-default mode so that the absence of an access control rule doesn't fail to restrict an operation) and what authorizations are required in order to override these defaults.

The evaluator shall review the operational guidance in order to ensure that it warns the reader of the restrictive nature of default values and provides instructions on how to override them.

The evaluator shall test this capability by using the associated Policy Management product to confirm that for each identified security attribute and restrictive initial state, the TOE implements the correct restrictive value and that it can be overridden in the manner specified by the operational guidance.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[**configuration of audited events, configuration of repository for trusted audit storage, configuration of Access Control SFP, querying of policy being implemented by the TSF, management of Access Control SFP behavior to enforce in the event of communications outage, [***assignment: other management functions to be provided by the TSF***]].

Application Note: The expectation of this requirement is that these management functions will be controlled through another ESM product rather than through direct administrative action.

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check the TSS in order to determine what Policy Management and Secure Configuration Management product(s) (if applicable) are compatible with the TOE.

The evaluator shall check the operational guidance in order to ensure that it describes how to configure the TOE to interface with the compatible products discussed in the TSS. The evaluator shall also check the operational guidance to verify that it provides instructions for performing each of the defined management functions.

The evaluator shall test this capability by configuring the TOE in a manner that is consistent with the evaluated configuration. For each management function that has been defined in the ST, the evaluator shall perform the function in a manner that is consistent with the operational guidance and verify that the observed behavior is consistent with the expectations of what the function should accomplish.

FMT_SMR.1 Security Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [***assignment: the role(s) associated with authorized Policy Management products upon establishment of connectivity to the TOE***].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of Identification

Assurance Activity:

The evaluator shall examine the TSS to verify that it describes how management authority is delegated via one or more roles and how an authorized Policy Management product is associated with those roles.

The evaluator shall review the operational guidance in order to verify that it discusses the various administrative role(s) that are used to manage the TSF and any applicable steps that are required for an administrator to assume such a role.

The evaluator shall use the associated Policy Management product to connect to the TOE and confirm that it is operating in the assigned role. The evaluation shall also confirm that a user or other external entity that has not been authorized for the indicated role

cannot assume the indicated role.

6.1.8 Class FPT: Protection of the TSF

FPT_APW_EXT.1 Protection of Stored Credentials

Hierarchical to: No other components.

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

Application Note: *The intent of the requirement is that raw password authentication data are not stored in the clear, and that no user or administrator is able to read the plaintext password through "normal" interfaces. An all-powerful administrator of course could directly read memory to capture a password but is trusted not to do so.*

If the TOE uses an external Identity and Credential Management product to define its administrator authentication data, the purpose of this SFR is to ensure that a copy of the data is not stored or retained by the TOE when it is input.

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall examine the TSS to determine that it details all authentication data , other than private keys addressed by FPT_SKP_EXT.1, that is used or stored by the TSF, and the method used to obscure the plaintext credential data when stored. This includes credential data stored by the TOE if the TOE performs authentication of users, as well as any credential data used by the TOE to access services in the operational environment (such as might be found in stored scripts). The TSS shall also describe the mechanisms used to ensure credentials are stored in such a way that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. Alternatively, if authentication data is not stored by the TOE because the authoritative repository for this data is in the Operational Environment, this shall be detailed in the TSS.

There are no operational guidance activities for this SFR.

The evaluator shall test this SFR by reviewing all the identified credential repositories to ensure that credentials are stored obscured, and that the repositories are not accessible to non-administrative users. The evaluator shall similarly review all scripts and storage for mechanisms used to access systems in the operational environment to ensure that credentials are stored obscured and that the system is configured such that data is inaccessible to non-administrative users.

FPT_FLS_EXT.1 Failure of Communications

Hierarchical to: No other components.

FPT_FLS_EXT.1.1 The TSF shall maintain policy enforcement in the following manner when the communication between the TSF and the Policy Management product encounters a failure state: [selection: deny all requests, enforce the last policy received, **[*assignment: characterization of failure state policy enforced*]**].

Application Note: *The refined requirement above is used by the ST author to describe the behavior of the TOE in the event there is a failure of the Policy Management product and TOE to communicate with one another. The specific nature of the policy to be enforced in this situation is to be completed by the ST author.*

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check the TSS in order to determine that it describes how the SFP(s) defined in FDP_ACC.1 are enforced when the TOE cannot communicate with the Policy Management product that provided the enforced policy. If communications are not expected to be severed (for example, if the TOE and Policy Management product run on the same system), the evaluator shall check the TSS in order to determine that this assertion has been made. If the assignment is chosen to define an alternate failure state behavior, the evaluator shall verify that the failure state behavior is documented in sufficient detail to be unambiguously verifiable.

The evaluator shall check the operational guidance (and developmental evidence, if available) in order to determine that it discusses how the TOE is deployed in relation to other ESM products. This is done so that the evaluator can determine the expected behavior if the TOE is unable to interact with its accompanying Policy Management product.

The evaluator shall test this capability by terminating the Policy Management product (if the TOE resides on the same system) or by severing the network connection between the Policy Management product and the TOE (if the TOE resides on a different system). The evaluator shall then interact with the TOE while these communications are suspended in order to determine that the behavior it exhibits in this state is consistent with the expected behavior. If the assignment is chosen to define an alternate failure state behavior, the evaluator shall verify that the observed behavior corresponds to its description in the TSS.

FPT_RPL.1 Replay Detection

Hierarchical to:	No other components.
FPT_RPL.1.1	The TSF shall detect replay for the following entities: [***assignment: list of identified entities***].
FPT_RPL.1.2	The TSF shall perform [***assignment: list of specific actions***] when replay is detected.
Application Note:	*It is not acceptable for the list of identified entities to be empty or "none", nor is it acceptable for the specific actions to be empty or "none".*
Dependencies:	No dependencies.

Assurance Activity:

The evaluator shall check the TSS in order to determine that it describes the method by which the TSF detects replayed data. For example, it may provide a certificate or other value that can be validated by the TSF to verify that the policy is consistent with some anticipated schema. Alternatively, the TOE may use a protocol such as SSL for transmitting data that immunizes it from replay threats.

If the method of replay detection is configurable, the evaluator shall check the operational guidance in order to determine that it provides instructions for setting up and

configuring the replay detection mechanism. This may be simple (e.g. setting up and enabling a TLS channel with shared secret) or complex (e.g. defining specific policy attributes that are positively associated with unauthorized changes), depending on how specifically replay detection is implemented by the TSF.

The evaluator shall test this capability by configuring replay detection in a manner specified by the operational guidance (if applicable), running a packet sniffer application (such as Wireshark) on the local network with the TOE, sending a valid policy to it, and observing the packets that comprise this policy. The evaluator can then take these packets and re-transmit them to the TOE. Once this has been done, the evaluator shall execute an appropriate subset of User Data Protection testing with the expectation that the policy enforced will be the first policy transmitted. If the expected results are met, the TOE is sufficiently resilient to rudimentary policy forgery.

FPT_SKP_EXT.1 Protection of Secret Key Parameters

Hierarchical to:	No other components.
FPT_SKP_EXT.1.1	The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.
Application Note:	*The intent of the requirement is that an administrator is unable to read or view the identified keys (stored or ephemeral) through "normal" interfaces. While it is understood that the administrator could directly read memory to view these keys, do so is not a trivial task and may require substantial work on the part of an administrator. Since the administrator is considered a trusted agent, it is assumed they would not endeavor in such an activity.*
Dependencies:	No dependencies.

Assurance Activity:

The evaluator shall examine the TSS to determine that it details how any pre-shared keys, symmetric keys, and private keys are stored and that they are unable to be viewed through an interface designed specifically for that purpose, as outlined in the application note. If these values are not stored in plaintext, the TSS shall describe how they are

protected/obscured.

There are no operational guidance or testing activities for this SFR.

6.1.9 Class FRU: Resource Utilization

FRU_FLT.1 Degraded Fault Tolerance

Hierarchical to:	No other components.
FRU_FLT.1.1	The TSF shall ensure the operation of [enforcing the most recent policy] when the following failures occur: [restoration of communications with the Policy Management product after an outage].
Dependencies:	FPT_FLS.1 Failure with Preservation of Secure State

Assurance Activity:

The evaluator shall check the TSS in order to determine that describes how the TSF ensures that it is enforcing the most up-to-date policy. If an a malicious user was able to disconnect their system and the TOE misses a policy update from Policy Management during this outage, it is expected that the updated policy will be received once communications are resumed.

The evaluator shall check the operational guidance in order to verify that it discusses how the TSF receives the latest policy from the Policy Management product once a communications failure has been resolved, including any options that an administrator has in configuring this capability.

The evaluator shall test this capability by severing the network connection between the TOE and the Policy Management product, defining an updated policy, and re-establishing the connection will determine if the TOE appropriately receives the new policy data within the time interval specified in FCO_NRR.2.3. The evaluator shall devise a scenario such that the old policy allows a specific action and that the new policy denies that same action. The evaluator shall then perform that action, observe that it is allowed, sever connection with the Policy Management product, define the new policy during that outage, re-establish the connection, wait for the interval defined by FCO_NRR.2.3, perform the same action again, and observe that it is no longer allowed.

6.1.10 Class FTP: Trusted Paths/Channels

FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to: No other components.

FTP_ITC.1.1 *Refinement:* The TSF shall *use [selection: IPsec, SSH, TLS, TLS/HTTPS] to* provide a *trusted* communication channel between itself and *authorized IT entities* that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_ITC.1.2 The TSF shall permit [selection: the TSF, another trusted IT product**]** to initiate communication via the trusted channel.

FTP_ITC.1.3 *Refinement:* The TSF shall initiate communication via the trusted channel for *transfer of policy data*, [***assignment: other functions***].

Application Note: *The intent of the above requirement is to use a cryptographic protocol to protect external communications with authorized IT entities that the TOE interacts with to perform its functions.*

In the selection for FTP_ITC.1.1, the ST author indicates the cryptographic protocol or protocols used to protect the communications channel. The ST author then includes the appropriate protocol requirement(s) from Appendix C.8 to reflect the implemented protocols. If the TOE implements its own cryptographic primitives (e.g., encryption/decryption, hashing), the ST author also includes the appropriate FCS requirements from Appendix C.6 in the ST.

The ST author must fill out the assignment in FTP_ITC.1.3 with all protected communications the TOE has with other ESM products (transfer of audit data, request for identity data, etc.). Note that transfer of authentication responses is

not listed here because it is assumed that the trusted channel for this transmission is either initiated by the product providing the response or is the same channel initiated by the TSF that was used to issue the transfer of the initial challenge.

If the TOE claims conformance to multiple PPs, remote interfaces to distributed components of the TOE must be claimed here and evaluated as if they were interfaces to the Operational Environment.

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall examine the TSS to determine that, for all communications with authorized IT entities identified in the requirement, each communications mechanism is identified in terms of the allowed protocols for that IT entity. The evaluator shall also confirm that all protocols listed in the TSS are specified and included in the requirements in the ST.

The evaluator shall confirm that the operational guidance contains instructions for establishing the allowed protocols with each authorized IT entity.

The evaluator shall also perform the following tests:

- *Test 1: The evaluators shall ensure that communications using each protocol with each authorized IT entity is tested during the course of the evaluation, setting up the connections as described in the operational guidance and ensuring that communication is successful.*
- *Test 2: For each protocol that the TOE can initiate as defined in the requirement, the evaluator shall follow the operational guidance to ensure that in fact the communication channel can be initiated from the TOE.*
- *Test 3: The evaluator shall ensure, for each communication channel with an authorized IT entity, the channel data is not sent in plaintext.*
- *Test 4: The evaluator shall ensure, for each communication channel with an authorized IT entity, modification of the channel data is detected by the TOE.*

Further assurance activities are associated with the specific FCS requirement(s) that are applicable to the TOE.

6.1.11 Unfulfilled Dependencies

This section details Security Functional Requirements (SFRs) that were listed as dependencies to requirements chosen for this PP but have not been claimed. For each such requirement, a rationale for its exclusion has been provided.

FIA_UID.1	This SFR is an unfulfilled dependency on FCO_NRR.2. It has not been included because the application notes and defined assignments of FCO_NRR.2 state that the identity of policy origin is limited to software/hardware information rather than the user identity of any user initiating the policy forwarding function. This SFR is also a dependency on FMT_SMR.1. It has not been included to satisfy this dependency because management roles will be associated with identified Policy Management products. Therefore, the SFRs mapped to O.MNGRID are considered to be sufficient to facilitate subject identification.
FMT_MTD.1	This SFR is an unfulfilled dependency on FAU_SEL.1 It has not been included because the intent of the dependency is that the TSF data governing the configuration of the auditing function is expected to be configurable. This dependency is satisfied by FMT_MOF.1(1) because the auditing behavior is considered to be a function of the TSF rather than a collection of TSF data.
FPT_STM.1	This SFR is an unfulfilled dependency on FAU_GEN.1. It has not been included because the TOE is not necessarily expected to include its own system clock. The ST author must examine the entire ESM under evaluation in order to determine the point of origin for system time. If the evaluation boundary is an entire ESM appliance that uses an internal system clock, FPT_STM.1 must be claimed. However, if the ESM relies on an environmental component such as a host operating system or NTP server, it is an acceptable alternative to represent accurate system time as an environmental objective.

FPT_FLS.1	This dependency is satisfied through the alternate explicit requirement FPT_FLS_EXT.1. Note: FPS_FLS.1 is included as an optional requirement, but the optional use of FPT_FLS.1 is completed in a different way than its use in the SFR with the FPT_FLS.1 dependency (for which FPT_FLS_EXT.1 is the correct satisfaction).

6.2 Security Assurance Requirements

The Security Objectives for the TOE in Section 8.4.1 were constructed to address threats identified in Section 8.2. The Security Functional Requirements (SFRs) in Section 6.1 are a formal instantiation of the Security Objectives. The PP draws from EAL1 the Security Assurance Requirements (SARs) to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

As indicated in the introduction to Section 6.1 while this section contains the complete set of SARs from the CC, the Assurance Activities to be performed by an evaluator are detailed both in Appendix C - as well as in this section.

For each family, "Developer Notes" are provided on the developer action elements to clarify what, if any, additional documentation/activity needs to be provided by the developer. For the content/presentation and evaluator activity elements, additional assurance activities (to those already contained in section 6.1) are described as a whole for the family, rather than for each element. Additionally, the assurance activities described in this section are complementary to those specified in section 6.1**Error! eference source not found.**.

The TOE security assurance requirements, summarized in Table 4, identify the management and evaluative activities required to address the threats identified in Section 8.2 of this PP. Section 6.3 provides a succinct justification for choosing the security assurance requirements in this section.

Table 4. TOE Security Assurance Requirements

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.1	Labeling of the TOE

Assurance Class	Assurance Components	Assurance Components Description
	ALC_CMS.1	TOE CM Coverage
Tests	ATE_IND.1	Independent Testing – Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Survey

6.2.1 Class ADV: Development

For TOEs conforming to this PP, it is anticipated that the information about the TOE is contained in the guidance documentation available to the end user as well as the TOE Summary Specification (TSS) portion of the ST.[5] While it is not required that the TOE developer write the TSS, the TOE developer must concur with the description of the product that is contained in the TSS as it relates to the functional requirements. The Assurance Activities associated with each SFR must provide the ST authors with sufficient information to determine the appropriate content for the TSS section.

