Standard Protection Profile for Enterprise Security Management Identity and Credential Management

August 31, 2012

Version 1.4

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

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 Overview

Enterprise Security Management (ESM) refers to a suite of product/product components[1] used to provide centralized management of a set of IT assets within an organization.[2] There are two types of ESM capabilities. The first type, *policy definition*, is used to define a central organizational policy that will be used to govern the behavior of a set of IT assets. The second type, *policy consumption*, consumes a defined policy and enforces it. These two types of ESM capabilities are represented in the overall suite of ESM Protection Profiles.

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

- **Access Control Polices:** Policies that authorize or deny specific actions of defined subjects (actors) against defined objects (IT assets or resources).
- **Identity and Credential Policies:** Policies that define and maintain attributes used for subject identification, authentication, authorization, and accountability.
- **Object Attribute Policies:** Policies that define and maintain attributes used for objects.

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

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

- **Authentication Policies:** Policies that define the circumstances under which users can authenticate to enterprise systems.
- **Secure Configuration Policies:** Polices that define baseline configurations for IT assets.
- **Audit Policies:** Policies that define how audit data is collected, aggregated, reported, and maintained across the enterprise.

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

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

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

Table 1. Summary of the ESM Protection Profile Suite

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

ESM Audit Management		C		$C_{(3)}$	C	$C_{(1)}$/E
ESM Secure Configuration Management				$C_{(3)}$	D/C/E	$C_{(1)}$
C = Consume; D = Define; E = Enforce						

Notes:

1) The audit policy is consumed as the TOE determines what events to audit.
2) Object attributes are defined either in the Identity and Credential Management PP or the Policy Management PP, but not both.
3) The authentication policy is consumed in the sense that authorized users must authenticate to the TOE.

1.3 Overview of the ESM 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 utilize it. It is necessary for the TSF to be able to securely transmit this data to those components.

The TOE is 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 source
- 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 utilize 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 remote repository where it can be aggregated with other data streams by a product that is compliant with the Standard Protection Profile for ESM Audit Management.

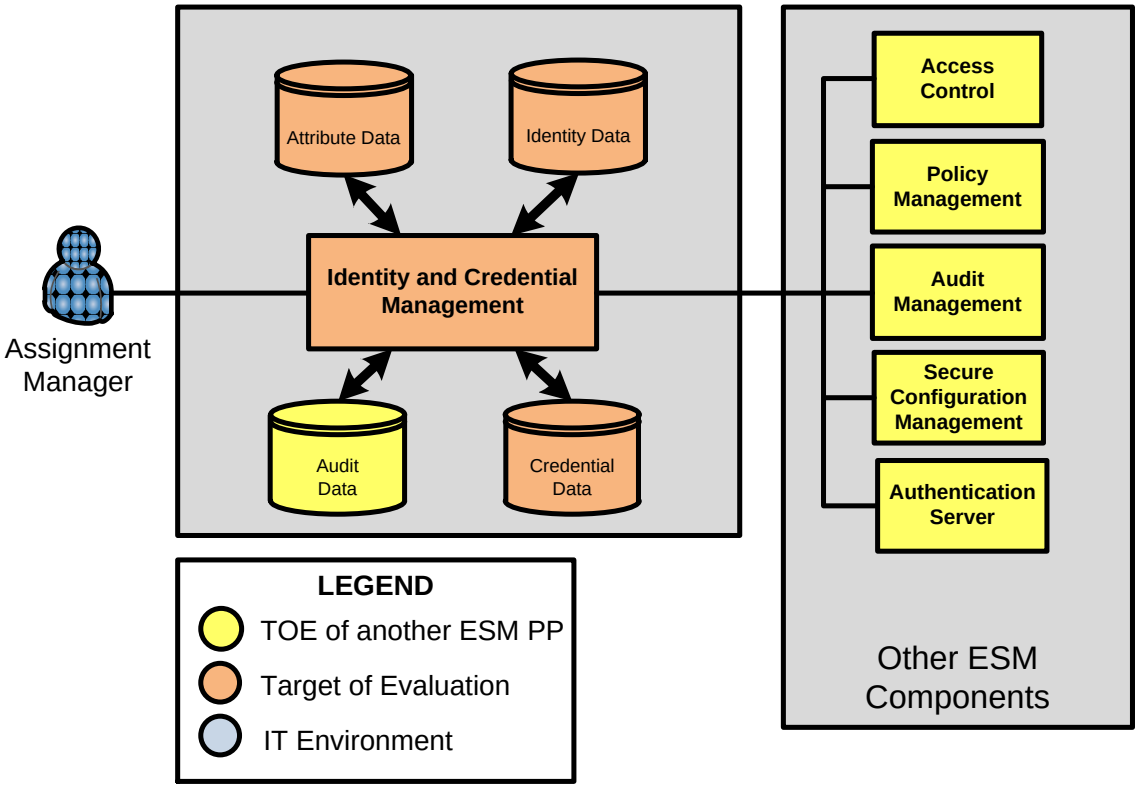

Figure 1. Context for Protection Profile

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. Note that operational environment objectives may not be claimed as being met by the TOE due to the nature of strict compliance. For common cases where operational environment objectives may be satisfied by ESM Identity and Credential Management products, the developer must work with CCEVS to add those SFRs as optional SFRs in a future version of this profile.

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 utilize, the trusted sources from which the data is received, and the mechanism by which this data is interpreted (such as SAML assertions or X.509 certificates).

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

1.7 Document Organization

Section 1 provides introductory material for the Protection Profile.

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

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

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

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

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

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

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

The document also contains the following appendices:

- Appendix A - This appendix provides a list of references and defines the acronyms used in this document.
- Appendix B - This appendix describes the Protection Profile's relationships with other standards so that the TOE's applicability to certification and accreditation efforts can be quickly identified.
- Appendix C - This appendix defines optional requirements that may be incorporated into compliant Protection Profiles, including the cryptographic

capabilities and the optional requirements for subject or object attribute management.

- 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-2009-07-004, Version 3.1 Revision 3 July 2009.

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

2.2 PP Conformance Claim

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

2.3 Package Conformance Claim

This Protection Profile claims a package of EAL1 augmented.

2.4 ST Conformance Requirements

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

Strict-PP conformance means the requirements in the PP are met and that the ST is an instantiation of the PP. The ST can be broader than the PP. The ST specifies that the TOE does at least the same as the PP, while the operational environment does at most the same as the PP. In this PP, application notes are provided to further clarify and explain the intent of the requirements specified and the expectation as to how the vendor will meet the requirements. It is expected that the evaluator of the ST will ensure strict-PP compliance by determining that the ST and its described TOE not only contain all the statements within this PP (and possibly more) but also met the expectations as stated by the application notes.

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

3 Threats

The following sections enumerate the threats that 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 provide sufficient measures to identify who is trying to use it and enforce authorizations based on this identity data, there will not be assurance that its management functions are capable of utilizing adequate access control. 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 utilize 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

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

4.2 System Monitoring

In order to identify incorrect TOE configuration and attempted malicious activity against protected objects, the TOE is expected to provide the ability to keep an audit trail. This audit trail should be able to provide administrative insight into system operations by identifying what policies are being defined by the TOE. It can also identify what types of activities are being performed against objects protected by the TSF.

In order to reduce the risk of the TOE being overwhelmed with a large volume of audit data and to facilitate potential compliance with an ESM Audit Management system, the TOE should be capable of sending audit information to an external trusted entity. This will increase the likelihood of the availability of audit data.

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

(O.AUDIT: FAU_GEN.1, 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 provide mechanisms that improve security relative to each of these factors. The TOE may

also provide (through optional SFRs defined in Appendix C.3) capabilities to deny session establishment and to suspend or terminate established sessions.

(O.ROBUST: FIA_AFL.1, FIA_SOS.1, 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, should use sufficiently strong and sufficiently trusted encryption algorithms to protect data in transit to and from the TOE. 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 include internal cryptographic capabilities or leverage a third-party operating system or cryptographic suite to provide the cryptographic functionality. Once a secure channel is established, it will subsequently be used to distribute identity and attribute data throughout the enterprise as needed.

