Standard Protection Profile for Enterprise Security Management Access Control

February 22, 2012

Version 2.0

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

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.

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] There are two 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. The second type, *policy consumption*, consumes a defined policy and enforces it. These two types of ESM capabilities are represented in the overall suite of ESM Protection Profiles.

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 object authorization.

[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.

- **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.
- **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

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/E	C	C	$C_{(3)}$	C	$C_{(1)}$
ESM Policy Management Protection Profile	D	C	D/$C_{(2)}$	$C_{(3)}$	C	$C_{(1)}$/D
ESM Identity and Credential Management	C	D	C/$D_{(2)}$	D/$C_{(3)}$	C	$C_{(1)}$
ESM Authentication Server	C	C/E		C/E	C	$C_{(1)}$
ESM Audit Management		C		$C_{(3)}$	C	$C_{(1)}$/E

ESM Secure Configuration Management				C(3)	D/C/E	C(1)
C = Consume; D = Define; E = Enforce						
Notes: (1) The audit policy is consumed as the TOE determines what events to audit. (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 consumed in the sense that authorized users must authenticate to the 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.

[3] Henceforth, just “product”.

- **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 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 utilize 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 Management 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.
- **Support for 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.

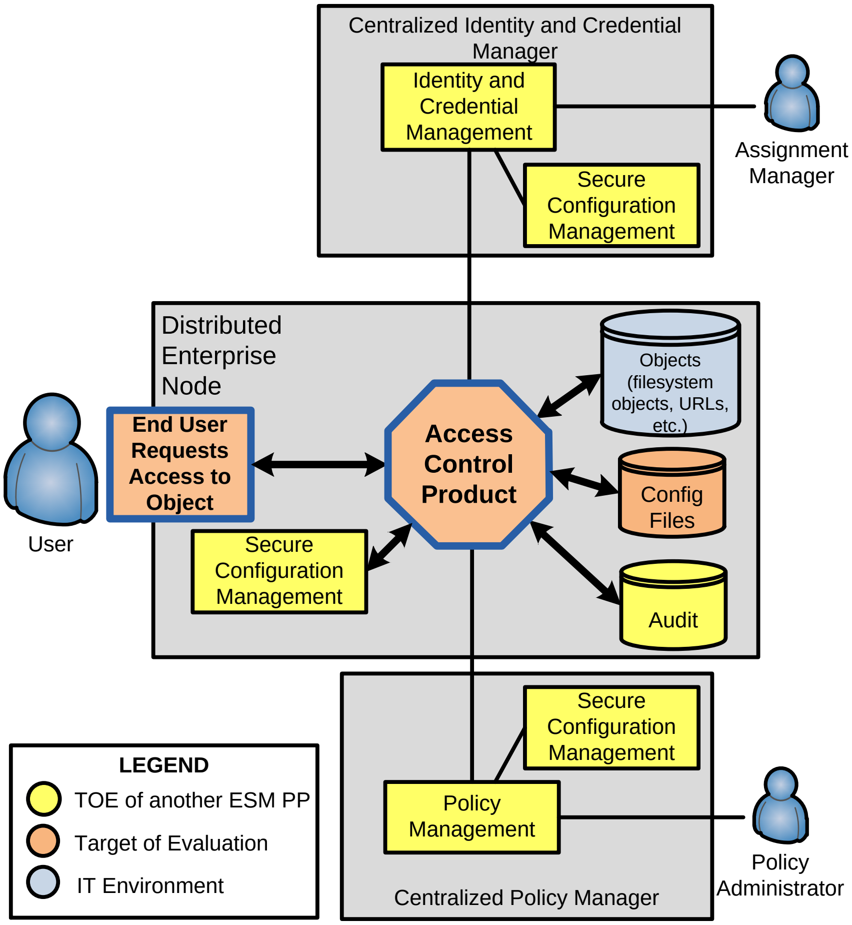
Centralized Identity and Credential Manager
Identity and Credential Management
Secure Configuration Management
Assignment Manager
Distributed Enterprise Node
User
End User Requests Access to Object
Access Control Product
Objects (filesystem objects, URLs, etc.)
Config Files
Audit
Secure Configuration Management
Secure Configuration Management
Policy Management
Centralized Policy Manager
Policy Administrator
LEGEND
TOE of another ESM PP
Target of Evaluation
IT Environment

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, one of a collection of client endpoints, or as a single agent that resides on a server or network boundary device. Note that operational environment objectives may not be claimed as being met by the TOE due to the nature of strict compliance. For common cases where operational environment objectives may be satisfied by ESM Access Control products, the developer must work with CCEVS to add those SFRs as optional SFRs in a future version of this profile.

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 utilize, 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.

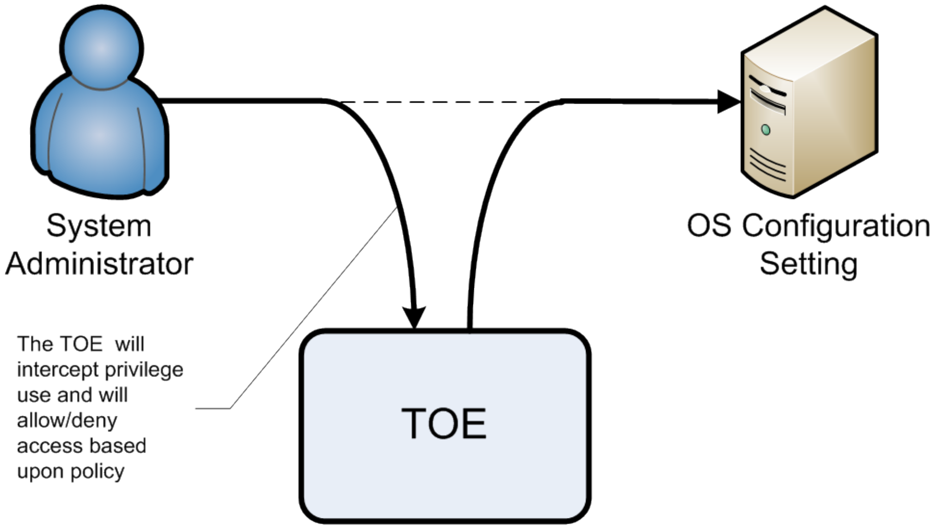
System Administrator
OS Configuration Setting
The TOE will intercept privilege use and will allow/deny access based upon policy
TOE

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 Audit Management
- Standard Protection Profile for ESM Secure Configuration Management

- Standard Protection Profile for ESM Authentication Server

Products claiming conformance to this protection profile must identify compatible environmental products that conform to the other Protection Profiles. If the TOE performs functionality that is compatible with multiple Protection Profiles, then conformance to all applicable Protection Profiles must be claimed.

1.7 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, and objectives that apply to the Protection Profile.

The document also contains the following appendicies:

- Appendix A - This appendix provides a list of references and defines the acronyms used in this document.
- Appendix B - 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 - Defines the potential architectural variations that PP-compliant products may exhibit, and enumerates the User Data Protection requirements for the different technology types. It also provides approved optional requirements.
- Appendix D - Describes the conventions used in the document.

- Appendix E - Defines the terminology used in the document.
- Appendix F - 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-2009-07-004, Version 3.1 Revision 3 July 2009.

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 shall meet a minimum standard of strict conformance as defined by section D.2 of CC Part 1.

Strict-PP conformance means the requirements in the PP are met and that the ST is an instantiation of the PP. The ST can be broader than the PP. The ST specifies that the TOE does at least the same as the PP, while the operational environment does at most the same as 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 evaluator of the ST will ensure strict-PP compliance by determining that the ST and its described TOE not only contain all the statements within this PP (and possibly more) 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 at least equal to or stronger than what is in the PP, and that all assurance activities stated in the PP will be performed.

3 Threats

The following sections enumerate the threats that could be used to adversely affect the TOE or the Operational Environment.

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

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: 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; ESM_DSC.1 (optional); FTA_SSL_EXT.1 (optional); FTA_SSL.3 (optional); FTA_SSL.4 (optional); 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(2))

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(2), FCS_CKM.1.1 (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))

4.4 Self-Protection

As discussed in section 1.4.1, 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 incorrect TOE configuration and attempted malicious activity against protected objects, the TOE is expected to provide the ability to generate audit data about its behavior. In order to reduce the risk of the TOE being overwhelmed with a large volume of audit data and to facilitate potential compliance with an ESM Audit Management system, the TOE must be capable of sending this audit information to an external trusted entity. This will increase the likelihood of the availability of audit data.