6.2.1.1 Basic Functional Specification (ADV_FSP.1)

The functional specification describes the TSFIs. It is not necessary to have a formal or complete specification of these interfaces. Additionally, because TOEs conforming to this PP will necessarily have interfaces to the Operational Environment that cannot be invoked by TOE users, there is little point specifying that such interfaces be described in and of themselves since only indirect testing of such interfaces may be possible. The activities for this family for this PP must focus on understanding the interfaces presented in the TSS in response to the functional requirement, and the interfaces presented in the AGD documentation. No additional "functional specification" document should be necessary to satisfy the assurance activities specified.

The interfaces that need to be evaluated are characterized through the information needed to perform the assurance activities listed, rather than as an independent, abstract list.

Developer action elements:

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.2D The developer shall provide a tracing from the functional

[5] The developer has the option of supplying additional documentation if proprietary details are required, but the vast bulk of the information should be in public facing documents.

specification to the SFRs.

Developer Note: As indicated in the introduction to this section, the functional specification is comprised of the information contained in the AGD_OPE and AGD_PRE documentation, coupled with the information provided in the TSS of the ST. This will also include any publically available protocol and/or API documentation that is referenced in the development evidence. The assurance activities in the functional requirements point to evidence that should exist in the documentation and TSS section; since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is implicitly already done and no additional documentation is necessary.

Content and presentation elements:

ADV_FSP.1.1C The functional specification shall describe the purpose and method of use for each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.2C The functional specification shall identify all parameters associated with each SFR-enforcing and SFR-supporting TSFI.

ADV_FSP.1.3C The functional specification shall provide rationale for the implicit categorization of interfaces as SFR-non-interfering.

ADV_FSP.1.4C The tracing shall demonstrate that the SFRs trace to TSFIs in the functional specification.

Evaluator action elements:

ADV_ FSP.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

ADV_ FSP.1.2E The evaluator shall determine that the functional specification is an accurate and complete instantiation of the SFRs.

Assurance Activity:

There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described for each SFR, and for other activities described for AGD, ATE, and AVA SARs. The

requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided. For example, if the TOE provides the capability to configure the key length for the encryption algorithm but fails to specify an interface to perform this function, then the assurance activity associated with FMT_SMF would fail.

The evaluator shall verify that the TOE functional specification describes the set of interfaces the TOE intercepts or works with. The evaluator shall examine the description of these interfaces and verify that they include a satisfactory description of their invocation.

6.2.2 Class AGD: Guidance Documentation

The guidance documents will be provided with the developer's security target. Guidance must include a description of how the authorized user verifies that the Operational Environment can fulfill its role for the security functionality. The documentation must be in an informal style and readable by an authorized user.

Guidance must be provided for every operational environment that the product supports as claimed in the ST. This guidance includes

- Instructions to successfully install the TOE in that environment; and
- Instructions to manage the security of the TOE as a product and as a component of the larger operational environment.

Guidance must also be provided regarding how to boot the TOE into a safe configuration on the host operating system such that it cannot be modified during system startup or removed from the system startup sequence entirely. It must also describe how to configure the product to prevent it from being disabled (e.g. shut down) by untrusted subjects.

Guidance pertaining to particular security functionality is also provided; requirements on such guidance are contained in the assurance activities specified with each SFR.

6.2.2.1 Operational User Guidance (AGD_OPE.1)

Developer action elements:

AGD_OPE.1.1D The developer shall provide operational user guidance.

Developer Note: Rather than repeat information here, the developer should review the assurance activities for this component and for the SFRs to understand the specifics of the guidance that the evaluators will be checking for. This will provide the necessary information for the preparation of acceptable guidance.

Content and presentation elements:

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.

Application Note: *The evaluator must perform these user-accessible functions on the TOE in order to ensure that this description is complete and accurate.*

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 fulfill 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.

Evaluator action elements:

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

Assurance Activity:

Some of the contents of the operational guidance will be verified by the assurance activities with each SFR. The following additional information is also required.

The operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

6.2.2.2 Preparative Procedures (AGD_PRE.1)

Developer action elements:

AGD_PRE.1.1D The developer shall provide the TOE including its preparative procedures.

Developer Note: As with the operational guidance, the developer should look to the assurance activities to determine the required content with respect to preparative procedures.

Content and presentation elements:

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.

Evaluator action elements:

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.

Assurance Activity

As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms (that is, combination of hardware and operating system) claimed for the TOE in the ST.

6.2.3 Class ALC: Life Cycle Support

At the assurance level provided for TOEs conformant to this PP, life-cycle support is limited to end-user-visible aspects of the life-cycle, rather than an examination of the TOE vendor's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation at this assurance level.

6.2.3.1 Labeling of the TOE (ALC_CMC.1)

This component is targeted at identifying the TOE such that it can be distinguished from other products or version from the same vendor and can be easily specified when being procured by an end user.

Developer action elements:

ALC_CMC.1.1D The developer shall provide the TOE and a reference for the TOE.

Content and presentation elements:

ALC_CMC.1.1C The TOE shall be labeled with its unique reference.

Evaluator action elements:

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

Assurance Activity:

The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

6.2.3.2 TOE CM Coverage (ALC_CMS.1)

Given the scope of the TOE and its associated evaluation evidence requirements, this component's assurance activities are covered by the assurance activities listed for ALC_CMC.1.

Developer action elements:

ALC_CMS.1.1D The developer shall provide a configuration list for the TOE.

Content and presentation elements:

ALC_CMS.1.1C The configuration list shall include the following: the TOE itself; and the evaluation evidence required by the SARs.

ALC_CMS.1.2C The configuration list shall uniquely identify the configuration items.

Evaluator action elements:

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

Assurance Activity:

The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component.

6.2.4 Class ATE: Tests

Testing is specified for functional aspects of the system as well as aspects that take advantage of design or implementation weaknesses. The former is done through ATE_IND family, while the latter is through the AVA_VAN family. At the assurance level specified in this PP, testing is based on advertised functionality and interfaces with dependency on the availability of design information. One of the primary outputs of the evaluation process is the test report as specified in the following requirements.

6.2.4.1 Independent Testing - Conformance (ATE_IND.1)

Testing is performed to confirm the functionality described in the TSS as well as the administrative (including configuration and operation) documentation provided. The focus of the testing is to confirm that the requirements specified with each SFR are being met, although some additional testing is specified for SARs in section 6.1. The Assurance Activities identify the minimum testing activities associated with these components. The evaluator produces a test report documenting the plan for and results of testing, as well as coverage arguments focused on the platform/TOE combinations that are claiming conformance to this PP.

Developer action elements:

ATE_IND.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

ATE_IND.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

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

ATE_IND.1.2E The evaluator shall test a subset of the TSF to confirm that the TSF operates as specified.

Assurance Activity:

The evaluator shall prepare a test plan and report documenting the testing aspects of the system. The test plan covers all of the testing actions contained in the body of this PP's Assurance Activities. While it is not necessary to have one test case per test listed in an Assurance Activity, the evaluators shall document in the test plan that each applicable

testing requirement in the ST is covered.

The Test Plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification shall address the differences between the tested platform and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale shall be provided. If all platforms claimed in the ST are tested, then no rationale is necessary.

The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluators are expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) is provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform. This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (IPsec, TLS/HTTPS, SSH).

The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results. The test report (that could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a "fail" and "pass" result (and the supporting details), and not just the "pass" result.

6.2.5 Class AVA: Vulnerability Assessment

For the first generation of this protection profile, the evaluation lab is expected to survey open sources to discover what vulnerabilities have been discovered in these types of products. In most cases, these vulnerabilities will require sophistication beyond that of a basic attacker. Until penetration tools are created and uniformly distributed to the evaluation labs, evaluators will not be expected to test for these vulnerabilities in the TOE. The labs will be expected to comment on the likelihood of these vulnerabilities given the documentation provided by the vendor. This information will be used in the

development of penetration testing tools and for the development of future protection profiles.

6.2.5.1 Vulnerability Survey (AVA_VAN.1)

Developer action elements:

AVA_VAN.1.1D The developer shall provide the TOE for testing.

Content and presentation elements:

AVA_VAN.1.1C The TOE shall be suitable for testing.

Evaluator action elements:

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

AVA_VAN.1.2E The evaluator shall perform a search of public domain sources to identify potential vulnerabilities in the TOE.

AVA_VAN.1.3E 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.

Assurance Activity:

As with ATE_IND, the evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to determine the vulnerabilities that have been found in this category of ESM application in general, as well as those that pertain to the particular TOE. The evaluator documents the sources consulted and the vulnerabilities found in the report. For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. For example, if the vulnerability can be detected by pressing a key combination on boot-up, for example, a test would be suitable at the assurance level of this PP. If exploiting the vulnerability requires an electron microscope and liquid nitrogen, for instance, then a test would not

be suitable and an appropriate justification would be formulated.

6.3 Rationale for Security Assurance Requirements

The rationale for choosing these security assurance requirements is that this is the first U.S. Government Protection Profile for this technology. If vulnerabilities are found in these types of products, then more stringent security assurance requirements will be mandated based on actual vendor practices.

7 Security Problem Definition Rationale

This section identifies the mappings between the threats and objectives defined in the Security Problem Definition as well as the mappings between the assumptions and environmental objectives. In addition, rationale is provided based on the SFRs that are used to satisfy the listed objectives so that it can be seen that the mappings are appropriate. In situations where these mappings will change based on whether or not certain optional SFRs have been claimed, **bold text** has been added at the end of the rationale to aid the ST author.

Table 5. Assumptions, Environmental Objectives, and Rationale

Assumptions	Objectives	Rationale
A.CRYPTO (optional) – The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.	**OE.CRYPTO (optional) –** The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.	It is expected that vendors will typically rely on the usage of cryptographic primitives implemented in the Operational Environment to perform cryptographic protocols provided by the TOE. If the TOE provides its own cryptographic primitives, then this becomes an objective for the TOE rather than for the environment.
A.INSTALL – There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.	**OE.INSTALL –** Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner.	Assigning specific individuals to install the TOE provides assurance that it has been installed in a manner that is consistent with the evaluated configuration.
A.POLICY – The TOE will receive policy data from the Operational Environment.	**OE.POLICY** – The Operational Environment will provide a policy that the TOE will enforce.	In order for the TSF to enforce an access control policy, it must receive and consume that policy from the Operational Environment.
A.SYSTIME -- The TOE will receive reliable time data from the Operational Environment.	**OE.SYSTIME** -- The Operational Environment will provide reliable time data to the TOE.	Providing reliable time data ensures accurate audit records.
A.USERID – The TOE will receive validated identity data from the Operational Environment.	**OE.USERID** – The Operational Environment shall be able to identify a user requesting access to resources that are protected by the TSF.	It is necessary for the TOE to receive identity data from the Operational Environment so that the TSF is able to properly enforce the consumed access control policy.

Table 6. Policies, Threats, Objectives, and Rationale

Threats	Objectives	Rationale
P.UPDATEPOL – The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.	**O.SELFID –** The TOE will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival.	**FCO_NRR.2** The TOE's ability to provide proof that updated policy data is received assists the organization in verifying that policy data is being kept up-to-date.
T.DISABLE – A malicious user or careless user may suspend or terminate the TOE's operation, thus making it unable to enforce its access controls upon the environment or TOE-protected data.	**O.RESILIENT –** If the TOE mediates actions performed by a user against resources on an operating system, that user shall not be able to alter those resources that would disable or otherwise modify the behavior of the TOE.	**ESM_EID.2** **FDP_ACC.1** **FDP_ACF.1** **FPT_FLS.1** If the TOE is able to protect operating system objects, the FDP requirements specified in this PP require the TOE to protect the objects that comprise or affect the behavior of the TOE. **If the TOE does not protect itself in this way, the ST author can remove this mapping. At least one of O.RESILIENT or OE.PROTECT must be mapped in order to mitigate this threat.**
	OE.PROTECT – The Operational Environment will protect the TOE from unauthorized modifications and access to its functions and data.	The Operational Environment may be used to protect TSF data that is stored in environmental repositories or run-time memory. For example, audit or policy data may be stored in an environmental SQL database. **If the TOE does not protect itself in this way, the ST author can remove this mapping. At least one of O.RESILIENT or OE.PROTECT must be mapped to mitigating this threat.**
T.EAVES – A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.	**O.CRYPTO –** The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of	**FCS_CKM.1 (optional)** **FCS_CKM_EXT.4 (optional)** **FCS_COP.1(1) (optional)**

Threats	Objectives	Rationale
	communications.	**FCS_COP.1(2) (optional)** **FCS_COP.1(3) (optional)** **FCS_COP.1(4) (optional)** **FCS_RBG_EXT.1 (optional)** By providing cryptographic primitives, the TOE is able to establish and maintain a trusted channel. **If the ST does not claim the cryptographic requirements listed above, the ST author must claim A.CRYPTO and OE.CRYPTO and map them based on Table 6 and Table 7 in this PP.**
	O.MNGRID – The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.	**FTP_ITC.1** Through the establishment of a trusted channel, each ESM component will have assured identification of any other component to which it connects. Therefore, if a trusted channel is established between the TOE and its Policy Management product, each of these components will be assured of the authenticity of the other.
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	**FCS_HTTPS_EXT.1 (optional)** **FCS_IPSEC_EXT.1 (optional)** **FCS_SSH_EXT.1 (optional)** **FCS_TLS_EXT.1 (optional)** **FPT_SKP_EXT.1** **FTP_ITC.1** Implementation of trusted channels ensures that communications are protected from eavesdropping.
	OE.CRYPTO – The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.	If the Operational Environment is able to perform cryptographic services at the request of the TOE, the TSF is able to establish and maintain a trusted channel when needed. **If the ST claims the cryptographic requirements**

Threats	Objectives	Rationale
		mapped to O.CRYPTO above, the ST author shall exclude this objective from the mapping.
T.FALSIFY – A malicious user can falsify the TOE's identity, giving the Policy Management product false assurance that the TOE is enforcing a policy.	**O.SELFID –** The TOE will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival.	**FCO_NRR.2** By providing verifiable evidence of policy receipt to the Policy Management product, the TSF can provide assurance that it is implementing the correct policy.
T.FORGE – A malicious user may create a false policy and send it to the TOE to consume, adversely altering its behavior.	**O.CRYPTO –** The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.	**FCS_CKM.1 (optional)** **FCS_CKM_EXT.4 (optional)** **FCS_COP.1(1) (optional)** **FCS_COP.1(2) (optional)** **FCS_COP.1(3) (optional)** **FCS_COP.1(4) (optional)** **FCS_RBG_EXT.1 (optional)** By providing cryptographic services, the TOE is able to establish and maintain a trusted channel. **If the ST does not claim the cryptographic requirements listed above, the ST author shall claim A.CRYPTO and OE.CRYPTO and map them based on Table 6 and Table 7 in this PP.**
	O.INTEGRITY – The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components.	**FTP_ITC.1** By providing a trusted channel between the TOE and remote trusted IT products, the TSF will be able to verify the integrity of received data.
	O.MNGRID – The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.	**FPT_APW_EXT.1** **FTP_ITC.1** Through the establishment of a trusted channel, each ESM component will have assured identification of any other component to which it connects. Therefore, if a trusted channel is established between the TOE and its Policy Management product, each of those components will