(O.EAVES: 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), FTP_ITC.1(1), FTP_ITC.1(2), 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_OAD.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(2))

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.MANAGE, O.AUTH: FIA_UAU.2, FIA_UID.2, FMT_MSA.1, 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)

5 Extended Components Definition

5.1 Class ESM: Enterprise Security Management

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

5.1.1 ESM_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.

5.1.1.1 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 utilizing 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.

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 a 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 shall 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 shall 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 must 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.

5.1.2 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_OAD.1 (optional) to compatible and authorized ESM products external to the TSF under conditions defined by the ST author.

5.1.2.1 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 utilizing 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 utilize 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***]].

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.

5.1.3 ESM_OAD Object 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 is only one component in this family, ESM_OAD.1. ESM_OAD.1, object attribute definition, requires the TSF to be able to define some set of object attributes. These attributes are expected to be subsequently associated with objects 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.

5.1.3.1 ESM_OAD.1 Object Attribute Definition

The ESM_OAD family defines requirements for specification of object attributes. This allows other ESM products to enforce their own security functions by utilizing attribute data defined by the TSF. The ESM_OAD.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_OAD.1.1	The TSF shall maintain the following list of security attributes belonging to individual objects: [**assignment: *list of security attributes***].
ESM_OAD.1.2	The TSF shall be able to associate security attributes with individual objects.

Management: ESM_OAD.1

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

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

Audit: ESM_ OAD.1

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

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

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.[3]

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 Management ESM component on an external machine, an evaluated operating system sharing the platform with the TOE, or a centralized logging component. Transmission to multiple sources is permitted.*

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

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

a. protects the stored audit records in the TOE-internal audit trail from unauthorised deletion; and

b. [selection, choose one of: prevent, detect]

[3] FAU_STG.1 could have been treated as an optional requirement in **Error! Reference source not found.Error! Reference source not found.**. However, as there might be systems that had only local storage, that would have meant FAU_STG_EXT.1 would also need to be optional. Combining both into a single non-optional SFR mandates protected audit storage and transmission, while still supporting an "all-in-one" product that combines ESM capabilities.

unauthorised 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.

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_RBG_EXT.1 Random Bit Generation

Family Behavior

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

Component Leveling

There is only one component in this family, FCS_RBG_EXT.1. FCS_RBG_EXT.1, cryptographic operation (random bit generation), requires the TOE to perform random bit generation in accordance with a defined standard.

5.3.2.1 FCS_RBG_EXT.1 Cryptographic Operation (Random Bit Generation)

Hierarchical to: No other components

Dependencies: No dependencies

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

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

Management: FCS_RBG_EXT.1

There are no management actions foreseen.

Audit: FCS_RBG_EXT.1

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

a) Basic: Failure of the randomization process.

5.4 Class FPT: Protection of the TSF

5.4.1 FPT_APW_EXT.1 Extended: 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.

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 authentication data are not stored in the clear, and that no user or administrator is able to read the raw authentication data through "normal" interfaces. An all-powerful administrator of course could directly read memory to capture a password but is trusted not to do so. In this version of the PP there are no requirements on the method used to store the credentials in non-plaintext form, but cryptographic methods based on the requirements in FCS_COP are preferred. In future versions of this PP, FCS_COP-based cryptographic methods that conform to the Level 2 Credential Storage requirements from NIST SP 800-63 will be required.

Dependencies: No dependencies.

Management: FPT_APW_EXT.1

There are no management actions foreseen.

Audit: FPT_APW_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, which were fixed in the base requirement in the Common Criteria.

Hierarchical to: No other components.

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

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

] after an Authorized Administrator specified time period of inactivity.

Dependencies: No dependencies.

Management: FTA_SSL_EXT.1

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

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

Audit: FTA_SSL_EXT.1

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

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

6 Security Requirements

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

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

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

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

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

6.1 Security Functional Requirements

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

Table 2. TOE Functional Components

Functional Component	
ESM_ICD.1	Identity and Credential Definition
ESM_ICT.1	Identity and Credential Transmission
ESM_OAD.1 (optional)	Object Attribute Definition *(optional—defined in Appendix C.1)*
FAU_GEN.1	Audit Data Generation
FAU_STG_EXT.1	External Audit Trail Storage
FCS_CKM.1 (optional)	Cryptographic Key Generation (for asymmetric keys) *(as defined in Appendix C.4.1 if the TOE provides cryptographic functionality)*
FCS_CKM_EXT.4 (optional)	Cryptographic Key Zeroization *(as defined in Appendix C.4.2 if the TOE provides cryptographic functionality)*
FCS_COP.1(1) (optional)	Cryptographic Operation (for data encryption/decryption) *(as defined in Appendix C.4.3 if the TOE provides cryptographic functionality)*
FCS_COP.1(2) (optional)	Cryptographic Operation (for cryptographic signature) *(as defined in Appendix C.4.4 if the TOE provides cryptographic functionality)*
FCS_COP.1(3) (optional)	Cryptographic Operation (for cryptographic hashing) *(as defined in Appendix C.4.5 if the TOE provides cryptographic functionality)*
FCS_COP.1(4) (optional)	Cryptographic Operation (for keyed-hash message authentication) *(as defined in Appendix C.4.6 if the TOE provides cryptographic functionality)*
FCS_RBG_EXT.1 (optional)	Extended: Cryptographic operation (Random Bit Generation) *(as defined in Appendix C.4.7 if the TOE provides cryptographic functionality)*

Functional Component	
FIA_AFL.1	Authentication Failure Handling
FIA_SOS.1	Verification of Secrets
FIA_UAU.2	User Authentication Before Any Action
FIA_UID.2	User Identification Before Any Action
FMT_MOF.1	Management of Functions Behavior
FMT_SMF.1	Specification of Management Functions
FMT_SMR.1	Security Management Roles
FPT_APW_EXT.1	Protection of Stored Credentials
FPT_STM.1 (optional)	Reliable Time Stamps *(as defined in Appendix C.2.1)*
FTA_SSL_EXT.1 (optional)	TSF-initiated Session Locking and Termination *(optional – defined in Appendix C.3)*
FTA_SSL.3 (optional)	TSF-initiated termination *(optional – defined in Appendix C.3)*
FTA_SSL.4 (optional)	User-initiated termination *(optional – defined in Appendix C.3)*
FTA_TAB.1	TOE Access Banner
FTA_TSE.1 (optional)	Management of session establishment conditions *(optional – defined in Appendix C.3.1)*
FTP_ITC.1(1)	Inter-TSF Trusted Channel (prevention of disclosure)
FTP_ITC.1(2)	Inter-TSF Trusted Channel (detection of modification)
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 should not reproduce any of these application notes in the ST.

6.1.1.2 Composition Philosophy

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

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

6.1.2 Class ESM: Enterprise Security Management

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 should 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 utilize 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 a 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 shall 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 shall 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 must 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 must do the following:

- *Verify that the ST identifies the compatible ESM products*
- *Verify that the ST describes the identity and credential data used by the compatible ESM products.*
- *Review STs (or operational guidance, for unevaluated products) for the compatible ESM products and verify that there is correspondence between the identity and credential data the TOE is capable of creating and the identity and credential data the ESM products are capable of consuming*
- *Verify that the TSS and guidance documentation indicates how the identity and credential data are identified*

The evaluator will 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 should 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[4] on the compatible ESM products that utilize 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 ST 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

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

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 should provide some evidence of the strength of function.*

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:	*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 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 obtain the compatible ESM products, and following the procedures in the operational guidance for both the ICM and other ESM products, 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[5]*, 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

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

[5] 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.