This PP does not mandate any specific actions to be taken in the event that this trusted entity is not accessible. The ST author should 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. Similarly, the TOE should be able to identify itself to other ESM components 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.

(O.SELFID, O.MNGRID: FCO_NRR.2, FTP_ITC.1(1), FTP_ITC.1(2))

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 and the optional components specified in the appendices.

5.1 Class ESM: Enterprise Security Management

ESM functional requirements pertain to behaviors that support the centralized management of authentication, authorization, accountability, and compliance activities in an organization. This class specifies functional activities that support class FDP and FIA by requiring the TSF to provide data that is used for data protection and authentication activities.

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***]].

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***]].

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 meet 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.

5.2 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 a specific external repository in a specific secure manner.

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 an external IT entity over a trusted channel defined in FTP_ITC.1.

Management: FAU_STG_EXT.1

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

a) Specification of the external IT entity 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 entity that is used to receive generated audit data.

5.3 Class FCS: Cryptographic Support

5.3.1 FCS_CKM_EXT.4 Cryptographic Key Zerioization

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 deletion 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 External audit trail storage is included in the PP/ST:

a) Basic: Failure of the key zeroization process.

5.3.2 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.

5.3.2.1 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 External audit trail storage is included in the PP/ST:

a) Basic: Failure of the randomization process.

5.4 Class FPT: Protection of the TSF

5.4.1 FPT_FLS_EXT.1 Failure of Communications

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.

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 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. 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.

Dependencies: No dependencies.

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) Failure of communication between the TOE and Policy Management product

5.5 Class FTA: TOE Access

5.5.1 FTA_SSL_EXT.1 TSF-initiated session locking

This SFR describes the behavior of the TOE when it must initiate session locks. An explicit requirement was required in order to narrow scope and to specify the locking actions, which were fixed in the base requirement in the Common Criteria.

Hierarchical to: No other components.

FTA_SSL_EXT.1.1 The TSF shall, for **local** interactive sessions, [selection:

- lock the session – clear or overwrite display devices, making the current contents unreadable, disable any activity of the user's data access/display devices other than unlocking the session, and require that the user re-authenticate to the TSF prior to unlocking the session;
- terminate the session

] after an Authorized Administrator specified time period of inactivity.

Dependencies: No dependencies.

Management: FTA_SSL_EXT.1

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

a) specification of the time of user inactivity after which lock-out occurs for an individual user;
b) specification of the default time of user inactivity after which lock-out occurs;
c) management of the events that should occur prior to unlocking the session.

Audit: FTA_SSL_EXT.1

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

a) Minimal: Locking of an interactive session by the session locking mechanism.
b) Minimal: Successful unlocking of an interactive session.
c) Basic: Any attempts at unlocking an interactive session.

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 functional security requirements for the PP consist of the following components, summarized in Table 2.

Table 2 — TOE Functional Components

Functional Component	
ESM_DSC.1 (optional)	Object Inventory *(as defined for specific technology types in Appendix C.1.5)*
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.1.1 (optional)	Cryptographic Key Generation (for asymmetric keys) *(as defined in Appendix C.3.1 if the TOE provides cryptographic functionality)*
FCS_CKM_EXT.4 (optional)	Cryptographic Key Zeroization *(as defined in Appendix C.3.2 if the TOE provides cryptographic functionality)*
FCS_COP.1(1) (optional)	Cryptographic Operation (for data encryption/decryption) *(as defined in Appendix C.3.3 if the TOE provides cryptographic functionality)*
FCS_COP.1(2) (optional)	Cryptographic Operation (for cryptographic signature) *(as defined in Appendix C.3.4 if the TOE provides cryptographic functionality)*
FCS_COP.1(3) (optional)	Cryptographic Operation (for cryptographic hashing) *(as defined in Appendix C.3.5 if the TOE provides cryptographic functionality)*
FCS_COP.1(4) (optional)	Cryptographic Operation (for keyed-hash message authentication) *(as defined in Appendix C.3.6 if the TOE provides cryptographic functionality)*
FCS_RBG_EXT.1 (optional)	Extended: Cryptographic operation (Random Bit Generation) *(as defined in Appendix C.3.7 if the TOE provides cryptographic*

Functional Component	
	functionality)

FDP_ACC.1
FDP_ACC.1(1)
FDP_ACC.1(2)
	Access Control Policy
	(as defined for specific technology types in Appendix C.1)

FDP_ACF.1
FDP_ACF.1(1)
FDP_ACF.1(2)
	Access Control Functions
	(as defined for specific technology types in Appendix C.1)

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 initialisation
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Roles
FPT_FLS.1 (optional)	Failure with Preservation of Secure State *(optional – defined in Appendix C.2.2)*
FPT_FLS_EXT.1	Failure of Communications
FPT_RPL.1	Replay Detection
FRU_FLT.1	Degraded Fault Tolerance
FTA_SSL_EXT.1 (optional)	TSF-initiated Session Locking and Termination *(optional – defined in Appendix C.2.1)*
FTA_SSL.3 (optional)	TSF-initiated termination *(optional – defined in Appendix C.2.1)*
FTA_SSL.4 (optional)	User-initiated termination *(optional – defined in Appendix C.2.1)*
FTA_TSE.1 (optional)	TOE Session Establishment *(optional – defined in Appendix C.2.1)*

Functional Component	
FTP_ITC.1(1)	Inter-TSF Trusted Channel (Prevention of Disclosure)
FTP_ITC.1(2)	Inter-TSF Trusted Channel (Detection of Modification)

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 should 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. Specific requirements may be excluded based on the specific architecture. For more details regarding potential exclusions, refer to Appendix C.1.

6.1.2 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(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.
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_RBG_EXT.1 (optional)	Failure of the randomization process.	None

Component	**Event**	**Additional Information**
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
FTP_ITC.1(1)	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_ITC.1(2)	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, [***the information in Table 3 and [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

Application Note: *The Standard Protection Profile for ESM Audit*

Management is responsible for storage and processing of audit events generated by the TOE.

The auditing of events on the TOE helps to mitigate a malicious user from masking their actions by ensuring that all events, both successful and unsuccessful, are captured and logged.

Assurance Activity:

The evaluator shall check the administrative guide 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 must be covered, and must 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 administrative and user 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 should then check the audit repository defined by the ST 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 access request is denied by a policy specified in FDP_ACF.1, then audit records will be expected to be generated as a result of testing the policy's effectiveness. 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 an access request is denied by policy, the corresponding audit record should correctly indicate the failure.

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]*; and*

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 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 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 Policy 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 **[assignment: amount of storage] locally 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 completes the assignment with 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 also 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.

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 an external IT entity over a trusted channel defined in FTP_ITC.1.

Dependencies: FAU_GEN.1 Audit data generation

FTP_ITC.1 Inter-TSF trusted channel

Assurance Activity:

The evaluator shall examine the administrative guidance to ensure it instructs the administrator how to establish communication with the audit server. The guidance must instruct how this channel is established in a secure manner (e.g., IPsec, TLS). The evaluator shall test the administrative guidance by establishing a link to the audit server, and confirming that the audit records generated have been transmitted to that server. Note that this will need to be done in order to perform the assurance activities prescribed under FAU_GEN.1.

6.1.3 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.

Application Note: The intent of this requirement is that the TSF be able to provide a receipt to the Policy Management product when a policy is successfully received.

FCO_NRR.2.2 The TSF shall be able to relate the [***software name, version,*** [***assignment: other identifying information***]] of the originator of the information, and the [**stored internal data identifying allowable Policy Management products**] of the information to which the evidence applies.

FCO_NRR.2.3 The TSF shall provide a capability to verify the evidence of receipt of information to [***the Policy Management product***] given ***[assignment: time interval in which the TSF is expected to provide a receipt of policy data to the originating Policy Management product].***

Application Note: The ST author must define the time interval in which the TSF is expected to provide a receipt of policy data to the originating Policy Management product. This should ideally be as close to immediacy as possible.

Dependencies: FIA_UID.1 Timing of identification

Assurance Activity:

The evaluator shall check the development evidence 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.

6.1.4 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 utilize 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 should clearly indicate what cryptographic capabilities are used by the TSF.

Refer to Appendix C.3 for the cryptographic requirements for the TOE.

6.1.5 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, and the four 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.

FDP_ACF.1 Access Control Functions

Refer to Appendix C.1.

Assurance Activity:

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

6.1.6 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 *query the behavior of, modify the behaviour of* the functions***: audited events, repository for remote 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.***

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

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.

Application Note: With respect to the ability to query, this can either 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.

