

Standard Protection Profile for Enterprise Security Management Policy Management

May 23, 2012

Version 1.4

Document History

| Version | Date | Comment |
|----------------|----------------------------|--|
| 1.0 | July 15, 2011 | First complete version |
| 1.1 | February 24-28, 2012 | (1.1) Update to implement changes from ESM Access Control PP. (1.1D1) Update to correct some mappings identified by Justin. |
| 1.2 | April 16, 2012-May 2, 2012 | Updated to incorporate comments received to date Update to incorporate comments from ESM PP Telecon Updates to address additional issues regarding FIA_UAU/UID Clarify the notion of “transmit” in FAU_STG_EXT.1 to include passive transmission. |
| 1.3 | May 4, 2012 | Version after 2012-05-04 Telecon |
| 1.4 | May 23, 2012 | Fix minor formatting nits discovered while developing the ESM ICM PP; identify missing |

| | | |
|--|--|--|
| | | assurance activity for ESM_ACT.1. Add assurance activity for ESM_ACT.1. |
|--|--|--|

Table of Contents

| | | |
|-----|---|----|
| 1 | Protection Profile (PP) Introduction | 9 |
| 1.1 | Introduction..... | 9 |
| 1.2 | Overview | 9 |
| 1.3 | Overview of the ESM Policy Management Protection Profile..... | 11 |
| 1.4 | Compliant Targets of Evaluation..... | 14 |
| 1.5 | Common Capabilities..... | 15 |
| 1.6 | Related Protection Profiles | 16 |
| 1.7 | Document Organization..... | 16 |
| 2 | Conformance Claims | 18 |
| 2.1 | CC Conformance Claims | 18 |
| 2.2 | PP Conformance Claim..... | 18 |
| 2.3 | Package Conformance Claim..... | 18 |
| 2.4 | ST Conformance Requirements..... | 18 |
| 3 | Threats..... | 19 |
| 3.1 | Administrator Error..... | 19 |
| 3.2 | Policy and ESM Data Disclosure..... | 19 |
| 3.3 | Unauthorized Policy Creation..... | 19 |
| 3.4 | Weak Policies..... | 20 |
| 3.5 | Contradictory Policy Data..... | 20 |
| 3.6 | False Updates | 20 |
| 3.7 | Weak Authentication Functions..... | 21 |
| 4 | Security Objectives | 22 |
| 4.1 | System Monitoring..... | 22 |

| | | |
|-------|--|----|
| 4.2 | Robust TOE Access | 22 |
| 4.3 | Administrator Authorization | 22 |
| 4.4 | Policy Definition | 23 |
| 4.5 | Dependent Product Configuration | 23 |
| 4.6 | Secure Distribution of Policies | 24 |
| 4.7 | Access Bannerng..... | 24 |
| 5 | Extended Components Definition..... | 25 |
| 5.1 | Class ESM: Enterprise Security Management..... | 25 |
| 5.1.1 | ESM_ACD Access Control Policy Definition..... | 25 |
| 5.1.2 | ESM_ACT Access Control Policy Transmission..... | 26 |
| 5.1.3 | ESM_ATD Attribute Definition | 28 |
| 5.2 | Class FAU: Security Audit | 30 |
| 5.2.1 | FAU_SEL_EXT.1 External Selective Audit | 30 |
| 5.2.2 | FAU_STG_EXT.1 External Audit Trail Storage..... | 31 |
| 5.3 | Class FCS: Cryptographic Support..... | 33 |
| 5.3.1 | FCS_CKM_EXT.4 Cryptographic Key Zeroization | 33 |
| 5.3.2 | FCS_RBG_EXT.1 Random Bit Generation | 34 |
| 5.4 | Class FMT: Security Management | 35 |
| 5.4.1 | FMT_MOF_EXT.1 External Management of Functions Behavior..... | 35 |
| 5.4.2 | FMT_MSA_EXT.5 Consistent Security Attributes..... | 36 |
| 5.5 | Class FTA: TOE Access | 37 |
| 5.5.1 | FTA_SSL_EXT.1 TSF-initiated session locking | 37 |
| 6 | Security Requirements | 39 |
| 6.1 | Security Functional Requirements..... | 40 |
| 6.1.1 | PP Application Notes..... | 42 |
| 6.1.2 | Class ESM: Enterprise Security Management..... | 43 |
| 6.1.3 | Class FAU: Security Audit | 46 |
| 6.1.4 | Class FCS: Cryptographic Support..... | 53 |

