Standard Protection Profile for Enterprise Security Management Identity and Credential Management

October 24, 2013

Version 2.1

Document History

Version	Date	Comment
1.0	July 13, 2011	First complete version
1.1	May 22, 2012	Update to bring in line with ESM Access Control and Policy Management PPs.
1.2	July 9, 2012 – August 8, 2012	Updated to address comments received on v1.1, as well as comments from CA, Tom Benkhart, and the ESM Telecon
1.3	August 8, 2012 – August 10, 2012	Detailed changes from ESM Telecon. Resolution of final issue regarding credential update
1.4	August 31, 2012	Final version – all changes accepted
1.5	June 13, 2013	Changes made based on consistency with ESM Authentication Server PP scope and formatting, ESM Technical Community feedback, and CCEVS input on cryptography.
2.1	October 24, 2013	Version updated to 2.1 to be consistent with Access Control Protection Profile

Table of Contents

List of Figures

List of Tables

1 Protection Profile (PP) Introduction

1.1 Introduction

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

1.2 ESM Protection Profile Suite Overview

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

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

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

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

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

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

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

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

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

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

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

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

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

examples:

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

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

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

Table 1. Summary of the ESM Protection Profile Suite

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

Notes:

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

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

1.3 Overview of the ESM Identity and Credential Management Protection Profile

This protection profile focuses on **the aspect of ESM that is responsible for enforcing identity and credential management**. Identity and Credential Management products will generate and issue credentials for subjects that reside within the enterprise. They will also maintain the organizational attributes that are associated with these subjects. By providing a means for subjects to validate their identities and determining the relationship these subjects have to the enterprise, an Identity and Credential Management product is able to support enterprise accountability and access control.

The establishment of unique, unambiguous identities is an important foundational capability that enables issuance and management of credentials and authorization attributes. The notion of identity refers to that unique identifier assigned to an individual against which credential and attribute data can be associated.

In order for an individual to be identified as a user within the ESM system, they must be enrolled. Enrollment refers to the act of assigning a unique identifier to a subject, generating and issuing credentials, defining attributes for a user, and propagating that data to any repositories that use it. It is necessary for the TSF to be able to securely transmit this data to those components.

TOEs compliant with this PP are expected to exhibit the following behavior:

- Provisioning of subjects (enroll new subjects to an organizational repository, associate and disassociate subjects with organizationally-defined attributes)
- Issue and maintain credentials associated with user identities
- Publish and change credential status (such as active, suspended, or terminated)
- Establish appropriate trusted channels between itself and compatible Policy Management and Authentication Server ESM products
- Generate an audit trail of configuration changes and subject identification and authentication activities
- Write audit trail data to a trusted repository
- Securely transmit identity and credential attribute data via a trusted channel

While this PP defines the capabilities of the TOE as if they belong to a standalone product, some or all of these capabilities may belong to an ESM Policy Management (PM) product as well. If an ST is written that claims conformance to this PP, the distribution of these capabilities must be clearly delineated.

Note that this is one of many Protection Profiles in the ESM PP family. This PP is meant to be used for one component in an ESM system and not to work in isolation. At minimum, at least one compatible Authentication Server product must be identified. Compatibility is defined by the ability of that product to authenticate identities and credentials that are defined by the TOE. Depending on how access control is implemented in the organization, ESM PP solutions for policy management, access control, and auditing may need to be implemented as well. If any of these components are expected to be deployed against an organizational baseline, a secure configuration management solution may also need to be deployed. A customer could seriously compromise the overall security of the enterprise architecture if they are to deploy a solution without using all applicable ESM PP evaluated products.

Figure 1 illustrates, at a basic level, the context in which the TOE is expected to be deployed. The TOE resides on a system and provides an interface to one or more repositories of subject data. One or more Assignment Managers will be given the authority to use the TOE to manipulate this data as needed. Subject data is used by other ESM components as necessary to carry out their duties. For example, a Policy Administrator may desire to write a policy that authorizes members of a certain department access to a specific web application. In order to do this, the Policy Management product must be capable of retrieving either the attribute that designates membership in this department or a list of subjects who belong to it. This will be done by accessing data from the relevant repositories.

Audit data can also be written to a trusted repository where it can be aggregated with other data streams by a product that is compliant with the Standard Protection Profile for ESM Audit Server.

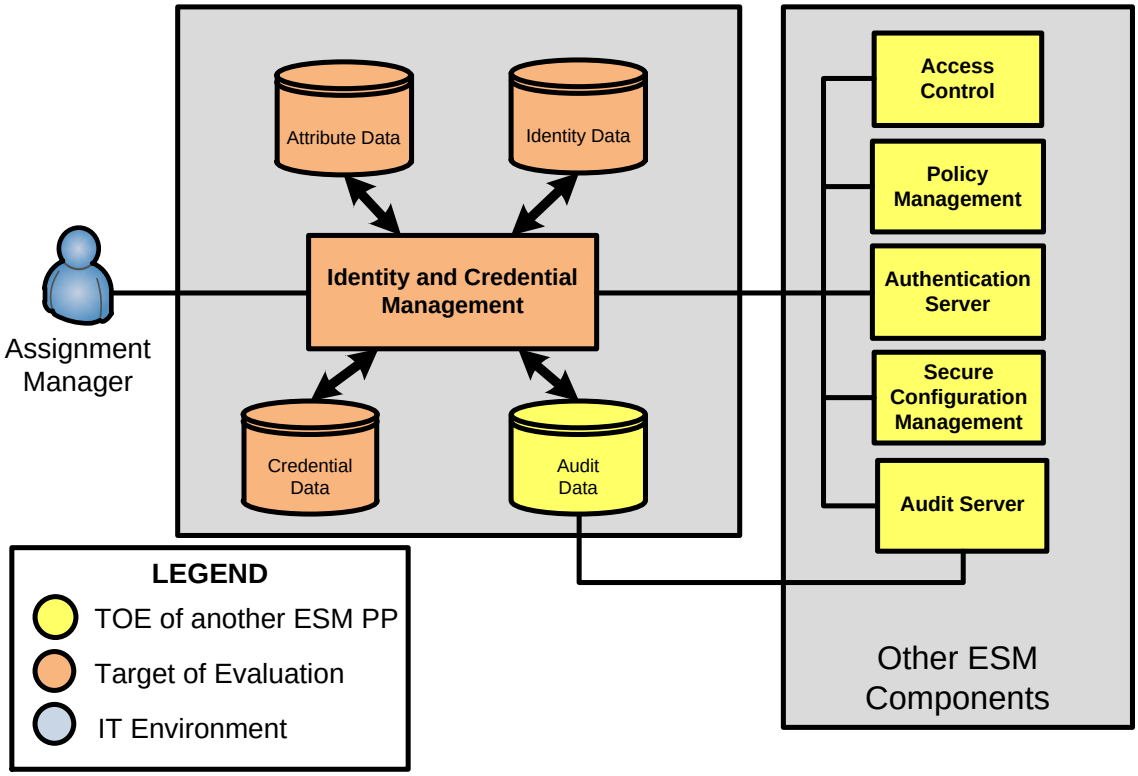

Figure 1. Context for Protection Profile

1.4 Compliant Targets of Evaluation

The purpose of an Identity and Credential Management product is to manage identities and credentials and associate attributes with users in an enterprise. It may also have the ability to maintain some or all of these attributes. This allows the ESM solution as a whole to identify who is performing actions in an enterprise and for other ESM components to take appropriate actions based on the privileges of identified subjects.

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

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

1.5 Common Capabilities

This Protection Profile defines a set of requirements that are expected to be fulfilled by all products that can perform identity and credential management in an ESM setting. Identity management refers to the notion of defining unique identifiers for entities. These identifiers are then associated with collections of attributes that are used by other products to determine the extent to which these entities are permitted to interact with objects in an ESM deployment. Credential management provides for the assured generation and validation of credentials used to support a claim of identity or an assertion of an attribute. Once a user has successfully authenticated as a particular subject, the identity data associated with that subject is bound to them for their duration of their activities within the enterprise.

It is essential for a product claiming conformance to an ESM Protection Profile to handle subjects and attributes that are **organizationally defined**. In other words, the TOE should make use of existing organizational repositories of users and user attributes whenever possible. The intent of ESM products is to provide *centralized* definition of subject and attribute data. The ST author must define the organizational data that the TOE will use, the trusted sources from which the data is received, and the mechanism by which this data is interpreted (such as SAML assertions or X.509 certificates).

When multiple domains are integrated in order to facilitate single sign-on (SSO) or authoritative validation of external attributes, it is called a federation. A federation can potentially be established between multiple instances of the same product or between two heterogeneous products. If the TOE is capable of establishing a federation, the ST author must indicate how this is accomplished. It is also necessary to mention any attributes the TOE exchanges with external entities via backend channels and how these exchanges occur.

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

1.7 Claiming Multiple Protection Profiles

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

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

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

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

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

Example: a single product that claims conformance to both the Identity and Credential Management PP and the Authentication Server PP can represent FAU_GEN.1 as a single iteration so long as the individual FAU_GEN.1 requirements for each PP are claimed and subsequently satisfied.

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

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

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

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

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

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

"the Operational Environment" actually refers to "the TSF of another claimed PP that is also part of the TOE".

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

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

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

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

1.8 Document Organization

Section 1 provides introductory material for the Protection Profile.

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

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

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

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

Section 6 lists and explains the security functional requirements and security assurance requirements that must be claimed in order for a TOE to be conformant with the Protection Profile.

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

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

The document also contains the following appendices:

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

2 Conformance Claims

2.1 CC Conformance Claims

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

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

2.2 PP Conformance Claim

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

2.3 Package Conformance Claim

This Protection Profile claims a package of EAL1 augmented.

2.4 ST Conformance Requirements

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

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

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

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

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

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

3 Threats

The following sections enumerate the threats that apply to the TOE.

3.1 Administrator Error

The security features offered by the TOE may be rendered irrelevant if a malicious or careless administrator configures or operates the TOE in a manner that is inconsistent with the defined security requirements. For example, they may fail to enable encrypted communications, configure an appropriate password policy, or assign excessive administrative privileges to a user who does not require them. While the TSF cannot truly prevent such incidents, the distribution of clear administrative guidance is expected to reduce unintentional errors, and the display of an acceptable use banner (with clearly enumerated consequences for unacceptable use) may deter some malicious activity.

[T.ADMIN_ERROR]

3.2 Credential, Identity, and ESM Data Disclosure

An Enterprise Security Management architecture will almost certainly require data to be transmitted between remote devices in order to function. The TOE may send credential and/or attribute data to remote repositories within an ESM deployment. It may receive data to be validated remotely from elsewhere in the environment, and it may 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]

3.3 Unauthorized Access to TOE Functions

If the TSF does not appropriately identify, authenticate, and authorize its administrators, there will not be assurance that its management functions are being performed appropriately. A poorly designed or implemented authentication function will allow an attacker to eavesdrop on the network and steal legitimate credentials for their own use or to bypass it entirely. An insufficiently robust authentication function will increase the odds of illicit entry through brute force guessing. A poorly designed or implemented data protection function will allow access control checks to be bypassed allowing for privilege

escalation. Regardless of the method by which an attacker gains illegitimate access to the ability to manage identity data, the resulting compromise of the integrity of the organization's identity and credential management is the same.

[T.UNAUTH]

3.4 False TOE Assurance

In order to provide assurance that information produced by the TOE is from a trusted source and should be enforced appropriately, the TOE should be able to assert its authenticity to dependent products. However, if the communications channel is not sufficiently protected from disclosure, an attacker may intercept the distribution of the data and provide false identity and/or credential data to dependent products. The result of this is that these dependent products do not use correct data and nothing appears amiss from an operational perspective, potentially making any ensuing security breach more difficult to detect.

[T.FALSIFY]

3.5 False Identity and Credential Mappings

The TOE must communicate with dependent products in order to provide identity and credential data to them. If the communications channel used to transfer this data is not properly secured, an attacker could intercept the traffic and modify it to provide false identity and credential mappings or authentication decisions that would disrupt the overall functionality of the ESM architecture. Alternatively, if the TOE interfaces with a separate authoritative source for attribute data such as in a federation, there is a threat that an attacker could use this interface to provide invalid attribute data to the TOE. This can potentially allow attackers access to protected resources or disallow legitimate users access to objects or functions to which they should have access.

[T.FORGE]

3.6 Hidden Actions

Part of the reason for implementing an Enterprise Security Management 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 identity and credential management functionality. If an attacker is able to alter audit data or prevent it

from being recorded, then they can begin to probe a system for 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 security functions were operating properly.

[T.MASK]

3.7 Insufficient Attributes

An Identity and Credential Management product must be capable of creating policies that provide the sufficient attributes that compatible ESM products can consume. Insufficient attributes can result in ineffective access control because they either allow unintended activity or incorrectly restrict legitimate usage.

[T.INSUFFATR]

3.8 Weak Authentication Functions

The ability of the TSF to define administrative privileges does not prevent malicious use if the TSF's authentication function can be subjected to brute force guessing. The TSF must provide sufficient login frustration mechanisms to limit the ability of an attacker to authenticate to the TOE through brute force.

[T.WEAKIA]

3.9 Insufficient Protection of Credentials

Protecting credentials during transmission does not necessarily protect them in storage on the TOE platform. The TOE must store credentials in a form that is not subject to extraction and replay.

[T.RAWCRED]

4 Security Objectives

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

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

4.1 ESM Component Validation

Since the TOE may be responsible for providing security data to other ESM products, it is important for the TSF to be able to validate the identity of potential recipients. In addition, the TSF should be able to provide information that confirms its own identity so that other ESM components (or distributed components of itself) have assurance that the data they receive is valid. Finally, the data transmitted between components must be protected from disclosure while in transit. Failure to implement these capabilities could allow a compromise of organizational security data that could provide a basis for subsequent attacks.

(O.ACCESSID, O.EAVES, O.SELFID: ESM_EID.2, FTP_ITC.1)

4.2 System Monitoring

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

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

(O.AUDIT: FAU_GEN.1, FAU_SEL.1 (optional), FAU_STG_EXT.1, FPT_STM.1 (optional))

4.3 Robust TOE Access

If an unsophisticated attacker attempts to illicitly authenticate to the TOE using repeated guesses, their likelihood of success will depend on two factors: how many authentication attempts they're able to make during the time they have access to the authentication function and the likelihood of success of each individual attempt. The TOE is expected to either implement mechanisms that improve security relative to each of these factors or enforce an externally-defined authentication policy that does. The TOE may also provide (through optional SFRs defined in Appendix **Error! Reference source not found.**) capabilities to deny session establishment and to suspend or terminate established sessions.

In cases where administrator credentials and authentication are handled by the Operational Environment, the responsibility for providing robust access to the TSF will be placed on the Operational Environment entities that define the appropriate policies (OE.ROBUST).

(O.ROBUST: FIA_AFL.1 (optional), FIA_SOS.1 (optional), FTA_TSE.1 (optional), FTA_SSL_EXT.1 (optional), FTA_SSL.3 (optional), FTA_SSL.4 (optional))

4.4 Confidential Communications

The TOE, to protect the confidentiality and integrity of transferred audit, policy, identity, or credential information to and from other ESM products (or distributed components of itself), should use sufficiently strong and sufficiently trusted encryption algorithms to protect data in transit to and from the TOE or between distributed TOE components. Failure to protect transferred ESM-relevant data from the Operational Environment could lead to attackers learning data that can assist them in compromising other parts of the Operational Environment. The TOE is expected to implement a cryptographic protocol to protect these data in transit. However, the cryptographic primitives employed by the protocol can be implemented by the TOE or through a capability provided by the operational environment. Once a secure channel is established, it will subsequently be used to transmit ESM data throughout the enterprise as needed.

(O.ACCESSID, O.AUTH, O.INTEGRITY, O.PROTCOMMS, O.SELFID: ESM_ACT.1,

ESM_EAU.2, ESM_EID.2, FCS_IPSEC_EXT.1 (optional), FCS_SSH_EXT.1 (optional), FCS_TLS_EXT.1 (optional), FCS_HTTPS_EXT.1 (optional), FIA_USB.1, FMT_MOF.1, FPT_SKP_EXT.1, FTP_ITC.1, FTP_TRP.1)

4.5 Protected Credentials

Protecting transmitted credential information is only part of the credential protection picture. It is also critical to protect the credentials as stored by the TOE so that they cannot be accessed in a raw plaintext form, and the subsequently replayed and used to impersonate a user.