Assurance Activity:

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 must configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator must use the Policy Management product to modify the behavior of the functions specified in the requirement above. For each function, the evaluator must verify that the modification applied appropriately by using the Policy Management product to query the behavior for and after the modification.

The evaluator must 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 remote 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 *query the behaviour 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 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 must configure this environment such that the Policy Management product is authorized to issue commands to the TOE. Once this has been done, the evaluator must 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 [***assignment: access control SFP(s)***] to restrict the ability to [selection: change_default, query, modify, delete, [***assignment: other operations***]] the security attributes [***assignment: list of security attributes***] to [***assignment: the authorised identified roles***].

Application Note: *At minimum, the defined security attributes shall include access control policies, the attributes which comprise them, and whether or not they are enabled.*

Application Note: *The assigned SFP(s) should be derived from the claimed FDP_ACC.1 requirements. See Appendix C for the applicable SFPs based on the TOE's access control technology types.*

Application Note: *It is anticipated that the authorized role will be associated with the external IT entity that is the Policy Definition component.*

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 guidance documentation to confirm that the indicated attributes are maintained by the TOE. The evaluation shall also confirm that the documentation indicates that the ability to perform the indicated operations are restricted to the identified roles (which is anticipated a function provided by components compliant with the ESM Policy Definition PP). The evaluator shall use the associated Policy Definition product to confirm 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 Initialisation

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 **[*assignment: the authorised identified roles***] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes

FMT_SMR.1 Security Roles

Application Note: *It is anticipated that the authorized role will be associated with the external IT entity that is the Policy Definition component.*

Assurance Activity:

1. *The evaluator shall review the TSS and the guidance documentation to confirm that they describe how restrictive default values are put 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) by the TOE. The evaluator shall use the associated Policy Definition product to confirm that for each identified security attribute and restrictive initial state, the TOE implements the correct restrictive value.*

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 remote 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 TOE summary specification in order to determine what Policy Management and Secure Configuration Management product(s) are compatible with the TOE. The evaluator shall deploy the TOE in a configuration with these compatible products and use these products to perform the functions defined in the Security Target and operational guidance. For each advertised management function in the ST and operational guidance, the evaluator shall use the Policy Management product to execute this management function. Then, for each management function, the evaluator shall attempt this behavior and verify that the behavior observed is consistent with the expectations of the management function executed.

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 review the TSS and the guidance documentation to confirm that they describe how management authority is delegated via one or more roles, and how an authorized Policy Definition product is associated with those roles. The evaluator shall use the associated Policy Definition 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. Class FPT: Protection of the TSF

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 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 product that distributes policy to the TOE and also by severing the network connection between the TOE and this product if applicable. The evaluator will 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.

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 administrative guidance and TSS (and developmental evidence, if available) 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 utilize a protocol such as SSL for transmitting data that immunizes it from replay threats.

The evaluator shall test this capability by 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.

6.1.7 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: [***failure 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 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.

6.1.8 Class FTP: Trusted Paths/Channels

FTP_ITC.1(1) Inter-TSF trusted channel (Prevention of Disclosure)

Hierarchical to: No other components.

FTP_ITC.1.1(1) **Refinement:** The TSF shall ***use [assignment: FCS-specified service] 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 disclosure.

Application Note: *The ST author must indicate whether the FCS service is internal to the TSF or provided by the Operational Environment.*

FTP_ITC.1.2(1) **Refinement:** The TSF shall permit ***the TSF or the authorized IT entities*** to initiate communication via the trusted channel.

FTP_ITC.1.3(1) The TSF shall initiate communication via the trusted channel for ***transfer of policy data,*** [***assignment: other functions***].

Application Note: *The ST author should fill out the assignment with all protected communications the TOE has with other ESM products (transfer of audit data, request for identity data, communications to authentication server, etc.).*

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check the administrative guidance in order to determine the mechanism by which secure communications are enabled. If the assurance evidence includes developmental evidence, the evaluator shall also check that evidence to ensure that a discussion is provided on the means by which secure communications are facilitated. Based on this, the following analysis will be required:

- *If cryptography is internal to the TOE, the evaluator shall verify that the product has been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national standard for the nation in which the evaluation is being conducted.*
- *If cryptography is provided by the Operational Environment, the evaluator shall review the design documentation to see how cryptography is utilized and to verify that the functions used have been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national standard for the nation in which the evaluation is being conducted.*

The evaluator shall test this capability by enabling secure communications on the TOE and placing a packet sniffer on the local network. They shall then use the TOE to perform actions that require communications to all trusted IT products with which it *communicates and observe the captured packet traffic that is directed to or from the TOE to ensure that their contents are obfuscated. The evaluator shall also run the packet sniffer during the establishment of these communications in order to verify that the cryptographic negotiation handshake is consistent with the claimed cryptographic algorithm(s) used to protect communications.*

FTP_ITC.1(2) Inter-TSF trusted channel (Detection of Modification)

Hierarchical to: No other components.

FTP_ITC.1.1(2) **Refinement:** The TSF shall ***use* [assignment: *FCS-specified service*] *in providing*** 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 ***detection of the modification of data***.

Application Note: *The ST author must indicate whether the FCS service is internal to the TSF or provided by the Operational Environment.*

FTP_ITC.1.2(2) **Refinement:** The TSF shall permit ***the TSF or the authorized IT entities*** to initiate communication via the trusted channel.

FTP_ITC.1.3(2) The TSF shall initiate communication via the trusted channel for ***transfer of policy data,*** [***assignment: other functions***].

Application Note: *The ST author should fill out the assignment with all protected communications the TOE has with other ESM products (transfer of audit data, request for identity data, communications to authentication server, etc.).*

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check the administrative guidance in order to determine the mechanism by which secure communications are enabled. If the assurance evidence includes developmental evidence, the evaluator shall also check that evidence to ensure that a discussion is provided on the means by which secure communications are facilitated. Based on this, the following analysis will be required:

- *If cryptography is internal to the TOE, the evaluator shall verify that the product has been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national standard for the nation in which the evaluation is being conducted.*
- *If cryptography is provided by the Operational Environment, the evaluator shall review the design documentation to see how cryptography is utilized and to verify that the functions used have been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national standard for the nation in which the evaluation is being conducted.*

The evaluator shall demonstrate that the TOE can detect any modification to the data received from a purportedly authorized IT entity. The desired approach to test this capability is for the evaluator to artificially introduce noise onto the network link between the TOE and a compatible and authorized Policy Management product. The evaluator shall then perform management activities on the Policy Management product to be distributed to the TOE and observe that they do not take effect due to the introduced noise causing modification of data. This observation can be performed either by stopping the noise and using the Policy Management product to query the TOE in order to show that its functions are the same as what they were prior to the attempt to send modified data to it or by performing before/after comparisons of the TOE's functions and observe that they were not changed as a result of receiving modified data from the Policy Management product.

Note: Depending on the technology used and access to interfaces, an alternate approach would be to "generate" (perhaps by a PM product) a proper "message" for the TOE, take that "message" and change one bit, submit the "message" to the TOE through the normal interface, and then observe that the modification is detected either through some action by the TOE or that there is no TOE response to the "message".

6.1.9 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 should 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 should 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 4 were constructed to address threats identified in Section 3. The Security Functional Requirements (SFRs) in Section 6 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, 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 section 6 as well as in this section.

The general model for evaluating TOEs against STs written to conform to this PP is as follows:

After the ST has been approved for evaluation, the Common Criteria Testing Laboratory (CCTL) will obtain the TOE, supporting IT environment, and the administrative guides for the TOE. The Assurance Activities listed in the ST (which will be refined by the CCTL to be TOE-specific, either within the ST or in a separate document) will then be performed by the CCTL. The CCTL is also expected to perform all of the actions mandated by the Common Evaluation Methodology (CEM) for EAL1. The results of these activities will be documented and presented (along with the administrative guidance used) for validation.

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) 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.

The TOE security assurance requirements, summarized in Table 4, identify the management and evaluative activities required to address the threats identified in Section 3 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
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability survey
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage

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.[4] 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 should provide the ST authors with sufficient information to determine the appropriate content for the TSS section.

6.2.1.1 ADV_FSP.1 Basic functional specification

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 are not directly invokable 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 should focus on understanding the

[4] 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.

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 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_OPR and AGD_PRE documentation, coupled with the information provided in the TSS of the ST. 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 Activities:

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 should examine the description of these interfaces and verify that they include a satisfactory description of their invocation.