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

Table 3. Auditable Events

Component	Event	Additional Information
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
ESM_OAD.1 (optional)	Definition of object attributes.	Identification of the attribute defined.
ESM_OAD.1 (optional)	Association of attributes with objects.	Identification of the object and the attribute.
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server	Identification of audit server
FCS_CKM.1(1) (optional)	Failure of the key generation activity.	None
FCS_CKM_EXT.4 (optional)	Failure of the key zeroization process.	Identity of subject requesting or causing zeroization, identity of object or entity being cleared.
FCS_COP.1(1) (optional)	Failure of encryption or decryption.	Cryptographic mode of operation, name/identifier of object being encrypted/decrypted.
FCS_COP.1(2) (optional)	Failure of cryptographic signature.	Cryptographic mode of operation, name/identifier of object being signed/verified.
FCS_COP.1(3)	Failure of hashing function.	Cryptographic mode of operation,

Component	Event	Additional Information
(optional)		name/identifier of object being hashed.
FCS_COP.1(4) (optional)	Failure in Cryptographic Hashing for Non-Data Integrity.	Cryptographic mode of operation, name/identifier of object being hashed.
FCS_RBG_EXT.1 (optional)	Failure of the randomization process.	None
FIA_AFL.1	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	Rejection or acceptance by the TSF of any tested secret	None
FIA_SOS.1	Identification of any changes to the defined quality metrics	The change made to the quality metric
FIA_UAU.2	All use of the authentication mechanism	None
FIA_UID.2	All use of the identification mechanism	Provided user identity
FMT_MOF.1	All modifications of TSF function behavior	None
FMT_SMF.1	Use of the management functions	Management function performed
FTA_TSE.1	Value of access parameters considered in the establishment determination	Variable depending on the parameters defined that control access, examples include time of access, location of access, subject suspended attribute
FTP_ITC.1(1)	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_ITC.1(2)	All use of trusted channel functions	Identity of the initiator and target of the trusted channel

Component	Event	Additional Information
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

Application Note: *The Standard Protection Profile for ESM Audit Management is responsible for storage and processing of audit events generated by the TOE.*

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

Assurance Activity:

The evaluator shall check the 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 must be covered, and must include a brief description of

each field. The evaluator shall check to make sure that every audit event type mandated by the PP is described and that the description of the fields contains the information required in FAU_GEN 1.2, and the additional information specified in Table 3.

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

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

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.

Application Note: *Examples of external IT entities could be an Audit Management 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 unauthorised deletion; and

b. [selection, choose one of: prevents, detects] unauthorised 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 operational and preparatory guidance in order to

determine that they describe how to configure and initiate transmissions to an external repository for audit storage. The evaluator shall also check the operational and preparatory 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 utilize a suite of cryptographic algorithms that have been previously validated rather than forcing vendors to implement their own unique and redundant cryptographic capabilities. The ST should clearly indicate what cryptographic capabilities are used by the TSF. Regardless of where the cryptographic capabilities reside, the expected capabilities are the same.

Refer to Appendix C.4 for the cryptographic requirements for the TOE.

6.1.5 Identification and Authentication (FIA)

Note that the FIA requirements apply to identification and authentication for the administrative users of the TOE. Requirements related to the authentication credentials defined for enterprise users are covered in the ESM family.

FIA_AFL.1 Authentication Failure Handling

Hierarchical to: FIA_UAU.1 Timing of authentication

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***].

Application Note: *The concern in FIA_AFL.1.1 and FIA_AFL.1.2 is consecutive unsuccessful attempts, not total unsuccessful attempts.*

Dependencies: FIA_UAU.1 Timing of authentication

Assurance Activity:

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 should observe that the proper action occurs after a sufficient number of incorrect authentication attempts. If the threshold value is configurable, the evaluator should also use the TSF to reconfigure the threshold value in a manner consistent with operational guidance to verify that it can be changed.

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 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 shall 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 shall 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 have a maximum lifetime, configurable by an administrator; and***

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

Application Note: *Clause 5 applies only to users changing their own passwords, at which time the user can be prompted for the*

old password. This clause should not be interpreted as requiring the storage of the unencrypted password.

6. ***Passwords must 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 examine the ST and operational guidance in order to identify whether password or non password based authentication is used:

a. *For password based authentication, 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 authentication, 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 should provide some evidence of the strength of function.*

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1 Timing of authentication

FIA_UAU.2.1	The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification

Assurance Activity:

The evaluator shall check the operational guidance and the TSS 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. The evaluator shall test this capability by accessing the TOE without having provided valid authentication information and observe that access to the TSF is subsequently denied.

This SFR also applies to authorized IT entities exchanging information with the TOE (such as authorized access control components). To address this, the evaluator shall review operational guidance and the TSS to determine the mechanism used to authorize communication with IT entities, and shall configure that mechanism to permit at least one IT entity to communicate with the TOE. The evaluator shall then attempt communication with that IT entity to ensure it successfully is authenticated and identified. The evaluator shall also attempt communications with unidentified or unauthenticated entities to ensure that such connections are not successful.

FIA_UID.2 User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.

Assurance Activity:

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

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 behaviour of, modify the behaviour of] the functions**:** ***management of identity and credential data*** to **[*assignment: the authorised identified roles*].**
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions

Assurance Activity:

The evaluator shall review the TSS and operational guidance to determine how the TSF captures the notion of administrative privilege. The evaluation of FMT_SMF.1 will demonstrate that the TSF provides all of the management functions claimed in the ST. For this requirement, the evaluator must determine how access to these management functions is mediated. For example, the TSF may statically associate the available functions with a set of defined administrative roles. The evaluator shall test this function by defining a set of administrative accounts that are sufficient to test the defined authority model. If scoping is used, for example, multiple accounts that are associated with the same authorized capabilities shall be defined with different levels of scope. Once these accounts have been created, the evaluator shall access the TSF using each of these accounts and determining that the allowed actions for each account is consistent with what would be expected based on the ST's depiction of how administrative authority is defined.

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, should*

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_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
ESM_OAD.1 (optional)	Definition of object attributes. Association of attributes with objects.
FAU_STG_EXT.1	Configuration of external audit storage location
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts, management of actions to be taken in the event of an authentication failure
FIA_SOS.1	Management of the metric used to verify secrets
FIA_UAU.2	Management of authentication data
FIA_UID.2	Management of user identities
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_TAB.1	Maintenance of the banner
FTA_TSE.1	Management of session establishment conditions

Requirement	Management Activities
FTP_ITC.1(1)	Configuration of actions that require trusted channel (if applicable)
FTP_ITC.1(2)	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 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.

Dependencies: FIA_UID.1 Timing of Authentication

Assurance Activity:

The evaluator shall review the ST and operational guidance to determine the roles that are defined for the TOE. The evaluator shall use the TOE to associate different users with different roles. This may be tested concurrently with other requirements if being assigned

to a role impacts how the user interacts with the TSF. For example, the TSF's internal access control mechanisms may grant different levels of authority to users who have different roles (only the super user can create new users, an auditor can only view policies and not change them, etc.), and so the effects of changing the user's role attribute would already have been tested by FMT_MOF.1.

6.1.7 Protection of the TSF

6.1.8 FPT_APW_EXT.1 Extended: 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 authentication data are not stored in the clear, and that no user or administrator is able to read the raw authentication data through "normal" interfaces. An all-powerful administrator of course could directly read memory to capture a password but is trusted not to do so. In this version of the PP there are no requirements on the method used to store the credentials in non-plaintext form, but cryptographic methods based on the requirements in FCS_COP are preferred. In future versions of this PP, FCS_COP-based cryptographic methods that conform to the Level 2 Credential Storage requirements from NIST SP 800-63 will be required.

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall examine the TSS to determine that it details all authentication data that are subject to this requirement, and the method used to obscure the plaintext credential data when stored. The TSS shall also describe how 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.

6.1.9 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 Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorized use of the TOE.

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall review the operational guidance to determine how the TOE banner is displayed and configured. The evaluation shall confirm that the guidance clearly configures the system to always display the banner for interactive sessions. The evaluator shall then attempt to access the TOE and verify that a TOE banner exists. If applicable, the evaluator will also attempt to utilize the functionality to modify the content of the TOE access banner as per the standards defined in FMT_SMF.1 and verify that the TOE access banner is appropriately updated.