Threats	Objectives	Rationale
		be assured of the authenticity of the other.
	O.OFLOWS – The TOE will be able to recognize and discard invalid or malicious input requests by users.	**FTP_ITC.1** **FPT_RPL.1** These SFRs work together to protect against the threat of the TOE accepting forged policies by detecting replayed input and by providing a mechanism for the TOE to determine that the received policy is genuine and appropriately structured.
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	**FCS_HTTPS_EXT.1 (optional)** **FCS_IPSEC_EXT.1 (optional)** **FCS_SSH_EXT.1 (optional)** **FCS_TLS_EXT.1 (optional)** **FPT_SKP_EXT.1** **FTP_ITC.1** Implementation of trusted channels prevents the disclosure and modification of data and transit and ensures that only data from valid sources is accepted.
T.MASK – A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.	**O.MONITOR** – The TOE will monitor the behavior of itself for anomalous activity (e.g., provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users).	**FAU_GEN.1** **FAU_SEL.1** **FAU_STG.1** **FAU_STG_EXT.1** If security relevant events are logged and backed up, an attacker will have difficulty performing actions for which they are not accountable. This allows an appropriate authority to be able to review the recorded data and acquire information about attacks on the TOE.
T.NOROUTE – A malicious or careless user may cause the TOE to lose connection to the source of its enforcement policies, adversely affecting access control behaviors.	**O.MAINTAIN –** The TOE will be capable of maintaining access control policy enforcement if it is unable to communicate with the Policy Management product which provided it the policy.	**FPT_FLS_EXT.1** **FRU_FLT.1** The fault tolerance requirements for the TOE define the actions the TOE should take when unable to communicate with the Policy Management product. This

Threats	Objectives	Rationale
		provides assurance that a connectivity issue will not disrupt the TOE's enforcement of the access control SFP. They also ensure that when communications are re-established, the TSF will immediately enforce recent policy data, even if it was generated while the two components were not connected.
T.OFLOWS – A malicious user may attempt to provide incorrect policy data to the TOE in order to alter its access control policy enforcement behavior.	**O.CRYPTO –** The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.	**FCS_CKM.1 (optional)** **FCS_CKM_EXT.4 (optional)** **FCS_COP.1(1) (optional)** **FCS_COP.1(2) (optional)** **FCS_COP.1(3) (optional)** **FCS_COP.1(4) (optional)** **FCS_RBG_EXT.1 (optional)** By providing cryptographic services, the TOE is able to establish and maintain a trusted channel. **If the ST does not claim the cryptographic requirements listed above, the ST author shall claim A.CRYPTO and OE.CRYPTO and map them based on Table 6 and Table 7 in this PP.**
	O.MNGRID – The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.	**FTP_ITC.1** By requiring assured identity of ESM components, an attacker will not be able to provide incorrect access control policy data to the TOE because the TOE will not trust the attacker.
	O.OFLOWS – The TOE will be able to recognize and discard invalid or malicious input provided by users.	**FTP_ITC.1** **FPT_RPL.1** The intent of this objective is to ensure that the policy data is originating from a known trusted source and does not represent a replay of information.
	O.PROTCOMMS – The TOE will provide protected	**FCS_HTTPS_EXT.1 (optional)**

Threats	Objectives	Rationale
	communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	**FCS_IPSEC_EXT.1 (optional)** **FCS_SSH_EXT.1 (optional)** **FCS_TLS_EXT.1 (optional)** **FPT_SKP_EXT.1** **FTP_ITC.1** Implementation of trusted channels prevents the disclosure and modification of data and transit and ensures that only data from valid sources is accepted.
	OE.CRYPTO – The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.	If the Operational Environment is able to perform cryptographic services at the request of the TOE, the TSF is able to establish and maintain a trusted channel when needed. **If the ST claims the cryptographic requirements mapped to O.CRYPTO above, the ST author shall exclude this objective from the mapping.**
T.UNAUTH – A malicious or careless user may access an object in the Operational Environment that causes disclosure of sensitive data or adversely affects the behavior of a system.	**O.DATAPROT** – The TOE will protect data from unauthorized modification by enforcing an access control policy produced by a Policy Management product.	**ESM_DSC.1 (optional)** **ESM_EID.2** **FDP_ACC.1** **FDP_ACF.1** **FMT_MOF.1(1)** **FMT_MOF.1(2)** **FMT_MSA.1** **FMT_MSA.3** **FMT_SMF.1** **FMT_SMR.1** **FTA_TSE.1 (optional)** The primary purpose of the TOE is to restrict access between subjects and objects. The ability of the TOE to enforce an access control policy against objects in the Operational Environment allows this purpose to be fulfilled. In order to enforce an access control policy, the TOE requires the ability for such a policy to be configured. In order to provide assurance that

Threats	Objectives	Rationale
		the policy is being enforced, the TOE requires the ability for the policy to be queried.

8 Security Problem Definition

The following sections list the assumptions, threats, and objectives for the PP.

8.1 Assumptions

The specific conditions listed in the following subsections are assumed to exist in the TOE's Operational Environment. These assumptions include both practical realities in the development of the TOE security requirements and the essential environmental conditions on the use of the TOE.

8.1.1 Connectivity Assumptions

Table 7. Connectivity Assumptions

Assumption Name	Assumption Definition
A.CRYPTO (optional)	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.POLICY	The TOE will receive policy data from the Operational Environment.
A.ROBUST (optional)	The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
A.SYSTIME (optional)	The TOE will receive reliable time data from the Operational Environment.
A.USERID	The TOE will receive identity data from the Operational Environment.

8.1.2 Physical Assumptions

No physical assumptions are prescribed in this Protection Profile.

8.1.3 Personnel Assumptions

Table 8. Personnel Assumptions

Assumption Name	Assumption Definition
A.INSTALL	There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.

8.2 Threats

The TOE, as potentially a separately acquired device, is not expected to have any direct user-facing interfaces. The only expected interfaces to the TOE would be configuration files, a logical interface to the ESM product that is used to manage the TOE (Policy Management product), a logical interface to the audit component, and an interface that intercepts requested accesses that goes through the ESM. The linkage between the PM and TOE is an important interface to protect because the TOE needs assurance that data it receives from the PM is genuine. Equally important is the linkage between the TOE and its associated configuration files. The TOE needs to have assurance of the integrity of the configuration data in these files so that the TOE operates in a known state. The PM requires a mechanism to verify the authenticity of the TOE and the version of the policy that it is implementing so that policies are only sent to trusted entities. Listed below are the applicable threats to the TOE. These threats concern attacks that could cause the TOE to function incorrectly or for an attacker to obtain TOE Security Function (TSF) data without permission.

Table 9. Threats

Threat Name	Threat Definition
T.DISABLE	A malicious user or careless user may suspend or terminate the TOE's operation, thus making it unable to enforce its access controls upon the environment or TOE-protected data.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FALSIFY	A malicious user can falsify the TOE's identity, giving the Policy Management product false assurance that the TOE is enforcing a policy.
T.FORGE	A malicious user may create a false policy and send it to the TOE to consume, adversely altering its behavior.
T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.NOROUTE	A malicious or careless user may cause the TOE to lose connection to the source of its enforcement policies, adversely affecting access control behaviors.
T.OFLOWS	A malicious user may attempt to provide incorrect policy data to the TOE in order to alter its access control policy enforcement behavior.
T.UNAUTH	A malicious or careless user may access an object in the Operational Environment that causes disclosure of sensitive data or adversely affects the behavior of a system.

8.3 Organizational Security Policies

The following organizational security policies are expected to be employed in an organization that deploys the TOE.

Table 10. Organizational Security Policies

Policy Name	Policy Definition
P.UPDATEPOL	The organization will exercise due diligence to ensure that the TOE is updated with relevant policy data.

8.4 Security Objectives

In order to ensure that the threats defined in this PP are appropriately mitigated, the security objectives for both the TOE and the Operational Environment must be satisfied. They are listed in the sections below.

8.4.1 Security Objectives for the TOE

The following security objectives are expected characteristics of the TOE.

Table 11. Security Objectives for the TOE

Objective	TOE Security Objective Definition
O.CRYPTO (optional)	The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.
O.DATAPROT	The TOE will protect data from unauthorized modification by enforcing an access control policy produced by a Policy Management product.
O.INTEGRITY	The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components.
O.MAINTAIN	The TOE will be capable of maintaining access control policy enforcement if it is unable to communicate with the Policy Management product which provided it the policy.
O.MNGRID	The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.
O.MONITOR	The TOE will monitor the behavior of itself for anomalous activity (e.g., provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users).
O.OFLOWS	The TOE will be able to recognize and discard invalid or malicious input provided by users.
O.PROTCOMMS	The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.
O.RESILIENT (optional)	If the TOE mediates actions performed by a user against resources on an

Objective	TOE Security Objective Definition
	operating system, the system administrator or user shall not be allowed to perform an operation in the Operational Environment that would disable or otherwise modify the behavior of the TOE.
O.SELFID	The TOE will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival.

8.4.2 Security Objectives for the Operational Environment

The following security objectives are expected characteristics of the Operational Environment in which the TOE is deployed.

Table 12. Security Objectives for the Operational Environment

Objective	Environmental Security Objective Definition
OE.CRYPTO (optional)	The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a secure manner.
OE.POLICY	The Operational Environment will provide a policy that the TOE will enforce.
OE.PROTECT (optional)	The Operational Environment will protect the TOE from unauthorized modifications and access to its functions and data.
OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.
OE.USERID	The Operational Environment shall be able to identify a user requesting access to resources that are protected by the TSF.

Appendix A - Supporting Tables and References

A.1 References

[1] Enterprise Security Management Technical Community, Standard Protection Profile for Enterprise Security Management Policy Management, version 2.1, June 13, 2013

[2] Enterprise Security Management Technical Community, Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1, June 13, 2013

[3] Enterprise Security Management Technical Community, Standard Protection Profile for Enterprise Security Management Secure Configuration Management, version *TBD*, forthcoming

[4] Enterprise Security Management Technical Community, Standard Protection Profile for Enterprise Security Management Audit Server, version *TBD*, forthcoming

[5] Enterprise Security Management Technical Community, Standard Protection Profile for Enterprise Security Management Authentication Server, version *TBD*, forthcoming

[6] National Information Assurance Partnership, Common Criteria for Information Technology Security Evaluation, version 3.1 Revision 4, September, 2012

[7] American National Standards Institute, ANSI X9.80 Prime Number Generation, Primality Testing, and Primality Certificates, 2005

[8] National Institute of Standards and Technology, NIST Special Publication 800-56A Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2007

[9] National Institute of Standards and Technology, NIST Special Publication 800-56B Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, August 2009

[10] National Institute of Standards and Technology, FIPS PUB 186-3 Digital Signature Standard (DSS), June 2009

[11] National Institute of Standards and Technology, NIST Special Publication 800-57 Recommendation for Key Management, March 2007

[12] National Institute of Standards and Technology, FIPS PUB 197 Advanced Encryption Standard, November 2001

[13] National Institute of Standards and Technology, NIST Special Publication 800-38A Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001

[14] National Institute of Standards and Technology, NIST Special Publication 800-38B Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, May 2005

[15] National Institute of Standards and Technology, NIST Special Publication 800-38C Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004

[16] National Institute of Standards and Technology, NIST Special Publication 800-38D Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM), November 2007

[17] National Institute of Standards and Technology, NIST Special Publication 800-38E Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, January 2010

[18] National Institute of Standards and Technology. "Recommended Security Controls for Federal Information Systems and Organizations". NIST SP 800-53 Revision 3 Errata 1. May 1, 2010.

[19] National Institute of Standards and Technology, The Advanced Encryption Standard Algorithm Validation Suite (AESAVS), November 2002

[20] National Institute of Standards and Technology, The XTS-AES Validation System (XTSVS), March 2011

[21] National Institute of Standards and Technology, The CMAC Validation System (CMACVS), March 2006

[22] National Institute of Standards and Technology, The CCM Validation System (CCMVS), March 2006

[23] National Institute of Standards and Technology, The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS), February 2009

[24] National Institute of Standards and Technology, The FIPS 186-3 Digital Signature Algorithm Validation System (DSA2VS), June 2011

[25] National Institute of Standards and Technology, The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS), June 2011

[26] National Institute of Standards and Technology, The RSA Validation System (RSAVS), November 2004

[27] National Institute of Standards and Technology, FIPS PUB 180-3 Secure Hash Standard (SHS), October 2008

[28] National Institute of Standards and Technology, The Secure Hash Algorithm Validation System (SHAVS), July 2004

[29] National Institute of Standards and Technology, The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS), December 2004

[30] National Institute of Standards and Technology, NIST Special Publication 800-90 Recommendation for Random Number Generation, March 2007

[31] National Institute of Standards and Technology, FIPS PUB 140-2, Security Requirements for Cryptographic Modules, May 2001

[32] National Institute of Standards and Technology, The Random Number Generator Validation System (RNGVS), January 2005

[33] National Institute of Standards and Technology, NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, January 2005

[34] Aerospace Corporation, "Exploding 800-53: An Analysis of NIST SP 800-53 Revision 3 as Completed by CNSSI 1253", March 2003. Aerospace Technical Operating Report TOR-2012(8506)-5. Distribution restricted to US Government and US Government Contractors.

A.2 Acronyms

Table 13. Acronyms and Definitions

Acronym	Definition
ABAC	Attribute-Based Access Control
CC	Common Criteria
CM	Configuration Management
CNSS	Committee on National Security Systems
COI	Communities of Interest
CSP	Critical Security Parameter
DAC	Discretionary Access Control
ESM	Enterprise Security Management
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPC	Inter-Process Communication
IT	Information Technology
MAC	Mandatory Access Control
NAC	Network Access Control
NIST	National Institute of Standards and Technology
OE	Operational Environment
OS	Operating System
OSP	Organizational Security Policy
PII	Personally Identifiable Information
PM	Policy Management
PP	Protection Profile
RBAC	Role-Based Access Control
RFC	Request for Comment
SA	Security Association
SAC	System Access Control
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSH	Secure Shell
SQL	Structured Query Language
ST	Security Target

TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
TSP	TOE Security Policy

Appendix B - NIST SP 800-53/CNSS 1253 Mapping

This section lists data that indicates requirements from other relevant standards that the TOE can be used to satisfy. This information is not required from a CC standpoint but its inclusion in a Security Target may aid the reader in identifying redundant work that can be reduced when conformance to multiple standards is necessary in their deployment.