(O.PROTCRED: FPT_APW_EXT.1)

4.6 Identity Definition

The primary purpose of the TOE is to serve as an attribute authority for identity data. In order to do this, the TSF must be able to define users, to define identity attributes that belong to them, and to securely transmit this data to other ESM components when necessary. In addition, depending on the needs of the enterprise, the TSF may also need to be able to define, maintain attributes for, and transmit attributes for non-person entities (NPEs) or objects.

(O.IDENT, O.EXPORT: ESM_ICD.1, ESM_ICT.1, ESM_ATD.1 (optional))

4.7 Guaranteed Integrity

The TOE, to validate the integrity of security information obtained from other ESM components, must be capable of interpreting the encrypted data it receives. The TOE must also provide a mechanism to assert the integrity of data that it sends to other ESM components so that this data can be trusted. The intent of this objective is to ensure that the TOE only acts upon data that can be proven to be unaltered. This objective also ensures that data that leaves the TOE can have its integrity verified. The TOE is expected to include internal cryptographic capabilities or leverage a third-party operating system or cryptographic suite to provide the cryptographic functionality.

(O.INTEGRITY: FTP_ITC.1)

4.8 Authorized Management

In order to properly facilitate identity and credential management, the TSF must have some way of allowing subject data to be defined and modified. In addition to this, the TSF must be able to determine the individuals that are allowed to have administrative authority over its behavior and the extent to which these authorizations should apply. This ensures that only trusted individuals are altering security data used by the remainder of the ESM.

(O.AUTH, O.MANAGE: ESM_EAU.2, ESM_EID.2, FIA_USB.1, FMT_MTD.1 (optional), FMT_SMF.1, FMT_SMR.1, FTP_TRP.1)

4.9 Access Bannering

In order to increase the likelihood that guidance for appropriate usage of the TOE is followed, the TOE is expected to display a banner prior to authentication that defines its acceptable use. This also provides legal notification for monitoring that allows audit data to be admissible in the event of any legal investigations.

(O.BANNER: FTA_TAB.1)

4.10 Cryptographic Services

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

(O.CRYPTO: FCS_CKM.1 (optional), FCS_CKM_EXT.4 (optional), FCS_COP.1(1) (optional), FCS_COP.1(2) (optional), FCS_COP.1(3) (optional), FCS_COP.1(4) (optional), FCS_RBG_EXT.1 (optional))

5 Extended Components Definition

This section provides a definition for all the extended components described within this PP. This includes both the required components specified in Section **Error! Reference source not found.** and the optional components specified in Appendix C.

Note that some extended classes and families refer to multiple extended requirements but only some of them are actually used in this PP. This is to give the reader a better awareness of the scope of the extended families and to consistently represent them between PPs. If the scope of the TOE is limited to this PP on its own, the extended components that are discussed here but are not included in section 6.1 are not to be included.

5.1 Class ESM: Enterprise Security Management

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

5.1.1 ESM_ATD Attribute Definition

Family Behavior

The requirements of this family ensure that the TSF will have the ability to authoritatively define attributes for Operational Environment attributes that can subsequently be used for access control policy definition and enforcement.

Component Leveling

There are two components in this family, ESM_ATD.1 and ESM_ATD.2. These are not hierarchical to each other. ESM_ATD.1, Object Attribute Definition, requires the TSF to be able to define some set of policy-related object attributes. ESM_ATD.2, Subject Attribute Definition, requires the TSF to be able to define some set of policy-related subject attributes[3]. In both cases, these attributes are expected to be subsequently

[3] In other words, attributes relevant to policies enforced by the access control component. Subjects may have additional attributes that are related to identity and credentials. The ability to manage of subject

associated with controlled entities in the Operational Environment for use in handling access control. Examples of object attributes include security labels for use in mandatory access control (MAC) environments and protection levels that can be associated with web pages that reside within an organization's intranet. Examples of subject attributes include clearances or MAC ranges that would be associated with defined identities.

5.1.1.1 ESM_ATD.1 Object Attribute Definition

The ESM_ATD.1 component defines requirements for specification of object attributes. This allows other ESM products to enforce their own security functions by using attribute data defined by the TSF. The ESM_ATD.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to define attributes that are associated with objects that reside in the Operational Environment.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
ESM_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual objects: [***assignment*: *list of object security attributes***].
Application Note:	*Object security attributes refer to attributes that may ultimately factor into an access control decision but are not associated with either a user or a policy. A TOE that defines access control policies for multi-level security may need to define security labels that can be associated with resources in order for the policy to be applicable to those resources.*
ESM_ATD.1.2	The TSF shall be able to associate security attributes with individual objects.

Management: ESM_ATD.1

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

a) Definition of object attributes.

attributes is optional in the Policy Management component; a system designer may choose to provide that capability within the Identity and Credential Management component.

b) Association of attributes with objects.

Audit: ESM_ATD.1

The following actions should be auditable if ESM_ATD.1 Object attribute definition is included in the PP/ST:

a) Minimal: Definition of object attributes.
b) Minimal: Association of attributes with objects.

5.1.2 ESM_EAU Enterprise Authentication

Family Behavior

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

Component Leveling

There are four non-hierarchical components in this family, ESM_EAU.1, ESM_EAU.2, ESM_EAU.5, and ESM_EAU.6.

ESM_EAU.1, Enterprise Authentication, requires the TSF to be able to receive authentication requests from a defined set of external entities, validate them by using some protocol, and returning the result of the decision to the requesting entity. ESM_EAU.1 is specific to the capability of an authentication server. Therefore, it is only discussed further in the ESM Authentication Server Protection Profile.

ESM_EAU.2, Reliance on Enterprise Authentication, is the opposite of ESM_EAU.1. This allows the TSF to take an authentication performed in the Operational Environment and use it as if the TSF had performed the authentication itself.

ESM_EAU.5, Multiple Enterprise Authentication Mechanisms, allows the TSF to provide multi-factor authentication. ESM_EAU.5 is specific to the capability of an authentication server. Therefore, it is only discussed further in the ESM Authentication Server Protection Profile.

ESM_EAU.6, Enterprise Re-authentication, allows the TSF to issue re-authentication challenges for established sessions. ESM_EAU.1 is specific to the capability of an authentication server. Therefore, it is only discussed further in the ESM Authentication Server Protection Profile.

Note that ESM_EAU.5 and ESM_EAU.6 were derived from FIA_UAU.5 and FIA_UAU.6, respectively. They were each assigned the same component level as their CC part 2 counterparts to emphasize the similarities.

5.1.2.1 ESM_EAU.2 Reliance on Enterprise Authentication

The ESM_EAU family defines requirements for facilitating enterprise user authentication. This allows other ESM products to enforce their own security functions by using this attribute data. This differs from FIA_UAU.1 and FIA_UAU.2 specified in CC Part 2 because these requirements specifically apply to a user authenticating to the TSF in order to perform activities that are mediated by the TSF. ESM_EAU.2 applies to the ability of the TSF to issue an authentication request that may be directed to the Operational Environment on behalf of a TOE user rather than being forced to perform its own authentication.

Hierarchical to:	No other components.
Dependencies:	ESM_EID.2 Reliance on Enterprise Identification
ESM_EAU.2.1	The TSF shall rely on [selection: [***assignment: identified TOE component(s) responsible for subject authentication***], [***assignment: identified Operational Environment component(s) responsible for subject authentication***]] for subject authentication.
Application Note:	*If the subjects being identified in this manner are users or administrators of the TSF, it is expected that the assignment(s) will be completed with one or more authentication servers. Future versions of this Protection Profile may require the entities named in this assignment to be compliant with the Standard Protection Profile for Enterprise Security Management Authentication Server.*
ESM_EAU.2.2	The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.
Application Note:	*If the TSF uses two different methods for authenticating two distinct sets of subjects, the ST author must represent this by creating a different iteration of this SFR for each*

method.

Management: ESM_EAU.2

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

a) Specification of entities used to perform authentication on behalf of the TSF.

Audit: ESM_EAU.2

The following actions should be auditable if ESM_EAU.2 Reliance on enterprise authentication is included in the PP/ST:

a) Minimal: All use of the authentication mechanism.

5.1.3 ESM_EID Enterprise Identification

Family Behavior

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

Component Leveling

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

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

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

5.1.3.1 ESM_EID.2 Reliance on Enterprise Identification

The ESM_EID family defines requirements for facilitating enterprise user identification. This allows for the subsequent execution of enterprise user authentication. This differs from FIA_UID.1 and FIA_UID.2 specified in CC Part 2 because these requirements specifically apply to a user presenting identification to the TSF in order to perform activities that are mediated by the TSF. ESM_EID.2 applies to the ability of the TSF to

be presented identification from the Operational Environment and to treat this as valid rather than performing its own identification request.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
ESM_EID.2.1	The TSF shall rely on [selection: [***assignment: identified TOE component(s) responsible for subject identification***], [***assignment: identified Operational Environment component(s) responsible for subject identification]***] for subject identification.
Application Note:	*If the subjects being identified in this manner are users or administrators of the TSF, it is expected that the assignment(s) will be completed with one or more authentication servers. Future versions of this Protection Profile may require the entities named in this assignment to be compliant with the Standard Protection Profile for Enterprise Security Management Authentication Server.*
ESM_EID.2.2	The TSF shall require each subject to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.
Application Note:	*If the TSF uses two different methods for identifying two distinct sets of subjects, the ST author must represent this by creating a different iteration of this SFR for each method.*

Management: ESM_EID.2

There are no management activities foreseen.

Audit: ESM_EID.2

There are no auditable events foreseen.

5.1.4 ESM_ICD Identity and Credential Definition

Family Behavior

The requirements of this family ensure that the TSF will have the ability to authoritatively define user attributes that can subsequently be used by other ESM products for various purposes.

Component Leveling

There is only one component in this family, ESM_ICD.1. ESM_ICD.1, Identity and Credential Definition, requires the TSF to be able to define some set of identity and/or credential attributes. These attributes are expected to be used by other ESM products in order to help satisfy the security requirements for those products. This requirement could define attributes such as authentication credentials used for enterprise user authentication or organizational role attributes that are used in access control policy definition.

5.1.4.1 ESM_ICD.1 Identity and Credential Definition

The ESM_ICD family defines requirements for defining enterprise user attributes. This allows other ESM products to enforce their own security functions by using this attribute data. The ESM_ICD.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to define attribute data for users that reside in the Operational Environment. This is distinct from FIA_ATD.1 because these attributes apply to users that do not necessarily access the TOE.

Hierarchical to:	No other components.
Dependencies:	No dependencies.
ESM_ICD.1.1	The TSF shall provide the ability to define identity and credential data for use with other Enterprise Security Management products.
Application Note:	*Security-relevant identity and credential attributes must constitute the full set of user attributes that other ESM products use to enforce their security functionality. Data such as a user ID or password is security-relevant because it will be used for authentication. Data such as a user's organizational role, title, or geographic location may be security-relevant if access control policies are expected to use this data. Data such as a telephone number is likely not security-relevant.*

ESM_ICD.1.2 The TSF shall define the following security-relevant identity and credential attributes for enterprise users: credential lifetime, credential status, [***assignment: list of any additional security-relevant identity and credential attributes the TSF is able to associate with enterprise users***].

ESM_ICD.1.3 The TSF shall provide the ability to enroll enterprise users through assignment of unique identifying data.

Application Note: It is possible that two users may have the same credential data. The intent of ESM_ICD.1.3 is that there be additional information maintained that uniquely identifies the particular enterprise user.

ESM_ICD.1.4 The TSF shall provide the ability to associate defined security-relevant attributes with enrolled enterprise users.

ESM_ICD.1.5 The TSF shall provide the ability to query the status of an enterprise user's credentials.

ESM_ICD.1.6 The TSF shall provide the ability to revoke an enterprise user's credentials.

ESM_ICD.1.7 The TSF shall provide the ability for a compatible Authentication Server ESM product to update an enterprise user's credentials.

ESM_ICD.1.8 The TSF shall ensure that the defined enterprise user credentials satisfy the following strength rules:

a) For password-based credentials, the following rules apply:

1. Passwords shall be able to be composed of a subset of the following character sets: [***assignment: list of character sets that are supported by the TSF for password entry***] that include the following values [***assignment: list of the supported characters for each supported character set***]; and

Application Note: *For the English character set, the types of characters are expected to include the 26 uppercase letters, 26 lowercase letters, 10 numbers, and 10 special characters "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". If non-English character sets are supported by the TOE, the ST author must specify the supported character sets along with the allowable character space of each sub-category of those sets.*

2. Minimum password length shall settable by an administrator, and support passwords of 15 characters or greater; and

Application Note: *The number of password combinations based on the minimum password length and the character space of the password must exceed 10^{14}. This could be satisfied by an English password using a character set of 72 that has a minimum length of 8 characters.*

3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and

4. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based credentials, the following rules apply:

1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}.

Management: ESM_ICD.1

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

a) Creation and modification of identity and credential data.

Audit: ESM_ICD.1

The following actions should be auditable if ESM_ICD.1 Identity and credential definition is included in the PP/ST:

a) Minimal: Creation and modification of identity and credential data.

5.1.5 ESM_ICT Identity and Credential Transmission

Family Behavior

The requirements of this family ensure that the TSF will have the ability to transfer user attributes to other ESM products.

Component Leveling

There is only one component in this family, ESM_ICT.1. ESM_ICT.1, Identity and Credential Transmission, requires the TOE to transmit identity and/or credential data defined by ESM_ICD.1 or ESM_ATD.1 (optional) to compatible and authorized ESM products external to the TSF under conditions defined by the ST author.

5.1.5.1 ESM_ICT.1 Identity and Credential Transmission

The ESM_ICT family defines requirements for transmitting enterprise user attributes. This allows other ESM products to enforce their own security functions by using attribute data defined by the TSF. The ESM_ICT.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to distribute attribute data for users that reside in the Operational Environment to other trusted IT products that use that data to perform their security functions.

Hierarchical to:	No other components.
Dependencies:	ESM_ICD.1 Identity and Credential Definition
ESM_ICT.1	The TSF shall transmit [selection: "identity and credential data", "identity, credential, and object attribute data"] to compatible and authorized Enterprise Security Management products under the following circumstances: [selection: choose one or more of: immediately following creation or modification of data, at a periodic interval, at the request of the product, [***assignment: other circumstances***]].

Application Note: *The intent of this requirement is to ensure that the TSF is making the identity and credential data it defines available to the Operational Environment in a timely manner so that there is assurance that the correct data is being used in the enforcement of various policies. If the assignment is selected, it must reflect that intent.*

Management: ESM_ICT.1

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

a) Specification of the specific identity and/or credential data values to be transmitted.
b) Specification of the specific object attributes to be transmitted.
c) Specification of the circumstances under which this data is transmitted.
d) Specification of the destinations to which this data is transmitted.

Audit: ESM_ICT.1

The following actions should be auditable if ESM_ICT.1 Identity and credential transmission is included in the PP/ST:

a) Minimal: Transmission of identity and credential data (and object attributes, if applicable) to external processes or repositories.

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

[4] FAU_STG.1 could have been treated as an optional requirement in Appendix C. However, as there might be systems that had only local storage, that would have meant FAU_STG_EXT.1 would also need to be

Hierarchical to: No other components.

Dependencies: FAU_GEN.1 Audit Data Generation

FTP_ITC.1 Inter-TSF Trusted Channel

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

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

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

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

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

1) protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and
2) prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

Management: FAU_STG_EXT.1

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

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

optional. Combining both into a single non-optional SFR mandates protected audit storage and transmission, while still supporting an "all-in-one" product that combines ESM capabilities.

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 generation than the corresponding requirements in CC Part 2.

Hierarchical to: No other components.

Dependencies: No dependencies.

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

Management: FCS_CKM_EXT.4

There are no management actions foreseen.

Audit: FCS_CKM_EXT.4

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

a) Basic: Failure of the key zeroization process.

5.3.2 FCS_HTTPS_EXT HTTPS

Family Behavior

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

Component Leveling

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

5.3.2.1 FCS_HTTPS_EXT.1 HTTPS

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

Management: FCS_HTTPS_EXT.1

There are no management actions foreseen.

Audit: FCS_HTTPS_EXT.1

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

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

5.3.3 FCS_IPSEC_EXT IPsec

Family Behavior

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

Component Leveling

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

5.3.3.1 FCS_IPSEC_EXT.1 IPsec

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), [selection: no other algorithms, AES-GCM-128, AES-GCM-256 as specified in RFC 4106], and using [selection, choose at least one of: IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]].