6.1.10 Trusted Paths/Channels (FTP)

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

Hierarchical to: No other components.

FTP_ITC.1.1(1) **Refinement:** The TSF shall ***use*** **[*assignment: Secure internal or FCS-specified services*] *to*** provide a ***trusted*** communication channel***(s)*** between itself and ***authorized IT entities*** that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure.

Application Note: *The ST author must indicate whether the FCS service is internal to the TSF or provided by the Operational Environment. If compatible ESM products are co-hosted on the same platform, a secure internal service, such as secure IPC, may be used. This service must be capable of providing assurance of the identity of the endpoints of the communication and that the contents of the internal messages are not visible to parties not involved in the communications.*

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

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

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

Dependencies: No dependencies.

Assurance Activity:

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

- *If cryptography is internal to the TOE, the evaluator shall verify that the product has been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national standard for the nation in which the evaluation is being conducted.*
- *If cryptography is provided by the Operational Environment, the evaluator shall review the design documentation to see how cryptography is utilized and to verify that the functions used have been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national standard for the nation in which the evaluation is being conducted.*
- *If a secure internal service is used, the evaluator shall examine the TSS to determine that it describes the mechanism used and how it restricts the ability to view communications to only the entities involved in the communication. The evaluation shall attempt to confirm through product documentation (potentially operational environment documentation) that the description of the mechanism is correct.*

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. Testing of secure internal mechanisms by any observational techniques should not be possible, and analysis must suffice.

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

Hierarchical to:	No other components.
FTP_ITC.1.1(2)	**Refinement:** The TSF shall *use* **[assignment: *Secure internal or FCS-specified services*] *in providing*** a ***trusted*** communication channel***(s)*** between itself and ***authorized IT entities*** that is logically distinct from other communication channels and provides assured identification of its end points and ***detection of the modification of data***.
Application Note:	*The ST author must indicate whether the FCS service is internal to the TSF or provided by the Operational Environment. If compatible ESM products are co-hosted on the same platform, a secure internal service, such as secure IPC, may be used. This service must be capable of providing assurance of the identity of the endpoints of the communication and that the contents of the internal messages are not accessible to parties not involved in the communications.*
Application Note:	*Determination of whether an IT entity is authorized is based on the entity identification and authentication mechanisms enforced via FIA_UID.2 and FIA_UAU.2.*
FTP_ITC.1.2(2)	**Refinement:** The TSF shall permit ***the TSF or the authorized IT entities*** to initiate communication via the trusted channel.
FTP_ITC.1.3(2)	The TSF shall initiate communication via the trusted channel for ***transfer of credential data, [assignment: other***

functions]].

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

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check the administrative guidance in order to determine the mechanism by which secure communications are enabled. The evaluator shall also check the TSS and administrative guidance 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 TSS and administrative guidance to see how cryptography is utilized and to verify that the functions used have been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national standard for the nation in which the evaluation is being conducted.*
- *If a secure internal service is used, the evaluator shall examine the TSS to determine that it describes the mechanism used and how it restricts the ability to modify communications to only the entities involved in the communication. The evaluation shall attempt to confirm through product documentation (potentially operational environment documentation) that the description of the mechanism is correct.*

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. Testing of secure internal mechanisms by

any observational techniques should not be possible, and analysis must suffice.

FTP_TRP.1 Trusted path

Hierarchical to:	No other components.
FTP_TRP.1.1	**Refinement:** The TSF shall ***leverage*** **[**selection: internal, third-party**]** ***cryptographic suites to*** provide a communication path between itself and remote users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from [selection: modification, disclosure, [***assignment: other types of integrity or confidentiality violation***]].
FTP_TRP.1.2	The TSF shall permit remote users to initiate communication via the trusted path.
FTP_TRP.1.3	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 administrative 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 check the development evidence to determine if the functional specification 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 FPT_ITC.1. If data transmitted between the user and the TOE is obfuscated, the trusted path can be assumed to have been established.

6.1.11 Unfulfilled Dependencies

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

FPT_STM.1	This SFR is an unfulfilled dependency on FAU_GEN.1. It

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

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.

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

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

For each family, “Developer Notes” are provided on the developer action elements to

clarify what, if any, additional documentation/activity needs to be provided by the developer. For the content/presentation and evaluator activity elements, additional assurance activities (to those already contained in Section 6.1) 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
Tests	ATE_IND.1	Independent testing – conformance
Vulnerability Assessment	AVA_VAN.1	Vulnerability analysis
Life Cycle Support	ALC_CMC.1	Labeling of the TOE
	ALC_CMS.1	TOE CM coverage
Security Target Evaluation	ASE_CCL.1	Conformance Claims
	ASE_ECD.1	Extended Components Definition
	ASE_INT.1	ST Introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security Problem Definition
	ASE_TSS.1	TOE Summary Specification

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.[6] 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 are not directly invokable by TOE users, there is little point specifying that such interfaces be described in and of themselves since only indirect testing of such interfaces may be possible. The activities for this family for this PP should focus on understanding the interfaces presented in the TSS in response to the functional requirement, and the interfaces presented in the AGD documentation. No additional "functional specification" document should be necessary to satisfy the assurance activities specified.

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

Developer action elements:

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

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

Developer Note: As indicated in the introduction to this section, the functional specification is comprised of the information contained in the AGD_OPR and AGD_PRE documentation, coupled with the

[6] 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.

information provided in the TSS of the ST. The assurance activities in the functional requirements point to evidence that should exist in the documentation and TSS section; since these are directly associated with the SFRs, the tracing in element ADV_FSP.1.2D is implicitly already done and no additional documentation is necessary.

Content and presentation elements:

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

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

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

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

Evaluator action elements:

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

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

Assurance Activities:

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

with FMT_SMF would fail.

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

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

6.2.2 Class AGD: Guidance Documentation

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

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

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

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

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

6.2.2.1 Operational User Guidance (AGD_OPE.1)

Developer action elements:

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

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

Content and presentation elements:

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

Application Note: *The evaluation team should perform evaluation activities to ensure management requirements are being satisfied appropriately.*

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

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

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

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

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

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

Evaluator action elements:

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

Assurance Activities:

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

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

6.2.2.2 Preparative Procedures (AGD_PRE.1)

Developer action elements:

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

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

Content and presentation elements:

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

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

Evaluator action elements:

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

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

Assurance Activities:

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

6.2.3 Class ALC: Life Cycle Support

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

6.2.3.1 Labeling of the TOE (ALC_CMC.1)

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

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

Assurance Activities:

The evaluator shall check the ST to ensure that it contains an identifier (such as a

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

6.2.3.2 TOE CM coverage (ALC_CMS.1)

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

Developer action elements:

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

Content and presentation elements:

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

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

Evaluator action elements:

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

Assurance Activity:

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

6.2.4 Class ASE: Security Target Evaluation

6.2.4.1 Conformance Claims (ASE_CCL.1)

Developer action elements:

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

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

Content and presentation elements:

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

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

ASE_CCL.1.3C The CC conformance claim shall describe the conformance of the ST to CC Part 3 as either CC Part 3 conformant or CC Part 3 extended.

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

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

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

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

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

Evaluator action elements:

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

6.2.4.2 Extended Components Definition (ASE_ECD.1)

Developer action elements:

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

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

Content and presentation elements:

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

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

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

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

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

Evaluator action elements:

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

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

6.2.4.3 ST Introduction (ASE_INT.1)

Developer action elements:

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

Content and presentation elements:

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

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

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

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

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

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

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

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

Evaluator action elements:

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

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

6.2.4.4 Security objectives (ASE_OBJ.2)

Developer action elements:

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

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

Content and presentation elements:

ASE_OBJ.2.1C The statement of security objectives shall describe the security

objectives for the TOE and the security objectives for the operational environment.