The table below lists the extended requirements defined as part of this PP and standard CC requirements that the PP may apply in an extended or unconventional manner and the NIST 800-53 security controls that apply to them. The forthcoming NIST SP 800-53 Revision 4 defines a mapping between NIST 800-53 security controls and CC requirements that are defined in CC parts 2 and 3. This will be published on the CCEVS website at a future date. This will be used to map security controls to the remaining requirements claimed in this PP.

The NIST 800-53 controls that are applicable to the claimed SFRs and SARs can be mapped to CNSSI 1253 by referencing the Aerospace Technical Operating Report TOR-2012(8506)-5, "Exploding 800-53: An Analysis of NIST SP 800-53 Revision 3 as Completed by CNSSI 1253".

Note that the guidelines listed below are based on the assumption that strict conformance to this PP is being claimed. If the ST author is augmenting the TOE through claiming conformance to multiple PPs, additional controls that are not documented here may be applicable.

Table 14. NIST 800-53 Requirements Compatibility

SFR		NIST 800-53 Control[6]		Comments and Observations
ESM_DSC.1 (optional)	**Object Discovery** Object Discovery	AU-13	**Monitoring for Information Disclosure**	**Full.** This control appears to be fully satisfied by the SFR.
		AC-4	**Access Enforcement**	**Partial**. This control can be used to help maintain access enforcement by detecting when objects are a not in an approved state.
ESM_EID.2	**Enterprise Identification** Reliance on Enterprise Identification	IA-2	**Identification and Authentication (Organizational Users)**	**Partial.** This addresses the identification of organizational users.
FAU_STG_EXT.1	**Security Audit Event Storage** External Audit Trail Storage	AU-9	**Protection of Audit Information**	**Partial.** The SFR addresses the basic intent of the control, although the repository/entity to which audit data is written must in turn prevent unauthorized modification of that data. However, the control not only protects the trail, but audit tools (which are not covered by the SFR).
FCS_CKM.1 (optional)	**Cryptographic Key Management** Cryptographic Key Generation	SC-12	**Cryptographic Key Establishment and Management**	**Partial.** The SFR addresses one of the aspects of the 800-53 control. The assignments for standards and protocols need to be compared against required enhancements.
		Note: The NIST 800-53 controls make no distinction between the various aspects of key management (generation, distribution, access, and destruction).		
FCS_CKM_EXT.4 (optional)	**Cryptographic Key Management** Cryptographic Key Destruction	SC-12	**Cryptographic Key Establishment and Management**	**Partial.** The SFR addresses one of the aspects of the 800-53 control. The assignments for standards and protocols need to be compared against required enhancements.
		Note: The NIST 800-53 controls make no distinction between the various aspects of key management (generation, distribution, access, and destruction).		
FCS_HTTPS_EXT.1 (optional)	**HTTPS** HTTPS	SC-8	**Transmission Confidentiality and Integrity**	**Partial.** The ability of the TOE to encrypt communications ensures the confidentiality and integrity of data and transit. Physical protection of this data is defined by the Operational Environment.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection	**Partial.** This addresses the requirement to use cryptography.

[6] This table reflects NIST SP 800-53 Revision 4. Significant differences for Revision 3 are noted, where appropriate.

		SC-13	**Cryptographic Protection**	**Partial.** This addresses the requirement to use cryptography; the assignment in the control should correspond with the type of crypto selected. For US evaluations, SC-13(1) may also apply.
		Note: In Revision 3, SC-9 and SC-9(1) are also applicable. Revision 3 distinguished between transmission integrity (SC-8) and transmission confidentiality (SC-9). Revision 4 combined SC-8 and SC-9 into a single control with assignments providing the type of protection.		
FCS_IPSEC_EXT.1 (optional)	**IPSEC** IPSEC	SC-8	**Transmission Confidentiality and Integrity**	**Partial.** The ability of the TOE to encrypt communications ensures the confidentiality and integrity of data and transit. Physical protection of this data is defined by the Operational Environment.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection	**Partial.** This addresses the requirement to use cryptography.
		SC-13	**Cryptographic Protection**	**Partial.** This addresses the requirement to use cryptography; the assignment in the control should correspond with the type of crypto selected. For US evaluations, SC-13(1) may also apply.
		Note: In Revision 3, SC-9 and SC-9(1) are also applicable. Revision 3 distinguished between transmission integrity (SC-8) and transmission confidentiality (SC-9). Revision 4 combined SC-8 and SC-9 into a single control with assignments providing the type of protection.		
FCS_RBG_EXT.1 (optional)	**Random Bit Generation** Random Bit Generation	SC-13	**Cryptographic Protection** (Revision 4 only)	**Partial.** The ability of the TOE to encrypt communications ensures the confidentiality and integrity of data and transit. Physical protection of this data is defined by the Operational Environment.
		Note: In Revision 3, there was no provision within SC-13 to specify the random number generator quality requirements.		
FCS_SSH_EXT.1 (optional)	**SSH** SSH	SC-8	**Transmission Confidentiality and Integrity**	**Partial.** The ability of the TOE to encrypt communications ensures the confidentiality and integrity of data and transit. Physical protection of this data is defined by the Operational Environment.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection	**Partial.** This addresses the requirement to use cryptography.
		SC-13	**Cryptographic Protection**	**Partial.** This addresses the requirement to use cryptography; the assignment in the control should correspond with the type of crypto selected. For US evaluations, SC-13(1) may also apply.
		Note: In Revision 3, SC-9 and SC-9(1) are also applicable. Revision 3 distinguished between transmission integrity (SC-8) and transmission confidentiality (SC-9). Revision 4 combined SC-8 and SC-9 into a single		

		control with assignments providing the type of protection.		
FCS_TLS_EXT.1 (optional)	**TLS** TLS	SC-8	**Transmission Confidentiality and Integrity**	**Partial.** The ability of the TOE to encrypt communications ensures the confidentiality and integrity of data and transit. Physical protection of this data is defined by the Operational Environment.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection	**Partial.** This addresses the requirement to use cryptography.
		SC-13	**Cryptographic Protection**	**Partial.** This addresses the requirement to use cryptography; the assignment in the control should correspond with the type of crypto selected. For US evaluations, SC-13(1) may also apply.
		Note: In Revision 3, SC-9 and SC-9(1) are also applicable. Revision 3 distinguished between transmission integrity (SC-8) and transmission confidentiality (SC-9). Revision 4 combined SC-8 and SC-9 into a single control with assignments providing the type of protection.		
FPT_APW_EXT.1	**Protection of Stored Credentials** Protection of Stored Credentials	IA-5	**Authenticator Management**	**Partial**. This SFR addresses the portion of the control that requires authentication data to be protected from unauthorized disclosure and modification.
		IA-5(1)	**Authenticator Management** | Password-Based Authentication	This addresses the portion of the control that requires passwords to be stored obscured.
FPT_FLS_EXT.1	**Fail Secure** Failure of Communications	SC-7(6)	**Boundary Protection** | When boundary protection mechanisms fail, organization prevents unauthorized release of information or communications across boundary	**Partial.** This control is a specific example of a failure secure condition for boundary protection devices.
		SC-7(18)	**Boundary Protection** | Fail secure when the boundary protection mechanism fails	**Partial.** This control is a specific example of a failure secure condition for boundary protection devices.
		SC-24	**Fail in Known State**	**Partial.** The SFR requires failure to a known secure state. That appears to fit with SC-24.
FPT_FLS.1 (optional)	**Fail Secure** Failure with Preservation of Secure State	SC-24	**Fail in Known State**	**Partial.** The SFR requires failure to a known secure state. That appears to fit with SC-24.
FPT_SKP_EXT.1	**Protection of Secret Key Parameters** Protection of Secret Key Parameters	IA-5	**Authenticator Management**	**Partial**. This SFR addresses the portion of the control that requires authentication data to be protected from unauthorized disclosure and modification.
		SC-12	**Cryptographic Key Establishment and Management**	**Partial**. This SFR addresses the portion of the control that discusses storage of keys.
FTA_SSL_EXT.1	**Session Locking**	AC-11	**Session Lock**	**Partial.** FTA_SSL_EXT.1 provides

(optional)	**and Termination** TSF-Initiated Session Locking			the system-initiated session lock.
		AC-11(1)	**Session Lock** | With screen saver	**Full.** FTA_SSL_EXT.1 provides the system-initiated session lock.

Appendix C - Architectural Variations and Additional Requirements

C.1 Architectural Variations for Access Control by Technology Type

The following scenarios address the various types of access control that may be enforced by TOEs meeting this Protection Profile. These are not optional components; they clarify how the data protection SFRs are to be completed and are only available to those architectures that specifically support the functionality as identified below.

C.1.1 Host-Based Access Control

Host-based Access Control is used to determine what a subject can do on a particular system. The intent of this technology is to prevent a subject from performing damaging, or otherwise inappropriate, acts against a host system such as running unauthorized software or modifying its configuration. This includes but is not limited to the following inappropriate behaviors:

- Program access: running a program that does not serve a legitimate organizational function, removing a program that serves a legitimate organizational function, or terminating a running program or process that serves a legitimate organizational function (e.g,. auditing).
- File access: creating a file in an invalid location, reading a file that contains data the subject should not be allowed to access, modifying or deleting a file that contains important information or affects the behavior of a legitimate program, or changing the permissions of a file to allow untrusted subjects to have access to it
- Host configuration: reading, modifying, or deleting values that define a host's functionality such as the Windows Registry in an attempt to alter the behavior of legitimate programs or the system as a whole

In order to enforce persistent access control, a TOE of this technology type is expected to reside locally to the system against which it controls access. Because of this, the TSF is expected to automatically employ access controls against itself to prevent an untrusted subject from terminating it, reconfiguring it, or preventing it from executing. Such access controls should be employed independently of any policies received from a Policy Management product. It is the responsibility of the ST author to indicate how such a self-protection mechanism is employed and what data is protected in this manner. For example, a program that runs as an endpoint agent on a Windows system might restrict

access to the directory to which it's installed, the Windows startup directory, the registry values that control its behavior, and the executable process itself. This way, a subject who has access control policies enforced against their behavior is unable to bypass the enforcement of those policies.

FDP_ACC.1(1) Access Control Policy

Hierarchical to: No other components.

FDP_ACC.1.1(1) The TSF shall enforce the [access control Security Function Policy (SFP)] on **[**

- subjects: subset of users from an organizational data store, **[*assignment: additional subjects*]**; and
- objects: programs, files, host configuration, authentication function, **[*assignment: additional objects*]**; and
- operations: ability to create, read, modify, execute, delete, terminate, or change permissions of objects, ability to use authentication function, [assignment: additional operations**]]**

Application Note: *The subjects, objects, and operations must be defined from the organization abstraction point of view as seen by the organizational policy manager. Within the TOE, there is a mapping from those abstractions to the specific subjects, objects, and operations at the platform level.*

The ST author must indicate the specific mechanism by which the TOE applies this SFP. For example, if the TOE enforces policies based on arbitrarily-defined containers of generic file system objects, the ST author must clearly indicate the correspondence between these tables and the elements discussed in Table 6.

Controlling the ability to use the authentication function requires the ST author to additionally claim FTA_TSE.1. Refer to Appendix C.4.1.

Dependencies: FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1(1) Access Control Functions

Hierarchical to: No other components.

FDP_ACF.1.1(1) The TSF shall enforce the [access control SFP] to objects based on the following: [all operations between subjects and objects defined in Table 6 below based upon some set of organizational attributes].

Application Note: *The TSF is not expected to define subject and object attributes; instead, it is expected to rely on the subject and object attribute data it receives.*

FDP_ACF.1.2(1) The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [***assignment: types of rules received from an authorized and compatible Policy Management product***].

FDP_ACF.1.3(1) The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **[*assignment: other additional rules*]**.

Application Note: *The ST author must consider specifying other explicit overrides to the access control SFP if the TSF affords this capability. For example, a Host-Based Access Control product may have an exemption to a default-deny policy that is based on the notion of trusted publisher or on specific trusted programs that may be allowed to run updates to themselves. Another example of an additional rule would be if the user is the owner of the object, any operation is allowed to that object by the user.*

FDP_ACF.1.4(1) The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **[*assignment: additional rules*]**.

Application Note: *The ST author must specify the specific objects protected by the explicit denial process. This explicit denial process must be implemented independent of any policy consumed by the TSF.*

The ST author must define the specific mechanism of enforcement for these additional rules in sufficient detail for the evaluator to devise testable scenarios to confirm the effectiveness of these rules.

Dependencies: FDP_ACC.1 Subset Access Control

FMT_MSA.3 Static Attribute Initialization

Table 6. FDP Requirement Table for Host-Based Access Control

Subject	Object	Operation
User	Processes	Execute | Delete | Terminate
		Change Permissions
	Files	Create | Read | Modify | Delete
		Change Permissions
	Host Configuration	Read | Modify | Delete
	Authentication Function	Login

Assurance Activity:

The evaluator shall check the TSS in order to verify that the TOE is capable of mediating the activities that are defined in Table 6 above and that the access control policy enforcement mechanism is described. The evaluator shall also check the TSS to determine that the method by which access control rules are applied is sufficiently detailed to allow for the creation of scenarios that allow for thorough positive and negative testing of the policy enforcement mechanism based on the types of policy rules and their contents.

The evaluator shall check the operational guidance in order to verify that it provides instructions on how it receives access control policy data. For example, if the TOE receives policy rules in some defined language, the operational guidance shall indicate the statements in this language that correspond with the activities that are defined in Table 15 above.

The evaluator shall also check the operational guidance to verify that it provides information about how the TOE's rule processing engine. This allows administrators to design access control policies with appropriate expectations for how they will be enforced.

The evaluator shall test this capability by using an authorized and compatible Policy Management product to define policies that contain rules for mediating the activities defined in Table 15. For each subject/object/operation/attribute combination, the evaluator shall execute at least one positive and one negative test in order to show that the TSF is capable of appropriately mediating these activities.

For example, the policy may define a rule that allows one user to execute a certain process and another that forbids a different user from executing the same process. Once this policy is implemented, the evaluator will access a system as each of these users and observe that the ability to execute the specified process is appropriately allowed or denied. Additionally, for each conditional attribute that is supported (such as time of day restrictions), the evaluator will devise a positive and negative test that proves that the conditional attribute affects whether or not the requested operation is allowed. This activity is then repeated for each other subject/object/operation/attribute tuple.

If the TOE enforces any additional access control policy rules, the evaluator shall devise positive and negative tests that cause these to be invoked and observe that appropriate behavior is performed.

FDP_ACC.1(2) Access Control Policy

Hierarchical to: No other components.

FDP_ACC.1.1(2) The TSF shall enforce the [self-protection Security Function Policy (SFP)] on [

- subjects: subset of users from an organizational data store, [***assignment: additional subjects***]; and
- objects: programs, files, and configuration values that comprise or contain TOE data [***assignment: additional objects***]; and

- operations: ability to create, read, modify, execute, delete, terminate, or change permissions of objects, [***assignment: additional operations***]]

Application Note: *The purpose of this policy is for the TSF to protect itself from unauthorized modification or termination independent of any policy that is being implemented at the request of a Policy Management product. This policy is therefore expected to be unmodifiable and permanently enforced.*

Objects protected by this policy may include, but are not necessarily limited to, the following:

- *One or more executable files that constitutes the TOE*
- *Registry or other system configuration values that define the TOE's behavior*
- *Files or directories that define the programs that are executed upon system boot*

The specific objects that are protected in this manner must be specified by the ST author. If multiple operating systems are supported by the TOE, multiple iterations of this requirement may be necessary due to the differences between operating systems.