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

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

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

for Phase 2 SAs.

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

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

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

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

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

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

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

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

FCS_IPSEC_EXT.1.8 The TSF shall support the following:

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

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

Management: FCS_IPSEC_EXT.1

There are no management actions foreseen.

Audit: FCS_ IPSEC _EXT.1

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

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

5.3.4 FCS_RBG_EXT Random Bit Generation

Family Behavior

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

Component Leveling

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

5.3.4.1 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_RBG_EXT.1.1 The TSF shall perform all random bit generation (RBG) services in accordance with [selection, choose one of: NIST Special Publication 800-90 using [selection: Hash_DRBG (any), HMAC_DRBG (any), CTR_DRBG (AES), Dual_EC_DRBG (any)]; FIPS Pub 140-2 Annex C: X9.31 Appendix 2.4 using AES] seeded by an entropy source that accumulates entropy from [selection: choose one of: (1) one or more independent hardware-based noise sources, (2) one or more independent software-based noise sources, (3) a combination of hardware-based and software-based noise sources.].

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

Management: FCS_RBG_EXT.1

There are no management actions foreseen.

Audit: FCS_RBG_EXT.1

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

a) Basic: Failure of the randomization process.

5.3.5 FCS_SSH_EXT SSH

Family Behavior

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

Component Leveling

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

5.3.5.1 FCS_SSH_EXT.1 SSH

Hierarchical to:	No other components.
Dependencies:	FCS_COP.1 Cryptographic Operation
FCS_SSH_EXT.1.1	The TSF shall implement the SSH protocol that complies with RFCs 4251, 4252, 4253, and 4254.
Application Note:	*The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done by adding additional detail in the TSS. In a future version of this PP, a requirement will be added regarding rekeying. The requirement will read "The TSF shall ensure that the SSH connection be rekeyed after no more than 2^{28} packets have been transmitted using that key."*
FCS_SSH_EXT.1.2	The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.
FCS_SSH_EXT.1.3	The TSF shall ensure that, as described in RFC 4253, packets greater than [***assignment: number of bytes***] bytes in an SSH transport connection are dropped.

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

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

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

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [selection: PGP-SIGN-RSA, PGP-SIGN-DSS, no other public key algorithms] as its public key algorithm(s).

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

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

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

Management: FCS_SSH_EXT.1

There are no management actions foreseen.

Audit: FCS_SSH_EXT.1

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

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

5.3.6 FCS_TLS_EXT TLS

Family Behavior

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

Component Leveling

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

5.3.6.1 FCS_TLS_EXT.1 TLS

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic Operation

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

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

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

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

The ciphersuites to be used in the evaluated configuration are limited by this requirement. The ST author should select the optional ciphersuites that are supported; if there are no ciphersuites supported other than the mandatory suites, then "None" should be selected. If administrative steps need to be taken so that the suites negotiated by the implementation are limited to those in this requirement, the appropriate instructions need to be contained in the guidance called for by AGD_OPE. The Suite B algorithms (RFC 5430) listed above are the preferred algorithms for implementation. Since the Dec. 2010 publication of this requirement in NDPP v1.0, there has been limited progress with respect to extending the prevalence of TLS 1.2 support in commercial products. Future publications of this PP will require support for TLS 1.2 (RFC 5246); however, it is

likely the next version of this PP will not include a requirement for TLS 1.2 support, but will require that the TOE offer a means to deny all connection attempts using SSL 2.0 or SSL 3.0.

Management: FCS_TLS_EXT.1

There are no management actions foreseen.

Audit: FCS_TLS_EXT.1

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

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

5.4 Class FPT: Protection of the TSF

5.4.1 FPT_APW_EXT Protection of Stored Credentials

Family Behavior

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

Component Leveling

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

5.4.1.1 FPT_APW_EXT.1 Protection of Stored Credentials

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

Hierarchical to: No other components.

Dependencies: No dependencies.

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

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

Management: FPT_APW_EXT.1

There are no management actions foreseen.

Audit: FPT_APW_EXT.1

There are no auditable actions foreseen.

5.4.1 FPT_SKP_EXT Protection of Secret Key Parameters

Family Behavior

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

Component Leveling

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

5.4.1.1 FPT_SKP_EXT.1 Protection of Secret Key Parameters

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

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Management: FPT_SKP_EXT.1

There are no management actions foreseen.

Audit: FPT_SKP_EXT.1

There are no auditable actions foreseen.

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 that were fixed in the base requirement in the Common Criteria.

Hierarchical to: No other components.

Dependencies: No dependencies.

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.

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 security functional requirements for the PP consist of the following components, summarized in **Error! Reference source not found.**. The formatting used for these

requirements is defined in Appendix D.1 – Operations.

Table 2. TOE Functional Components

Functional Component	
ESM_ATD.1 (optional)	Object Attribute Definition *(optional—defined in Appendix C.1.1)*
ESM_EAU.2	Reliance on Enterprise Authentication
ESM_EID.2	Reliance on Enterprise Identification
ESM_ICD.1	Identity and Credential Definition
ESM_ICT.1	Identity and Credential Transmission
FAU_GEN.1	Audit Data Generation
FAU_SEL.1 (optional)	Selectable Audit *(optional – defined in Appendix C.3.1)*
FAU_STG_EXT.1	External Audit Trail Storage
FCS_CKM.1 (optional)	Cryptographic Key Generation (for Asymmetric Keys) *(optional – defined in Appendix C.8.1)*
FCS_CKM_EXT.4 (optional)	Cryptographic Key Zeroization *(optional – defined in Appendix C.8.2)*
FCS_COP.1(1) (optional)	Cryptographic Operation (for Data Encryption/Decryption) *(optional – defined in Appendix C.8.3)*
FCS_COP.1(2) (optional)	Cryptographic Operation (for Cryptographic Signature) *(optional – defined in Appendix C.8.4)*
FCS_COP.1(3) (optional)	Cryptographic Operation (for Cryptographic Hashing) *(optional – defined in Appendix C.8.5)*
FCS_COP.1(4) (optional)	Cryptographic Operation (for Keyed-Hash Message Authentication) *(optional – defined in Appendix C.8.6)*
FCS_HTTPS_EXT.1 (optional)	HTTPS *(optional – defined in Appendix* C.8.7*)*
FCS_IPSEC_EXT.1 (optional)	IPsec *(optional – defined in Appendix C.8.8)*
FCS_RBG_EXT.1 (optional)	Cryptographic Operation (Random Bit Generation) *(optional – defined in Appendix C.8.9)*
FCS_SSH_EXT.1 (optional)	SSH *(optional – defined in Appendix C.8.10)*
FCS_TLS_EXT.1 (optional)	TLS *(optional – defined in Appendix C.8.11)*
FIA_AFL.1 (optional)	Authentication Failure Handling *(optional – defined in Appendix C.7.1)*
FIA_SOS.1 (optional)	Verification of Secrets

Functional Component	
	(optional – defined in Appendix C.2.1)
FIA_USB.1	User-Subject Binding
FMT_MOF.1	Management of Functions Behavior
FMT_MTD.1	Management of TSF Data *(optional – defined in Appendix C.5.1)*
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Management Roles
FPT_APW_EXT.1	Protection of Stored Credentials
FPT_SKP_EXT.1	Protection of Secret Key Parameters
FPT_STM.1 (optional)	Reliable Time Stamps *(as defined in Appendix C.6.1)*
FTA_SSL_EXT.1 (optional)	TSF-initiated Session Locking *(optional – defined in Appendix C.4.1)*
FTA_SSL.3 (optional)	TSF-initiated Termination *(optional – defined in Appendix C.4.2)*
FTA_SSL.4 (optional)	User-initiated Termination *(optional – defined in Appendix C.4.3)*
FTA_TAB.1	TOE Access Banner
FTA_TSE.1 (optional)	TOE Session Establishment *(optional – defined in Appendix C.7.2)*
FTP_ITC.1	Inter-TSF Trusted Channel
FTP_TRP.1	Trusted Path

6.1.1 PP Application Notes

6.1.1.1 Usage

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

6.1.1.2 Composition Philosophy

The ESM PPs represent a family of related Protection Profiles written to encompass the variable capabilities of ESM products. For an ST that claims conformance to multiple PPs within the ESM PP family, it is recommended that the ST author clarify how the ESM components relate to one another through usage of application notes. This will

assist the reader in determining how the parts of the product that are to be evaluated correspond with the CC's notion of different ESM capabilities.

For example, multiple parts of the ESM may be deployed as a single appliance, as a series of redundant servers that also contain policy enforcement mechanisms, or as a client-server deployment in which enforcement points reside on individual client systems that report to a single server. Usage of application notes makes it easy to determine the requirements that are unnecessary to claim based on the architecture of the ESM system.

6.1.2 Class ESM: Enterprise Security Management

ESM_EAU.2 Reliance on Enterprise Authentication

Hierarchical to:	No other components.
ESM_EAU.2.1	The TSF shall rely on [selection: [***assignment: identified TOE component(s) responsible for subject authentication***], [***assignment: identified Operational Environment component(s) responsible for subject authentication***]] for subject authentication.
Application Note:	*If the subjects being identified in this manner are users or administrators of the TSF, it is expected that the assignment(s) will be completed with one or more authentication servers. Future versions of this Protection Profile may require the entities named in this assignment to be compliant with the Standard Protection Profile for Enterprise Security Management Authentication Server.*
ESM_EAU.2.2	The TSF shall require each subject to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.
Application Note:	*If the TSF uses two different methods for authenticating two distinct sets of subjects, the ST author must represent this by creating a different iteration of this SFR for each method.*
Dependencies:	ESM_EID.2 Reliance on Enterprise Identification

Assurance Activity:

The evaluator shall check the TSS in order to determine that it describes the TSF as requiring authentication to use and that it describes, for each type of user or IT entity that authenticates to the TOE, the identification and authentication mechanism that is used. The evaluator shall also check to ensure that this information is appropriately represented by iterating the SFR for each authentication mechanism that is used by the TSF.

The evaluator shall check the operational guidance in order to determine how the TOE determines whether an interactive user requesting access to it has been authenticated and how the TOE validates authentication credentials or identity assertions that it receives. If any IT entities authenticate to the TOE, the evaluator shall also check the operational guidance to verify that it identifies how these entities are authenticated and what configuration steps must be performed in order to set up the authentication.

The evaluator shall test this capability by accessing the TOE without having provided valid identification and authentication information and observe that access to the TSF is subsequently denied. If any IT entities authenticate to the TOE, the evaluator shall instruct these IT entities to provide invalid identification and authentication information and observe that they are not able to access the TSF.

Note that positive testing of the identification and authentication is assumed to be tested by other requirements because successful authentication is a prerequisite to manage the TSF (and possibly for the TSF to interact with external IT entities).

ESM_EID.2 Reliance on Enterprise Identification

Hierarchical to:	No other components.
ESM_EID.2.1	The TSF shall rely on [selection: [***assignment: identified TOE component(s) responsible for subject identification***], [***assignment: identified Operational Environment component(s) responsible for subject identification]***] for subject identification.
Application Note:	*If the subjects being identified in this manner are users or administrators of the TSF, it is expected that the assignment(s) will be completed with one or more authentication servers. Future versions of this Protection Profile may require the entities named in this assignment to*

be compliant with the Standard Protection Profile for Enterprise Security Management Authentication Server.

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

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

Dependencies: No dependencies.

Assurance Activity:

This functionality—for both interactive users and authorized IT entities—is verified concurrently with ESM_EAU.2.

ESM_ICD.1 Identity and Credential Definition

Hierarchical to: No other components.

ESM_ICD.1.1 The TSF shall provide the ability to define identity and credential data for use with other Enterprise Security Management products.

ESM_ICD.1.2 The TSF shall define the following security-relevant identity and credential attributes for enterprise users: credential lifetime, credential status, [***assignment: list of any additional security-relevant identity and credential attributes the TSF is able to associate with enterprise users***].

Application Note: *Security-relevant identity and credential attributes must constitute the full set of user attributes that other ESM products use to enforce their security functionality. Data such as a user ID or password is security-relevant because it will be used for authentication. Data such as a user's organizational role, title, or geographic location may be security-relevant if access control policies are expected to*

use this data. Data such as a telephone number is likely not security-relevant.

ESM_ICD.1.3 The TSF shall provide the ability to enroll enterprise users through assignment of unique identifying data.

Application Note: It is possible that two users may have the same credential data. The intent of ESM_ICD.1.3 is that there be additional information maintained that uniquely identifies the particular enterprise user.

ESM_ICD.1.4 The TSF shall provide the ability to associate defined security-relevant attributes with enrolled enterprise users.

Application Note: *The act of associating security attributes with enterprise users is expected to include the issuance of credentials and the management of their status.*

ESM_ICD.1.5 The TSF shall provide the ability to query the status of an enterprise user's credentials.

ESM_ICD.1.6 The TSF shall provide the ability to revoke an enterprise user's credentials.

ESM_ICD.1.7 The TSF shall provide the ability for a compatible Authentication Server ESM product to update an enterprise user's credentials.

ESM_ICD.1.8 The TSF shall ensure that the defined enterprise user credentials satisfy the following strength rules:

a) For password-based credentials, the following rules apply:

1. Passwords shall be able to be composed of a subset of the following character sets: [***assignment: list of character sets that are supported by the TSF for password entry***] that include the following values [***assignment: list of the supported characters for each supported character set***]; and

Application Note: *For the English character set, the types of characters are expected to include the 26 uppercase letters, 26 lowercase letters, 10 numbers, and 10 special characters "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". If non-English character sets are supported by the TOE, the ST author must specify the supported character sets along with the allowable character space of each sub-category of those sets.*

2. Minimum password length shall settable by an administrator, and support passwords of 15 characters or greater; and

Application Note: *The number of password combinations based on the minimum password length and the character space of the password must exceed 10^{14}. This could be satisfied by an English password using a character set of 72 that has a minimum length of 8 characters.*

3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and

4. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based credentials, the following rules apply:

1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}.

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall review the TSS to verify that it identifies compatible ESM products

and describes the identity and credential data that are used by those products. The evaluator shall review public documentation for compatible products and verify that they actually use the data in the compatible way asserted by the TSS.

The evaluator shall review the operational guidance in order to verify that it indicates how identity and credential data are supplied to the TOE and this data is identified.

The evaluator shall test this capability by using the TOE to create identity and credential data and sending this data to the compatible ESM product(s) for consumption. These tests shall exercise each capability described in the SFR, including the ability to enforce credential complexity requirements. The evaluator will then perform basic identity and credential-related actions[5] *on the compatible ESM products that use the identity and credential data in order to confirm that the data was applied appropriately.*

With respect to the requirements regarding credential complexity: the evaluator shall examine the TSS and operational guidance in order to identify the form of credentials collected:

a. *For password-based credentials, the evaluator shall identify that all password composition, configuration, and aging requirements specified in the ST are discussed in the TSS and AGD and test these capabilities one at a time (for example: set minimum password length to 6, observe that a 7 character password and a 16 character password are both accepted, then change the minimum length to 8, observe that a 7 character password is rejected but that a 16 character password is accepted)*

b. *For non-password based credentials, the evaluator shall perform a basic strength of function analysis to determine the solution space of the authentication mechanism and the frequency with which password attempts can be made. For example, if the authentication is a 4-digit PIN that can be attempted once an hour, this requirement would not pass. If the strength of the authentication mechanism can't be determined by strength of function metrics at face value (for example, if a biometric authentication mechanism is being used), the vendor shall provide some evidence of the strength of function.*

[5] That is, exhaustive testing of edge conditions is not required.

ESM_ICT.1 Identity and Credential Transmission

Hierarchical to: No other components.

ESM_ICT.1.1 The TSF shall transmit [selection: "identity and credential data", "identity, credential, and object attribute data"] to compatible and authorized Enterprise Security Management products under the following circumstances: [selection: choose one or more of: immediately following creation or modification of data, at a periodic interval, at the request of a compatible Secure Configuration Management product, [***assignment: other circumstances***]].

Application Note: *The intent of this requirement is to ensure that the TSF is making the identity and credential data it defines available to the Operational Environment in a timely manner so that there is assurance that the correct data is being used in the enforcement of various policies. If the assignment is selected, it must reflect that intent.*

If "at the request of a compatible Secure Configuration Management product" is selected, the ST author must indicate the compatible product(s).

Dependencies: ESM_ICD.1 Identity and Credential Definition

Assurance Activity:

The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it describes the ESM data that the TSF transmits to other ESM products and the circumstances that cause it to be transmitted.