The evaluator shall also verify that the TOE functional specification describes how the TOE deals with the possibility of acceptance of invalid data. The possibility of invalid data acceptance, if not properly protected, could alter access control decisions to give access to unauthorized users or deny access to authorized users.

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 should 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 to ascertain 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: *Because there is no required management functionality within the TOE for this Protection Profile, the evidence and analysis of AGD_OPE.1 should focus primarily on the management of the TOE’s relationship to other ESM products. Additionally, it is expected that defining the behavior of the TOE (e.g. policy enforcement) is addressed by the evaluation of AGD_OPE for the Policy Management product connected to the TOE. In the event that the TOE does contain management functionality, the evaluation team should use the original intent of the AGD_OPE.1 requirements and perform evaluation activities to ensure that they are being satisfied appropriately.*

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 Activities:

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 Activities:

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 Activities:

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 ASE: Security Target Evaluation

6.2.4.1 Conformance Claims (ASE_CCL.1)

Developer action elements:

ASE_CCL.1.1D The developer shall provide a conformance claim.

ASE_CCL.1.2D The developer shall provide a conformance claim rationale.

Content and presentation elements:

ASE_CCL.1.1C The conformance claim shall contain a CC conformance claim that identifies the version of the CC to which the ST and the TOE claim conformance.

ASE_CCL.1.2C The CC conformance claim shall describe the conformance of the ST to CC Part 2 as either CC Part 2 conformant or CC Part 2 extended.

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the

ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

ASE_CCL.1.4C The CC conformance claim shall be consistent with the extended components definition.

ASE_CCL.1.5C The conformance claim shall identify all PPs and security requirement packages to which the ST claims conformance.

ASE_CCL.1.6C The conformance claim shall describe any conformance of the ST to a package as either package-conformant or package-augmented.

ASE_CCL.1.7C The conformance claim rationale shall demonstrate that the TOE type is consistent with the TOE type in the PPs for which conformance is being claimed.

ASE_CCL.1.8C The conformance claim rationale shall demonstrate that the statement of the security problem definition is consistent with the statement of the security problem definition in the PPs for which conformance is being claimed.

Evaluator action elements:

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

6.2.4.2 Extended Components Definition (ASE_ECD.1)

Developer action elements:

ASE_ECD.1.1D The developer shall provide a statement of security requirements.

ASE_ECD.1.2D The developer shall provide an extended components definition.

Content and presentation elements:

ASE_ECD.1.1C The statement of security requirements shall identify all extended security requirements.

ASE_ECD.1.2C The extended components definition shall define an extended component for each extended security requirement.

ASE_ECD.1.3C The extended components definition shall describe how each extended component is related to the existing CC components, families, and classes.

ASE_ECD.1.4C The extended components definition shall use the existing CC components, families, classes, and methodology as a model for presentation.

ASE_ECD.1.5C The extended components shall consist of measurable and objective elements such that conformance or nonconformance to these elements can be demonstrated.

Evaluator action elements:

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

ASE_ECD.1.2E The evaluator shall confirm that no extended component can be clearly expressed using existing components.

6.2.4.3 ST Introduction (ASE_INT.1)

Developer action elements:

ASE_INT.1.1D The developer shall provide an ST introduction.

Content and presentation elements:

ASE_INT.1.1C The ST introduction shall contain an ST reference, a TOE reference, a TOE overview and a TOE description.

ASE_INT.1.2C The ST reference shall uniquely identify the ST.

ASE_INT.1.3C The TOE reference shall identify the TOE.

ASE_INT.1.4C The TOE overview shall summarize the usage and major security features of the TOE.

ASE_INT.1.5C The TOE overview shall identify the TOE type.

ASE_INT.1.6C The TOE overview shall identify any non-TOE hardware/software/firmware required by the TOE.

ASE_INT.1.7C The TOE description shall describe the physical scope of the TOE.

ASE_INT.1.8C The TOE description shall describe the logical scope of the TOE.

Evaluator action elements:

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

ASE_INT.1.2E The evaluator shall confirm that the TOE reference, the TOE overview, and the TOE description are consistent with each other.

6.2.4.4 Security objectives (ASE_OBJ.2)

Developer action elements:

ASE_OBJ.2.1D The developer shall provide a statement of security objectives.

ASE_OBJ.2.2D The developer shall provide security objectives rationale.

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security objectives for the TOE and the security objectives for the operational environment.

ASE_OBJ.2.2C The security objectives rationale shall trace each security objective for the TOE back to threats countered by that security objective and OSPs enforced by that security objective.

ASE_OBJ.2.3C The security objectives rationale shall trace each security objective for the operational environment back to threats countered by that security objective, OSPs enforced by that security objective, and assumptions upheld by that security objective.

ASE_OBJ.2.4C The security objectives rationale shall demonstrate that the security objectives counter all threats.

ASE_OBJ.2.5C The security objectives rationale shall demonstrate that the security objectives enforce all OSPs.

ASE_OBJ.2.6C The security objectives rationale shall demonstrate that the security objectives for the operational environment uphold all assumptions.

Evaluator action elements:

ASE_OBJ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4.5 Derived security requirements (ASE_REQ.2)

Developer action elements:

ASE_REQ.2.1D The developer shall provide a statement of security requirements.

ASE_REQ.2.2D The developer shall provide a security requirement’s rationale.

Content and presentation elements:

ASE_REQ.2.1C The statement of security requirements shall describe the SFRs and the SARs.

ASE_REQ.2.2C All subjects, objects, operations, security attributes, external entities and other terms that are used in the SFRs and the SARs shall be defined.

ASE_REQ.2.3C The statement of security requirements shall identify all operations on the security requirements.

ASE_REQ.2.4C All operations shall be performed correctly.

ASE_REQ.2.5C Each dependency of the security requirements shall either be satisfied, or the security requirements rationale shall justify the dependency not being satisfied.

ASE_REQ.2.6C The security requirements rationale shall trace each SFR back to the security objectives for the TOE.

ASE_REQ.2.7C The security requirements rationale shall demonstrate that the SFRs meet all security objectives for the TOE.

ASE_REQ.2.8C The security requirements rationale shall explain why the SARs were chosen.

ASE_REQ.2.9C The statement of security requirements shall be internally consistent.

Evaluator action elements:

ASE_REQ.2.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6.2.4.6 Security Problem Definition (ASE_SPD.1)

Developer action elements:

ASE_SPD.1.1D The developer shall provide a security problem definition.

Content and presentation elements:

ASE_SPD.1.1C The security problem definition shall describe the threats.

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

ASE_SPD.1.3C The security problem definition shall describe the OSPs.

ASE_SPD.1.4C The security problem definition shall describe the assumptions about the operational environment of the TOE.

Evaluator action elements:

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

6.2.4.7 TOE Summary Specification (ASE_TSS.1)

Developer action elements:

ASE_TSS.1.1D The developer shall provide a TOE summary specification.

ASE_TSS.1.1C The TOE summary specification shall describe how the TOE meets each SFR.

Evaluator action elements:

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

ASE_TSS.1.2E The evaluator shall confirm that the TOE summary specification is consistent with the TOE overview and the TOE description.

6.2.5 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.

6.2.5.1 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 6.2. 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 Activities:

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 must 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 must 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 must 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 (which 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.

6.2.6 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.

6.2.6.1 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 Activities:

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 do not necessarily have to exist in order to demonstrate PP conformance, **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.AUDIT – The TOE will be able to establish connectivity to other ESM products in order to share security data.	**OE.AUDIT** – The Operational Environment will provide a remote location for storage of audit data.	Requiring the OE to provide a remote location for audit data to be stored allows for FAU_STG_EXT.1 to be satisfied.
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.	Requiring the OE to provide policies to the TOE allows the TOE to function according to its core functionality.
A.USERID – The TOE will receive validated identity data from the Operational Environment.	**OE.USERID** – The Operational Environment must be able to identify the user and convey validation of this to the TOE.	Validating and providing the validated user identity to the TOE is required such that the TOE has information on which user requests access to data for access control functionality.

Assumptions	Objectives	Rationale
A.INSTAL – There will be a competent and trusted administrator who will follow the guidance provided in order to install the TOE.	**OE.INSTAL –** Those responsible for the TOE must ensure that the TOE is delivered and installed in a manner that is consistent with administrative guidance.	Providing one or more administrators to set up the TOE helps satisfy the assumption that it will be installed by a competent individual.
A.TIMESTAMP -- The TOE will receive a reliable timestime from the Operational Environment.	**OE.TIME** -- The Operational Environment must provide a reliable timestamp to the TOE.	Providing a reliable timestamp ensures accurate audit records.