The requirement of the TOE to protect its own components ensures that no user may mask their actions by ensuring that auditing cannot be disabled along with any other functionality that protects against unauthorized activity on the system. If this SFR is included in the ST, it will be mapped to satisfy the objective O.RESILIENT.

Dependencies: FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1(2) Access Control Functions

Hierarchical to: No other components.

FDP_ACF.1.1(2)	The TSF shall enforce the [self-protection SFP] to objects based on the following: [all operations between subjects and objects based upon some set of organizational attributes].
Application Note:	*The TSF is not expected to define subject and object attributes; instead, it is expected to rely on the subject and object attribute data it receives.*
FDP_ACF.1.2(2)	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [the TOE will not permit requested operations against objects that are defined to be protected unless the acting subject is the individual that was responsible for the TOE's installation and initial configuration].
FDP_ACF.1.3(2)	The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [none**]**.
FDP_ACF.1.4(2)	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [none].
Dependencies:	FDP_ACC.1 Subset Access Control FMT_MSA.3 Static Attribute Initialization

Assurance Activity:

The evaluator shall check the TSS in order to verify that it identifies the objects that reside in the Operational Environment that impact the TOE's behavior such as registry values, executable processes, and/or configuration files.

Since this behavior is expected to be enforced automatically, there are no expected operational guidance activities.

The evaluator shall test this capability by performing the following actions:

- *Attempting to terminate the process or processes that comprise the TOE*
- *Attempting to delete or make arbitrary modifications to the defined configuration files or registry values*

- *Attempting to modify the system's startup sequence such that the TOE's associated process or processes is excluded from system startup.*

Throughout this, the evaluator shall observe that the TOE never stops running, that the TOE appropriately prevents the relocation, alteration, and/or removal of the parts that comprise it, and in the third case above, that the TOE is still started during system boot.

C.1.2 Optional Host-Based Access Control Capability – Protection from System Administrators

In this optional scenario, the TOE is capable of restricting the permissions of *system administrators* in the Operational Environment. For example, the TOE may be an application that is deployed on an operating system that imposes constraints on what a root user is capable of performing on that system. By virtue of the fact that this user's access is being limited, they cannot be considered trusted. Therefore, they must not have the authority to modify or disable the TOE or else there is no purpose in restricting their activity.

Applicable Requirements

1. The ST author must be clear that this scenario exists for this product.
2. The FDP_ACC.1 and FDP_ACF.1 requirements must document the objects that are automatically protected by the TSF that impact its behavior (see Appendix C.1.1**Error! Reference source not found.**). This should include, where pplicable:
    a. any part of the TOE's implementation that resides on the environmental system
    b. any configuration files or repositories such as a local audit data store used by the TOE
    c. the system clock
3. If TOE resources must be protected manually, the evidence for AGD_PRE.1 must identify the objects that must be protected and how this is to be accomplished.

C.1.3 Web-Based Access Control

Web-based Access Control is used to determine the online resources a subject can access on a particular system. The intent of this technology is to prevent a subject from

interacting with unauthorized online content within the context of an otherwise allowable application. For example, an organization may wish to use a streaming media application to display training sessions to remote participants while preventing this same application from being used to watch live sporting events. More generally, this is including but not necessarily limited to the following behaviors:

- URL access: accessing online content identified by a URL that may contain malicious or inappropriate content
- File access: opening web content or downloading documents, images, executable binaries, and other files that are hosted online and may contain malicious or inappropriate content
- Executable script access: running an executable script such as JSP or ActiveX that is contained within a web page or controlling (enabling/disabling) one's own ability to run these
- Form access: uploading a file or posting data to a web page via an HTTP operation (GET, POST) that does not serve a valid organizational purpose such as a social networking site or general interest message board

For more information regarding the implementation of HTTP operations, refer to RFC 2616, Hypertext Transfer Protocol – HTTP/1.1 at http://www.ietf.org/rfc/rfc2616.txt.

FDP_ACC.1 Access Control Policy

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the [access control Security Function Policy (SFP)] on [

- Subjects: subset of users from an organizational data store; and
- Objects: URLs, files, executable scripts, forms; and
- Operations: access, open, download, execute, enable, disable, HTTP operations]

Application Note: *Examples of access control SFPs based on the types of devices outlined in section 1.4 are listed below. Note that these examples are only representative of the types of*

subjects, objects, and operations that can be used when completing the assignment for this requirement. The ST author must develop their own assignment data based on the behavior of the TSF as opposed to using any of these examples verbatim. It may be possible for multiple instances of the TOE to be in one ESM system. If this is the case, then each unique TOE policy must be captured in a new iteration of this requirement.

Dependencies: FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1 Access Control Functions

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the [access control SFP] to objects based on the following: [all operations between users and objects based upon the attributes defined in Table 7 below].

Application Note: *Consistent with the intent of ESM, the SFP-relevant security attributes that define subjects are expected to exist in the Operational Environment. The TOE should enforce policy based on legacy subjects that are globally defined by the organization deploying it.*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [rules received from an authorized and compatible Policy Management product].

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [***assignment: additional rules***]

Application Note: *The intent of this requirement is to allow for an explicitly authorized bypass of the regular rule enforcement process for situations where access control should never be applied.*

An example of this is the support of anonymous access.

Such access might be permitted based on the source of the address (i.e., internal requests do not require authentication), using wording such as "if web content is located on the organizational web domain, allow all users of the TOE to read the data if it does not require authentication".

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***assignment: additional rules***].

Application Note: *The ST author must specify the specific objects protected by the explicit denial process. This explicit denial process must be implemented independent of any policy consumed by the TSF.*

The ST author must define the specific mechanism of enforcement for these additional rules in sufficient detail for the evaluator to devise testable scenarios to confirm the effectiveness of these rules.

Dependencies: FDP_ACC.1 Subset Access Control

FMT_MSA.3 Static Attribute Initialization

Application Note: *Application of a web-based access control policy is dependent on an authenticated subject attempting to access environmental web resources through a centralized TOE that enforces this policy. In addition to controlling access based on an established session, the TOE may also prevent the establishment of such a session (FTA_TSE.1). The ST author should consider incorporating this optional requirement (found in Appendix C.4.1) if the TOE provides this capability.*

Table 7. FDP Requirement Table for Web-Based Access Control

Subject	Object	Operation
User	URLs	Access via HTTP operation
	Files	Open | Download

	Executable Scripts	Execute
		Enable | Disable
	Forms	HTTP GET | HTTP POST

Assurance Activity:

The evaluator shall check the TSS in order to verify that the TOE is capable of mediating the activities that are defined in Table 6 above and that the access control policy enforcement mechanism is described.

The evaluator shall check the operational guidance in order to verify that it provides instructions on how it receives access control policy data. For example, if the TOE receives policy rules in some defined language, the operational guidance shall indicate the statements in this language that correspond with the activities that are defined in Table 16 above.

The evaluator shall also check the operational guidance to verify that it provides information about how the TOE's rule processing engine. This allows administrators to design access control policies with appropriate expectations for how they will be enforced.

The evaluator shall then use an authorized and compatible Policy Management product to define policies that contain rules for mediating these activities. For each subject/object/operation/attribute combination, the evaluator shall execute at least one positive and one negative test in order to show that the TSF is capable of appropriately mediating these activities.

For example, consider the following combinations:

- *authorized users/groups (subject),* http*://www.test.url (object), access via HTTP operation (operation), 1:00 PM (attribute)*

The evaluator could test this combination by deploying a policy that allows a certain user and a certain group the ability to access http://www.test.url *in their web browser between the hours of 9:00 AM and 5:00 PM. They can then log in as that user and observe that they are allowed to access the website at 1:00 PM. They can then test other aspects of this combination in the following manner:*

- *logging in as a different user and observing that they are not allowed to access the website*

- *assigning the unauthorized user to the group that is authorized to access the website and observing that they can now access it themselves*
- *accessing a different website that is not allowed by the policy and observing that this site cannot be accessed*
- *accessing the same website at 5:30 PM and observing that their access attempt is rejected due to the time attribute*

This activity is then repeated for each other subject/object/operation/attribute combination.

C.1.4 Data Loss Prevention Access Control

Data Loss Prevention Access Control is used to reduce the risk of inadvertent data leakage between different security domains. This can be used to protect proprietary or sensitive information from disclosure. For example, certain "dirty" words, phrases, or regular expressions may be indicative of proprietary, sensitive, or personally identifiable data such as ###-##-#### being the standard format of a United States Social Security number. A Data Loss Prevention Access Control TOE should be able to identify when these types of data are potentially being conveyed to an external domain (or a less sensitive internal domain) and prohibit the action. This includes but is not necessarily limited to the following types of disclosure:

- Print spool disclosure: printing sensitive data by submitting it to the print spool so that it can be physically moved to an unauthorized location
- Application layer protocol disclosure: transmitting sensitive data via an application such as sending an email that contains it or uploading a file that contains it via a web form
- File disclosure: viewing a file that contains sensitive data that the subject is not authorized to view or moving or copying it into a less secure domain such as another hard drive
- Clipboard disclosure: copying sensitive data within an open file so that it may subsequently be pasted into an open file in a less secure domain
- Removable device disclosure: writing a file that contains sensitive data to a removable device that may be physically moved to an unauthorized location

Note that the intent of this type of access control is not to provide a comprehensive safeguard against malicious internal "leaks" entirely on its own. If mitigation of that threat is desired, sufficiently strong physical security, personnel security, and network boundary flow control devices also need to be employed to thwart a determined adversary.

FDP_ACC.1 Access Control Policy

Hierarchical to: No other components.

FDP_ACC.1.1 The TSF shall enforce the [access control Security Function Policy (SFP)] on [

- Subjects: subset of users from an organizational data store; and
- Objects: local and remote locations that are capable of receiving and subsequently storing or otherwise acting upon received data; and
- Operations: submit, transmit, view, move, copy, paste, write to; and
- Attributes: strings of sensitive data and files or repositories that may contain that data such that the data has a verified sensitivity level (e.g. PII)]

Application Note: *The intent of this policy is to ensure that data defined as proprietary or sensitive should not be able to leave a computer through some set of common means. For example, the TSF should prevent such data from being sent via email or exported to a different logical drive unless explicitly allowed.*

A Data Loss Prevention product may include the ability to examine the Operational Environment for unencrypted or misplaced sensitive data and correct the discrepancy. This capability is represented by the optional requirement ESM_DSC.1 included in this PP.

Dependencies: FDP_ACF.1 Security Attribute Based Access Control

FDP_ACF.1 Access Control Functions

Hierarchical to: No other components.

FDP_ACF.1.1 The TSF shall enforce the [access control SFP] to objects based on the following: [all operations between users and objects based upon the attributes defined in Table 8 below].

Application Note: *Consistent with the intent of ESM, the SFP-relevant security attributes that define subjects are expected to exist in the Operational Environment. The TOE should enforce policy based on legacy subjects that are globally defined by the organization deploying it.*

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [rules received from an authorized and compatible Policy Management product that encompass the following notions:

- Attributes of environmental data may be marked with a security attribute such as sensitive, proprietary, or not otherwise allowed to be disclosed (e.g. PII, classified data); and
- Objects that contain this data shall be forbidden from leaving the system unless the intended destination is an explicitly trusted location; and
- Mechanisms of leaving the system shall constitute, at minimum, transfer to other logical devices, printing, e-mailing, and copying to clipboard].

Application Note: *The ST author is expected to specify certain types and values of data that the TSF considers sensitive and the certain types of files and metadata that can be examined in order to determine if they contain this sensitive data.*

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: [if the

object is being moved to a destination such as a mail recipient or logical drive that is explicitly flagged as trusted or otherwise fully internal to the organization, the operation will be allowed].

Application Note: *The ST author is expected to define requirements for the ability of the TOE to determine if a logical device is flagged as trusted.*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [***assignment: additional rules***].

Application Note: *The ST author must specify the specific objects protected by the explicit denial process. This explicit denial process must be implemented independent of any policy consumed by the TSF.*

The ST author must define the specific mechanism of enforcement for these additional rules in sufficient detail for the evaluator to devise testable scenarios to confirm the effectiveness of these rules.

Dependencies: FDP_ACC.1 Subset Access Control

FMT_MSA.3 Static Attribute Initialization

Table 8. FDP Requirement Table for Data Loss Prevention Access Control

Subject	Object	Operation
User	Print Spool	Submit (transfer outside security domain)
	Application Layer Protocol	Transmit (transfer outside security domain)
	File	View | Move | Copy (to another security domain)
	Clipboard	Copy | Paste (to another security domain)
	Removable Drive	Write To (transfer outside security domain)

Assurance Activity:

The evaluator shall check the TSS in order to verify that the TOE is capable of mediating the activities that are defined in Table 6 above and that the access control policy

enforcement mechanism is described.

The evaluator shall check the operational guidance in order to verify that it provides instructions on how it receives access control policy data. For example, if the TOE receives policy rules in some defined language, the operational guidance shall indicate the statements in this language that correspond with the activities that are defined in Table 17 above.

The evaluator shall also check the operational guidance to verify that it provides information about how the TOE's rule processing engine. This allows administrators to design access control policies with appropriate expectations for how they will be enforced.

The evaluator shall then use an authorized and compatible Policy Management product to define policies that contain rules for mediating these activities. For each subject/object/operation/attribute combination, the evaluator shall execute at least one positive and one negative test in order to show that the TSF is capable of appropriately mediating these activities.

For example, the policy may define a rule that allows a user to only print documents that do not contain some specific sensitive data values. Once this policy is implemented, the evaluator will access a system and observe that a document containing sensitive data cannot be printed and that another document that does not contain sensitive data can be printed. Additionally, for each conditional attribute (such as a time of day restriction) that is supported, the evaluator will devise a positive and negative test that proves that the conditional attribute affects whether or not the requested operation is allowed. This activity is then repeated for each other subject/object/operation/attribute tuple.

For example, consider the following combinations:

- *untrusted user/group (subject), print spool (object), submit (operation), any file (attribute)*

The evaluator could test this combination by deploying a policy that unconditionally prohibits all members of a certain group from printing files. They can then log in as a user who belongs to that group, attempt to print a file, and observe that they are not able to print. They can then test other aspects of this combination in the following manner:

- *logging in as a user that doesn't belong to the untrusted group and observing that they are able to print the same file*

- *opening files in a variety of different applications (email, drawing, text editor, etc.) and observing that none of them can be used to print*

This activity is then repeated for each other subject/object/operation/attribute combination.

C.2 Object Discovery for Data Loss Prevention

In the case where a Data Loss Prevention Access Control TOE is able to examine the Operational Environment to identify objects which may not be stored in acceptable locations, the ST author shall claim the following optional SFR:

C.2.1 ESM_DSC.1 Object Discovery

Hierarchical to: No other components.