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

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

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

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

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

Evaluator action elements:

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

6.2.4.5 Derived security requirements (ASE_REQ.2)

Developer action elements:

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

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

Content and presentation elements:

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

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

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

ASE_REQ.2.4C All operations shall be performed correctly.

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

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

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

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

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

Evaluator action elements:

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

6.2.4.6 Security Problem Definition (ASE_SPD.1)

Developer action elements:

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

Content and presentation elements:

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

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

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

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

Evaluator action elements:

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

6.2.4.7 TOE Summary Specification (ASE_TSS.1)

Developer action elements:

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

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

Evaluator action elements:

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

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

6.2.5 Class ATE: Tests

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

6.2.5.1 Independent testing - Conformance (ATE_IND.1)

Testing is performed to confirm the functionality described in the TSS as well as the administrative (including configuration and operation) documentation provided. The focus of the testing is to confirm that the requirements specified with each SFR are being met, although some additional testing is specified for SARs in section 6.2. The Assurance Activities identify the minimum testing activities associated with these components. The evaluator produces a test report documenting the plan for and results of testing, as well as coverage arguments focused on the platform/TOE combinations that are claiming conformance to this PP.

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

Assurance Activities:

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

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

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

engine are those specified by this PP and used by the cryptographic protocols being evaluated (IPsec, TLS/HTTPS, SSH).

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

6.2.6 Class AVA: Vulnerability Assessment

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

6.2.6.1 Vulnerability survey (AVA_VAN.1)

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

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

Assurance Activities:

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

6.3 Rationale for Security Assurance Requirements

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

7 Security Problem Definition Rationale

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

Table 6. Assumptions, Environmental Objectives, and Rationale

Assumptions	Objectives	Rationale
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.AUDIT** – The Operational Environment will provide a remote location for storage of audit data.	In order to be able to satisfy FAU_STG_EXT.1, the Operational Environment must provide a remote repository for audit data. This is assumed to be managed by an ESM Audit Management product.
	OE.MANAGEMENT – The Operational Environment will provide a Authentication Server component that utilizes 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, a Authentication Server component needs to be in place to consume the identity

Assumptions	Objectives	Rationale
		data provided by the TOE or else the TOE does not provide a benefit to the environment in which it is deployed.
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.	Defining identity data that will be used by the ESM is an activity that belongs to the Operational Environment because the TSF is not intended to introduce new subject data into the enterprise.
	OE.INSTAL – Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.	Providing one or more administrators to set up the TOE helps satisfy the assumption that it will be configured by a competent individual.

Assumptions	Objectives	Rationale
	OE.PERSON – Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.	The careful selection and training of personnel should ensure that no one administrator is given too much authority over the enterprise.

Table 7. Policies, Threats, Objectives, and Rationale

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.	**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.	This objective requires the TOE to have designated administrators for the configuration of the TOE, which allows the TOE some assurance that the TOE will be managed and configured consistently.
	OE.INSTAL – Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.	This objective requires those installing and configuring the TOE to be set up in such a manner as IT security is paramount. This helps assure that the TOE will be installed in a correct and secure manner.

Threats	Objectives	Rationale
	OE.PERSON – Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.	This objective requires the personnel in charge of installing, configuring, and managing the TOE to be appropriately vetted by the organization that purchases and intends to utilize the TOE. This offers some assurance that these personnel are not negligent or malicious.
T.EAVES – A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.	**O.EXPORT** – The TOE will provide the ability to transmit user attribute data to trusted IT products using secure channels.	**ESM_ICD.1** **ESM_ICT.1** The primary reason for the TOE's deployment in an organization is to serve as an authoritative source for identity and credential data. In order to reduce the threat of this data being compromised, the TSF must be able to transmit this data over secure channels and only to trusted sources.

Threats	Objectives	Rationale
	O.EAVES – The TOE will provide the ability to encrypt and decrypt information using validated cryptographic algorithms.	**FTP_ITC.1(1)** **FTP_ITC.1(2)** **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)** **FTP_TRP.1** It is expected that the TOE be able to encrypt information (either natively or by relying on 3rd party cryptography) sent to it by other ESM products (Policy Management, Access Control, etc.). This functionality allows the TOE to receive sensitive data without the threat of disclosure. Using cryptographic functionality to protect data in transit will allow the TOE reasonable assurance that the data will not be disclosed to or modified by an unauthorized party.

Threats	Objectives	Rationale
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.INTEGRITY –** The TOE will contain the ability to assert the integrity of identity, credential, or authorization data.	**FTP_ITC.1(2)** 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 reduced.
	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.	**FIA_UID.2** **FTP_ITC.1(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.
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.	**OE.FEDERATE** – Data the TOE exchanges with trusted external entities is trusted.	In the case where the TOE 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.

Threats	Objectives	Rationale
	O.ACCESSID – The TOE will include the ability to validate the identity of other ESM products prior to distributing data to them.	**FIA_UID.2** **FTP_ITC.1(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.
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 security relevant events that will detect access attempts to TOE-protected resources by users.	**FAU_GEN.1** **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.
	OE.AUDIT – The Operational Environment will provide a remote location for storage of audit data.	This objective works in conjunction with the requirement FAU_STG_EXT.1 by providing the external repository for audit data that is referred to within that requirement.

Threats	Objectives	Rationale
T.UNAUTH – A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to access the ESM.	**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.	**FIA_UAU.2** **FIA_UID.2** **FMT_MOF.1** **FMT_SMR.1** **FTP_TRP.1** The TOE will use the identity data it maintains for the enterprise to authenticate its own users. Users won't be able to perform actions prior to authentication and TOE session establishment.
	O.MANAGE – The TOE will provide Assignment Managers with the capability to manage the TSF.	**FMT_MOF.1** **FMT_SMF.1** The TOE will maintain mechanisms for Assignment Managers to perform user management functions within the TOE.
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** **FIA_SOS.1** **FTA_TSE.1 (optional)** **FTA_SSL_EXT.1 (optional)** **FTA_SSL.3 (optional)** **FTA_SSL.4 (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 failure

Threats	Objectives	Rationale
		handling, it decreases the number of individual guesses an attacker can make.
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 sufficient identity and credential attributes.	**ESM_ICD.1** **ESM_OAD.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 utilizing the full set of access control functions of compatible products.
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.

8 Security Problem Definition

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

8.1 Assumptions

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

8.1.1 Connectivity Assumptions

Table 8. TOE Assumptions

Assumption Name	Assumption Definition
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.

8.1.2 Physical Assumptions

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

8.1.3 Personnel Assumptions

Table 9. TOE 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.MASK	A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.
T.UNAUTH	A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to access the ESM.
T.WEAKIA	A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.
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.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.

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
P.BANNER[7]	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.

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

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 Name	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 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.EAVES	The TOE will provide the ability to encrypt and decrypt information using validated cryptographic algorithms.
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 sufficient identity and credential attributes.
O.INTEGRITY	The TOE will contain 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.ROBUST	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.
O.PROTCRED	The TOE will be able to protect stored credentials.

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

Environment Security Obj.	Environment 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

Environment Security Obj.	Environment Security Objective Definition
	TOE.
OE.AUDIT	The Operational Environment will provide a remote location for storage of audit data.
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.INSTAL	Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
OE.MANAGEMENT	The Operational Environment will provide a Authentication Server component that utilizes 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.

Appendix A - Supporting Tables and References

A.1 References

[1] Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Policy Management, version 1.4, May 23, 2012

[2] Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Access Control, version 2.0, March 14, 2012

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

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

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

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

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

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

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

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

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

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

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

[14] National Institute of Standards and Technology, NIST Special Publication 800-38C

Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, May 2004

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[30] National Institute of Standards and Technology, The Random Number Generator

Validation System (RNGVS), January 2005

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

A.2 Acronyms

Table 14. Acronyms and Definitions

Term	Definition
CC	Common Criteria
COI	Communities of Interest
ESM	Enterprise Security Management
I&C	Identity and Credential
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
SAML	Security Assertion Markup Language
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TFSI	TOE Security Function Interface

Term	Definition
TSF	TOE Security Function
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 functional and assurance requirements defined as part of this PP and the NIST 800-53 security controls that apply to them. The mappings for the functional and assurance requirements that were defined in CC Part 2 and CC Part 3 have been derived from the Aerospace Technical Operating Report TOR-2012(8506)-5, "Exploding 800-53: An Analysis of NIST SP 800-53 Revision 3 as Completed by CNSSI 1253".