The evaluator shall review the operational guidance to determine how to create and update identity, credential (and potentially object attribute) data, and the circumstances under which new or updated data are transmitted to consuming ESM products (and how those circumstances are managed, if applicable).

The evaluator shall test this capability by obtaining the compatible ESM products.

Following the procedures in the operational guidance for both the ICM and other ESM products, the evaluator shall create the indicated data (i.e., identity, credential, and potentially object attribute data) and ensure that the defined data is transmitted and installed successfully in compatible ESM products[6], in accordance with the circumstances defined in the SFR. In other words, (a) if the selection is completed to transmit after creation of new data, then the evaluator shall create the new data and ensure that, after a reasonable window for transmission, the new data is installed; (b) if the selection is completed to transmit periodically, the evaluator shall create the new data, wait until the periodic period has passed, and then confirm that the new data is present in the appropriate ESM components; or (c) if the section is completed to transmit upon the request of a compatible Secure Configuration Management component, the evaluator shall create the data, use the Secure Configuration Management component to request transmission, and the confirm that the appropriate ESM components have received and installed the data. If the ST author has specified "other circumstances", then a similar test shall be executed to confirm transmission under those circumstances.

The evaluator shall then make a change to the previously created data, and then repeat the previous procedure to ensure that the updated data is transmitted to the compatible ESM components in accordance with the SFR-specified circumstances. Lastly, as updating data encompasses deletion of data, the evaluator shall repeat the process a third time, this time deleting the data to ensure it is removed as active data from the compatible ESM components.

Note: This testing will likely be performed in conjunction with the testing of ESM_ICD.1.

6.1.3 Security Audit (FAU)

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

[6] For testing purposes, it is acceptable to group compatible ESM products into equivalence groups and provide an argument as to why testing one member from a group is sufficient to cover all members of the group.

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
ESM_ATD.1 (optional)	Definition of object attributes	Identification of the attribute defined
ESM_ATD.1 (optional)	Association of attributes with objects	Identification of the object and the attribute
ESM_EAU.2	All use of the authentication mechanism	None
ESM_ICD.1	Creation or modification of identity and credential data	The attribute(s) modified
ESM_ICD.1	Enrollment or modification of subject	The subject created or modified, the attribute(s) modified (if applicable)
ESM_ICT.1	All attempts to transmit information	The destination to which the transmission was attempted
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
FCS_CKM.1 (optional)	Failure of the key generation activity	None
FCS_CKM_EXT.4 (optional)	Failure of the key zeroization process	Identity of subject requesting or causing zeroization, identity of object or entity being cleared
FCS_COP.1(1) (optional)	Failure of encryption or decryption	Cryptographic mode of operation, name/identifier of object being encrypted/decrypted
FCS_COP.1(2) (optional)	Failure of cryptographic signature	Cryptographic mode of operation, name/identifier of object being signed/verified
FCS_COP.1(3) (optional)	Failure of hashing function	Cryptographic mode of operation, name/identifier of object being hashed
FCS_COP.1(4) (optional)	Failure in cryptographic hashing for non-data integrity	Cryptographic mode of operation, name/identifier of object being hashed
FCS_HTTPS_EXT.1 (optional)	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FCS_IPSEC_EXT.1 (optional)	Failure to establish an SA, establishment/termination of an SA	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FCS_RBG_EXT.1 (optional)	Failure of the randomization process	None

Component	Event	Additional Information
FCS_SSH_EXT.1 (optional)	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FCS_TLS_EXT.1 (optional)	Failure to establish a session, establishment/termination of a session	Non-TOE endpoint of connection (IP address), reason for failure (if applicable)
FIA_AFL.1 (optional)	The reaching of an unsuccessful authentication attempt threshold, the actions taken when the threshold is reached, and any actions taken to restore the normal state	Action taken when threshold is reached
FIA_SOS.1 (optional)	Rejection or acceptance by the TSF of any tested secret	None
FIA_SOS.1 (optional)	Identification of any changes to the defined quality metrics	The change made to the quality metric
FMT_MOF.1	All modifications of TSF function behavior	None
FMT_SMF.1	Use of the management functions	Management function performed
FTA_SSL_EXT.1 (optional)	All session locking and unlocking events	None
FTA_SSL.3 (optional)	All session termination events	None
FTA_SSL.4 (optional)	All session termination events	None
FTA_TSE.1 (optional)	Denial of session establishment	None
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [***assignment: other audit relevant***

information].

Application Note: *The "other audit relevant information" must include sufficient information to identify the responsible individual and the specific action taken by the individual, if these are not already addressed by the information captured in clause a).*

Dependencies: FPT_STM.1 Reliable Time Stamps

Assurance Activity:

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

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

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

The evaluator shall test the TOE's audit function by having the TOE generate audit records for all events that are defined in the ST and/or have been identified in the previous two activities. The evaluator shall then check the audit repository defined by the ST, operational guidance, or developmental evidence (if available) in order to determine that the audit records were written to the repository and contain the attributes as defined by the ST.

This testing may be done in conjunction with the exercise of other functionality. For example, if the ST specifies that an audit record will be generated when an incorrect authentication secret is entered, then audit records will be expected to be generated as a result of testing identification and authentication. The evaluator shall also check to ensure that the content of the logs are consistent with the activity performed on the TOE. For example, if a test is performed that revokes a credential from a user, the audit log for the event should correctly indicate a revocation operation.

FAU_STG_EXT.1 External Audit Trail Storage

Hierarchical to: No other components.

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

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

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

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

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

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

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

Dependencies: FAU_GEN.1 Audit Data Generation

FTP_ITC.1 Inter-TSF Trusted Channel

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

Assurance Activity:

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

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

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

6.1.4 Cryptographic Support (FCS)

The cryptographic requirements for the TOE can either be implemented by the TSF or by reliance on non-ESM Operational Environment components. The expectation is that the

TSF is able to use a suite of cryptographic algorithms that have been previously validated rather than forcing vendors to implement their own unique and redundant cryptographic capabilities. The ST must clearly indicate what cryptographic capabilities are used by the TSF. Regardless of where the cryptographic capabilities reside, the expected capabilities are the same.

Refer to Appendix C.8 for the cryptographic requirements needed to support the cryptographic protocols implemented by the TOE.

6.1.5 Identification and Authentication (FIA)

FIA_USB.1 User-Subject Binding

Hierarchical to:	No other components.
FIA_USB.1.1	The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [***assignment: list of user security attributes***].
FIA_USB.1.2	The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [***assignment: rules for the initial association of attributes***].
FIA_USB.1.3	The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [***assignment: rules for the changing of attributes***].
Dependencies:	FIA_ATD.1 User Attribute Definition

Assurance Activity:

The evaluator shall check the TSS in order to determine that it describes the security attributes that are assigned to administrators and the means by which the administrator is associated with these attributes, both during initial assignment and when any changes are made to them.

The evaluator shall check the operational guidance in order to verify that it describes the mechanism by which external data sources are invoked and mapped to user data that is controlled by the TSF.

The evaluator shall test this capability by configuring the TSF to accept user information from external sources as defined by the ST. The evaluator shall then perform authentication activities using these methods and validate that authentication is successful in each instance. Based on the defined privileges assigned to each of the subjects, the evaluator shall then perform various management tests in order to determine that the user authorizations are consistent with their externally-defined attributes and the configuration of the TSF's access control policy. For example, if a user who is defined in an LDAP repository belongs to a certain group and the TSF is configured such that members of that group only have read-only access to a certain set of data, the evaluator shall authenticate to the TSF as that user and verify that as a subject under the control of the TSF, they do not have write access to that data. This verifies that the aspects of the user's identity data that are pertinent to how the TSF treats the user are appropriately taken from external sources and used in order to determine what the user is able to do.

6.1.6 Security Management (FMT)

FMT_MOF.1 Management of Functions Behavior

Hierarchical to:	No other components.
FMT_MOF.1	The TSF shall restrict the ability to [selection: determine the behavior of, disable, enable, modify the behavior of] the functions**:** [***assignment: list of functions***] to **[*assignment: the authorized identified roles*]**.
Application Note:	*The first assignment is expected to correspond with the management functions that are defined in FMT_SMF.1.* *The second assignment is expected to correspond with the roles that are identified in FMT_SMR.1.*
Dependencies:	FMT_SMR.1 Security Roles FMT_SMF.1 Specification of Management Functions

Assurance Activity:

The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it describes the ability of the

TSF to perform the required management functions and the authorizations that are required to do this.

The evaluator shall review the operational guidance in order to determine what restrictions are in place on management of these attributes and how the TSF enforces them. For example, if management authority is role-based, then the operational guidance shall indicate this.

The evaluator shall test this function by accessing the TSF using one or more appropriately privileged administrative accounts and determining that the management functions as described in the ST and operational guidance can be managed in a manner that is consistent with any instructions provided in the operational guidance. If the TSF can be configured by an authorized and compatible Secure Configuration Management product, the evaluator shall also configure such a product to manage the TSF and use this product to perform the defined management activities. In addition, any access restrictions to this behavior should be enforced in a manner that is consistent with the relevant documentation. The evaluator shall test this by attempting to perform a sampling of the available management functions using one or more unprivileged accounts to observe that the activities are rejected or unavailable.

FMT_SMF.1 Specification of Management Functions

Hierarchical to:	No other components.
FMT_SMF.1	The TSF shall be capable of performing the following management functions: **[*assignment: list of management functions to be provided by the TSF*].**
Dependencies:	No dependencies.
Application Note:	*The management functions, at their broadest level, must include at minimum the capabilities specified in Table 4 below. The ST author must ensure that the capabilities defined are sufficient to manage any functional behavior that is claimed in the remainder of the document.*

Table 4. TOE Management Functions

Requirement	Management Activities
ESM_ATD.1 (optional)	Definition of object attributes

	Association of attributes with objects
ESM_EAU.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
ESM_EID.2	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)
ESM_ICD.1	Management of credential status
ESM_ICD.1	Enrollment of users into repository
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed
FAU_SEL.1 (optional)	Configuration of auditable events
FAU_STG_EXT.1	Configuration of external audit storage location
FIA_AFL.1 (optional)	Management of the threshold for unsuccessful authentication attempts Management of actions to be taken in the event of an authentication failure
FIA_SOS.1 (optional)	Management of the metric used to verify secrets
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes
FMT_MOF.1	Management of sets of users that can interact with security functions
FMT_SMR.1	Management of the users that belong to a particular role
FTA_SSL_EXT.1 (optional)	Configuration of the inactivity period for session termination
FTA_SSL.3 (optional)	Configuration of the inactivity period for session termination
FTA_TAB.1	Maintenance of the banner
FTA_TSE.1 (optional)	Management of session establishment conditions
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)

Assurance Activity:

The evaluator shall check the TSS in order to determine that it summarizes the management functions that are available.

The evaluator shall check the operational guidance in order to determine that it defines all of the management functions that can be performed against the TSF, how to perform them, and what they accomplish.

The evaluator shall test this capability by accessing the TOE and verifying that all of the defined management functions exist, that they can be performed in the prescribed

manner, and that they accomplish the documented capability.

FMT_SMR.1 Security Management Roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [***assignment: the authorized identified roles***].
Application Note:	*This Protection Profile uses the term Assignment Manager to refer to an individual who is authorized to define and manage identity and credential (and possibly object) attributes. This should be interpreted as a logical construct to reflect that individuals should be given this authority and not an explicit mandate that the TSF must refer to anyone with this authority by the term "Assignment Manager".*
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Application Note:	*An authorized and compatible Secure Configuration Product acting on behalf of a user may also be associated with a role.*
Dependencies:	FIA_UID.1 Timing of Authentication

Assurance Activity:

The evaluator shall review the TSS to determine the roles that are defined for the TOE. The evaluator shall also review the TSS to verify that the roles defined by this SFR are consistently referenced when discussion how management authorizations are determined.

The evaluator shall review the operational guidance in order to verify that it provides instructions on how to assign users to roles. If the TSF provides only a single role that is automatically assigned to all users, then the evaluator shall review the operational guidance to verify that this fact is asserted.

The evaluator shall test this capability by using the TOE in the manner prescribed by the operational guidance to associate different users with each of the available roles. If the TSF provides the capability to define additional roles, the evaluator shall create at least one new role and ensure that a user can be assigned to it. Since other assurance activities for management requirements involve the evaluator assuming different roles on

the TOE, it is possible that these testing activities will be addressed in the course of performing these other assurance activities.

6.1.7 Protection of the TSF

FPT_APW_EXT.1 Protection of Stored Credentials

Hierarchical to: No other components.

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

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

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

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

Dependencies: No dependencies.

Assurance Activity:

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

detailed in the TSS.

There are no operational guidance activities for this SFR.

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

FPT_SKP_EXT.1 Protection of Secret Key Parameters

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

Assurance Activity:

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

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

6.1.8 TOE Access (FTA)

Note: The SFRs in this family refer to user sessions for administrative users.

FTA_TAB.1 TOE Access Banner

Hierarchical to:	No other components.
FTA_TAB.1.1	*Refinement:* Before establishing a user session, the TSF shall display a *configurable* advisory warning message regarding unauthorized use of the TOE.
Dependencies:	No dependencies.

Assurance Activity:

The evaluator shall check the TSS in order to determine that it discusses the ability of the TSF to display a configurable banner prior to administrator authentication.

The evaluator shall review the operational guidance to determine how the TOE banner is displayed and configured.

If the banner is not displayed by default, the evaluator shall configure the TOE in accordance with the operational guidance in order to enable its display. The evaluator shall then attempt to access the TOE and verify that a TOE banner exists. If applicable, the evaluator will also attempt to use the functionality to modify the TOE access banner as per the standards defined in FMT_SMF.1 and verify that the TOE access banner is appropriately updated.

6.1.9 Trusted Paths/Channels (FTP)

FTP_ITC.1 Inter-TSF Trusted Channel

Hierarchical to:	No other components.
FTP_ITC.1.1	*Refinement:* The TSF shall *use [selection: [**assignment: cryptographic protocol(s) implemented via FCS-specified service**], [**assignment: unambiguously defined FIPS-compliant protocol implemented by a component in the operational environment**]] to* provide a *trusted* communication channel between itself and *authorized IT entities* that is logically distinct from other communication

channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

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

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

Application Note: *The ST author must fill out the assignment with all protected communications the TOE has with other ESM products (transfer of audit data, request for identity data, etc.). Note that transfer of authentication responses is not listed here because it is assumed that the trusted channel for this transmission is either initiated by the product providing the response or is the same channel initiated by the TSF that was used to issue the transfer of the initial challenge.*

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

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check the TSS in order to determine that the assignments were completed in a manner that is consistent with the guidance provided by the application note(s). The evaluator shall also check the TSS to see that it identifies the trusted channels that are established and the protocols that they use. If third-party cryptography is used, the evaluator shall check to ensure that the specific third-party products that are

used are identified along with the channel(s) that they are responsible for securing. The evaluator shall also check the TSS 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 used 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 check the operational guidance in order to determine the mechanism by which secure communications are enabled.

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.

FTP_TRP.1 Trusted Path

Hierarchical to:	No other components.
FTP_TRP.1.1	*Refinement:* The TSF shall *use [selection: [**assignment: cryptographic protocol(s) implemented via FCS-specified service**], [**assignment: unambiguously defined FIPS-compliant protocol implemented by a component in the operational environment**]] to* provide a communication path between itself and [remote] users that is logically distinct from other communication channels and provides assured identification of its end points and protection of the communicated data from [modification, disclosure].
FTP_TRP.1.2	The TSF shall permit [remote users] to initiate

communication via the trusted path.

FTP_TRP.1.3 *Refinement:* The TSF shall require the use of the trusted path for *initial user authentication, execution of management functions*.

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check the TSS to ensure that it identifies the protocol(s) used to establish the trusted path. If third-party cryptography is used, the evaluator shall check to ensure that the specific third-party products that are used are identified.

The evaluator shall check the operational guidance to verify that it discusses the methods by which users will interact with the TOE such as a web application via HTTPS. The evaluator shall also check the operational guidance to determine if it discusses the mechanism by which a trusted path to the TOE is established and what environmental components (if any) the TSF relies on to assist in this establishment.

The evaluator shall test this capability in a similar manner to the assurance activities for FTP_ITC.1. If data transmitted between the user and the TOE is obfuscated, the trusted path can be assumed to have been established.

6.1.10 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_ATD.1 This SFR is an unfulfilled dependency on FIA_USB.1. It has not been included because ESM_ICD.1 is expected to satisfy the dependency in the same manner.