Table 6 — Threats, Objectives, and Rationale

Threats	Objectives	Rationale
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.	**FDP_ACC.1** **FDP_ACF.1** **FPT_FLS.1 (optional)** 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 should be**

Threats	Objectives	Rationale
		mapped to mitigating 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 should be mapped to mitigating this threat.**

Threats	Objectives	Rationale

T.EAVES – A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.	**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(1)**
		FTP_ITC.1(2)
		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 be assured of the authenticity of the other.

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.

Threats	Objectives	Rationale

T.FORGE – A malicious user may create a false policy and send it to the TOE to consume, adversely altering its behavior.	**O.INTEGRITY** – The TOE will contain the ability to verify the integrity of transferred data from Operational Environment components using secure hash algorithms in hashing and keyed message authentication modes.	**FTP_ITC.1(2)**
		FCS_CKM.1.1 (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 requiring the TOE to perform hashing or digital signatures on transmitted data from other ESM products in, the TOE can have reasonable assurance that the transferred data is the data intended to be transferred by the ESM product and has not been intercepted and changed by a third party.

	O.OFLOWS – The TOE will be able to recognize and discard invalid or malicious input requests by users.	**FTP_ITC.1(2)** **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.

Threats	Objectives	Rationale

	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(1)**
		FTP_ITC.1(2)
		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 be assured of the authenticity of the other.

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 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 the TOE's audit generation capabilities function properly, any attempt by a malicious user to mask their actions will fail.
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 policy enforcement if disconnected from Policy Management.	**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 provides assurance that a connectivity issue will not disrupt the TOE's enforcement

Threats	Objectives	Rationale
		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 Management data to the TOE in order to alter its access control policy enforcement behavior.	**O.OFLOWS –** The TOE will be able to recognize and discard invalid or malicious input provided by users.	**FTP_ITC.1(2)** **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.MNGRID – The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.	**FTP_ITC.1(1)** By requiring assured identity of ESM components, an attacker will not be able to provide incorrect Policy Management data to the TOE because their identity as a valid source of policy data will not be able to be verified.
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)** **FDP_ACC.1** **FDP_ACF.1** **FMT_MOF.1(1)** **FMT_MOF.1(2)** **FMT_MSA.1**

Threats	Objectives	Rationale
		FMT_MSA.3 **FMT_SMF.1** **FMT_SMR.1** **FTA_SSL_EXT.1 (optional)** **FTA_SSL.3 (optional)** **FTA_SSL.4 (optional)** **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 the policy is being enforced, the TOE requires the ability for the policy to be queried.
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.

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 — TOE Assumptions

Assumption Name	Assumption Definition
A.AUDIT	A protected repository will exist in the Operational Environment to which audit data can be written.
A.POLICY	The TOE will receive policy data from the Operational Environment.
A.USERID	The TOE will receive validated identity data from the Operational Environment.
A.TIMESTAMP	The TOE will receive a reliable timestime from the Operational Environment.

8.1.2 Physical Assumptions

No physical assumptions are prescribed in this Protection Profile because the architecture of the TOE can vary. The ST author should add assumptions that are consistent with the expected usage of the TOE.

8.1.3 Personnel Assumptions

Table 8 — TOE Assumptions

Assumption Name	Assumption Definition
A.INSTAL	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 Management 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

TOE Security Obj.	TOE Security Objective Definition
O.MONITOR	The TOE will monitor the behavior of itself for anomalous activity (e.g., provide measures for generating security relevant events that will detect access attempts to TOE-protected resources by users).
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 using secure hash algorithms in hashing and keyed message authentication modes.
O.RESILIENT	If the TOE mediates actions performed by a user against resources on an 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.MAINTAIN	The TOE will be capable of maintaining policy enforcement if disconnected from the Policy Management product.
O.OFLOWS	The TOE will be able to recognize and discard invalid or malicious input provided by users.
O.SELFID	The TOE will be able to confirm its identity to the Policy Management product while sending receipt of a new policy arrival.
O.MNGRID	The TOE will be able to identify and authorize a Policy Management product prior to accepting policy data from it.

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

TOE Security Obj.	TOE Security Objective Definition

TOE Security Obj.	TOE Security Objective Definition
OE.AUDIT	The Operational Environment will provide a remote location for storage of audit data.
OE.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
OE.POLICY	The Operational Environment will provide a policy that the TOE will enforce.
OE.PROTECT	The Operational Environment will protect the TOE from unauthorized modifications and access to its functions and data.
OE.USERID	The Operational Environment must be able to identify the user and convey validation of this to the TOE.
OE.TIME	The Operational Environment must provide a reliable timestamp to the TOE.

Appendix A - Supporting Tables and References

A.1 References

[1] Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Policy Management, version 1.0, forthcoming

[2] Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Authentication Server, version 1.0, forthcoming

[3] Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Secure Configuration Management, version 1.0, forthcoming

[4] Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Audit Management, version 1.0, forthcoming

[5] Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Authentication Server, version 1.0, forthcoming

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

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

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

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

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

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

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

[13] 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

[14] 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

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

[16] 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

[17] 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.

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

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

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

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

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

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

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

[25] National Institute of Standards and Technology, The RSA Validation System

(RSAVS), November 2004

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

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

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

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

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

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

[32] 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

A.2 Acronyms

Table 13 — Acronyms and Definitions

Acronym	Definition
ABAC	Attribute-Based Access Control
CC	Common Criteria
CM	Configuration Management
COI	Communities of Interest
DAC	Discretionary Access Control
ESM	Enterprise Security Management
IT	Information Technology

Acronym	Definition
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
SAC	System Access Control
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SQL	Structured Query Language
ST	Security Target
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 functional and assurance requirements defined as part of this PP and the NIST 800-53 security controls that apply to them. The mappings for the functional and assurance requirements that were defined in CC Part 2 and CC Part 3 have been derived from 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

CC SFR/SAR		NIST 800-53 Control		Comments and Observations
Common Criteria Version 3.x Security Functional Requirements (SFRs) and PP extended SFRs				
ESM_DSC.1	**Object Inventory** Object Inventory	AU-13	**Monitoring for Information Disclosure** | detection of unauthorized exfiltration	**Full.** This control appears to be fully satisfied by the SFR.
		AC-4	**Access Enforcement** | enforcement of approved authorizations	**Partial**. This control can be used to help maintain access enforcement by detecting when objects are a not in an approved state.
FAU_GEN.1	**Security Audit Data Generation** Audit Data Generation	AU-2	**Auditable Events** | [auditable events], rationale, and coordination	**Partial**. FAU_GEN.1.1 gives the definition of what events should be audited (addressing the bulk of this control), but the assignments need to be compared to see if the sets are equivalent. Note also that FAU_GEN implies both auditable and

CC SFR/SAR		NIST 800-53 Control		Comments and Observations
				audited, which is two distinct controls under 800-53.
		AU-12	**Audit Generation** | Generate and pre-select on [components]	**Partial.** The generation aspect of FAU_GEN provides the generation aspect of AU-12.
		AC-17(1)	**Remote Access** | Automated monitoring/control	**Partial.** If the assignment in FAU_GEN.1 includes auditing of remote access, then this control is partially met (the monitoring aspect).
		AU-3	**Content of Audit Records** | Minimal audit record information	**Partial**. FAU_GEN.1.2 details the list of what must be contained in each audit record. The assignment must be compared to the controls to see if AU-3/AU-3(1) are satisfied.
		AU-3(1)	**Content of Audit Records** | Additional detailed information: [list]	**Partial**. FAU_GEN.1.2 details the list of what must be contained in each audit record. The assignment must be compared to the controls to see if AU-3/AU-3(1) are satisfied.
		Note: The SFR bases the auditable events on the other SFRs included in the Security Target, as well as the desired level of information (minimal, basic, etc.). NIST has no predefined set, although CNSS does provide a definition for NSS. There is no mandated correlation between the SFR and NIST assignments.		
FAU_SEL.1	**Security Audit Event Selection** Selective Audit	AU-12	**Audit Generation** | Generate and pre-select on [components]	**Partial**. FAU_SEL.1 goes to item b of the AU-12 control. The FAU_SEL.1 SFR is much more flexible in terms of what is required for selection than the AU-12 control.
FAU_STG.1	**Protected Audit Trail Storage (Local Storage)**	AU-9	**Protection of Audit Information** | Protect information/tools from unauthorized access	**Partial.** The SFR addresses the basic intent of the control, although FAU_STG.1.2 needs to be completed with