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

Table 15. NIST 800-53 Requirements Compatibility

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 3 Control		Comments and Observations
Common Criteria Version 3.x Security Functional Requirements				
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.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 3 Control		Comments and Observations
ESM_OAD.1 (optional)	**Object Attribute Definition** Object Attribute Definition			**No Mapping.** There appears to be no control corresponding to this. This optional SFR defines the attributes used for selected non-user objects that are defined by the TSF.
FAU_GEN.1	**Security Audit Data Generation** Audit Data Generation	AU-2	**Auditable Events** | [auditable events], rationale, and coordination	**Partial**. FAU_GEN.1.1 gives the definition of what events should be audited (addressing the bulk of this control), but the assignments need to be compared to see if the sets are equivalent. Note also that FAU_GEN implies both auditable and audited, which is two distinct controls under 800-53.
		AU-12	**Audit Generation** | Generate and pre-select on [components]	**Partial.** The generation aspect of FAU_GEN provides the generation aspect of AU-12.
		AC-17(1)	**Remote Access** | Automated monitoring/control	**Partial.** If the assignment in FAU_GEN.1 includes auditing of remote access, then this control is partially met (the monitoring aspect).
		AU-3	**Content of Audit Records** | Minimal audit record information	**Partial**. FAU_GEN.1.2 details the list of what must be contained in each audit record. The assignment must be compared to the controls to see if AU-3/AU-3(1) are satisfied.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 3 Control		Comments and Observations
		AU-3(1)	**Content of Audit Records** | Additional detailed information: [list]	**Partial**. FAU_GEN.1.2 details the list of what must be contained in each audit record. The assignment must be compared to the controls to see if AU-3/AU-3(1) are satisfied.
		Note: The SFR bases the auditable events on the other SFRs included in the Security Target, as well as the desired level of information (minimal, basic, etc.). NIST has no predefined set, although CNSS does provide a definition for NSS. There is no mandated correlation between the SFR and NIST assignments.		
FAU_STG_EXT.1	**Security Audit Event Storage** Remote Audit Trail Storage	AU-9	**Protection of Audit Information** | Protect information/tools from unauthorized access	**Partial.** The SFR addresses the basic intent of the control, although the repository/entity to which audit data is written must in turn prevent unauthorized modification of that data. However, the control not only protects the trail, but audit tools (which are not covered by the SFR).
FCS_CKM_EXT.1 (optional)	**Cryptographic Key Management** Cryptographic Key Generation	SC-12	**Cryptographic Key Establishment and Management |** Organization establishes/manages cryptographic keys	**Partial.** The SFR addresses one of the aspects of the 800-53 control. The assignments for standards and protocols need to be compared against required enhancements.
		Note: The NIST 800-53 controls make no distinction between 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** | Organization establishes/manages cryptographic keys	**Partial.** The SFR addresses one of the aspects of the 800-53 control. The assignments for standards and protocols need to be compared against required enhancements.
		Note: The NIST 800-53 controls make no distinction between the various aspects of key management (generation, distribution, access, and destruction).		

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 3 Control		Comments and Observations
FCS_COP.1(1) FCS_COP.1(2) FCS_COP.1(3) FCS_COP.1(4) (all optional)	**Cryptographic Operation** Cryptographic Operation	SC-13	**Use of Cryptography** | Cryptographic implementation via modules that meet regulations	**Partial.** The extent to which the SFR meets the control depends on how the assignments have been completed.
		Note: The SFR is very broad, and may be completed to cover all sorts of cryptographic operations, many of which are not covered in the NIST 800-53 SFRs. Examples of areas *not* covered in NIST include standards for secure cryptographic hashes and when they must be used and standards for the quality of random number generators used.		
FCS_RBG_EXT.1 (optional)	**Random Bit Generation** Random Bit Generation			**No Mapping.** There appears to be no control corresponding to this. The SFR defines the expected characteristics of random number generation.
FIA_AFL.1	**Authentication Failure** Authentication Failure Handling	AC-7	**Unsuccessful Login Attempts |** Limit and lock	**Full.** This SFR appears to cover all aspects of the control.
FIA_SOS.1	**Specification of Secrets** Verification of Secrets	IA-5(1)	**Authenticator Management |** Password complexity, lifetime, reuse	**Partial.** The complexity mechanisms in the assignment address the verification of strength for user-generated passwords (secrets).
FIA_UAU.2	**User Authentication** User Authentication Before Any Action	IA-2	**Identification and Authentication (Organizational Users) |** Unique I&A for organizational users	**Partial.** This addresses the authentication of organizational users.
		IA-8	**Identification and Authentication (Non-Organizational Users) |** Unique I&A for non-organizational users	**Partial.** This addresses the authentication of non-organizational users.
FIA_UID.2	**User Identification** User Identification Before Any Action	IA-2	**Identification and Authentication (Organizational Users) |** Unique I&A for organizational users	**Partial.** This addresses the identification of organizational users.
		IA-8	**Identification and Authentication (Non-Organizational Users) |** Unique I&A for non-organizational users	**Partial.** This addresses the identification of non-organizational users.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 3 Control		Comments and Observations
FMT_MOF.1	**Management of Functions in TSF** Management of Security Functions Behavior	AC-3(3)	**Access Enforcement** | Non-discretionary access control	**Partial.** Restriction of management functions to particular roles is at least a partial implementation of RBAC.
FMT_SMF.1	**Specification of Management Functions** Specification of Management Functions			**No Mapping.** This SFR is an open ended SFR to specify management functions not captured elsewhere. It could correspond to almost any control, depending on assignment.
FMT_SMR.1	**Security Management Roles** Security Roles	AC-2(7)	**Account Management |** Role-based schemes	**Partial.** The SFR is on the information system, and the control is on the organization, yet this seems to be saying that all users are assigned a role, which fits with FMT_SMR.
		AC-5	**Separation of Duties |** Organizational level	**Partial.** Arguably, if a system provides distinct roles, that supports the provision of separation of duties and the application of the principle of least privilege.
		AC-6	**Least Privilege |** Employs concept of Least Privilege	**Partial.** Arguably, if a system provides distinct roles, that supports the provision of separation of duties and the application of the principle of least privilege.
FPT_APW_EXT.1	**Protection of the TSF** Protection of Stored Credentials	IA-5	**Authenticator Management** | Basic management of authenticators for users/devices	**Partial**. Addresses item h) in the control: Protecting authenticator content from unauthorized disclosure and modification