| | | |
|--|--|-----|
| 6.1.5 | Class FIA: Identification and Authentication | 54 |
| 6.1.6 | Class FMT: Security Management | 59 |
| 6.1.7 | Class FTA: TOE Access | 68 |
| 6.1.8 | Class FTP: Trusted Paths/Channels | 69 |
| 6.1.9 | Unfulfilled Dependencies | 73 |
| 6.2 | Security Assurance Requirements | 74 |
| 6.2.1 | Class ADV: Development..... | 75 |
| 6.2.2 | Class AGD: Guidance Documentation | 78 |
| 6.2.3 | Class ALC: Life Cycle Support | 81 |
| 6.2.4 | Class ASE: Security Target Evaluation | 83 |
| 6.2.5 | Class ATE: Tests..... | 88 |
| 6.2.6 | Class AVA: Vulnerability Assessment..... | 90 |
| 6.3 | Rationale for Security Assurance Requirements | 92 |
| 7 | Security Problem Definition Rationale..... | 93 |
| 8 | Security Problem Definition | 102 |
| 8.1 | Assumptions..... | 102 |
| 8.1.1 | Connectivity Assumptions..... | 102 |
| 8.1.2 | Physical Assumptions | 102 |
| 8.1.3 | Personnel Assumptions..... | 102 |
| 8.2 | Threats..... | 102 |
| 8.3 | Organizational Security Policies..... | 103 |
| 8.4 | Security Objectives | 103 |
| 8.4.1 | Security Objectives for the TOE..... | 104 |
| 8.4.2 | Security Objectives for the Operational Environment..... | 104 |
| Appendix A - Supporting Tables and References..... | | 106 |
| A.1 | References..... | 106 |
| A.2 | Acronyms..... | 108 |
| Appendix B - NIST SP 800-53/CNSS 1253 Mapping..... | | 110 |

| | |
|---|-----|
| Appendix C - Architectural Variations and Additional Requirements | 124 |
| C.1 Attribute Definition..... | 124 |
| C.1.1 ESM_ATD.1 Object attribute definition..... | 124 |
| C.1.2 ESM_ATD.2 Subject attribute definition | 125 |
| C.2 Timestamps | 126 |
| C.2.1 FPT_STM.1 Reliable Time Stamps..... | 126 |
| C.3 Optional SFRs for Session Management | 126 |
| C.3.1 FTA_TSE.1 TOE Session Establishment..... | 126 |
| C.3.2 FTA_SSL Session Locking and Termination..... | 127 |
| C.4 Cryptographic Functional Requirements | 129 |
| C.4.1 FCS_CKM.1 Cryptographic Key Generation (for asymmetric keys) | 130 |
| C.4.2 FCS_CKM_EXT.4 Cryptographic Key Zeroization | 132 |
| C.4.3 FCS_COP.1(1) Cryptographic Operation (for data encryption/decryption)..... | 133 |
| C.4.4 FCS_COP.1(2) Cryptographic Operation (for cryptographic signature)..... | 134 |
| C.4.5 FCS_COP.1(3) Cryptographic Operation (for cryptographic hashing)..... | 136 |
| C.4.6 FCS_COP.1(4) Cryptographic Operation (for keyed-hash message authentication)..... | 137 |
| C.4.7 FCS_RBG_EXT.1 Extended: Cryptographic operation (Random Bit Generation) | 138 |
| Appendix D - Document Conventions..... | 144 |
| D.1 Operations | 144 |
| D.2 Extended Requirement Convention | 144 |
| D.3 Application Notes | 144 |
| D.4 Assurance Activities | 145 |
| Appendix E - Glossary of Terms | 146 |
| Appendix F - Identification..... | 148 |