ESM_DSC.1.1 The TSF shall be able to discover objects in the Operational Environment that meet the following conditions: [selection: unencrypted data that policy requires to be encrypted, data that resides in a domain that is inconsistent with the data's defined sensitivity attributes, [***assignment: other condition that indicates that data that resides in the Operational Environment should be cataloged by the TSF***]].

Application Note: *The specific purpose of object discovery in this Protection Profile is for the TSF to detect objects that are entering or residing a domain in which they should not be allowed to exist.*

ESM_DSC.1.2 The TSF shall take the following actions upon discovery of an object as defined by ESM_DSC.1.1: [selection: encrypt the object, move the object to a location consistent with its sensitivity attributes, delete the object, [***assignment: other action***]].

Application Note: *If the assignment is selected, the specific action taken must relate to corrective action taken against the discovered object.*

If this SFR is included, the audit events must be adjusted to

include audit of objects containing discovered content and the action that was taken.

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it discusses the objects that the TOE can look for in the Operational Environment and the actions that are taken against these objects when they are discovered.

The evaluator shall check the operational guidance in order to identify that the existence of this capability is made clear to the administrator and that its configuration options, if any (for example, the administrator may have the ability to supply the key words/phrases that should be scanned for sanitizing), are described.

The evaluator shall test this capability by placing objects in the Operational Environment that are representative of objects that can be discovered by the TOE. The evaluator shall then verify that appropriate objects are discovered and appropriate actions are taken against them based on the TOE's configured behavior.

C.3 Self-Monitoring of TOE Components

A Host-Based Access Control TOE may provide additional resistance against termination by an untrusted user by monitoring itself and ensuring its continued operations. If this is the case, the ST author must claim the following SFR:

C.3.1 FPT_FLS.1 Failure with Preservation of a Secure State

Hierarchical to: No other components.

FPT_FLS.1.1 The TSF shall preserve a secure state when the following types of failures occur: [***assignment: list of TOE components and possible malfunctioning states***].

Application Note: *A secure state is preserved if the TSF can automatically resolve the failure or if it goes into a default-deny state and issues some sort of notification that makes it known that manual corrective action is required.*

An example of this requirement is the situation where the TSF is comprised of three running processes, each of which polls continuously to ensure the others are still running. In the case where a user tries to circumvent the TSF's access control by terminating one of the processes that comprises it, one of the other processes will restart the terminated one and prevent a disruption in access control enforcement. It may also create some sort of notification so that an administrator is aware that possible malicious activity is occurring.

The requirement of the TOE to perform monitoring of its components ensures that no user may mask their actions by ensuring that auditing cannot be disabled along with any other functionality that protects against unauthorized activity on the system. If this SFR is included in the ST, it will be mapped to satisfy the objective O.RESILIENT.

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check the TSS in order to determine that it describes the failure states the TOE may encounter and the actions that are taken by the TSF to resolve these states. The evaluator shall use this information to confirm that the TSF resolves the failure states in a manner that preserves a secure state as defined by the application note.

The evaluator shall check the operational guidance to verify that it documents all failure states of the TSF, what actions are performed by the TOE in response, and what actions, if any, must be performed by the administrator in order to clear the failure state. The evaluator shall confirm that this information is sufficient to ensure that a secure state is preserved.

The evaluator shall test this capability by deliberately inducing the failure states described in the SFR and observing whether or not the TSF reacts in a manner that is consistent with the Security Target's description of its expected behavior.

C.4 Conditional Enforcement of Session Establishment

A Host-Based Access Control TOE is expected to control access to the authentication function for one or more Operational Environment systems (see Appendix C.1.1). If this is enforced in a conditional manner, the ST author must claim the following optional SFR:

C.4.1 FTA_TSE.1 TOE Session Establishment

Hierarchical to: No other components.

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [selection: day, time, **[*assignment: other attributes***]].

Application Note: *Session establishment is to the host that is managed by the TSF. This requirement is included to provide a mechanism for the TSF to exert access control over the host's authentication function by determining the situations in which authentication credentials are valid such as time of day, day of week, or geographic location.*

If this SFR is claimed, the ST author must include success or denial of session establishment as an auditable event; audit of success may be disabled during operation for all levels of audit.

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall examine the TSS to determine that all of the attributes on which a session can be denied are specifically defined.

The evaluator shall examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS.

The evaluator shall test this capability by performing positive and negative testing for each attribute that can be used to conditionally allow session establishment. For example, if a time of day restriction applies, the evaluator shall successfully log on during an acceptable time and shall be prevented from logging on during an unacceptable time.

C.5 Cryptographic Functional Requirements

This Protection Profile was written to allow and encourage TOE developers to use third-party technologies to provide cryptographic functionality to protect the TOE, such as an Operating System or cryptographic library. In the event of the TOE providing its own internal cryptographic functionality and not relying on third-party technologies, the following requirements must also be taken into account.

Applicable Requirements

1. The ST author must be clear that this scenario exists for this product.
2. The evaluator must claim the requirements in this appendix within the ST.
3. The developer must provide assurance evidence that the requirements in this appendix are appropriately addressed.
4. The evaluator must devise and perform tests to test the functionality referred to within the requirements in this appendix.

These requirements must only be claimed in the event of the TOE performing its own cryptographic functionality and not relying on an OS or cryptographic library to perform the functionality. These requirements were taken from the Security Requirements for IPsec Virtual Private Network (VPN) Gateways. Note that that cryptographic standards used to define these capabilities are specific to the United States; for evaluations that are to be overseen by other countries, the applicable equivalent national standards must be used by the ST author.

C.5.1 FCS_CKM.1 Cryptographic Key Generation (for Asymmetric Keys)

Hierarchical to: No other components.

FCS_CKM.1.1 *Refinement:* The TSF shall generate *asymmetric* cryptographic keys *used for key establishment* in accordance with:

[selection:

- *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;*
- *NIST Special Publication 800-56A, "Recommendation*

for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard")

- *NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes]*

and specified cryptographic key sizes [***equivalent to, or greater than, 112 bits of security***] that meet the following: [***standards defined in first selection***].

Application Note: *This component requires that the TOE be able to generate the public/private key pairs that are used for key establishment purposes for the various cryptographic protocols used by the TOE (e.g., IPsec). If multiple schemes are supported, then the ST author must iterate this requirement to capture this capability. The scheme used will be chosen by the ST author from the selection.*

Since the domain parameters to be used are specified by the requirements of the protocol in this PP, it is not expected that the TOE will generate domain parameters, and therefore there is no additional domain parameter validation needed when the TOE complies with the protocols specified in this PP.

The generated key strength of 2048-bit DSA and rDSA keys need to be equivalent to, or greater than, 112 bits of security. See NIST Special Publication 800-57, "Recommendation for Key Management" for information about equivalent key strengths.

Dependencies: [FCS_CKM.2 Cryptographic Key Distribution, or

FCS_COP.1 Cryptographic Operation]

FCS_CKM.4 Cryptographic Key Destruction

Assurance Activity:

The evaluator shall use the key pair generation portions of "The FIPS 186-3 Digital Signature Algorithm Validation System (DSA2VS)", "The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)", and "The RSA Validation System (RSA2VS)" as a guide in testing the requirement above, depending on the selection performed by the ST author. This will require that the evaluator have a trusted reference implementation of the algorithms that can produce test vectors that are verifiable during the test.

In order to show that the TSF complies with 800-56A and/or 800-56B, depending on the selections made, the evaluator shall ensure that the TSS contains the following information:

- *The TSS shall list all sections of the appropriate 800-56 standard(s) to which the TOE complies.*
- *For each applicable section listed in the TSS, for all statements that are not "shall" (that is, "shall not", "should", and "should not"), if the TOE implements such options it shall be described in the TSS. If the included functionality is indicated as "shall not" or "should not" in the standard, the TSS shall provide a rationale for why this will not adversely affect the security policy implemented by the TOE;*
- *For each applicable section of 800-56A and 800-56B (as selected), any omission of functionality related to "shall" or "should" statements shall be described;*
- *Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described.*

C.5.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

Hierarchical to: No other components.

FCS_CKM_EXT.4.1 The TSF shall zeroize all plaintext secret and private cryptographic keys and cryptographic security parameters

when no longer required.

Application Note: *Any security related information (such as keys, authentication data, and passwords) shall be zeroized when no longer in use to prevent the disclosure or modification of security critical data.*

The zeroization indicated above applies to each intermediate storage area for plaintext key and/or critical security parameter (i.e., any storage, such as memory buffers, that is included in the path of such data) upon the transfer of the key/critical security parameter to another location.

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and critical security parameters used to generate key; when they are zeroized (for example, immediately after use, on system shutdown, etc.); and the type of zeroization procedure that is performed (overwrite with zeros, overwrite three times with random pattern, etc.). If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS describes the zeroization procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are zeroized by overwriting once with zeros, while secret keys stored on the internal hard drive are zeroized by overwriting three times with a random pattern that is changed before each write").

C.5.3 FCS_COP.1(1) Cryptographic Operation (for Data Encryption/Decryption)

Hierarchical to: No other components.

FCS_COP.1.1(1) *Refinement:* The TSF shall perform *encryption and decryption* in accordance with a specified cryptographic algorithm *AES operating in [assignment: one or more modes]* and cryptographic key sizes *128-bits, 256-bits, and [selection: 192 bits, no other key sizes]* that meets the following:

- *FIPS PUB 197, "Advanced Encryption Standard (AES)"*
- *[selection: NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D, NIST SP 800-38E]*

Application Note: *For the assignment, the ST author must choose the mode or modes in which the AES operates. For the first selection, the ST author must choose the key sizes that are supported by this functionality. For the second selection, the ST author must choose the standards that describe the modes specified in the assignment.*

Dependencies: [FDP_ITC.1 Import of User Data without Security Attributes, or

FDP_ITC.2 Import of User Data with Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic Key Destruction

Assurance Activity:

The evaluators shall use tests appropriate to the modes selected in the above requirement from "The Advanced Encryption Standard Algorithm Validation Suite (AESAVS)", "The XTS-AES Validation System (XTSVS)", The CMAC Validation System (CMACVS)", "The Counter with Cipher Block Chaining-Message Authentication Code (CCM) Validation System (CCMVS)", and "The Galois/Counter Mode (GCM) and GMAC Validation System (GCMVS)" (these documents are available from http://csrc.nist.gov/groups/STM/cavp/index.html) as a guide in testing the requirement above. This will require that the evaluators have a reference implementation of the algorithms that can produce test vectors that are verifiable during the test.

C.5.4 FCS_COP.1(2) Cryptographic Operation (for Cryptographic Signature)

Hierarchical to: No other components.

FCS_COP.1.1(2) *Refinement:* The TSF shall perform *cryptographic*

signature services in accordance with a *selection:*

(1) Digital Signature Algorithm (DSA) with a key size (modulus) of 2048 bits or greater,

(2) RSA Digital Signature Algorithm (rDSA) with a key size (modulus) of 2048 bits or greater, or

(3) Elliptic Curve Digital Signature Algorithm (ECDSA) with a key size of 256 bits or greater

that meets the following:

Case: Digital Signature Algorithm

- *FIPS PUB 186-3, "Digital Signature Standard"; or*

Case: RSA Digital Signature Algorithm

- *FIPS PUB 186-3, "Digital Signature Standard"; or*

Case: Elliptic Curve Digital Signature Algorithm

- *FIPS PUB 186-3, "Digital Signature Standard"; and*
- *The TSF shall implement "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard").*

Application Note: *As the preferred approach for cryptographic signature, elliptic curves will be required in future publications of this PP.*

The ST author must choose the algorithm implemented to perform digital signatures; if more than one algorithm is available, this requirement (and the corresponding FCS_CKM.1 requirement) must be iterated to specify the functionality. For the algorithm chosen, the ST author must make the appropriate assignments/selections to specify the parameters that are implemented for that algorithm.

For elliptic curve-based schemes, the key size refers to the log_2 of the order of the base point. As the preferred approach for digital signatures, ECDSA will be required in future publications of this PP.

Dependencies: [FDP_ITC.1 Import of User Data without Security Attributes, or

FDP_ITC.2 Import of User Data with Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic Key Destruction

Assurance Activity:

The evaluators shall use the signature generation and signature verification portions of "The FIPS 186-3 Digital Signature Algorithm Validation System (DSAVS)", "The FIPS 186-3 Elliptic Curve Digital Signature Algorithm Validation System (ECDSA2VS)", and "The RSA Validation System (RSAVS)" as a guide in testing the requirement above. This will require that the evaluators have a reference implementation of the algorithms that can produce test vectors that are verifiable during the test.

C.5.5 FCS_COP.1(3) Cryptographic Operation (for Cryptographic Hashing)

Hierarchical to: No other components.

FCS_COP.1.1(3) *Refinement:* The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm *[selection: SHA-1, SHA-256, SHA-384] and message digest sizes [selection: 160, 256, 384] bits* that meet the following: *FIPS Pub 180-3, "Secure Hash Standard."*

Application Note: *For this version of the PP, use of SHA-1 is allowed only for TLS for backward compatibility reasons. The next version of the PP will most likely completely exclude the use of SHA-1.*

The selection of the hashing algorithm shall correspond to

the selection of the message digest size; for example, if SHA-1 is chosen, then the only valid message digest size selection would be 160 bits.

Dependencies: [FDP_ITC.1 Import of User Data without Security Attributes, or

FDP_ITC.2 Import of User Data with Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic Key Destruction

Assurance Activity:

The evaluators shall use "The Secure Hash Algorithm Validation System (SHAVS)" as a guide in testing the requirement above. This will require that the evaluators have a reference implementation of the algorithms that can produce test vectors that are verifiable during the test.

C.5.6 FCS_COP.1(4) Cryptographic Operation (for Keyed-Hash Message Authentication)

Hierarchical to: No other components.

FCS_COP.1.1(4) *Refinement:* The TSF shall perform *keyed-hash message authentication* in accordance with a specified cryptographic algorithm *HMAC-[selection: SHA-1, SHA-256, SHA-384]***,** *key size [assignment: key size (in bits) used in HMAC], and message digest sizes [selection: 160, 256, 384] bits* that meet the following: *FIPS Pub 198-1, "The Keyed-Hash Message Authentication Code, and FIPS Pub 180-3, "Secure Hash Standard."*

Application Note: *For this version of the PP, use of SHA-1 is allowed only for TLS for backward compatibility reasons. The next version of the PP will most likely completely exclude the use of SHA-1.*

The selection of the hashing algorithm must correspond to

the selection of the message digest size; for example, if HMAC-SHA-256 is chosen, then the only valid message digest size selection would be 256 bits.

The message digest size above corresponds to the underlying hash algorithm used. Note that truncating the output of the HMAC following the hash calculation is an appropriate step in a variety of applications. This does not invalidate compliance with this requirement, however, the ST must state that truncation is performed, the size of the final output, and the standard to which this truncation complies.