FIA_UAU.1 This SFR is an unfulfilled dependency on FIA_AFL.1. ESM_EAU.2 satisfies this dependency by providing equivalent functionality.

FIA_UID.1 This SFR is an unfulfilled dependency on FMT_SMR.1. ESM_EID.2 satisfies this dependency by providing equivalent functionality.

FPT_STM.1	This SFR is an unfulfilled dependency on FAU_GEN.1. It has not been included because the TOE is not necessarily expected to include its own system clock. The ST author must examine the entire ESM under evaluation in order to determine the point of origin for system time. If the evaluation boundary is an entire ESM appliance that uses an internal system clock, FPT_STM.1 must be claimed. However, if the ESM relies on an environmental component such as a host operating system or NTP server, it is an acceptable alternative to represent accurate system time as an environmental objective.

6.2 Security Assurance Requirements

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

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

For each family, “Developer Notes” are provided on the developer action elements to clarify what, if any, additional documentation/activity needs to be provided by the developer. For the content/presentation and evaluator activity elements, additional assurance activities (to those already contained in Section 6.1) are described as a whole for the family, rather than for each element. Additionally, the assurance activities described in this section are complementary to those specified in Section 6.1.

The TOE security assurance requirements, summarized in Table 5, identify the management and evaluative activities required to address the threats identified in Section 8.2 of this PP. Section 6.3 provides a succinct justification for choosing the security assurance requirements in this section.

Table 5. TOE Security Assurance Requirements

Assurance Class	Assurance Components	Assurance Components Description
Development	ADV_FSP.1	Basic Functional Specification
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM Coverage
Tests	ATE_IND.1	Independent Testing – Conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability Survey

6.2.1 Class ADV: Development

For TOEs conforming to this PP, it is anticipated that the information about the TOE is contained in the guidance documentation available to the end user as well as the TOE Summary Specification (TSS) portion of the ST.[7] 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 Basic Functional Specification (ADV_FSP.1)

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

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

[7] 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.

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

Content and presentation elements:

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

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

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

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

Evaluator action elements:

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

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

Assurance Activity:

There are no specific assurance activities associated with these SARs. The functional specification documentation is provided to support the evaluation activities described for each SFR, and for other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because the there is insufficient interface information, then an adequate functional specification has not been provided. For example, if the TOE provides the capability to configure the key length for the encryption algorithm but fails to specify an interface to perform this function, then the assurance activity associated with FMT_SMF would fail.

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

6.2.2 Class AGD: Guidance Documentation

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

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

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

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

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

6.2.2.1 Operational User Guidance (AGD_OPE.1)

Developer action elements:

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

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

Content and presentation elements:

AGD_OPE.1.1C The operational user guidance shall describe, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings.

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

AGD_OPE.1.2C The operational user guidance shall describe, for each user role, how to use the available interfaces provided by the TOE in a secure manner.

AGD_OPE.1.3C The operational user guidance shall describe, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate.

AGD_OPE.1.4C The operational user guidance shall, for each user role, clearly present each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_OPE.1.5C The operational user guidance shall identify all possible modes of operation of the TOE (including operation following failure or operational error), their consequences and implications for maintaining secure operation.

AGD_OPE.1.6C The operational user guidance shall, for each user role, describe the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST.

AGD_OPE.1.7C The operational user guidance shall be clear and reasonable.

Evaluator action elements:

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

Assurance Activity:

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

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

6.2.2.2 Preparative Procedures (AGD_PRE.1)

Developer action elements:

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

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

Content and presentation elements:

AGD_ PRE.1.1C The preparative procedures shall describe all the steps necessary for secure acceptance of the delivered TOE in accordance with the developer's delivery procedures.

AGD_ PRE.1.2C The preparative procedures shall describe all the steps necessary for secure installation of the TOE and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST.

Evaluator action elements:

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

AGD_ PRE.1.2E The evaluator shall apply the preparative procedures to confirm that the TOE can be prepared securely for operation.

Assurance Activity:

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

6.2.3 Class ALC: Life Cycle Support

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

6.2.3.1 Labeling of the TOE (ALC_CMC.1)

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

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

Assurance Activity:

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

6.2.3.2 TOE CM Coverage (ALC_CMS.1)

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

Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

Assurance Activity:

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

6.2.4 Class ATE: Tests

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

6.2.4.1 Independent Testing - Conformance (ATE_IND.1)

Testing is performed to confirm the functionality described in the TSS as well as the administrative (including configuration and operation) documentation provided. The focus of the testing is to confirm that the requirements specified with each SFR are being met, although some additional testing is specified for SARs in section 6.2. 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 Activity:

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

testing requirement in the ST is covered.

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

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

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

6.2.5 Class AVA: Vulnerability Assessment

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

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

6.2.5.1 Vulnerability Survey (AVA_VAN.1)

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

AVA_VAN.1.3E The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

Assurance Activity:

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

be suitable and an appropriate justification would be formulated.

6.3 Rationale for Security Assurance Requirements

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

7 Security Problem Definition Rationale

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

Table 6. Assumptions, Environmental Objectives, and Rationale

Assumptions	Objectives	Rationale
A.CRYPTO (optional) – The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.	**OE.CRYPTO (optional) –** The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.	It is expected that vendors will typically rely on the usage of cryptographic primitives implemented in the Operational Environment to perform cryptographic protocols provided by the TOE. If the TOE provides its own cryptographic primitives, then this becomes an objective for the TOE rather than for the environment.
A.ENROLLMENT – There will be a defined enrollment process that confirms user identity before the assignment of credentials.	**OE.ENROLLMENT --** The Operational Environment will provide a defined enrollment process that confirms user identity before the assignment of credentials.	NIST SP 800-63 stresses the importance of having a process that confirms an individual's identity before assigning that individual credentials. This process is assumed to provide that confirmation.
A.ESM – The TOE will be able to establish connectivity to other ESM products in order to share security data.	**OE.MANAGEMENT** – The Operational Environment will provide an Authentication Server component that uses identity and credential data maintained by the TOE.	In order for the TOE to establish connection to other ESM products, these products must already be deployed in the Operational Environment. In particular, an Authentication Server component needs to be in place to consume the identity data provided by the TOE or else the TOE does not provide a benefit to the environment in which it is deployed. **If the TOE claims conformance to the Standard Protection Profile for**

Assumptions	Objectives	Rationale
		Enterprise Security Management Authentication Server, this objective is considered to be satisfied by the TSF as opposed to the Operational Environment.
A.FEDERATE – Third-party entities that exchange attribute data with the TOE are assumed to be trusted.	**OE.FEDERATE** – Data the TOE exchanges with trusted external entities is trusted.	If the TOE uses third-party entities (for example, another instance of the same product that is deployed in a different organization) for attribute exchange or validation such as in a federation, it is necessary to assume that these entities are trusted. They are likely to reside in different networks and so an administrator for the TOE will not be able to take direct action to ensure their security.
A.MANAGE – There will be one or more competent individuals assigned to install, configure, and operate the TOE.	**OE.ADMIN –** There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.	Assigning specific individuals to manage the TSF provides assurance that management activities are being carried out appropriately.
	OE.INSTALL – Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.	Assigning specific individuals to install the TOE provides assurance that it has been installed in a manner that is consistent with the evaluated configuration.
	OE.PERSON – Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.	Ensuring that administrative personnel have been vetted and trained helps reduce the risk that they will perform malicious or careless activity.
A.ROBUST (optional) – The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.	**OE.ROBUST (optional)** – The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.	The ESM deployment as a whole is expected to provide a login frustration mechanism that reduces the risk of a brute force authentication attack being used successfully against the TSF and defines allowable conditions for authentication (e.g. day, time, location). It is expected that if the TSF does not provide this mechanism, then it will receive this capability from elsewhere in the ESM

Assumptions	Objectives	Rationale
		deployment. **If the ST claims FIA_AFL.1, FIA_SOS.1, and FTA_TSE.1, the ST author must exclude this mapping because robust TOE authentication will be provided by the TSF.**
A.SYSTIME (optional) – The TOE will receive reliable time data from the Operational Environment.	**OE. SYSTIME (optional)** – The Operational Environment will provide reliable time data to the TOE.	The TSF is expected to use reliable time data in the creation of its audit records. If the TOE is a software-based product, then it is expected that the TSF will receive this time data from a source within the Operational Environment such as a system clock or NTP server. **If the ST claims FPT_STM.1, the ST author must exclude this mapping because system time functionality will be provided by the TSF.**

Table 7. Policies, Threats, Objectives, and Rationale

Policies and Threats	Objectives	Rationale
P.BANNER – The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.	**O.BANNER –** The TOE will display an advisory warning regarding use of the TOE.	**FTA_TAB.1** The requirement for the TOE to display a banner is sufficient to ensure that this policy is implemented.
T.ADMIN_ERROR – An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.	**O.MANAGE –** The TOE will provide Authentication Managers with the capability to manage the TSF.	**FMT_MOF.1** **FMT_MTD.1 (optional)** **FMT_SMF.1** By requiring authenticated users to have certain privileges in order to perform different management functions, the TSF can enforce separation of duties and limit the consequences of improper administrative behavior.
	OE.ADMIN – There will be one or more administrators of the	This objective requires the TOE to have designated

Policies and Threats	Objectives	Rationale
	Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.	administrators for the operation of the TOE. This provides some assurance that the TOE will be managed and configured consistently.
	OE.INSTALL – Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.	This objective reduces the threat of administrative error by ensuring that the TOE is installed in a manner that is consistent with the evaluated configuration.
	OE.PERSON – Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.	This objective reduces the threat of administrative error by ensuring that administrators have been properly vetted and trained prior to having access to the TOE.
T.EAVES – A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.	**O.CRYPTO –** The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.	**FCS_CKM.1 (optional)** **FCS_CKM_EXT.4 (optional)** **FCS_COP.1(1) (optional)** **FCS_COP.1(2) (optional)** **FCS_COP.1(3) (optional)** **FCS_COP.1(4) (optional)** **FCS_RBG_EXT.1 (optional)** By providing cryptographic primitives, the TOE is able to establish and maintain trusted channels and paths. **If the ST does not claim the cryptographic requirements listed above, the ST author must claim A.CRYPTO and OE.CRYPTO and map them based on Table 6 and Table 7 in this PP.**
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	**FCS_HTTPS_EXT.1 (optional)** **FCS_IPSEC_EXT.1 (optional)** **FCS_SSH_EXT.1 (optional)** **FCS_TLS_EXT.1 (optional)** **FPT_SKP_EXT.1** **FTP_ITC.1** **FTP_TRP.1** Implementation of trusted channels and paths ensures that communications are

Policies and Threats	Objectives	Rationale
		protected from eavesdropping.
	O.EAVES – The TOE will either leverage a third-party cryptographic suite or contain the ability to use cryptographic algorithms to secure the communication channels to and from itself.	**FTP_ITC.1** **FTP_TRP.1** Establishing trusted channels and paths for external communications will provide the TOE with reasonable assurance that transmitted data will not be disclosed to or modified by an unauthorized party.
	OE.CRYPTO – The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.	If the Operational Environment implements cryptographic primitives at the request of the TOE, the TSF is able to establish and maintain trusted channels and paths when needed. **If the ST claims the cryptographic requirements mapped to O.CRYPTO above, the ST author must exclude this objective from the mapping.**
T.FALSIFY – A malicious user may falsify the TOE's identity and transmit false data that purports to originate from the TOE to provide invalid data to the ESM deployment.	**O.CRYPTO –** The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.	**FCS_CKM.1 (optional)** **FCS_CKM_EXT.4 (optional)** **FCS_COP.1(1) (optional)** **FCS_COP.1(2) (optional)** **FCS_COP.1(3) (optional)** **FCS_COP.1(4) (optional)** **FCS_RBG_EXT.1 (optional)** By providing cryptographic primitives, the TOE is able to establish and maintain trusted channels and paths. **If the ST does not claim the cryptographic requirements listed above, the ST author must claim A.CRYPTO and OE.CRYPTO and map them based on Table 6 and Table 7 in this PP.**
	O.INTEGRITY – The TOE will provide the ability to assert the integrity of identity, credential, or authorization data.	**FTP_ITC.1** If the TSF is able to transmit data in such a way that its integrity can be validated, the risk of it being altered in transit by a malicious agent is

Policies and Threats	Objectives	Rationale
		reduced.
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	**FCS_HTTPS_EXT.1 (optional)** **FCS_IPSEC_EXT.1 (optional)** **FCS_SSH_EXT.1 (optional)** **FCS_TLS_EXT.1 (optional)** **FPT_SKP_EXT.1** **FTP_ITC.1** **FTP_TRP.1** Implementation of a trusted channel between the TOE and other ESM products ensures that the TOE will securely assert its identity when transmitting data over this channel.
	O.SELFID – The TOE will be able to confirm its identity to the ESM deployment upon sending identity, credential, or authorization data to dependent machines within the ESM deployment.	**ESM_EID.2** **FTP_ITC.1** By establishing a trusted channel and providing a means for the TSF to validate its own identity to other ESM components, the source of transmitted data can be trusted and the risk of spoofing the TOE is diminished.
	OE.CRYPTO – The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.	If the Operational Environment implements cryptographic primitives at the request of the TOE, the TSF is able to establish and maintain trusted channels and paths when needed. **If the ST claims the cryptographic requirements mapped to O.CRYPTO above, the ST author must exclude this objective from the mapping.**
T.FORGE – A malicious user may falsify the identity of an external entity in order to illicitly request to receive security attribute data or to provide invalid data to the TOE.	**O.ACCESSID –** The TOE will include the ability to validate the identity of other ESM products prior to distributing data to them.	**FTP_ITC.1** By establishing a trusted channel that provides identification of end points, the TSF is able to assert that any data it may be transmitting will only be going to valid ESM components.

Policies and Threats	Objectives	Rationale
	O.CRYPTO – The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.	**FCS_CKM.1 (optional)** **FCS_CKM_EXT.4 (optional)** **FCS_COP.1(1) (optional)** **FCS_COP.1(2) (optional)** **FCS_COP.1(3) (optional)** **FCS_COP.1(4) (optional)** **FCS_RBG_EXT.1 (optional)** By providing cryptographic primitives, the TOE is able to establish and maintain trusted channels and paths. **If the ST does not claim the cryptographic requirements listed above, the ST author must claim A.CRYPTO and OE.CRYPTO and map them based on Table 6 and Table 7 in this PP.**
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	**FCS_HTTPS_EXT.1 (optional)** **FCS_IPSEC_EXT.1 (optional)** **FCS_SSH_EXT.1 (optional)** **FCS_TLS_EXT.1 (optional)** **FPT_SKP_EXT.1** **FTP_ITC.1** **FTP_TRP.1** Implementation of a trusted channel between the TOE and other ESM products ensures that the TOE will have a means to verify the identity of external entities that access it.
	OE.CRYPTO – The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.	If the Operational Environment implements cryptographic primitives at the request of the TOE, the TSF is able to establish and maintain trusted channels and paths when needed. **If the ST claims the cryptographic requirements mapped to O.CRYPTO above, the ST author must exclude this objective from the mapping.**
	OE.FEDERATE – Data the TOE	In the case where the TOE

Policies and Threats	Objectives	Rationale
	exchanges with trusted external entities is trusted.	uses external attribute authorities to provide or validate certain attribute data it maintains, the authenticity of these entities must be trusted in order for the data they produce to be trusted.
T. INSUFFATR – An Assignment Manager may be incapable of using the TOE to define identities, credentials, and attributes in sufficient detail to facilitate authorization and access control, causing other ESM products to behave in a manner that allows illegitimate activity or prohibits legitimate activity.	**O.IDENT** – The TOE will provide the Assignment Managers with the ability to define detailed identity and credential attributes.	**ESM_ICD.1** **ESM_ATD.1 (optional)** The Identity and Credential Management product must provide the ability to define subject (and optionally object) attributes. These attributes must be sufficient to support use by other ESM products and must be sufficient to support policies defined by Policy Management components. This will ensure that strong policies are created that are capable of using the full set of access control functions of compatible products.
T.MASK – A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.	**O.AUDIT –** The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.	**FAU_GEN.1** **FAU_SEL.1 (optional)** **FAU_STG_EXT.1** **FPT_STM.1 (optional)** If security relevant events are logged and backed up, an attacker will have difficulty performing actions for which they are not accountable. This allows an appropriate authority to be able to review the recorded data and acquire information about attacks on the TOE. **If the ST does not claim FPT_STM.1, the ST author must claim A.SYSTIME and OE.SYSTIME and map them based on Table 6 and Table 7 in this PP.**
	OE.SYSTIME – The TOE will receive reliable time data from the Operational Environment.	This objective helps ensure the accuracy of audit data by providing an accurate record of the timing and sequence of activities which were