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 3 Control		Comments and Observations
FPT_STM.1 (optional)	**Time Stamps** Reliable Time Stamps	AU-8	**Time Stamps** | Internal clocks	**Full.** The SFR talks about providing reliable time stamps, presumably for auditing purposes. Most profiles modify this to integrate with NTP in the environment (giving AU-8(1)), but that's not mandated from the base SFR.
FTA_SSL_EXT.1 (optional)	**Session Locking and Termination** TSF-Initiated Session Locking	AC-11	**Session Lock** | Timeout Lock until Re-identified and Authenticated	**Partial.** FTA_SSL.1.1 provides the system-initiated session lock. FTA_SSL.1.2, with the proper assignment, addresses the actions required to unlock.
		AC-11(1)	**Session Lock** | With screen saver	**Full.** FTA_SSL.1.1 provides the system-initiated clearing or overwriting of the screen.
FTA_SSL.3 (optional)	**Session Locking and Termination** TSF-Initiated Termination	SC-10	**Network Disconnect** | Terminate network connections at session end or [time]	**Full.** Note that the former AC-10 was incorporated into SC-10, making clear that this refers not only to network termination but session termination.
FTA_SSL.4 (optional)	**Session Locking and Termination** User-Initiated Termination	SC-23(2)	**Session Authenticity** | Provide a readily observable session logout capability	**Full.** The SFR would imply that there be a logout capability for web sessions.
		Note: There appears to be no control mandating that there be a user-visible logout capability for non-web sessions.		
FTA_TAB.1	**TOE Access Banners** Default TOE Access Banners	AC-8	**System Use Notification** | Banners	**Full.** This control appears to address all aspects of the SFR. Note that there are additional requirements in the control, such as requiring a positive action to clear the message.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 3 Control		Comments and Observations
FTP_ITC.1(1) FTP_ITC.1(2)	**Inter-TSF Trusted Channel** Inter-TSF Trusted Channel	IA-3(1)	**Device Identification and Authentication |** Before remote/wireless connection with bidirectional cryptography-based authentication	**Partial.** The SFR discusses provision of a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. This control provides the identification of the end-points.
FTP_TRP.1	**Trusted Path** Trusted Path	SC-11	**Trusted Path** | Trusted path between users and [functions]	**Partial.** Whether the SFR provides the control depends on the assignments.
Common Criteria Version 3.x Security Target Assurance Requirements				
ASE_INT.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**ST Introduction** ST Introduction			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_CCL.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Conformance Claims** Conformance Claims			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_SPD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Problem Definition** Security Problem Definition			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_OBJ.1 EAL1	**Security Objectives** Security Objectives for the Operational			**No Mapping.** This SAR deals with format and structure of the Security

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 3 Control		Comments and Observations
	Environment			Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_OBJ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Objectives** Security Objectives			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_ECD.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Extended Components Definition** Extended Components Definition			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_REQ.1 EAL1	**Security Requirements** Stated Security Requirements			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_REQ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Requirements** Derived Security Requirements			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_SPD.1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Security Problem Definition** Security Problem Definition			**No Mapping.** This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated.
ASE_TSS.1	**TOE Summary**	SA-4(1)	**Acquisitions** |	**Partial.** The TSS in

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 3 Control		Comments and Observations
EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Specification** TOE Summary Specification		Acquisition documents describe functional properties of security controls to support analysis/test	the ST describes *how* the product implements the security functional requirements, and provides the high-level basis for all subsequent analysis and testing.
		SA-5(1)	**Information System Documentation** | Organization obtains vendor documentation on security-relevant functional properties	**Partial.** The TSS in the ST describes security-relevant functional properties for the security behaviors claimed in the ST.
Common Criteria Version 3.x Security Assurance Requirements				
ADV_FSP.1 EAL1	**Functional Specification** Basic Functional Specification	SA-4(2)	**Acquisitions** | Acquisition documents describe design/implementation of security controls to support analysis/test	**Partial.** The ADV_FSP family provides information about functional interfaces.
		SA-5(2)	**Information System Documentation** | Documents describe security-relevant external interfaces to support analysis/test	**Partial.** The ADV_FSP family provides information about functional interfaces.
AGD_OPE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Operational User Guidance** Operational User Guidance	SA-5	**Information System Documentation** | SFUG + TFM	**Full.** AGD_OPE is the combined requirement for administrator and user documentation.
		Note: NIST 800-53 parallels the CC v2 approach, which distinguished administrator and user documentation (AGD_USR, AGD_ADM). CC v3 combined these into a single SAR, reflecting the situation that some products do not have non-administrative users.		
AGD_PRE.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7	**Preparative Procedures** Preparative Procedures	SA-5	**Information System Documentation** | SFUG + TFM	**Full.** The SFR calls for describing all the steps necessary for secure acceptance and secure delivery. The control calls for documentation or secure configuration and installation.
Note: A general observation regarding the differences between CM under 800-53 and CM under the Common Criteria. The Common Criteria's CM refers to the CM of the development of the product, not its fielding in a system. NIST 800-53 focuses on controlling the configuration of the fielded system, and focuses less on developer CM.				
ALC_CMC.1 EAL1	**CM Capabilities** **Labeling of the TOE**	CM-9	**Configuration Management Plan** | Has CM plan with necessary information	**Partial.** This addresses defining the configuration items. Note that ALC_CMC is focused on the *product*, whereas CM-9 is focused on the *system.*

Common Criteria Version 3.x SFR/SAR			NIST SP 800-53 Revision 3 Control		Comments and Observations
			SA-10	**Developer Configuration Management** | Developer has configuration management during development; flaw tracking	**Partial.** ALC_CMC captures some of the developer aspects of the CM process.
	ALC_CMS.1 EAL1	**CM Scope** **TOE CM Coverage**	CM-9	**Configuration Management Plan** | Has CM plan with necessary information	**Partial.** This addresses defining the configuration items and the method of identification of configuration items. Note that ALC_CMC is focused on the *product*, whereas CM-9 is focused on the *system.*
			SA-10	**Developer Configuration Management** | Developer has configuration management during development; flaw tracking	**Partial.** ALC_CMS captures some of the developer aspects of the CM process.
ATE_IND.1 EAL1	**Independent Testing** **Independent Testing – Conformance**		CA-2	**Security Assessments** | Develop plan, assess, produce report	**Partial.** This control addresses the aspect of development of an independent test plan for security functions, and the assessment of those functions.
			CA-2(1)	**Security Assessments** | … with independent assessor	**Partial**. This addresses the fact that assessment is done by the CCTL, not the vendor.
			SA-11(3)	**Developer Security Testing** | Implement ST&E under independent validation and verification	**Partial.** ATE_IND requires independent testing by the validators, including rerunning of all or a portion of the test suite.
			Note: There is a key difference between ATE_IND and SA-11(3). ATE_IND requires the independent evaluators to run the tests. SA-11(3) has the developers running the tests under the oversight of the independent evaluators. There are key differences in this approach, primarily in assessing the actual quality of the test procedures and the repeatability. **Note:** ATE_IND.1 only has independent oversight for a portion of the test suite.		
AVA_VAN.1 EAL1	**Vulnerability Analysis** **Vulnerability**		CA-2(2)	**Security Assessments** | [announced/ unannounced] security testing (e.g., penetration	**Partial.** This addresses the requirement to conduct penetration

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 3 Control		Comments and Observations
	Survey		testing)	testing.
		RA-3	**Risk Assessment** | Conduct/document/review risk assessments	**Partial**. Conceivably, part of a risk assessment is doing a survey of vulnerabilities. Note that the CC does not imply formal vulnerability scanning, which is RA-5.
		SA-11(2)	**Developer Security Testing** | Developer vulnerability analysis	**Partial.** AVA_VAN requires that there be a vulnerability analysis performed.
		Note: The different AVA_VAN components differ on the depth and extent of the vulnerability analysis. NIST SP 800-53 Revision 3 appears to have no controls that dictate the quality of the vulnerability assessment.		

Appendix C - Architectural Variations and Additional Requirements

C.1 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 it must be compatible with a Policy Management product that does.

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

ESM_OAD.1 Object attribute definition

Hierarchical to:	No other components.
ESM_OAD.1.1	The TSF shall maintain the following list of security attributes belonging to individual objects: [**assignment: *list of 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.*
ESM_OAD.1.2	The TSF shall be able to associate security attributes with individual objects.
Dependencies:	No dependencies.

Assurance Activity:

The evaluator must determine through the evaluation of design documents how exactly to generate and utilize object data within the TOE. The evaluator must then generate this

information through normal TOE functionality that will apply the data to a desired object or set of objects. The evaluator must then use a Policy Management product to write a policy that utilizes this applied attribute data in access control decisions. Once the policy has been consumed by an Access Control product, the evaluator should attempt to perform actions against the object with both positive and negative expected results.