CC SFR/SAR		NIST 800-53 Control		Comments and Observations
				"prevent". However, the control not only protects the trail, but audit tools (which are not covered by the SFR).
FAU_STG_EXT.1	**Security Audit Event Storage** **Remote Audit Trail Storage**	AU-9	**Protection of Audit Information** | Protect information/tools from unauthorized access	**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).
FCO_NRR.2	**Non-Repudiation of Receipt** **Enforced Proof of Receipt**	AU-10	**Non-Repudiation** | Protect against repudiation	**Partial.** This SFR talks about non-repudiation of receipt for a particular action; non-repudiation of receipt is one of the actions mentioned in the control. The phrase "a particular action" is vague enough to correspond with the assignments in the SFR.
		AU-10(1)	**Non-Repudiation** | Associate identity of information producer with the information	**Partial.** For proof of receipt, this appears to correspond to FCO_NRR.2.2.
		AU-10(2)	**Non-Repudiation** | Validate identity and information binding	**Partial.** For proof of receipt, this appears to correspond to FCO_NRR.2.3.
FCS_CKM.1	**Cryptographic Key Management** Cryptographic Key Generation	SC-12	**Cryptographic Key Establishment and Management |** Organization establishes/manages cryptographic keys	**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		

CC SFR/SAR		NIST 800-53 Control		Comments and Observations
		the various aspects of key management (generation, distribution, access, and destruction).		
FCS_CKM_EXT.4	**Cryptographic Key Management** Cryptographic Key Destruction	SC-12	**Cryptographic Key Establishment and Management** | Organization establishes/manages cryptographic keys	**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_COP.1	**Cryptographic Operation** Cryptographic Operation	SC-13	**Use of Cryptography** | Cryptographic implementation via modules that meet regulations	**Partial.** The extent to which the SFR meets the control depends on how the assignments have been completed.
		Note: The SFR is very broad, and may be completed to cover all sorts of cryptographic operations, many of which are not covered in the NIST 800-53 SFRs. Examples of areas *not* covered in NIST include standards for secure cryptographic hashes and when they must be used and standards for the quality of random number generators used.		
FCS_RBG_EXT.1	**Random Bit Generation** Random Bit Generation			**No Mapping.** There appears to be no control corresponding to this. The SFR defines the expected characteristics of random number generation.
FDP_ACC.1	**Access Control Policy** Subset Access Control	AC-3	**Access Enforcement** | System enforces authorizations	**Partial.** Access controls implies specification of the objects controlled by the policy, but NIST makes no distinction between subset and complete access controls.
		AC-3(3)	**Access Enforcement** | Non-discretionary access control	**Partial.** Appropriate assignments would be required to specify the covered operations on objects for roles.
		AC-3(4)	**Access Enforcement** | Discretionary access control	**Partial.** Appropriate assignments would be required to specify the covered

CC SFR/SAR		NIST 800-53 Control		Comments and Observations
				operations on named objects for subjects.
		SC-7	**Boundary Protection** | System monitors and controls communications at boundaries	**Partial**. If the TOE performs Data Loss Prevention access control, it is capable of controlling communications that pertain to the exfiltration of data. If the TOE performs Web access control, it is capable of controlling communications that involve internal or external web servers.
		Note: The CC takes a different approach on access control, with the FDP_ACC family defining the subjects, objects, and attributes of interest, and the FDP_ACF family defining the access control rules that define how subjects may access objects based on those attributes.		
FDP_ACF.1	**Access Control Functions** Security Attribute Based Access Control	AC-3	**Access Enforcement** | System enforces authorizations	**Partial.** This captures the general notion of access enforcement, but is unspecified in terms of any policy. The supplemental guidance makes clear this could be used for MAC as well as DAC, so this could be met by either FDP_ACF or FDP_IFF.
		AC-3(3)	**Access Enforcement** | Non-discretionary access control	**Partial.** If FDP_ACF is used to specify an RBAC policy, that would be an appropriate assignment under AC-3(3).
		AC-3(4)	**Access Enforcement** | Discretionary access control	**Partial.** If FDP_ACF is used to specify a traditional DAC policy, that would be an appropriate assignment under AC-3(4).
		SC-7	**Boundary Protection** | System monitors and controls communications at boundaries	**Partial**. If the TOE performs Data Loss Prevention access control, it is capable of

CC SFR/SAR		NIST 800-53 Control		Comments and Observations
				controlling communications that pertain to the exfiltration of data. If the TOE performs Web access control, it is capable of controlling communications that involve internal or external web servers.
		Note: The CC takes a different approach on access control, with the FDP_ACC family defining the subjects, objects, and attributes of interest, and the FDP_ACF family defining the access control rules that define how subjects may access objects based on those attributes. **Note:** The general flexibility of FDP_ACF permits a wide variety of information flow policies to be specified. In reality, many of the policies in AC-3 could be written using FDP_ACF, so one would need to look at the assignment closely.		
FMT_MOF.1	**Management of Functions in TSF** Management of Security Functions Behavior	AC-3(3)	**Access Enforcement** | Non-discretionary access control	**Partial.** Restriction of management functions to particular roles is at least a partial implementation of RBAC.
FMT_MSA.1	**Management of Security Attributes** Management of Security Attributes	SI-9	**Information Input Restrictions** | Restricts ability to input information to authorized persons	**Partial.** The SFR would seem to imply this control, although the SFR is much more specific.
FMT_MSA.3	**Management of Security Attributes** Static Attribute Initialization			**No Mapping.** There appears to be no control corresponding to this SFR. The SFR requires the TOE to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the security policy, as well as allowing the [assignment: the authorised identified roles] to specify alternative initial values to override the default values when an object or information is created.
FMT_SMF.1	**Specification of**			**No Mapping.** This

CC SFR/SAR		NIST 800-53 Control		Comments and Observations
	Management Functions Specification of Management Functions	▨	▨	SFR is an open ended SFR to specify management functions not captured elsewhere. It could correspond to almost any control, depending on assignment.
FMT_SMR.1	**Security Management Roles** Security Roles	AC-2(7)	**Account Management** | Role-based schemes	**Partial.** The SFR is on the information system, and the control is on the organization, yet this seems to be saying that all users are assigned a role, which fits with FMT_SMR.
		AC-5	**Separation of Duties** | Organizational level	**Partial.** Arguably, if a system provides distinct roles, that supports the provision of separation of duties and the application of the principle of least privilege.
		AC-6	**Least Privilege** | Employs concept of Least Privilege	**Partial.** Arguably, if a system provides distinct roles, that supports the provision of separation of duties and the application of the principle of least privilege.
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** | Fails to [known state] preserving [information]	**Partial.** The SFR requires failure to a known secure

CC SFR/SAR		NIST 800-53 Control		Comments and Observations
				state. That appears to fit with SC-24.
FPT_FLS.1	**Fail Secure** Failure with Preservation of Secure State	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** | Fails to [known state] preserving [information]	**Partial.** The SFR requires failure to a known secure state. That appears to fit with SC-24.
FPT_RPL.1	**Replay Detection** Replay Detection	SC-23	**Session Authenticity** | Mechanisms to protect authenticity of communication sessions	**Partial.** Depending on the assignment, the replay detection mechanisms may provide session authenticity and address man-in-the-middle attacks.
FRU_FLT.1	**Fault Tolerance** Degraded Fault Tolerance			**No Mapping.** This SFR requires that the TSF ensure the operation correct policy enforcement upon resumption of communications. Although there are a few cases where NIST 800-53 controls address continuation in the case of specific failures (which are actually covered by other SFRs, such as audit failures), there's no general fault tolerance requirement.