Dependencies: [FDP_ITC.1 Import of User Data without Security Attributes, or

FDP_ITC.2 Import of User Data with Security Attributes, or

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic Key Destruction

Assurance Activity:

The evaluators shall use "The Keyed-Hash Message Authentication Code (HMAC) Validation System (HMACVS)" as a guide in testing the requirement above. This will require that the evaluators have a reference implementation of the algorithms that can produce test vectors that are verifiable during the test.

C.5.7 FCS_HTTPS_EXT.1 HTTPS

Hierarchical to: No other components.

Dependencies: FCS_TLS_EXT.1 TLS

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

Application Note: *The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by*

adding elements to this component, or by additional detail in the TSS.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS as specified in FCS_TLS_EXT.1.

Dependencies: FCS_TLS_EXT.1 TLS

Assurance Activity:

The evaluator shall check the TSS to ensure that it is clear on how HTTPS uses TLS to establish an administrative session, focusing on any client authentication required by the TLS protocol vs. security administrator authentication which may be done at a different level of the processing stack. The evaluator shall also check the TSS to verify that it describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall check the TSS to ensure it describes—for each platform identified in the ST—the interface(s) used by the TOE to invoke this functionality.

There are no assurance activities to be performed against the operational guidance for this requirement.

Testing for this activity is done as part of the TLS testing; this may result in additional testing if the TLS tests are done at the TLS protocol level.

C.5.8 FCS_IPSEC_EXT.1 IPsec

Hierarchical to: No other components.

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), [selection: no other algorithms, AES-GCM-128, AES-GCM-256 as specified in RFC 4106], and using [selection, choose at least one of: IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996 (with mandatory support for

NAT traversal as specified in section 2.23), 4307, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]].

Application Note: *The first selection is used to identify additional cryptographic algorithms supported. Either IKEv1 or IKEv2 support must be provided, although conformant TOES can provide both; the second selection is used to make this choice. For IKEv1, the requirement is to be interpreted as requiring the IKE implementation conforming to RFC 2409 with the additions/modifications as described in RFC 4109. RFC 4868 identifies additional hash functions for use with both IKEv1 and IKEv2; if these functions are implemented, the third (for IKEv1) and fourth (for IKEv2) selection can be used. IKEv2 will be required after January 1st, 2014.*

FCS_IPSEC_EXT.1.2 The TSF shall ensure that IKEv1 Phase 1 exchanges use only main mode.

FCS_IPSEC_EXT.1.3 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to 24 hours for Phase 1 SAs and 8 hours for Phase 2 SAs.

Application Note: *The above requirement can be accomplished either by providing Security Administrator-configurable lifetimes (with appropriate FMT requirements and instructions in documents mandated by AGD_OPE, as necessary), or by "hard coding" the limits in the implementation.*

FCS_IPSEC_EXT.1.4 The TSF shall ensure that IKEv1 SA lifetimes are able to be limited to [***assignment: number between 100 - 200***] MB of traffic for Phase 2 SAs.

Application Note: *The above requirement can be accomplished either by providing Security Administrator-configurable lifetimes (with appropriate FMT requirements and instructions in documents mandated by AGD_OPE), or by "hard*

coding" the limits in the implementation. The ST author selects the amount of data in the range specified by the requirement.

FCS_IPSEC_EXT.1.5 The TSF shall ensure that all IKE protocols implement DH Groups 14 (2048-bit MODP), and [selection: 24 (2048-bit MODP with 256-bit POS), 19 (256-bit Random ECP), 20 (384-bit Random ECP), [***assignment: other DH groups that are implemented by the TOE***], no other DH groups].

Application Note: *The above requires that the TOE support DH Group 14. If other groups are supported, then those should be selected (for groups 24, 19, and 20) or specified in the assignment above; otherwise "no other DH groups" should be selected. This applies to IKEv1 and (if implemented) IKEv2 exchanges. In future publications of this PP DH Groups 19 (256-bit Random ECP) and 20 (384-bit RandomECP) will be required.*

FCS_IPSEC_EXT.1.6 The TSF shall ensure that all IKE protocols implement Peer Authentication using the [selection: DSA, rDSA, ECDSA] algorithm.

Application Note: *The selected algorithm should correspond to an appropriate selection for FCS_COP.1(2).*

FCS_IPSEC_EXT.1.7 The TSF shall support the use of pre-shared keys (as referenced in the RFCs) for use in authenticating its IPsec connections.

FCS_IPSEC_EXT.1.8 The TSF shall support the following:

1. Pre-shared keys shall be able to be composed of any combination of upper and lower case letters, numbers, and special characters: [selection: "!", "@", "#", "$", "%", "^", "&", "*", "(", ")", [***assignment: other characters***];

2. Pre-shared keys of 22 characters and [selection:

[***assignment: other supported lengths***], no other lengths].

Application Note: *The ST author selects the special characters that are supported by TOE; they may optionally list additional special characters supported using the assignment. For the length of the pre-shared keys, a common length (22 characters) is required to help promote interoperability. If other lengths are supported they should be listed in the assignment; this assignment can also specify a range of values (e.g., "lengths from 5 to 55 characters") as well.*

Dependencies: FCS_COP.1 Cryptographic Operation

Assurance Activity:

The evaluator shall examine the TSS to verify the following:

1. *It specifies the hash functions used for integrity protection from the RFCs specified in the requirement.*
2. *It describes how "confidentiality only" ESP mode is disabled.*
3. *In the description of the IPsec protocol supported by the TOE, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used.*
4. *It describes how lifetimes for IKEv1 SAs (both Phase 1 and Phase 2) are established.*
5. *It describes how lifetimes for IKEv1 Phase 2 SAs--with respect to the amount of traffic that is allowed to flow using a given SA--are established.*
6. *It describes how the DH groups specified in the requirement are listed as being supported. If there is more than one DH group supported, it describes how a particular DH group is specified/negotiated with a peer.*
7. *It describes how pre-shared keys are established and used in authentication of IPsec connections. The description shall also indicate how pre-shared key establishment is accomplished for both TOEs that can generate a pre-shared key*

as well as TOEs that simply use a pre-shared key.

8. *It describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall perform the following activities:*

    a. *Ensure the ST contains a list of representative platforms (hardware and software) compromising the operational environment.*

    b. *Check the TSS to ensure it describes-for each platform identified in the ST-the interface(s) used by the TOE to invoke this functionality.*

    c. *For each platform identified in the ST, check the OE documentation to ensure the interfaces identified in the previous step exist.*

The evaluator shall examine the operational guidance to determine the following:

1. *If the cryptographic parameters for a connection are settable by an administrator, it provides instructions for setting these parameters, how to establish an IPsec connection using these parameters, and what parameter values are allowed in the evaluated configuration.*

2. *It describes any configuration necessary to ensure that "confidentiality only" mode is disabled, and that an advisory is present indicating that tunnel mode is the preferred ESP mode since it protects the entire packet.*

3. *It contains instructions for configuring the TOE prior to the use of main mode if such configuration is necessary.*

4. *It contains instructions for configuring lifetimes for IKEv1 SAs if these values are configurable.*

5. *It contains instructions for configuring the maximum amount of traffic that can flow using a given SA if this value is configurable.*

6. *It describes how pre-shared keys are to be generated and established for a TOE. The description shall also indicate how pre-shared key establishment is accomplished for both TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key.*

7. *It describes the generation of preshared keys, including guidance on generating*

strong keys and the allowed character set. The evaluator shall also check that this guidance does not limit the pre-shared key in a way that would not satisfy the requirement. It should be noted that while the administrator (in contravention to the operational guidance) can choose a key that does not conform to the requirement, there is no requirement that the TOE check the key to ensure that it meets the rules specified in this component. However, should the administrator choose to create a password that conforms to the rules above (and the operational guidance); the TOE should not prohibit such a choice.

The evaluator shall also perform the following tests. Note that aspects of these tests may be combined so long as the evaluator can demonstrate that each individual test is satisfied.

- *Test 1: The evaluator shall configure and establish IPsec connections using each parameter specified in FCS_IPSEC_EXT.1.1. While it is not necessary to perform connections using all combinations of all parameters, it must be clear what combinations were tested and why the subset chosen is representative. It is sufficient to observe (on the wire) the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES). In cases where the negotiation may be obscured (phase 2 negotiations, for example) alternative means of showing that the required parameters are being used are allowable (for instance, administrative commands designed to show the parameters in use for a particular established connection).*
- *Test 2: The evaluator shall configure the TOE as indicated in the operational guidance, and attempt to establish a connection using an IKEv1 Phase 1 connection in aggressive mode. This attempt should fail. The evaluator should then show that main mode exchanges are supported.*
- *Test 3: The evaluator shall configure the TOE as indicated in the operational guidance, and attempt to establish a connection using ESP in "confidentiality only" mode. This attempt should fail. The evaluator shall then establish a connection using ESP in confidentiality and integrity mode.*
- *Test 4: The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The*

evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.

- *Test 5: The evaluator shall perform a test similar to Test 1 for Phase 2 SAs, except that the lifetime will be 8 hours instead of 24.*
- *Test 6: The evaluator shall construct a test where a Phase 2 SA is established and attempted to be maintained while more data than is specified in the above assignment flows over the connection. The evaluator shall observe that this SA is closed or renegotiated before the amount of data specified is exceeded. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.*
- *Test 7: For each supported DH group, the evaluator shall test to ensure that all IKE protocols can be successfully completed using that particular DH group.*
- *Test 8: The evaluator shall generate a pre-shared key and use it, as indicated in the operational guidance, to establish an IPsec connection between two peers. If the TOE supports generation of the pre-shared key, the evaluator shall ensure that establishment of the key is carried out for an instance of the TOE generating the key as well as an instance of the TOE merely taking in and using the key.*
- *Test 9: The evaluator shall generate a pre-shared key that is 22 characters long that meets the composition requirements above. The evaluator shall then use this key to successfully establish an IPsec connection. While the evaluator is not required to test that all of the special characters or lengths listed in the requirement are supported, it is required that they justify the subset of those characters chosen for testing, if a subset is indeed used.*

C.5.9 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

Hierarchical to: No other components.

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: NIST Special Publication 800-90 using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES),

Dual_EC_DRBG (any)]; FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES] seeded by an entropy source that accumulates entropy from [selection: choose one of: (1) one or more independent hardware-based noise sources, (2) one or more independent software-based noise sources, (3) a combination of hardware-based and software-based noise sources.].

FCS_RBG_EXT.1.2 The deterministic RBG shall be seeded with a minimum of [selection, choose one of: 112 bits, 128 bits, 256 bits] of entropy at least equal to the greatest security strength of the keys and hashes that it will generate.

Application Note: *NIST Special Pub 800-90, Appendix C describes the minimum entropy measurement that will probably be required future versions of FIPS-140. If possible this should be used immediately and will be required in future versions of this PP.*

For the first selection in FCS_RBG_(EXT).1.1, the ST author must select the standard to which the RBG services comply (either 800-90 or 140-2 Annex C).

SP 800-90 contains four different methods of generating random numbers; each of these, in turn, depends on underlying cryptographic primitives (hash functions/ciphers). The ST author will select the function used (if 800-90 is selected), and include the specific underlying cryptographic primitives used in the requirement or in the TSS. While any of the identified hash functions (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) are allowed for Hash_DRBG or HMAC_DRBG, only AES-based implementations for CT_DRBG are allowed. While any of the curves defined in 800-90 are allowed for Dual_EC_DRBG, the ST author not only must include the curve chosen, but also the hash algorithm used.

Note that for FIPS Pub 140-2 Annex C, currently only the

method described in NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, Section 3 is valid. If the key length for the AES implementation used here is different than that used to encrypt the user data, then FCS_COP.1 may have to be adjusted or iterated to reflect the different key length. For the selection in FCS_RBG_EXT.1.2, the ST author selects the minimum number of bits of entropy that is used to seed the RBG.

The ST author also ensures that any underlying functions are included in the baseline requirements for the TOE.

For the selection in FCS_RBG_EXT.1.2, the ST author selects the appropriate number of bits of entropy that corresponds to the greatest security strength of the algorithms included in the ST. Security strength is defined in Tables 2 and 3 of NIST SP 800-57A. For example, if the implementation includes 2048-bit RSA (security strength of 112 bits), AES 128 (security strength 128 bits), and HMAC-512 (security strength 256 bits), then the ST author would select 256 bits.

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall review the TSS section to determine the version number of the product containing the RBG(s) used in the TOE. The evaluator shall also review the TSS to determine that it includes discussions that are sufficient to address the requirements described in Appendix C.6 Entropy Documentation and Assessment. This documentation may be included as a supplemental addendum to the Security Target.

Regardless of the standard to which the RBG is claiming conformance, the evaluator performs the following test:

Test 1: The evaluator shall determine an entropy estimate for each entropy source by using the Entropy Source Test Suite. The evaluator shall ensure that the TSS includes an entropy estimate that is the minimum of all results obtained from all entropy sources.

Implementations Conforming to FIPS 140-2, Annex C

The reference for the tests contained in this section is The Random Number Generator Validation System (RNGVS) [RNGVS]. The evaluators shall conduct the following two tests. Note that the "expected values" are produced by a reference implementation of the algorithm that is known to be correct. Proof of correctness is left to each Scheme.

The evaluators shall perform a Variable Seed Test. The evaluators shall provide a set of 128 (Seed, DT) pairs to the TSF RBG function, each 128 bits. The evaluators shall also provide a key (of the length appropriate to the AES algorithm) that is constant for all 128 (Seed, DT) pairs. The DT value is incremented by 1 for each set. The seed values shall have no repeats within the set. The evaluators ensure that the values returned by the TSF match the expected values.

The evaluators shall perform a Monte Carlo Test. For this test, they supply an initial Seed and DT value to the TSF RBG function; each of these is 128 bits. The evaluators shall also provide a key (of the length appropriate to the AES algorithm) that is constant throughout the test. The evaluators then invoke the TSF RBG 10,000 times, with the DT value being incremented by 1 on each iteration, and the new seed for the subsequent iteration produced as specified in NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, Section 3. The evaluators ensure that the 10,000th value produced matches the expected value.

Implementations Conforming to NIST Special Publication 800-90

The evaluator shall perform 15 trials for the RNG implementation. If the RNG is configurable, the evaluator shall perform 15 trials for each configuration. The evaluator shall also confirm that the operational guidance contains appropriate instructions for configuring the RNG functionality.

If the RNG has prediction resistance enabled, each trial consists of (1) instantiate drbg, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "generate one block of random bits"

means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90).

If the RNG does not have prediction resistance, each trial consists of (1) instantiate drbg, (2) generate the first block of random bits (3) reseed, (4) generate a second block of random bits (5) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The fifth value is additional input to the first call to generate. The sixth and seventh are additional input and entropy input to the call to reseed. The final value is additional input to the second generate call.

The following paragraphs contain more information on some of the input values to be generated/selected by the evaluator.

> ***Entropy input:*** *the length of the entropy input value must equal the seed length.*
>
> ***Nonce:*** *If a nonce is supported (CTR_DRBG with no df does not use a nonce), the nonce bit length is one-half the seed length.*
>
> ***Personalization string:*** *The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.*
>
> ***Additional input:*** *the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.*

C.5.10 FCS_SSH_EXT.1 SSH

Hierarchical to: No other components.