Policies and Threats	Objectives	Rationale
		performed against the TOE. **If the ST claims FPT_STM.1, the ST author must exclude this objective from the mapping.**
T.RAWCRED -- A malicious user may attempt to access stored credential data directly, in order to obtain credentials that may be replayed to impersonate another user.	**O.PROTCRED --** The TOE will be able to protect stored credentials.	**FPT_APW_EXT.1** The Identity and Credential Management Product must protect stored credentials such that they cannot be accessed in their raw, replayable form.
T.UNAUTH – A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.	**O.AUTH –** The TOE will provide a mechanism to securely validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.	**ESM_EAU.2** **ESM_EID.2** **FIA_USB.1** **FMT_SMR.1** **FTP_TRP.1** If the TOE requires all TSF-mediated activites to be performed following authentication via a trusted path and a user is bound to a defined role during authentication, an attacker will be unable to perform unauthenticated actions against the TSF.
	O.CRYPTO – The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.	**FCS_CKM.1 (optional)** **FCS_CKM_EXT.4 (optional)** **FCS_COP.1(1) (optional)** **FCS_COP.1(2) (optional)** **FCS_COP.1(3) (optional)** **FCS_COP.1(4) (optional)** **FCS_RBG_EXT.1 (optional)** By providing cryptographic primitives, the TOE is able to establish and maintain trusted channels and paths. **If the ST does not claim the cryptographic requirements listed above, the ST author must claim A.CRYPTO and OE.CRYPTO and map them based on Table 6 and Table 7 in this PP.**
	O.MANAGE – The TOE will provide Authentication Managers with the capability to manage the	**FMT_MOF.1** **FMT_MTD.1 (optional)**

Policies and Threats	Objectives	Rationale
	TSF.	**FMT_SMF.1** By requiring authenticated users to have certain privileges in order to perform different management functions, the TSF can enforce separation of duties and limit the consequences of improper administrative behavior..
	O.PROTCOMMS – The TOE will provide protected communication channels for administrators, other parts of a distributed TOE, and authorized IT entities.	**FCS_HTTPS_EXT.1 (optional)** **FCS_IPSEC_EXT.1 (optional)** **FCS_SSH_EXT.1 (optional)** **FCS_TLS_EXT.1 (optional)** **FTP_ITC.1** **FTP_TRP.1** By implementing cryptographic protocols, the TOE is able to prevent the manipulation of data in transit that could lead to unauthorized administration.
	OE.CRYPTO – The Operational Environment will provide cryptographic primitives that can be used by the TOE to provide services such as ensuring the confidentiality and integrity of communications.	If the Operational Environment implements cryptographic primitives at the request of the TOE, the TSF is able to establish and maintain trusted channels and paths when needed. **If the ST claims the cryptographic requirements mapped to O.CRYPTO above, the ST author must exclude this objective from the mapping.**
T.WEAKIA - A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.	**O.ROBUST** - The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.	**FIA_AFL.1 (optional)** **FIA_SOS.1 (optional)** **FTA_SSL_EXT.1 (optional)** **FTA_SSL.3 (optional)** **FTA_SSL.4 (optional)** **FTA_TSE.1 (optional)** If the TOE applies a strength of secrets policy to user passwords, it decreases the likelihood that an individual guess will successfully identify the password. If the TOE applies authentication

Policies and Threats	Objectives	Rationale
		failure handling, it decreases the number of individual guesses an attacker can make. If the TOE provides session denial functionality, it rejects login attempts made during unacceptable circumstances. If the TOE performs session locking and termination due to administrator inactivity, it decreases the likelihood that an unattended session is hijacked. **If the ST does not claim FIA_AFL.1, FIA_SOS.1, and FTA_TSE.1, the ST author must claim A.ROBUST and OE.ROBUST and map them based on Table 6 and Table 7 in this PP.**
	OE.ROBUST – The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.	This objective helps ensure that administrative access to the TOE is robust by externally defining strength of secrets, authentication failure, and session denial functionality that is enforced by the TSF. **If the ST claims FIA_AFL.1, FIA_SOS.1, and FTA_TSE.1 in a manner that applies to administrative authentication to the TSF, the ST author must exclude this objective from the mapping.**

8 Security Problem Definition

The following sections list the assumptions, threats, objectives, and organizational security policies 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 8. Connectivity Assumptions

Assumption Name	Assumption Definition
A.CRYPTO (optional)	The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
A.ESM	The TOE will be able to establish connectivity to other ESM products in order to share security data.
A.FEDERATE	Third-party entities that exchange attribute data with the TOE are assumed to be trusted.
A.ROBUST (optional)	The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
A.SYSTIME (optional)	The TOE will receive reliable time data from the Operational Environment.

8.1.2 Physical Assumptions

No physical assumptions are prescribed in this Protection Profile.

8.1.3 Personnel Assumptions

Table 9. Personnel Assumptions

Assumption Name	Assumption Definition
A.MANAGE	There will be one or more competent individuals assigned to install, configure, and operate the TOE.
A.ENROLLMENT	There will be a defined enrollment process that confirms user identity before the assignment of credentials.

8.2 Threats

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 10. Threats

Threat Name	Threat Definition
T.ADMIN_ERROR	An administrator may unintentionally install or configure the TOE incorrectly, resulting in ineffective security mechanisms.
T.EAVES	A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
T.FALSIFY	A malicious user may falsify the TOE's identity and transmit false data that purports to originate from the TOE to provide invalid data to the ESM deployment.
T.FORGE	A malicious user may falsify the identity of an external entity in order to illicitly request to receive security attribute data or to provide invalid data to the TOE.
T. INSUFFATR	An Assignment Manager may be incapable of using the TOE to define identities, credentials, and attributes in sufficient detail to facilitate authorization and access control, causing other ESM products to behave in a manner that allows illegitimate activity or prohibits legitimate activity.
T.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.RAWCRED	A malicious user may attempt to access stored credential data directly, in order to obtain credentials that may be replayed to impersonate another user.
T.UNAUTH	A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.
T.WEAKIA	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.

8.3 Organizational Security Policies

Listed below are the applicable organizational security policies for the TOE.

Table 11. Organizational Security Policies

Assumption Name	Assumption Definition

Assumption Name	Assumption Definition
P.BANNER[8]	The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

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. Section 7 describes how these objectives relate to the Security Functional Requirements defined for this PP.

Table 12. Security Objectives for the TOE

Objective	TOE Security Objective Definition
O.ACCESSID	The TOE will include the ability to validate the identity of other ESM products prior to distributing data to them.
O.AUDIT	The TOE will provide measures for generating and recording security relevant events that will detect access attempts to TOE-protected resources by users.
O.AUTH	The TOE will provide a mechanism to validate requested authentication attempts and to determine the extent to which any validated subject is able to interact with the TSF.
O.BANNER	The TOE will display an advisory warning regarding use of the TOE.
O.CRYPTO (optional)	The TOE will provide cryptographic primitives that can be used to provide services such as ensuring the confidentiality and integrity of communications.
O.EXPORT	The TOE will provide the ability to transmit user attribute data to trusted IT products using secure channels.
O.IDENT	The TOE will provide the Assignment Managers with the ability to define detailed identity and credential attributes.
O.INTEGRITY	The TOE will provide the ability to assert the integrity of identity, credential, or authorization data.
O.MANAGE	The TOE will provide Assignment Managers with the capability to manage the TSF.
O.PROTCOMMS	The TOE will provide protected communication channels for

[8] This policy is based on the control AC-8 in NIST SP 800-53.

Objective	TOE Security Objective Definition
	administrators, other parts of a distributed TOE, and authorized IT entities.
O.PROTCRED	The TOE will be able to protect stored credentials.
O.ROBUST (optional)	The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
O.SELFID	The TOE will be able to confirm its identity to the ESM deployment upon sending identity, credential, or authorization data to dependent machines within the ESM deployment.

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 13. Security Objectives for the Operational Environment

Objective	Environmental Security Objective Definition
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.
OE.CRYPTO (optional)	The Operational Environment will provide cryptographic mechanisms that are used to ensure the confidentiality and integrity of communications.
OE.ENROLLMENT	The Operational Environment will provide a defined enrollment process that confirms user identity before the assignment of credentials.
OE.FEDERATE	Data the TOE exchanges with trusted external entities is trusted.
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
OE.MANAGEMENT	The Operational Environment will provide an Authentication Server component that uses identity and credential data maintained by the TOE.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
OE.ROBUST (optional)	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
OE.SYSTIME (optional)	The Operational Environment will provide reliable time data to the TOE.

Appendix A - Supporting Tables and References

A.1 References

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

[2] Enterprise Security Management Technical Community, Standard Protection Profile for Enterprise Security Management Access Control, version 2.1, June 13, 2013

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

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

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

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

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

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

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

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

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

[12] National Institute of Standards and Technology, FIPS PUB 197 Advanced

Encryption Standard, November 2001

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

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

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

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

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

[18] National Institute of Standards and Technology, 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

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

A.2 Acronyms

Table 14. Acronyms and Definitions

Term	Definition
CC	Common Criteria
COI	Communities of Interest
CNSS	Committee on National Security Systems
ESM	Enterprise Security Management
FIPS	Federal Information Processing Standard
HTTP	Hypertext Transfer Protocol

Term	Definition
I&C	Identity and Credential
IKE	Internet Key Exchange
IP	Internet Protocol
IT	Information Technology
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NTP	Network Time Protocol
OE	Operational Environment
OS	Operating System
OSP	Organizational Security Policy
PM	Policy Management
PP	Protection Profile
RFC	Request for Comment
SA	Security Association
SAML	Security Assertion Markup Language
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function
TSFI	TOE Security Function Interface
VPN	Virtual Private Network

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

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

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

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

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

Table 15. NIST 800-53 Requirements Compatibility

SFR		NIST 800-53 Control[9]		Comments and Observations
ESM_ATD.1 (optional)	**Attribute Definition** Object Attribute Definition	AC-3	**Access Enforcement**	**Partial.** This control defines the object attributes critical to policy enforcement. The assignment should be completed to be consistent with the policy, and the applicability of this enhancement depends on the policy defined.
		AC-3(3)	**Access Enforcement** | Mandatory Access Control	**Partial.** This control defines the object attributes critical to policy enforcement. The assignment should be completed to be consistent with the policy, and the applicability of this enhancement

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

SFR		NIST 800-53 Control[9]		Comments and Observations
				depends on the policy defined. **Note:** Revision 3 AC-3(3) is used for both mandatory access control and role-based access control.
		AC-3(4)	**Access Enforcement** | Discretionary Access Control	**Partial.** This control defines the object attributes critical to policy enforcement. The assignment should be completed to be consistent with the policy, and the applicability of this enhancement depends on the policy defined.
		AC-3(7)	**Access Enforcement** | Role-Based Access Control	**Partial.** This control defines the object attributes critical to policy enforcement. The assignment should be completed to be consistent with the policy, and the applicability of this enhancement depends on the policy defined. (Revision 4 only)
ESM_EAU.2	**Enterprise Authentication** Reliance on Enterprise Authentication	IA-2	**Identification and Authentication (Organizational Users)**	**Partial.** This addresses the authentication of organizational users.
ESM_EID.2	**Enterprise Identification** Reliance on Enterprise Identification	IA-2	**Identification and Authentication (Organizational Users)**	**Partial.** This addresses the identification of organizational users.
ESM_ICD.1	**Identity and Credential Definition** Identity and Credential Definition			**No Mapping.** There appears to be no control corresponding to this. The SFR defines the identity and/or credential data for enterprise users that are defined by the TSF.
ESM_ICT.1	**Identity and Credential Transmission** Identity and Credential Transmission			**No Mapping.** There appears to be no control corresponding to this. The SFR defines the conditions for transmission of defined identity and/or credential data.
FAU_STG_EXT.1	**Security Audit Event Storage** External Audit Trail Storage	AU-9	**Protection of Audit Information**	**Partial.** The SFR addresses the basic intent of the control, although the repository/entity to which audit data is written must in turn prevent unauthorized modification of that data. However, the control not only protects the trail, but audit tools (that are not covered by the SFR).
FCS_CKM.1 (optional)	**Cryptographic Key Manageme**	SC-12	**Cryptographic Key Establishment and Management**	**Partial.** The SFR addresses one of the aspects of the 800-53 control. The assignments for standards and protocols need to

SFR		NIST 800-53 Control[9]		Comments and Observations
	nt Cryptographic Key Generation			be compared against required enhancements.
		Note: In Revision 3, the NIST 800-53 controls made no distinction between the various aspects of key management (generation, distribution, access, and destruction).		
FCS_CKM_EXT.4 (optional)	Cryptographic Key Management Cryptographic Key Destruction	SC-12	**Cryptographic Key Establishment and Management**	**Partial.** The SFR addresses one of the aspects of the 800-53 control. The assignments for standards and protocols need to be compared against required enhancements.
		Note: In Revision 3, the NIST 800-53 controls made no distinction between the various aspects of key management (generation, distribution, access, and destruction).		
FCS_HTTPS_EXT.1 (optional)	HTTPS HTTPS	SC-8	**Transmission Confidentiality and Integrity**	**Partial.** The ability of the TOE to encrypt communications ensures the confidentiality and integrity of data and transit. Physical protection of this data is defined by the Operational Environment.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection	**Partial.** This addresses the requirement to use cryptography.
		SC-13	**Cryptographic Protection**	**Partial.** This addresses the requirement to use cryptography; the assignment in the control should correspond with the type of crypto selected. For US evaluations, SC-13(1) may also apply.
		Note: In Revision 3, SC-9 and SC-9(1) are also applicable. Revision 3 distinguished between transmission integrity (SC-8) and transmission confidentiality (SC-9). Revision 4 combined SC-8 and SC-9 into a single control with assignments providing the type of protection.		
FCS_IPSEC_EXT.1 (optional)	IPSEC IPSEC	SC-8	**Transmission Confidentiality and Integrity**	**Partial.** The ability of the TOE to encrypt communications ensures the confidentiality and integrity of data and transit. Physical protection of this data is defined by the Operational Environment.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection	**Partial.** This addresses the requirement to use cryptography.
		SC-13	**Cryptographic Protection**	**Partial.** This addresses the requirement to use cryptography; the assignment in the control should correspond with the type of crypto selected. For US evaluations, SC-13(1) may also apply.
		Note: In Revision 3, SC-9 and SC-9(1) are also applicable. Revision 3 distinguished between transmission integrity (SC-8) and transmission confidentiality (SC-9). Revision 4 combined SC-8 and SC-9 into a single control with assignments providing the type of protection.		