CC SFR/SAR		NIST 800-53 Control		Comments and Observations
FTA_SSL_EXT.1	**Session Locking and Termination** TSF-Initiated Session Locking	AC-11	**Session Lock** | Timeout Lock until Re-identified and Authenticated	**Partial.** FTA_SSL.1.1 provides the system-initiated session lock. FTA_SSL.1.2, with the proper assignment, addresses the actions required to unlock.
		AC-11(1)	**Session Lock** | With screen saver	**Full.** FTA_SSL.1.1 provides the system-initiated clearing or overwriting of the screen.
		Note: FTA_SSL.1, by itself, does not meet AC-11 as it does not require the ability for user-initiated locking. Both FTA_SSL.1 and FTA_SSL.2 are required to meet AC-11.		
FTA_SSL.2	**Session Locking and Termination** User-Initiated Locking	AC-11	**Session Lock** | Timeout Lock until Re-identified and Authenticated	**Partial.** FTA_SSL.2.1 provides the user-initiated session lock. FTA_SSL.2.2, with the proper assignment, addresses the actions required to unlock.
		AC-11(1)	**Session Lock** | With screen saver	**Full.** FTA_SSL.2.1 provides the user-initiated clearing or overwriting of the screen.
		Note: FTA_SSL.2, by itself, does not meet AC-11 as it does not require the ability for user-initiated locking. Both FTA_SSL.1 and FTA_SSL.2 are required to meet AC-11.		
FTA_SSL.3	**Session Locking and Termination** TSF-Initiated Termination	SC-10	**Network Disconnect** | Terminate network connections at session end or [time]	**Full.** Note that the former AC-10 was incorporated into SC-10, making clear that this refers not only to network termination but session termination.
FTA_SSL.4	**Session Locking and Termination** User-Initiated Termination	SC-23(2)	**Session Authenticity** | Provide a readily observable session logout capability	**Full.** The SFR would imply that there be a logout capability for web sessions.
		Note: There appears to be no control mandating that there be a user-visible logout capability for non-web sessions.		
FTA_TSE.1	**TOE Session Establishment** TOE Session Establishment	▨	▨	**No Mapping.** This SFR requires that the TOE be able to deny session

CC SFR/SAR		NIST 800-53 Control		Comments and Observations
				establishment based on [assignment: attributes]. This is too broad to map to a NIST control.
FTP_ITC.1	**Inter-TSF Trusted Channel** Inter-TSF Trusted Channel	IA-3(1)	**Device Identification and Authentication |** Before remote/wireless connection with bidirectional cryptography-based authentication	**Partial.** The SFR discusses provision of a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. This control provides the identification of the end-points.
FTP_TRP.1	**Trusted Path** Trusted Path	SC-11	**Trusted Path** | Trusted path between users and [functions]	**Partial.** Whether the SFR provides the control depends on the assignments.
Common Criteria Version 3.x Security Target Assurance Requirements				
ASE_INT.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**ST Introduction** ST Introduction			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_CCL.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Conformance Claims** Conformance Claims			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_SPD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Problem Definition** Security Problem Definition			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of

CC SFR/SAR		NIST 800-53 Control		Comments and Observations
				the product to be evaluated.
ASE_OBJ.1 EAL1	**Security Objectives** Security Objectives for the Operational Environment			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_OBJ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Objectives** Security Objectives			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_ECD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Extended Components Definition** Extended Components Definition			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_REQ.1 EAL1	**Security Requirements** Stated Security Requirements			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_REQ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Requirements** Derived Security Requirements			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_SPD.1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Problem Definition** Security Problem Definition			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and

CC SFR/SAR		NIST 800-53 Control		Comments and Observations
		▨	▨	assurance requirements of the product to be evaluated.
ASE_TSS.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**TOE Summary Specification** TOE Summary Specification	SA-4(1)	**Acquisitions** | Acquisition documents describe functional properties of security controls to support analysis/test	**Partial.** The TSS in the ST describes *how* the product implements the security functional requirements, and provides the high-level basis for all subsequent analysis and testing.
		SA-5(1)	**Information System Documentation** | Organization obtains vendor documentation on security-relevant functional properties	**Partial.** The TSS in the ST describes security-relevant functional properties for the security behaviors claimed in the ST.
Common Criteria Version 3.x Security Assurance Requirements				
ADV_FSP.1 EAL1	**Functional Specification** Basic Functional Specification	SA-4(2)	**Acquisitions** | Acquisition documents describe design/implementation of security controls to support analysis/test	**Partial.** The ADV_FSP family provides information about functional interfaces.
		SA-5(2)	**Information System Documentation** | Documents describe security-relevant external interfaces to support analysis/test	**Partial.** The ADV_FSP family provides information about functional interfaces.
AGD_OPE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Operational User Guidance** Operational User Guidance	SA-5	**Information System Documentation** | SFUG + TFM	**Full.** AGD_OPE is the combined requirement for administrator and user documentation.
		Note: NIST 800-53 parallels the CC v2 approach, which distinguished administrator and user documentation (AGD_USR, AGD_ADM). CC v3 combined these into a single SAR, reflecting the situation that some products do not have non-administrative users.		
AGD_PRE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Preparative Procedures** Preparative Procedures	SA-5	**Information System Documentation** | SFUG + TFM	**Full.** The SFR calls for describing all the steps necessary for secure acceptance and secure delivery. The control calls for documentation or secure configuration and installation.
Note: A general observation regarding the differences between CM under 800-53 and CM under the Common Criteria. The Common Criteria's CM refers to the CM of the development of the product, not its fielding in a system.				

CC SFR/SAR			NIST 800-53 Control		Comments and Observations
NIST 800-53 focuses on controlling the configuration of the fielded system, and focuses less on developer CM.					
	ALC_CMC.1 EAL1	CM Capabilities Labeling of the TOE	CM-9	**Configuration Management Plan** | Has CM plan with necessary information	**Partial.** This addresses defining the configuration items. Note that ALC_CMC is focused on the *product*, whereas CM-9 is focused on the *system.*
			SA-10	**Developer Configuration Management** | Developer has configuration management during development; flaw tracking	**Partial.** ALC_CMC captures some of the developer aspects of the CM process.
	ALC_CMS.1 EAL1	CM Scope TOE CM Coverage	CM-9	**Configuration Management Plan** | Has CM plan with necessary information	**Partial.** This addresses defining the configuration items and the method of identification of configuration items. Note that ALC_CMC is focused on the *product*, whereas CM-9 is focused on the *system.*
			SA-10	**Developer Configuration Management** | Developer has configuration management during development; flaw tracking	**Partial.** ALC_CMS captures some of the developer aspects of the CM process.
ATE_IND.1 EAL1		Independent Testing Independent Testing – Conformance	CA-2	**Security Assessments** | Develop plan, assess, produce report	**Partial.** This control addresses the aspect of development of an independent test plan for security functions, and the assessment of those functions.
			CA-2(1)	**Security Assessments** | … with independent assessor	**Partial**. This addresses the fact that assessment is done by the CCTL, not the vendor.
			SA-11(3)	**Developer Security Testing** | Implement ST&E under independent validation and verification	**Partial.** ATE_IND requires independent testing by the validators, including rerunning of all or a portion of the test suite.
			Note: There is a key difference between ATE_IND and SA-		

CC SFR/SAR		NIST 800-53 Control		Comments and Observations
		11(3). ATE_IND requires the independent evaluators to run the tests. SA-11(3) has the developers running the tests under the oversight of the independent evaluators. There are key differences in this approach, primarily in assessing the actual quality of the test procedures and the repeatability. **Note:** ATE_IND.1 only has independent oversight for a portion of the test suite.		
AVA_VAN.1 EAL1	Vulnerability Analysis Vulnerability Survey	CA-2(2)	**Security Assessments** | [announced/unannounced] security testing (e.g., penetration testing)	**Partial.** This addresses the requirement to conduct penetration testing.
		RA-3	**Risk Assessment** | Conduct/document/review risk assessments	**Partial**. Conceivably, part of a risk assessment is doing a survey of vulnerabilities. Note that the CC does not imply formal vulnerability scanning, which is RA-5.
		SA-11(2)	**Developer Security Testing** | Developer vulnerability analysis	**Partial.** AVA_VAN requires that there be a vulnerability analysis performed.
		Note: The different AVA_VAN components differ on the depth and extent of the vulnerability analysis. NIST SP 800-53 Revision 3 appears to have no controls that dictate the quality of the vulnerability assessment.		

Appendix C - Architectural Variations and Additional Requirements

C.1 Architectural Variations

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 utilize 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.

Application Note: 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 should clearly indicate the correspondence between these tables and the elements discussed in Table 15.

Application Note: Controlling the ability to utilize the authentication function requires the ST author to additionally claim FTA_TSE.1. Refer to Appendix C.2.1.

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 15below 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: [***rules received from an authorized and compatible Policy Management product***].
FDP_ACF.1.3(1)	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [***assignment: other additional rules***]
Application Note:	*The ST author should 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: [***none***].
Application Note:	*The ST author must specify the specific objects protected by the explicit denial process. This explicit denial process should be implemented independent of any policy consumed by the TSF.*

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

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

Table 15 — FDP Requirement Table for Host-Based Access Control

Assurance Activity:

The evaluator shall check the ST and operational guidance in order to verify that the TOE is capable of mediating the activities that are defined in Table 15 above.

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 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, 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.

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 may include, but is 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.