C.2 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 should be included:

C.2.1 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 evaluation team must determine through the evaluation of operational guidance how the TOE initializes and initiates the clock. The evaluation team must then follow those instructions to set the clock to a known value, and observe that the clock monotomically increments in a reliable fashion (comparison to a reference timepiece is sufficient). Through its exercise of other TOE functions, the evaluation team must confirm that the value of the timestamp is used appropriately.

C.3 Optional SFRs for Session Management

C.3.1 FTA_TSE.1 TOE Session Establishment

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

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

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

Assurance Activity:

The evaluator shall examine the TSS to determine that all of the attributes on which a session can be denied are specifically defined. The evaluator shall examine the operational guidance to determine that it contains guidance for configuring each of the attributes identified in the TSS. The evaluator shall also perform the following test for each attribute:

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

C.3.2 FTA_SSL Session Locking and Termination

C.3.2.1 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:

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

to unlocking the session;

- terminate the session

] after an Authorized Administrator specified time period of inactivity.

Dependencies: No dependencies

Assurance Activity:

The evaluator shall perform the following test:

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

C.3.2.2 FTA_SSL.3 TSF-initiated termination

Hierarchical to: No other components

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

Dependencies: No dependencies

Assurance Activity:

The evaluator shall perform the following test:

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

C.3.2.3 FTA_SSL.4 User-initiated termination

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

Assurance Activity:

The evaluator shall perform the following tests:

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

C.4 Cryptographic Functional Requirements

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

Applicable Requirements

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

These requirements should only be claimed in the event of the TOE performing its own cryptographic functionality and not relying on an OS or cryptographic library to perform

the functionality. These requirements were taken from the Security Requirements for IPsec Virtual Private Network (VPN) Gateways. Note that that cryptographic standards used to define these capabilities are specific to the United States; for evaluations that are to be overseen by other countries, the applicable equivalent national standards shall be used by the ST author.

C.4.1 FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys)

Hierarchical to: No other components

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

[selection:

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

and specified cryptographic key sizes **equivalent to, or greater than,** 112 bits **of security**.

Application Note: *This component requires that the TOE be able to generate the public/private key pairs that are used for key establishment purposes for the various cryptographic protocols used by the TOE (e.g., IPsec). If multiple*

schemes are supported, then the ST author should iterate this requirement to capture this capability. The scheme used will be chosen by the ST author from the selection.

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

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

Dependencies: [FCS_CKM.2 Cryptographic key distribution, or

FCS_COP.1 Cryptographic operation]

FCS_CKM.4 Cryptographic key destruction

Assurance Activity:

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

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

- *The TSS shall list all sections of the appropriate 800-56 standard(s) to which the TOE complies.*
- *For each applicable section listed in the TSS, for all statements that are not*

"shall" (that is, "shall not", "should", and "should not"), if the TOE implements such options it shall be described in the TSS. If the included functionality is indicated as "shall not" or "should not" in the standard, the TSS shall provide a rationale for why this will not adversely affect the security policy implemented by the TOE;

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

C.4.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization

Hierarchical to: No other components

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

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

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

Dependencies: No dependencies

Assurance Activity:

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

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

C.4.3 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 should choose the mode or modes in which the AES operates. For the first selection, the ST author should choose the key sizes that are supported by this functionality. For the second selection, the ST author should choose the standards that describe the modes specified in the assignment.*

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

Assurance Activity:

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

C.4.4 FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)

Hierarchical to: No other components

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

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

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

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

that meets the following:

Case: Digital Signature Algorithm

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

Case: RSA Digital Signature Algorithm

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

Case: Elliptic Curve Digital Signature Algorithm

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

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

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

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

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

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

Assurance Activity:

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

C.4.5 FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing)

Hierarchical to: No other components

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

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

Application Note: *The selection of the hashing algorithm must correspond to the selection of the message digest size; for example, if SHA-1 is chosen, then the only valid message digest size selection would be 160 bits.*

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

Assurance Activity:

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

C.4.6 FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication)

Hierarchical to: No other components

FCS_COP.1.1(4) **Refinement:** The TSF shall perform ***keyed-hash message authentication*** in accordance with a specified

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

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

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

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

Dependencies: [FDP_ITC.1 Import of user data without security attributes, or

FDP_ITC.2 Import of user data with security attributes, or

FCS_CKM.1 Cryptographic key generation]

FCS_CKM.4 Cryptographic key destruction

Assurance Activity:

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

produce test vectors that are verifiable during the test.

C.4.7 FCS_RBG_EXT.1 Extended: Cryptographic operation (Random Bit Generation)

Hierarchical to: No other components

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

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

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

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

SP 800-90 contains four different methods of generating random numbers; each of these, in turn, depends on underlying cryptographic primitives (hash functions/ciphers). The ST author will select the function used (if 800-90 is selected), and include the specific

underlying cryptographic primitives used in the requirement or in the TSS. While any of the identified hash functions (SHA-1, SHA-224, SHA-256, SHA-384, SHA-512) are allowed for Hash_DRBG or HMAC_DRBG, only AES-based implementations for CT_DRBG are allowed. While any of the curves defined in 800-90 are allowed for Dual_EC_DRBG, the ST author not only must include the curve chosen, but also the hash algorithm used.

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

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

In the future, most of the requirements described in A Method for Entropy Source Testing: Requirements and Test Suite Description will be required by this PP. The follow Assurance Activities currently reflect only that subset of activities that are required.

Dependencies: No dependencies

Assurance Activity:

The evaluator shall review the TSS section to determine the version number of the product containing the RBG(s) used in the TOE. The evaluator shall also confirm that the TSS describes the noise source from which entropy is gathered, and further confirm the location of this noise source. The evaluator will further verify that all of the underlying functions and parameters used in the RBG are listed in the TSS.

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

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

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

Implementations Conforming to FIPS 140-2, Annex C

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

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

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

Section 3. The evaluators ensure that the 10,000th value produced matches the expected value.

Implementations Conforming to NIST Special Publication 800-90

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

If the RNG has prediction resistance enabled, each trial consists of (1) instantiate drbg, (2) generate the first block of random bits (3) generate a second block of random bits (4) uninstantiate. The evaluator verifies that the second block of random bits is the expected value. The evaluator shall generate eight input values for each trial. The first is a count (0 – 14). The next three are entropy input, nonce, and personalization string for the instantiate operation. The next two are additional input and entropy input for the first call to generate. The final two are additional input and entropy input for the second call to generate. These values are randomly generated. "generate one block of random bits" means to generate random bits with number of returned bits equal to the Output Block Length (as defined in NIST SP 800-90).

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

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

> ***Entropy input:*** *the length of the entropy input value must equal the seed length.*
>
> ***Nonce:*** *If a nonce is supported (CTR_DRBG with no df does not use a nonce), the nonce bit length is one-half the seed length.*

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

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

Appendix D - Document Conventions

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

D.1 Operations

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

- **Assignment**: allows the specification of an identified parameter. Indicated with ***bold and italicized text*** inside square brackets that contain the prompt "assignment:" if further operations are necessary by the Security Target author;
- **Refinement**: allows the addition of details. Indicated with *italicized text*
- **Selection:** allows the specification of one or more elements from a list. Indicated with 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, ***bold and italicized text*** indicates where an assignment operation has already been completed in order to ensure these requirements apply to the PP.

D.2 Extended Requirement Convention

Extended requirements are permitted if the CC does not offer suitable requirements to meet the authors' needs. Extended requirements must be identified and are required to use the CC class/family/component model in articulating the requirements. Extended requirements will be indicated with the "EXT" inserted within the component.

D.3 Application Notes

Application notes contain additional supporting information that is considered relevant or useful for the construction of security targets for conformant TOEs, as well as general

information for developers, evaluators, and ISSEs. Application notes also contain advice relating to the permitted operations of the component.

D.4 Assurance Activities

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

Appendix E - Glossary of Terms

Table 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 IT 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	An individual that uses a Policy Management product to define access control policies for the

Term	Definition
Administrator	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 vendor community

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

Version: PP Version 1.4

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

Evaluation Assurance Level (EAL): EAL 1 augmented