SFR		NIST 800-53 Control[9]		Comments and Observations
FCS_RBG_EXT.1 (optional)	**Random Bit Generation** Random Bit Generation	SC-13	**Cryptographic Protection** (Revision 4 only)	**Partial.** The assignment in the control should be completed to address the random number and entropy quality requirements.
		Note: In Revision 3, there was no provision within SC-13 to specify the random number generator quality requirements.		
FCS_SSH_EXT.1 (optional)	**SSH** SSH	SC-8	**Transmission Confidentiality and Integrity**	**Partial.** The ability of the TOE to encrypt communications ensures the confidentiality and integrity of data and transit. Physical protection of this data is defined by the Operational Environment.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection	**Partial.** This addresses the requirement to use cryptography.
		SC-13	**Cryptographic Protection**	**Partial.** This addresses the requirement to use cryptography; the assignment in the control should correspond with the type of crypto selected. For US evaluations, SC-13(1) may also apply.
		Note: In Revision 3, SC-9 and SC-9(1) are also applicable. Revision 3 distinguished between transmission integrity (SC-8) and transmission confidentiality (SC-9). Revision 4 combined SC-8 and SC-9 into a single control with assignments providing the type of protection.		
FCS_TLS_EXT.1 (optional)	**TLS** TLS	SC-8	**Transmission Confidentiality and Integrity**	**Partial.** The ability of the TOE to encrypt communications ensures the confidentiality and integrity of data and transit. Physical protection of this data is defined by the Operational Environment.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection	**Partial.** This addresses the requirement to use cryptography.
		SC-13	**Cryptographic Protection**	**Partial.** This addresses the requirement to use cryptography; the assignment in the control should correspond with the type of crypto selected. For US evaluations, SC-13(1) may also apply.
		Note: In Revision 3, SC-9 and SC-9(1) are also applicable. Revision 3 distinguished between transmission integrity (SC-8) and transmission confidentiality (SC-9). Revision 4 combined SC-8 and SC-9 into a single control with assignments providing the type of protection.		
FPT_APW_EXT.1	**Protection of the TSF** Protection of Stored Credentials	IA-5	**Authenticator Management**	**Partial**. Addresses item h) in the control: Protecting authenticator content from unauthorized disclosure and modification
FMT_MTD.1 (optional)	**Management of TSF**	SI-9	**Information Input Restrictions** | Restricts ability to input information to	**Partial.** The SFR would seem to imply this control, although the

SFR		NIST 800-53 Control[9]		Comments and Observations
	Data Management of TSF Data		authorized persons (Revision 3 only)	SFR is much more specific.
		Note: SI-9 was withdrawn in Revision 4, and its capabilities incorporated into AC-2 (Account Management), AC-3 (Access Enforcement), AC-5 (Separation of Duties), and AC-6 (Least Privilege).		
FPT_APW_EXT.1	**Protection of Stored Credentials** Protection of Stored Credentials	IA-5	**Authenticator Management**	**Partial**. This SFR addresses the portion of the control that requires authentication data to be protected from unauthorized disclosure and modification.
		IA-5(1)	**Authenticator Management** | Password-Based Authentication	This addresses the portion of the control that requires passwords to be stored obscured.
FPT_SKP_EXT.1	**Protection of Secret Key Parameters** Protection of Secret Key Parameters	IA-5	**Authenticator Management**	**Partial**. This SFR addresses the portion of the control that requires authentication data to be protected from unauthorized disclosure and modification.
		SC-12	**Cryptographic Key Establishment and Management**	**Partial**. This SFR addresses the portion of the control that discusses storage of keys.
FTA_SSL_EXT.1 (optional)	**Session Locking and Termination** TSF-Initiated Session Locking	AC-11	**Session Lock**	**Partial.** FTA_SSL_EXT.1 provides the system-initiated session lock.
		AC-11(1)	**Session Lock** | With screen saver	**Full.** FTA_SSL_EXT.1 provides the system-initiated session lock.

Appendix C - Architectural Variations and Additional Requirements

C.1 Object Attribute Data

At minimum, this Protection Profile requires a conformant TOE to be able to define and maintain subject attribute data. However, the ESM as a whole also requires the capability to define and maintain object attribute data. The notion of ESM access control is predicated on a subject with some set of attributes requesting an operation against an object with its own set of attributes. A policy will determine what actions should be taken when the operation, based on the two sets of attributes, is attempted.

The ESM must therefore include the capability to define and maintain both subject and object attribute data. It is considered to be an optional component of both this Protection Profile and the Standard Protection Profile for ESM Policy Management. If a TOE claiming conformance to this PP does not include this capability, then the ST author must indicate the sources of authoritative attribute data in the Operational Environment.

If this capability is provided, the following SFR must be included in the ST:

C.1.1 ESM_ATD.1 Object Attribute Definition

Hierarchical to:	No other components.
ESM_ATD.1.1	The TSF shall maintain the following list of security attributes belonging to individual objects: [***assignment: list of object security attributes***].
Application Note:	*Object security attributes refer to attributes that may ultimately factor into an access control decision but are not associated with either a user or an access control policy. A TOE that defines access control policies for multi-level security may need to use defined security labels that can be associated with resources in order for the policy to be applicable to those resources.*
ESM_ATD.1.2	The TSF shall be able to associate security attributes with individual objects.
Dependencies:	No dependencies.

Assurance Activity:

The evaluator shall check the TSS to ensure that it describes the object attributes that are defined by the TOE and the purpose for their definition.

The evaluator shall check the operational guidance to ensure that it provides instructions on how to define and configure the object attributes.

The evaluator shall test this capability by using a Policy Management product to create an access control policy that uses the defined attributes and having an Access Control product consume it. They shall then perform actions that will be allowed by the Access Control product and actions that will be denied by the Access Control product based on the object attributes that were associated with the policy.

C.2 Password Policy Definition

The TOE is not required to define a password policy; this capability is typically expected to be associated with Identity and Credential Management products. However, it is possible that the TSF defines a configurable password policy. For example, if the TOE allows for user self-service password changes (see Appendix C.5), a configurable password policy may govern allowable changes independent of the Operational Environment. If this is the case, the following requirement must be claimed:

C.2.1 FIA_SOS.1 Verification of Secrets

Hierarchical to: No other components.

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet the following:

a) For environmental password-based authentication, the following rules apply:

1. Passwords shall be able to be composed of a subset of the following character sets: [assignment: list of character sets that are supported by the TSF for password entry] that include the following values [assignment: list of the supported characters for each supported character set]; and

Application Note: *For the English character set, the types of characters are expected to include the 26 uppercase letters, 26 lowercase letters, 10 numbers, and 10 special characters "!", "@", "#", "$", "%", "^", "&", "*", "(", and ")". If non-English character sets are supported by the TOE, the ST author must specify the supported character sets along with the allowable character space of each sub-category of those sets.*

2. Minimum password length shall settable by an administrator, and support passwords of 16 characters or greater; and

Application Note: *The number of password combinations based on the minimum password length and the character space of the password must exceed 10^{14}. This is approximately equivalent to an English password using a character set of 72 that has a minimum length of 8 characters.*

3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and

4. Passwords shall have a maximum lifetime, configurable by an administrator; and

5. New passwords shall contain a minimum of an administrator-specified number of character changes from the previous password; and

6. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based authentication, the following rules apply:

1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}.

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check the TSS in order to verify that it discusses the TOE's strength of secrets capability to a level of detail that is consistent with the SFR.

The evaluator shall check the operational guidance in order to verify that it provides information to administrators about the TOE's enforcement of password composition, reuse, and aging or of a non-password-based credential. If the TOE does not support password-based credentials, the evaluator shall check to verify that the operational guidance provides information about the credential that is used by the TSF and how it is supplied to the TOE.

The evaluator shall also check the operational guidance to verify that it discusses the aspects of the strength of secrets policy that can be configured and what steps an administrator needs to perform in order to configure it.

The evaluator shall test this capability in the following manner:

- *If password-based authentication is supported, the evaluator shall supply valid and invalid passwords in order to verify that the length and composition requirements function as described in the TSS. The evaluator shall test the password aging requirements by setting a password and observing that it expires after the appropriate length of time. The evaluator shall test reuse requirements by providing a series of valid and invalid changed passwords, first to test that a changed password must be sufficiently distinct and then to test that passwords cannot be reused within a certain number.*
- *If password-based authentication is supported, the evaluator shall perform the steps described in the operational guidance to alter each configurable parameter of the password policy and to supply passwords before and after the parameter is altered to verify that the change appropriately took effect.*
- *If non-password-based authentication is supported, the evaluator shall follow the steps described in the operational guidance to create a credential. The evaluator shall then observe that providing that credential to the TOE allows access and an invalid credential is rejected. An example of this is fingerprint biometrics. In this case, the evaluator would associate a user account with their own fingerprint. They would then log on to their account by providing their fingerprint and then observe failure when someone else tries to provide their fingerprint instead.*

If only non-password-based authentication is supported, it is sufficient for the evaluator to justify the unlikelihood of brute force guessing using evidence provided by the vendor and/or published research.

C.3 Selectable Auditing

The TOE is not required to perform selectable auditing. However, in some cases, the set of events audited by the TSF may be configurable.

If this is the case, the following activities must be performed:

- FAU_SEL.1 as described below must be claimed
- The entity that is responsible for performing this function (either the TSF or an external product such as Secure Configuration Management) must be identified
- The communications between the TOE and this entity, if remote, must be protected by a trusted channel as defined in FTP_ITC.1
- If the TSF is configured by an external entity, the role this entity assumes must be identified in FMT_SMR.1 and the process by which the entity is bound to this role must be identified in FIA_USB.1

C.3.1 FAU_SEL.1 Selective Audit

Hierarchical to: No other components.

FAU_SEL.1.1 *Refinement:* The TSF shall be able to select the set of events to be audited from the set of all auditable events *from [selection: [**assignment: ESM product**] in the Operational Environment, local definition]* 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 ST author must indicate how the set of auditable events is defined. For example, it may be configurable by an administrator who is using the TSF or it may be defined in an auditing policy that is sent to the TOE from a remote*

trusted IT entity for consumption.

Dependencies: FAU_GEN.1 Audit Data Generation

FMT_MTD.1 Management of TSF Data

Assurance Activity:

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

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

The evaluator shall test this capability by using all allowable vectors that are defined in FMT_MOF.1 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.

C.4 Session Management

The TSF is not required to define session locking, unlocking, and termination capabilities. However, if the TOE does perform these functions, the ST author may include the following requirements:

C.4.1 FTA_SSL_EXT.1 TSF-initiated Session Locking

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.

Assurance Activity:

The evaluator shall check the TSS in order to determine that it discusses how inactivity is handled for local administrative sessions.

The evaluator shall check the operational guidance in order to determine that it describes what happens when a local interactive session exceeds its idle time threshold. The evaluator shall also check the operational guidance in order to verify that it describes how to set the idle time threshold and, if applicable, how to configure the behavior the TSF performs when the idle time threshold is exceeded.

The evaluator shall test this capability by following 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.

C.4.2 FTA_SSL.3 TSF-initiated Termination

Hierarchical to: No other components.

FTA_SSL.3.1 *Refinement:* 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 check the TSS in order to determine that it discusses how inactivity is handled for remote administrative sessions.

The evaluator shall also check the operational guidance in order to verify that it describes how to set the idle time threshold.

The evaluator shall test this capability by following 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.

C.4.3 FTA_SSL.4 User-initiated Termination

Hierarchical to:	No other components.
FTA_SSL.4.1	*Refinement:* The TSF shall allow *Administrator*-initiated termination of the *Administrato*r's own interactive session.
Dependencies:	No dependencies.

Assurance Activity:

The evaluator shall check the TSS in order to determine that it discusses the ability of an administrator to terminate their own session.

The evaluator shall check the operational guidance in order to verify that it describes how an administrator can terminate their own administrative session for each administrative interface that is supported by the TOE.

The evaluator shall test this capability by establishing a session with the TOE using an administrative interface. The evaluator then follows the operational guidance to exit or log off of the session and observes that the session has been terminated. If applicable, the evaluator shall repeat this test for each administrative interface that is supported by the TOE.

C.5 Management of Environmental Authentication Data

In some cases, it is expected that the TOE will provide the ability to manage attributes that are authoritatively defined by an Identity and Credential Management product. For

example, a self-service option may allow the TOE to interface with an Identity and Credential Management product so that a user can change their password. In this situation, the ST author may claim the following requirement:

C.5.1 FMT_MTD.1 Management of TSF Data

Hierarchical to:	No other components.
FMT_MTD.1.1	The TSF shall restrict the ability to [selection: change_default, query, modify, delete, clear, **[*assignment: other operations***]] the [***assignment: list of authentication data***] to **[*assignment: the authorized identified roles***].
Application Note:	*Authentication data can be stored in a repository that is external to the TSF. For example, the TSF may facilitate user self-service password changes that are stored in an environmental LDAP server.*
Dependencies:	FMT_SMR.1 Security Roles FMT_SMF.1 Specification of Management Functions

Assurance Activity:

The evaluator shall review the TSS in order to determine the repository in which the authentication data used by the TOE is stored. The evaluator shall also determine how communications with this repository is secured.

The evaluator shall review the operational guidance in order to determine that it includes the data that can be managed and who is able to manage this data. This can be separated over multiple roles to distinguish between user administration and self-service; for example, both a Security Administrator and a specific user may be able to modify that user's own password.

The evaluator shall test this capability by performing the identified management activities with authorized roles in order to determine that they are allowed. The evaluator shall also attempt to perform these activities with unauthorized roles in order to determine that they are not allowed. Finally, the evaluator shall verify that communications between the TSF and the authentication data repository are secured by repeating the testing for FTP_ITC.1 over the interface between the two components.

C.6 Timestamps

This Protection Profile was written under the assumption that timestamps would be provided by the Operational Environment. If the TOE is implemented as an appliance, the timestamp function may be internal to the TOE. If that is the case, the following SFR must be included:

C.6.1 FPT_STM.1 Reliable Time Stamps

Hierarchical to:	No other components.
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps for its own use.
Dependencies:	No dependencies.

Assurance Activity:

The evaluator shall check the TSS in order to determine that it discusses the TOE's inclusion of a system clock.

The evaluator examines the operational guidance to ensure it instructs the administrator how to set the time. If the TOE supports the use of an NTP server, the operational guidance instructs how a communication path is established between the TOE and the NTP server, and any configuration of the NTP client on the TOE to support this communication.

The evaluator shall determine through the evaluation of operational guidance how the TOE initializes and initiates the clock. The evaluator shall then follow those instructions to set the clock to a known value, and observe that the clock monotonically increments in a reliable fashion (comparison to a reference timepiece is sufficient). Through its exercise of other TOE functions, the evaluator shall confirm that the value of the timestamp is used appropriately. If the TOE supports multiple protocols for establishing a connection with an NTP server, the evaluator shall perform this test using each supported protocol claimed in the operational guidance.

C.7 Authentication Policy Definition

In general, it is expected that other ESM products will define and authenticate administrators that log on to the TOE. Because of this, it is likely that the policy for allowable authentication will not be defined by the TSF. However, it is still possible that

the TSF defines its own authentication policy. If this is the case, the following requirements must be claimed:

C.7.1 FIA_AFL.1 Authentication Failure Handling

Hierarchical to:	No other components.
FIA_AFL.1.1	The TSF shall detect when [selection: [***assignment: positive integer number***], an administrator configurable positive integer within [***assignment: range of acceptable values***]] unsuccessful authentication attempts occur related to [***assignment: list of authentication events***].
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [***assignment: list of actions***].
Dependencies:	FIA_UAU.1 Timing of Authentication

Assurance Activity:

The evaluator shall check the TSS in order to determine that the authentication failure handling function is described in sufficient detail to affirm the SFR.

The evaluator shall check the operational guidance to verify that a discussion on authentication failure handling is present and consistent with the representation in the Security Target.

The evaluator shall test this capability by using the authentication function of the TSF to deliberately enter incorrect credentials. The evaluator shall observe that the proper action occurs after a sufficient number of incorrect authentication attempts. The evaluator shall also use the TSF to reconfigure the threshold value in a manner consistent with operational guidance to verify that it can be changed.

C.7.2 FTA_TSE.1 TOE Session Establishment

Hierarchical to:	No other components.
FTA_TSE.1.1	The TSF shall be able to deny session establishment based on [selection: day, time, **[*assignment: other attributes***]].
Dependencies:	No dependencies.

Assurance Activity:

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

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

The evaluator shall test this capability by first fully establishing 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.

C.8 Cryptographic Functional Requirements

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

Applicable Requirements

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

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

used by the ST author.

C.8.1 FCS_CKM.1 Cryptographic Key Generation (for Asymmetric Keys)

Hierarchical to: No other components.

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

[selection:

- *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for finite field-based key establishment schemes;*
- *NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography" for elliptic curve-based key establishment schemes and implementing "NIST curves" P-256, P-384 and [selection: P-521, no other curves] (as defined in FIPS PUB 186-3, "Digital Signature Standard")*
- *NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography" for RSA-based key establishment schemes]*

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

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

will be chosen by the ST author from the selection.

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

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

Dependencies: [FCS_CKM.2 Cryptographic Key Distribution, or

FCS_COP.1 Cryptographic Operation]

FCS_CKM.4 Cryptographic Key Destruction

Assurance Activity:

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

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

- *The TSS shall list all sections of the appropriate 800-56 standard(s) to which the TOE complies.*
- *For each applicable section listed in the TSS, for all statements that are not "shall" (that is, "shall not", "should", and "should not"), if the TOE implements such options it shall be described in the TSS. If the included functionality is*

indicated as "shall not" or "should not" in the standard, the TSS shall provide a rationale for why this will not adversely affect the security policy implemented by the TOE;

- *For each applicable section of 800-56A and 800-56B (as selected), any omission of functionality related to "shall" or "should" statements shall be described;*
- *Any TOE-specific extensions, processing that is not included in the documents, or alternative implementations allowed by the documents that may impact the security requirements the TOE is to enforce shall be described.*

C.8.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

Hierarchical to: No other components.