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 authorise 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 development documentation 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, or configuration files. The evaluator shall verify the self-protection mechanisms are sufficient 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 SFR - 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). This should include, where applicable:
   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 utilize 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 should 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 should 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 16 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 authorise access of subjects to objects based on the following additional rules: [***assignment: additional rules***]

Application Note: The intent here is to support 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: [

- ***if a requested object is not explicitly allowed by policy, then the access to the requested object is denied by default***

].

Application Note: *The ST author should consider incorporating the requirements FTA_TSE.1, and FTA_SSL found in Appendix C. The ST author may wish to iterate the FTA_TSE.1 requirement if the TOE provides the capability to control when/how sessions can be established for administrators versus web server session establishment for non-administrative users. The FTA_SSL requirements should be used if the TOE provides the capability to lock, or terminate sessions.*

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

Subject	Object	Operation
User	URLs	Access via HTTP operation
	Files	Open | Download
	Executable Scripts	Execute
		Enable | Disable
	Forms	HTTP GET | HTTP POST

Table 16 — FDP Requirement Table for Web-Based Access Control

Assurance Activity:

The evaluator shall check the ST and operational guidance in order to verify that the TOE is capable of mediating the activities that are defined in Table 16 above.

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 one user to visit a certain URL and another that forbids a different user from visiting the same URL. Once this policy is implemented, the evaluator will access a system as each of these users and observe that the ability to visit the specified URL is appropriately allowed or denied. 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.

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.*

Application Note: *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 17 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 will be forbidden from leaving the system unless the intended destination is an explicitly trusted location; and***
- ***Mechanisms of leaving the system will 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 authorise 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: [***none*]**.

Dependencies: FDP_ACC.1 Subset access control

FMT_MSA.3 Static attribute initialization

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)

Table 17 — FDP Requirement Table for Data Loss Prevention Access Control

Assurance Activity:

The evaluator shall check the ST and operational guidance in order to verify that the TOE is capable of mediating the activities that are defined in Table 17above.

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.

C.1.5 Optional Data Loss Prevention SFR: Content Discovery

Object Inventory

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 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 should relate to corrective action taken against the* *discovered object.*

Application Note: *If this SFR is included, the audit events should be adjusted to include audit of objects containing discovered content and the action that was taken.*

Dependencies: No dependencies

Assurance Activity:

Note: The assurance activity for this SFR is still under development. Users of this production profile should document the process and procedures they use to verify this SFR, and provide a copy of those process and procedures to CCEVS as input to the generalized assurance activity that will be included in the next version of this PP.

C.2 Additional Optional SFRs

C.2.1 Optional SFRs for Session Management

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***]].

Dependencies: No dependencies

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.*

Application Note: *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.*

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 also perform the following test for each attribute:

- *Test 1: The evaluator successfully establishes a session to the TOE. The evaluator then follows the operational guidance to configure the TOE so that that access is denied based on a specific value of the attribute. The evaluator shall then attempt to establish a session in contravention to the attribute setting (for instance, the location is denied based upon the time of day). The evaluator shall observe that the session establishment attempt fails.*

TSF-initiated Session Locking and Termination (FTA_SSL)

Hierarchical to: No other components

FTA_SSL_EXT.1 TSF-initiated session locking

FTA_SSL_EXT.1.1 The TSF shall, for local interactive sessions, [selection:

- o <u>lock the session – clear or overwrite display devices, making the current contents unreadable, disable any activity of the user's data access/display devices other than unlocking the session, and require that the user re-authenticate to the TSF prior to unlocking the session;</u>

- terminate the session

] after an Authorized Administrator specified time period of inactivity.

Dependencies: No dependencies

Assurance Activity:

The evaluator shall perform the following test:

- *Test 1: The evaluator follows the operational guidance to configure several different values for the inactivity time period referenced in the component. For each period configured, the evaluator establishes a local interactive session with the TOE. The evaluator then observes that the session is either locked or terminated after the configured time period. If locking was selected from the component, the evaluator then ensures that re-authentication is needed when trying to unlock the session.*

FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components

FTA_SSL.3.1 The TSF shall terminate a remote interactive session after an Authorized Administrator-configurable time interval of session inactivity.

Dependencies: No dependencies

Assurance Activity:

The evaluator shall perform the following test:

- *Test 1: The evaluator follows the operational guidance to configure several different values for the inactivity time period referenced in the component; these shall consist at least of the minimum and maximum allowed values as specified in the operational guidance, as well as one other value. For each period configured, the evaluator establishes a remote interactive session with the TOE. The evaluator then observes that the session is terminated after the configured time period.*

FTA_SSL.4 User-initiated termination

Hierarchical to: No other components

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

Dependencies: No dependencies

Assurance Activity:

The evaluator shall perform the following tests:

- *Test 1: The evaluator initiates an interactive local session with the TOE. The evaluator then follows the operational guidance to exit or log off the session and observes that the session has been terminated.*
- *Test 2: The evaluator initiates an interactive remote session with the TOE. The evaluator then follows the operational guidance to exit or log off the session and observes that the session has been terminated.*

C.2.2 Optional SFR for Ensuring Continued Access Enforcement

Failure with Preservation of Secure State

Hierarchical to: No other components

FPT_FLS.1 The TSF shall [refinement: ***perform the following actions: [selection: one or more of log an event, restart the component, send an alarm to an administrator]***] when the following types of failures occur: [***assignment: list of TOE components and possible malfunctioning states***].

Application Note: 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.

Application Note: *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:

Note: The assurance activity for this SFR is still under development. Users of this production profile should document the process and procedures they use to verify this SFR, and provide a copy of those process and procedures to CCEVS as input to the generalized assurance activity that will be included in the next version of this PP.

C.3 Internal 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 evaluation team 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 evaluation team must devise and perform tests to test the functionality referred to within these requirements.

These requirements should 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 shall be used by the ST author.

C.3.1 FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys)

Hierarchical to: No other components

FCS_CKM.1.1 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**.

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 should 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 to 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 implements 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.3.2 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) must 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.3.3 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*** [<u>selection: 192 bits, no other key sizes</u>] that meets the following:

- ***FIPS PUB 197, “Advanced Encryption Standard (AES)”***
- [<u>selection: NIST SP 800-38A, NIST SP 800-38B, NIST SP 800-38C, NIST SP 800-38D, NIST SP</u>

800-38E]

Application Note: *For the assignment, the ST author should choose the mode or modes in which the AES operates. For the first selection, the ST author should choose the key sizes that are supported by this functionality. For the second selection, the ST author should 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.3.4 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.*

Application Note: *The ST Author should choose the algorithm implemented to perform digital signatures; if more than one algorithm is available, this requirement (and the corresponding FCS_CKM.1 requirement) should be iterated to specify the functionality. For the algorithm chosen, the ST author should 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.3.5 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.*

Application Note: *The selection of the hashing algorithm must 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.3.6 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.

Application Note: 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 should 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.3.7 FCS_RBG_EXT.1 Extended: 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: 128 bits, 256 bits] of entropy at least equal to the greatest bit length of the keys and authorization factors 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 should 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.

In the future, most of the requirements described in A

Method for Entropy Source Testing: Requirements and Test Suite Description will be required by this PP. The follow Assurance Activities currently reflect only that subset of activities that are required.

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 confirm that the TSS describes the noise source from which entropy is gathered, and further confirm the location of this noise source. The evaluator will further verify that all of the underlying functions and parameters used in the RBG are listed in the TSS.

The evaluator shall verify that the TSS contains a description of the RBG model, including the method for obtaining entropy input, as well as identifying the entropy source(s) used, how much entropy is produced by each entropy source. The evaluator shall also ensure that the TSS describes known modes of entropy source failure. Finally, the evaluator shall ensure that the TSS contains a description of the RBG outputs in terms of the independence of the output and variance with time and/or environmental conditions.Regardless of the standard to which the RBG is claiming conformance, the evaluator perform 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.*

The evaluator shall also perform the following tests, depending on the standard to which the RBG conforms.

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.*

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*
- **Selection:** allows the specification of one or more elements from a list. Indicated with <u>underlined text</u> inside square brackets that contain the prompt "selection:"<u>.</u>
- **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, ***bold and italicized text*** indicates where an assignment operation has already been completed in order to ensure these requirements apply to the PP.

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 will be indicated with the "EXT" inserted within the component.

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 18 — 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	The collection of hardware and software resources in an enterprise that are not within the

Term	Definition
Environment	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.
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 - PP Identification

F.1 Identification

Title: Standard Protection Profile for Enterprise Security Management Access Control

Author: Booz Allen Hamilton, on behalf of and with approval from the ESM Protection Profile vendor community

Common Criteria Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1, July 2009

Version: PP Version 2.0

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.