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

Application Note: *The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to this component, or by additional detail in the TSS. In a*

future version of this PP, a requirement will be added regarding rekeying. The requirement will read "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.1.2 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.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [***assignment: number of bytes***] bytes in an SSH transport connection are dropped.

Application Note: *RFC 4253 provides for the acceptance of "large packets" with the caveat that the packets should be of "reasonable length" or dropped. The assignment should be filled in by the ST author with the maximum packet size accepted, thus defining "reasonable length" for the TOE.*

FCS_SSH_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms: AES-CBC-128, AES-CBC-256, [selection: AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other algorithms].

Application Note: *In the assignment, the ST author can select the AES-GCM algorithms, or "no other algorithms" if AES-GCM is not supported. If AES-GCM is selected, there should be corresponding FCS_COP entries in the ST. Since the Dec. 2010 publication of NDPP v1.0, there has been consider progress with respect to the prevalence of AES-GCM support in commercial network devices. It is likely that an updated version of this PP will be published in the future which will require AES-GCM and AES-CBC will become optional.*

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [selection: PGP-SIGN-

RSA, PGP-SIGN-DSS, no other public key algorithms] as its public key algorithm(s).

Application Note: *RFC 4253 specifies required and allowable public key algorithms. This requirement makes SSH-RSA "required" and allows two others to be claimed in the ST. The ST author should make the appropriate selection, selecting "no other public key algorithms" if only SSH_RSA is implemented.*

FCS_SSH_EXT.1.6 The TSF shall ensure that data integrity algorithms used in SSH transport connection is [selection: hmac-sha1, hmac-sha1-96, hmac-md5, hmac-md5-96].

FCS_SSH_EXT.1.7 The TSF shall ensure that diffie-hellman-group14-sha1 is the only allowed key exchange method used for the SSH protocol.

Dependencies: FCS_COP.1 Cryptographic Operation

Assurance Activity:

The evaluator shall examine the TSS to verify the following:

1. *It contains a description of the public key algorithms that are acceptable for use for authentication, that this list conforms to FCS_SSH_EXT.1.5, and that password-based authentication methods are also allowed.*
2. *It describes how "large packets" in terms of RFC 4253 are detected and handled.*
3. *It specifies any encryption algorithms and optional characteristics, and that this information is consistent which the SFR.*
4. *It lists the supported data integrity algorithms, and that that list corresponds to the list in this SFR.*
5. *It describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall perform the following activities:*

   a. Ensure the ST contains a list of representative platforms (hardware and

software) compromising the operational environment.

b. *Check the TSS to ensure it describes-for each platform identified in the ST-the interface(s) used by the TOE to invoke this functionality.*

c. *For each platform identified in the ST, check the OE documentation to ensure the interfaces identified in the previous step exist.*

The evaluator shall examine the operational guidance to verify the following:

1. *It contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).*
2. *It contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the "none" MAC algorithm is not allowed).*
3. *It contains configuration information that will allow the security administrator to configure the TOE so that all key exchanges for SSH are performed using DH group 14. If this capability is "hard-coded" into the TOE, the evaluator shall check the TSS to ensure that this is stated in the discussion of the SSH protocol.*

The evaluator shall test this capability by performing the following tests:

- *Test 1: The evaluator shall, for each public key algorithm supported, show that the TOE supports the use of that public key algorithm to authenticate a user connection. Any configuration activities required to support this test shall be performed according to instructions in the operational guidance.*
- *Test 2: Using the operational guidance, the evaluator shall configure the TOE to accept password-based authentication, and demonstrate that a user can be successfully authenticated to the TOE over SSH using a password as an authenticator.*
- *Test 3: The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in FCS_SSH_EXT.1.3, that packet is dropped.*
- *Test 4: The evaluator shall establish a SSH connection using each of the encryption and integrity algorithms specified by FCS_SSH_EXT.1.4 and FCS_SSH_EXT.1.6. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.*

- *Test 5: The evaluator shall attempt to perform a diffie-hellman-group1-sha1 key exchange, and observe that the attempt fails. The evaluator shall then attempt to perform a diffie-hellman-group14-sha1 key exchange, and observe that the attempt succeeds.*

C.5.11 FCS_TLS_EXT.1 TLS

Hierarchical to: No other components.

FCS_TLS_EXT.1.1 The TSF shall implement one or more of the following protocols [selection: TLS 1.0 (RFC 2246), TLS 1.1 (RFC 4346), TLS 1.2 (RFC 5246)] supporting the following ciphersuites:

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

[selection:
None
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
].

Application Note: *The ST author must make the appropriate selections and assignments to reflect the TLS implementation. The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done either by adding elements to*

this component, or by additional detail in the TSS.

The ciphersuites to be used in the evaluated configuration are limited by this requirement. The ST author should select the optional ciphersuites that are supported; if there are no ciphersuites supported other than the mandatory suites, then "None" should be selected. If administrative steps need to be taken so that the suites negotiated by the implementation are limited to those in this requirement, the appropriate instructions need to be contained in the guidance called for by AGD_OPE. The Suite B algorithms (RFC 5430) listed above are the preferred algorithms for implementation. Since the Dec. 2010 publication of this requirement in NDPP v1.0, there has been limited progress with respect to extending the prevalence of TLS 1.2 support in commercial products. Future publications of this PP will require support for TLS 1.2 (RFC 5246); however, it is likely the next version of this PP will not include a requirement for TLS 1.2 support, but will require that the TOE offer a means to deny all connection attempts using SSL 2.0 or SSL 3.0.

Dependencies: FCS_COP.1 Cryptographic Operation

Assurance Activity:

The evaluator shall check the description of the implementation of this protocol in the TSS to ensure that optional characteristics (e.g., extensions supported, client authentication supported) are specified, and the ciphersuites supported are specified as well. The evaluator shall check the TSS to ensure that the ciphersuites specified are identical to those listed for this component. The evaluator shall also check the TSS to verify that it describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall perform the following activities:

a. *Ensure the ST contains a list of representative platforms (hardware and software) compromising the operational environment.*

b. *Check the TSS to ensure it describes-for each platform identified in the ST-the interface(s) used by the TOE to invoke this functionality.*

c. *For each platform identified in the ST, check the OE documentation to ensure the interfaces identified in the previous step exist.*

The evaluator shall check the operational guidance to ensure that it contains instructions on configuring the TOE in the Operational Environment so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements or an administrator is expected to deploy a particular client to access the TOE).

The evaluator shall test this capability by establishing a TLS connection using each of the ciphersuites specified by the requirement. This connection may be established as part of the establishment of a higher-level protocol, e.g., as part of a HTTPS session. It is sufficient to observe (on the wire) the successful negotiation of a ciphersuite to satisfy the intent of the test; it is not necessary to examine the characteristics of the encrypted traffic in an attempt to discern the ciphersuite being used (for example, that the cryptographic algorithm is 128-bit AES and not 256-bit AES).

C.6 Entropy Documentation and Assessment

The documentation of the entropy source should be detailed enough that, after reading, the evaluator will thoroughly understand the entropy source and why it can be relied upon to provide entropy. This documentation should include multiple detailed sections: design description, entropy justification, operating conditions, and health testing. This documentation is not required to be part of the TSS.

Design Description

Documentation shall include the design of the entropy source as a whole, including the interaction of all entropy source components. It will describe the operation of the entropy source to include how it works, how entropy is produced, and how unprocessed (raw) data can be obtained from within the entropy source for testing purposes. The documentation should walk through the entropy source design indicating where the random comes from, where it is passed next, any postprocessing of the raw outputs (hash, XOR, etc.), if/where it is stored, and finally, how it is output from the entropy source. Any conditions placed on the process (e.g., blocking) should also be described in the entropy source design. Diagrams and examples are encouraged. This design must also

include a description of the content of the security boundary of the entropy source and a description of how the security boundary ensures that an adversary outside the boundary cannot affect the entropy rate.

Entropy Justification

There should be a technical argument for where the unpredictability in the source comes from and why there is confidence in the entropy source exhibiting probabilistic behavior (an explanation of the probability distribution and justification for that distribution given the particular source is one way to describe this). This argument will include a description of the expected entropy rate and explain how you ensure that sufficient entropy is going into the TOE randomizer seeding process. This discussion will be part of a justification for why the entropy source can be relied upon to produce bits with entropy.

Operating Conditions

Documentation will also include the range of operating conditions under which the entropy source is expected to generate random data. It will clearly describe the measures that have been taken in the system design to ensure the entropy source continues to operate under those conditions. Similarly, documentation shall describe the conditions under which the entropy source is known to malfunction or become inconsistent. Methods used to detect failure or degradation of the source shall be included.

Health Testing

More specifically, all entropy source health tests and their rationale will be documented. This will include a description of the health tests, the rate and conditions under which each health test is performed (e.g., at startup, continuously, or on-demand), the expected results for each health test, and rationale indicating why each test is believed to be appropriate for detecting one or more failures in the entropy source.

Appendix D - Document Conventions

Except for replacing United Kingdom spelling with American spelling, the notation, formatting, and conventions used in this PP are consistent with version 3.1 of the Common Criteria (CC). Selected presentation choices are discussed here to aid the PP reader.

D.1 Operations

The CC permits four functional component operations—assignment, refinement, selection, and iteration—to be performed on functional requirements. This PP will highlight the four operations in the following manner:

- **Assignment**: allows the specification of an identified parameter. Indicated with ***bold and italicized text*** inside square brackets that contain the prompt "assignment:" if further operations are necessary by the Security Target author;
- **Refinement**: allows the addition of details. Indicated with *italicized text.* An SFR with a refinement is also preceded with "*Refinement:*" unless it is only an editorial refinement (i.e. only functional refinements are labeled in this way).
- **Selection:** allows the specification of one or more elements from a list. Indicated with underlined text inside square brackets that contain the prompt "selection:".
- **Iteration**: allows a component to be used more than once with varying operations. Indicated with a sequential number in parentheses following the element number of the iterated SFR.

For requirements taken from CC part 2 where selections and assignments have already been completed to ensure they apply to the PP, the substituted text is placed in square brackets but no additional formatting is applied.

D.2 Extended Requirement Convention

Extended requirements are permitted if the CC does not offer suitable requirements to meet the authors' needs. Extended requirements must be identified and are required to use the CC class/family/component model in articulating the requirements. Extended requirements that are based on CC Part 2 classes or families will be indicated with the "EXT" inserted within the component. Extended requirements that were defined

specifically for Enterprise Security Management functional capabilities will be indicated with the "ESM" class name.

D.3 Application Notes

Application notes contain additional supporting information that is considered relevant or useful for the construction of Security Targets for conformant TOEs, as well as general information for developers, evaluators, and ISSEs. Application notes also contain advice relating to the permitted operations of the component.

D.4 Assurance Activities

Assurance activities serve as a Common Evaluation Methodology for the functional requirements levied on the TOE to mitigate the threat. The activities include instructions for evaluators to analyze specific aspects of the TOE as documented in the TSS, thus levying implicit requirements on the ST author to include this information in the TSS section. In this version of the PP these activities are directly associated with the functional and assurance components, although future versions may move these requirements to a separate appendix or document.

Appendix E - Glossary of Terms

Table 9. Terms and Definitions

Term	Definition
Access Control	A mechanism put in place to allow or deny the execution of defined operations requested by defined subjects to be performed against defined objects or the result achieved by employing such a mechanism.
Access Control SFP	The definition of what attributes the TOE uses to perform access control. This differs from a policy because the policy is an instance of the Access Control SFP that associates specific values used for access control rather than defining the abstract attributes that these values will represent.
Attribute-Based Access Control	A means of access control that is based upon the attributes of a user rather than static permissions and access control lists. An example would be a system that grants access to specific resources if a user is an engineer and denies access to the same resources if the user is a contractor.
Consume	The act of the TOE receiving a policy, parsing it, and storing it in a manner such that it can be used to perform access control determinations.
Discretionary Access Control	A means of access control based on authorizations issued to a subject by virtue of their identity or group membership.
End User	An individual attempting to access a resource protected by the TOE, defined in the Access Control SFP as a subject.
Enterprise Security Management	The systems and resources required to order, create, disseminate, modify, suspend and terminate management controls to provision and operate Information Assurance services, processes and devices across the enterprise.
Mandatory Access Control	A means of access control based on the notion that all subjects and objects within an enterprise are associated with one or more hierarchical labels. The dominance relationship assigned to these labels determines if access is permitted.
Network Access Control	A form of access control where the subject is a collection of network traffic.
Operational Environment	The collection of hardware and software resources in an enterprise that are not within the TOE boundary. This may include but is not limited to third-party software components the TOE requires to operate, resources protected by the TOE, and the hardware upon which the TOE is installed.
Policy	A collection of rules that determine how the Access Control SFP is instantiated. These rules define the conditions under which defined subjects are allowed to perform defined operations against defined objects.
Policy Decision Point	A component of an ESM solution that is responsible for consuming access control policies and adjudicating observed environmental behavior against applicable rules in order to determine their validity.

Term	Definition
Policy Enforcement Point	A component of an ESM solution that is responsible for acting upon decisions reached by a Policy Decision Point.
Policy Management Product	An application that is responsible for creating policies that are consumed by the Policy Decision Point. These policies may be created through automated mechanisms, by manual administrative input, or by some combination of the two.
Role-Based Access Control	A means of access control that authorizes subject requests based on the roles to which they are assigned and the authorizations that are associated with those roles.
Secure Configuration Management Product	A product that is compliant with the Standard Protection Profile for ESM Secure Configuration Management. Such a product is capable of determining the status of deployed systems and/or applications in the Operational Environment, comparing this status to a defined organizational security baseline, and performing corrective or notifying actions when the deployment is inconsistent with the baseline.
System Access Control	A form of access control where the object is a binary or resource on a computer system.
System Administrator	An individual who has management authority over objects in the Operational Environment.
TOE Administrator	Within the context of the PP this refers to the one or more individuals who are responsible for setting up the TOE, using the Policy Management product to define policies the TOE consumes, and reviewing audit data the TOE generates.
User	See End User.

Appendix F - Identification

F.1 Identification

Title: Standard Protection Profile for Enterprise Security Management Access Control

Author: ESM Protection Profile Technical Community

Common Criteria Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1, September 2012

Version: PP Version 2.1

Keywords: enterprise security, enterprise security management, enterprise security management, access control, policy enforcement, data protection

Evaluation Assurance Level (EAL): EAL 1 augmented

F.2 Acknowledgements

This Protection Profile was originally proposed at the International Common Criteria Conference, Jeju, South Korea September 2008 by Eric Winterton from Booz | Allen | Hamilton (BAH) and Joshua Brickman from CA Technologies. It was authored by Booz | Allen | Hamilton along with industry, government/ scheme input, Common Criteria consultants and labs. The authors wish to thank the members of the Enterprise Security Management Protection Profile Technical Committee for their hard work and commitment to creating this document.