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

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

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

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check to ensure the TSS describes each of the secret keys (keys used for symmetric encryption), private keys, and critical security parameters used to generate key; when they are zeroized (for example, immediately after use, on system shutdown, etc.); and the type of zeroization procedure that is performed (overwrite with zeros, overwrite three times with random pattern, etc.). If different types of memory are used to store the materials to be protected, the evaluator shall check to ensure that the TSS

describes the zeroization procedure in terms of the memory in which the data are stored (for example, "secret keys stored on flash are zeroized by overwriting once with zeros, while secret keys stored on the internal hard drive are zeroized by overwriting three times with a random pattern that is changed before each write").

C.8.3 FCS_COP.1(1) Cryptographic Operation (for Data Encryption/Decryption)

Hierarchical to: No other components.

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

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

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

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

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

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic Key Destruction

Assurance Activity:

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

C.8.4 FCS_COP.1(2) Cryptographic Operation (for Cryptographic Signature)

Hierarchical to: No other components.

FCS_COP.1.1(2) *Refinement:* The TSF shall perform *cryptographic signature services* in accordance with a *selection:*

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

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

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

that meets the following:

Case: Digital Signature Algorithm

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

Case: RSA Digital Signature Algorithm

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

Case: Elliptic Curve Digital Signature Algorithm

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

defined in FIPS PUB 186-3, "Digital Signature Standard").

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

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

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

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

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

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic Key Destruction

Assurance Activity:

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

C.8.5 FCS_COP.1(3) Cryptographic Operation (for Cryptographic Hashing)

Hierarchical to:	No other components.
FCS_COP.1.1(3)	*Refinement:* The TSF shall perform *cryptographic hashing services* in accordance with a specified cryptographic algorithm *[selection: SHA-1, SHA-256, SHA-384] and message digest sizes [selection: 160, 256, 384] bits* that meet the following: *FIPS Pub 180-3, "Secure Hash Standard."*
Application Note:	*For this version of the PP, use of SHA-1 is allowed only for TLS for backward compatibility reasons. The next version of the PP will most likely completely exclude the use of SHA-1.* *The selection of the hashing algorithm shall correspond to the selection of the message digest size; for example, if SHA-1 is chosen, then the only valid message digest size selection would be 160 bits.*
Dependencies:	[FDP_ITC.1 Import of User Data without Security Attributes, or FDP_ITC.2 Import of User Data with Security Attributes, or FCS_CKM.1 Cryptographic Key Generation] FCS_CKM.4 Cryptographic Key Destruction

Assurance Activity:

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

C.8.6 FCS_COP.1(4) Cryptographic Operation (for Keyed-Hash Message Authentication)

Hierarchical to:	No other components.
FCS_COP.1.1(4)	*Refinement:* The TSF shall perform *keyed-hash message*

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

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

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

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

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

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

FCS_CKM.1 Cryptographic Key Generation]

FCS_CKM.4 Cryptographic Key Destruction

Assurance Activity:

The evaluators shall use "The Keyed-Hash Message Authentication Code (HMAC)

Validation System (HMACVS)" as a guide in testing the requirement above. This will require that the evaluators have a reference implementation of the algorithms that can produce test vectors that are verifiable during the test.

C.8.7 FCS_HTTPS_EXT.1 HTTPS

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

Assurance Activity:

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

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

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

C.8.8 FCS_IPSEC_EXT.1 IPsec

Hierarchical to: No other components.

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms AES-CBC-128, AES-CBC-256 (both specified by RFC 3602), [selection: no other algorithms, AES-GCM-128, AES-GCM-256 as specified in RFC 4106], and using [selection, choose at least one of: IKEv1 as defined in RFCs 2407, 2408, 2409, RFC 4109, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]; IKEv2 as defined in RFCs 5996 (with mandatory support for NAT traversal as specified in section 2.23), 4307, and [selection: no other RFCs for hash functions, RFC 4868 for hash functions]].

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

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

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

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

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

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

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

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

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

Application Note: *The selected algorithm should correspond to an*

appropriate selection for FCS_COP.1(2).

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

FCS_IPSEC_EXT.1.8 The TSF shall support the following:

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

2. Pre-shared keys of 22 characters and [selection: [***assignment: other supported lengths***], no other lengths].

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

Dependencies: FCS_COP.1 Cryptographic Operation

Assurance Activity:

The evaluator shall examine the TSS to verify the following:

1. *It specifies the hash functions used for integrity protection from the RFCs specified in the requirement.*
2. *It describes how "confidentiality only" ESP mode is disabled.*
3. *In the description of the IPsec protocol supported by the TOE, it states that aggressive mode is not used for IKEv1 Phase 1 exchanges, and that only main mode is used.*

4. *It describes how lifetimes for IKEv1 SAs (both Phase 1 and Phase 2) are established.*
5. *It describes how lifetimes for IKEv1 Phase 2 SAs--with respect to the amount of traffic that is allowed to flow using a given SA--are established.*
6. *It describes how the DH groups specified in the requirement are listed as being supported. If there is more than one DH group supported, it describes how a particular DH group is specified/negotiated with a peer.*
7. *It describes how pre-shared keys are established and used in authentication of IPsec connections. The description shall also indicate how pre-shared key establishment is accomplished for both TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key.*
8. *It describes how the cryptographic functions in the FCS requirements associated with this protocol (FCS_COP.1(1), etc.) are being used to perform the encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall perform the following activities:*
    a. *Ensure the ST contains a list of representative platforms (hardware and software) compromising the operational environment.*
    b. *Check the TSS to ensure it describes-for each platform identified in the ST-the interface(s) used by the TOE to invoke this functionality.*
    c. *For each platform identified in the ST, check the OE documentation to ensure the interfaces identified in the previous step exist.*

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

1. *If the cryptographic parameters for a connection are settable by an administrator, it provides instructions for setting these parameters, how to establish an IPsec connection using these parameters, and what parameter values are allowed in the evaluated configuration.*
2. *It describes any configuration necessary to ensure that "confidentiality only" mode is disabled, and that an advisory is present indicating that tunnel mode is the preferred ESP mode since it protects the entire packet.*
3. *It contains instructions for configuring the TOE prior to the use of main mode if such configuration is necessary.*
4. *It contains instructions for configuring lifetimes for IKEv1 SAs if these values are configurable.*
5. *It contains instructions for configuring the maximum amount of traffic that can flow using a given SA if this value is configurable.*

6. *It describes how pre-shared keys are to be generated and established for a TOE. The description shall also indicate how pre-shared key establishment is accomplished for both TOEs that can generate a pre-shared key as well as TOEs that simply use a pre-shared key.*
7. *It describes the generation of preshared keys, including guidance on generating strong keys and the allowed character set. The evaluator shall also check that this guidance does not limit the pre-shared key in a way that would not satisfy the requirement. It should be noted that while the administrator (in contravention to the operational guidance) can choose a key that does not conform to the requirement, there is no requirement that the TOE check the key to ensure that it meets the rules specified in this component. However, should the administrator choose to create a password that conforms to the rules above (and the operational guidance); the TOE should not prohibit such a choice.*

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

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

connection using ESP in confidentiality and integrity mode.

- *Test 4: The evaluator shall construct a test where a Phase 1 SA is established and attempted to be maintained for more than 24 hours before it is renegotiated. The evaluator shall observe that this SA is closed or renegotiated in 24 hours or less. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.*
- *Test 5: The evaluator shall perform a test similar to Test 1 for Phase 2 SAs, except that the lifetime will be 8 hours instead of 24.*
- *Test 6: The evaluator shall construct a test where a Phase 2 SA is established and attempted to be maintained while more data than is specified in the above assignment flows over the connection. The evaluator shall observe that this SA is closed or renegotiated before the amount of data specified is exceeded. If such an action requires that the TOE be configured in a specific way, the evaluator shall implement tests demonstrating that the configuration capability of the TOE works as documented in the operational guidance.*
- *Test 7: For each supported DH group, the evaluator shall test to ensure that all IKE protocols can be successfully completed using that particular DH group.*
- *Test 8: The evaluator shall generate a pre-shared key and use it, as indicated in the operational guidance, to establish an IPsec connection between two peers. If the TOE supports generation of the pre-shared key, the evaluator shall ensure that establishment of the key is carried out for an instance of the TOE generating the key as well as an instance of the TOE merely taking in and using the key.*
- *Test 9: The evaluator shall generate a pre-shared key that is 22 characters long that meets the composition requirements above. The evaluator shall then use this key to successfully establish an IPsec connection. While the evaluator is not required to test that all of the special characters or lengths listed in the requirement are supported, it is required that they justify the subset of those characters chosen for testing, if a subset is indeed used.*

C.8.9 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

Hierarchical to: No other components.

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

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

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

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

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

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

Note that for FIPS Pub 140-2 Annex C, currently only the method described in NIST-Recommended Random Number Generator Based on ANSI X9.31 Appendix A.2.4 Using the 3-Key Triple DES and AES Algorithms, Section 3 is valid. If the key length for the AES implementation used here is different than that used to encrypt the user data, then FCS_COP.1 may have to be adjusted or iterated to reflect the different key length. For the selection in FCS_RBG_EXT.1.2, the ST author selects the minimum number of bits of entropy that is used to seed the RBG.

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

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

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall review the TSS section to determine the version number of the product containing the RBG(s) used in the TOE. The evaluator shall also review the TSS to determine that it includes discussions that are sufficient to address the requirements described in Appendix C.9 Entropy Documentation and Assessment. This documentation may be included as a supplemental addendum to the Security Target.

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

Test 1: The evaluator shall determine an entropy estimate for each entropy source by using the Entropy Source Test Suite. The evaluator shall ensure that the TSS includes an

entropy estimate that is the minimum of all results obtained from all entropy sources.

Implementations Conforming to FIPS 140-2, Annex C

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

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

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

Implementations Conforming to NIST Special Publication 800-90

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

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

call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90).

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

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

Entropy input: *the length of the entropy input value must equal the seed length.*

Nonce: *If a nonce is supported (CTR_DRBG with no df does not use a nonce), the nonce bit length is one-half the seed length.*

Personalization string: *The length of the personalization string must be <= seed length. If the implementation only supports one personalization string length, then the same length can be used for both values. If more than one string length is support, the evaluator shall use personalization strings of two different lengths. If the implementation does not use a personalization string, no value needs to be supplied.*

Additional input: *the additional input bit lengths have the same defaults and restrictions as the personalization string lengths.*

C.8.10 FCS_SSH_EXT.1 SSH

Hierarchical to: No other components.

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

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

identified; this can be done either by adding elements to this component, or by additional detail in the TSS. In a future version of this PP, a requirement will be added regarding rekeying. The requirement will read "The TSF shall ensure that the SSH connection be rekeyed after no more than 2^{28} packets have been transmitted using that key."

FCS_SSH_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSH_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [***assignment: number of bytes***] bytes in an SSH transport connection are dropped.

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

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

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

FCS_SSH_EXT.1.5 The TSF shall ensure that the SSH transport implementation uses SSH_RSA and [selection: PGP-SIGN-RSA, PGP-SIGN-DSS, no other public key algorithms] as its public key algorithm(s).

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

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

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

Dependencies: FCS_COP.1 Cryptographic Operation

Assurance Activity:

The evaluator shall examine the TSS to verify the following:

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

Environment, the evaluator shall perform the following activities:

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

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

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

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

1. *It contains instructions on configuring the TOE so that SSH conforms to the description in the TSS (for instance, the set of algorithms advertised by the TOE may have to be restricted to meet the requirements).*

2. *It contains instructions to the administrator on how to ensure that only the allowed data integrity algorithms are used in SSH connections with the TOE (specifically, that the "none" MAC algorithm is not allowed).*

3. *It contains configuration information that will allow the security administrator to configure the TOE so that all key exchanges for SSH are performed using DH group 14. If this capability is "hard-coded" into the TOE, the evaluator shall check the TSS to ensure that this is stated in the discussion of the SSH protocol.*

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

- *Test 1: The evaluator shall, for each public key algorithm supported, show that the TOE supports the use of that public key algorithm to authenticate a user connection. Any configuration activities required to support this test shall be performed according to instructions in the operational guidance.*

- *Test 2: Using the operational guidance, the evaluator shall configure the TOE to accept password-based authentication, and demonstrate that a user can be successfully authenticated to the TOE over SSH using a password as an authenticator.*

- *Test 3: The evaluator shall demonstrate that if the TOE receives a packet larger than that specified in FCS_SSH_EXT.1.3, that packet is dropped.*

- *Test 4: The evaluator shall establish a SSH connection using each of the*

encryption and integrity algorithms specified by FCS_SSH_EXT.1.4 and FCS_SSH_EXT.1.6. It is sufficient to observe (on the wire) the successful negotiation of the algorithm to satisfy the intent of the test.

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

C.8.11 FCS_TLS_EXT.1 TLS

Hierarchical to: No other components.

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

Mandatory Ciphersuites:

TLS_RSA_WITH_AES_128_CBC_SHA

Optional Ciphersuites:

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

Application Note: *The ST author must make the appropriate selections and*

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

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

Dependencies: FCS_COP.1 Cryptographic Operation

Assurance Activity:

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

encryption functions. For the cryptographic functions that are provided by the Operational Environment, the evaluator shall perform the following activities:

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

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

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

The evaluator shall check the operational guidance to ensure that it contains instructions on configuring the TOE so that TLS conforms to the description in the TSS (for instance, the set of ciphersuites advertised by the TOE may have to be restricted to meet the requirements).

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

C.9 Entropy Documentation and Assessment

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

Design Description

Documentation shall include the design of the entropy source as a whole, including the interaction of all entropy source components. It will describe the operation of the entropy source to include how it works, how entropy is produced, and how unprocessed (raw) data can be obtained from within the entropy source for testing purposes. The documentation should walk through the entropy source design indicating where the

random comes from, where it is passed next, any postprocessing of the raw outputs (hash, XOR, etc.), if/where it is stored, and finally, how it is output from the entropy source. Any conditions placed on the process (e.g., blocking) should also be described in the entropy source design. Diagrams and examples are encouraged. This design must also include a description of the content of the security boundary of the entropy source and a description of how the security boundary ensures that an adversary outside the boundary cannot affect the entropy rate.

Entropy Justification

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

Operating Conditions

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

Health Testing

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

Appendix D - Document Conventions

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

D.1 Operations

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

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

For requirements taken from CC part 2 where selections and assignments have already been completed to ensure they apply to the PP, the conventions used are identical to the normal operations except that the "selection:" and "assignment:" prompts are not present.

D.2 Extended Requirement Convention

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

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

D.3 Application Notes

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

D.4 Assurance Activities

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

Appendix E - Glossary of Terms

Table 16. Terms and Definitions

Term	Definition
Access Control Product	An Enterprise Security Management product that is responsible for enforcing defined access control policies.
Assignment Manager	An individual authorized to use the TSF to define and maintain subject identity and credential data.
Credential	A collection of one or more pieces of information associated with an identity that can be used to assert that identity.
End User	An individual that is managed by the ESM system in order to have their authorizations clearly delineated and their activities unambiguously accounted.
Enrollment	The act of defining a new user in the ESM system.
Enterprise Security Management	Systems and personnel required to order, create, disseminate, modify, suspend, and terminate security management controls.
Federation	Two or more domains that have mutual assurance that a subject authenticated by one domain will be similarly valid on the other(s).
Identity	A unique identifier that is assigned to an individual that remains static for the duration of the user's lifecycle.
Managed Repository	A data store that is used to contain identity and credential attribute data. A managed repository does not have to be part of the TSF, but the TSF should be the only subject that is allowed to alter its contents.
Non-Person Entity	An identified subject that serves some function in an organization's operational environment that does not represent a human user, such as hardware or software.
Operational Environment	The collection of hardware and software resources in an enterprise that are not within the TOE boundary. This may include but is not limited to third-party software components the TOE requires to operate, resources protected by the TOE, and the hardware upon which the TOE is installed.
Policy Administrator	An individual that uses a Policy Management product to define access control policies for the ESM.
Policy Management Product	An Enterprise Security Management product that is responsible for defining and transmitting access control policies that are subsequently implemented by Access Control products.
User	See End User.

Appendix F - Identification

Title: Standard Protection Profile for Enterprise Security Management Identity and Credential Management

Author: ESM Protection Profile Technical Community

Common Criteria Identification: Common Criteria for Information Technology Security Evaluation, Version 3.1, September 2012

Version: PP Version 2.1

Keywords: enterprise security, enterprise security management, identity management, credential management, user enrollment, mission management, attribute management

Evaluation Assurance Level (EAL): EAL 1 augmented