List of Figures

Figure 1. Context for Protection Profile14

List of Tables

Table 1. Summary of the ESM Protection Profile Suite.....10

Table 2. TOE Functional Components40

Table 3. Auditable Events.....47

Table 4. Management Functions within the TOE.....66

Table 5. TOE Security Assurance Requirements75

Table 6. Assumptions, Environmental Objectives, and Rationale.....93

Table 7. Policies, Threats, Objectives, and Rationale.....94

Table 8. TOE Assumptions.....102

Table 9. TOE Assumptions.....102

Table 10. Threats103

Table 11. Organizational Security Policies.....103

Table 12. Security Objectives for the TOE.....104

Table 13. Security Objectives for the Operational Environment.....104

Table 14. Acronyms and Definitions108

Table 15. NIST 800-53 Requirements Compatibility.....110

Table 16. Terms and Definitions146

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 components¹ 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).

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.

- **Identity and Credential Policies:** Policies that define and maintain attributes used for subject identification, authentication, authorization, and accountability.
- **Object Attribute Policies:** Policies that define and maintain attributes used for objects.
- **Authentication Policies:** Policies that define the circumstances under which users can authenticate to enterprise systems.
- **Secure Configuration Policies:** Policies 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 Policy Management Protection Profile

This protection profile focuses on **access control policy definition and management**. ESM Policy Management products (PMs) will allow ESM Policy Administrators to configure and manage Access Control products in order to determine how objects should be protected throughout the enterprise. The output of this administrative action will be the production and distribution of policies to Access Control products. PMs should also be able to control the basic behavior of these products such as what events they audit, where they store audited event data, and how they should operate in the event of a loss of communications with the PM.

A TOE that is compliant with the ESM PM PP is expected to exhibit the following behavior:

- Establish a trusted channel between itself and other Enterprise Security Management products
- Provide evidence of its identity to other Enterprise Security Management products
- Utilize organizational subject and attribute data to validate the identities and determine the authorities of Policy Administrators

- Provide a trusted remote or local interface for Policy Administrators to create and distribute policies
- Deconflict a policy that may contain contradictory data such as rules that both authorize and deny the same activity
- Provide the ability to configure the policy enforcement behavior of Access Control products
- Generate an audit trail of administrative behavior

Optionally, the TOE may provide the ability to define subject or object attributes that are subsequently used in the enforcement of policies. For example, if the TOE manages a Host-Based Access Control product that utilizes a Mandatory Access Control model, it is necessary for sensitivity labels to be authoritatively defined and associated with objects and for clearances to be associated with subjects. This capability may be implemented by the TSF. If subject or object attribute management is necessary for access control enforcement and this is not enforced by the TSF, the Security Target (ST) author must indicate how these attributes are defined and maintained. For example, object attributes may be maintained by an operating system in the Operational Environment.

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 Access Control product must be identified. Compatibility is defined by the ability of that product to consume policies that are produced by the TOE. Depending on how access control is implemented in the organization, ESM PP solutions for identity management, authentication, 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 defines access policies between subjects and objects. The identity of subjects is expected to be defined by a source external to the TOE

such as a product that is compliant with the Standard Protection Profile for ESM Identity and Credential Management. Security relevant data such as audit logs, configuration information, and policy information may need to be stored locally in order for the TOE to operate. Policies defined by the TOE are sent to a product that is compliant with the Standard Protection Profile for ESM Access Control for consumption. 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. The TOE is expected to be monitored by a Secure Configuration Management product that contains overarching ESM rules for configuration items within the system. It will also monitor the policy versions upon the TOE and its connected Access Control product to determine when policies must be updated.

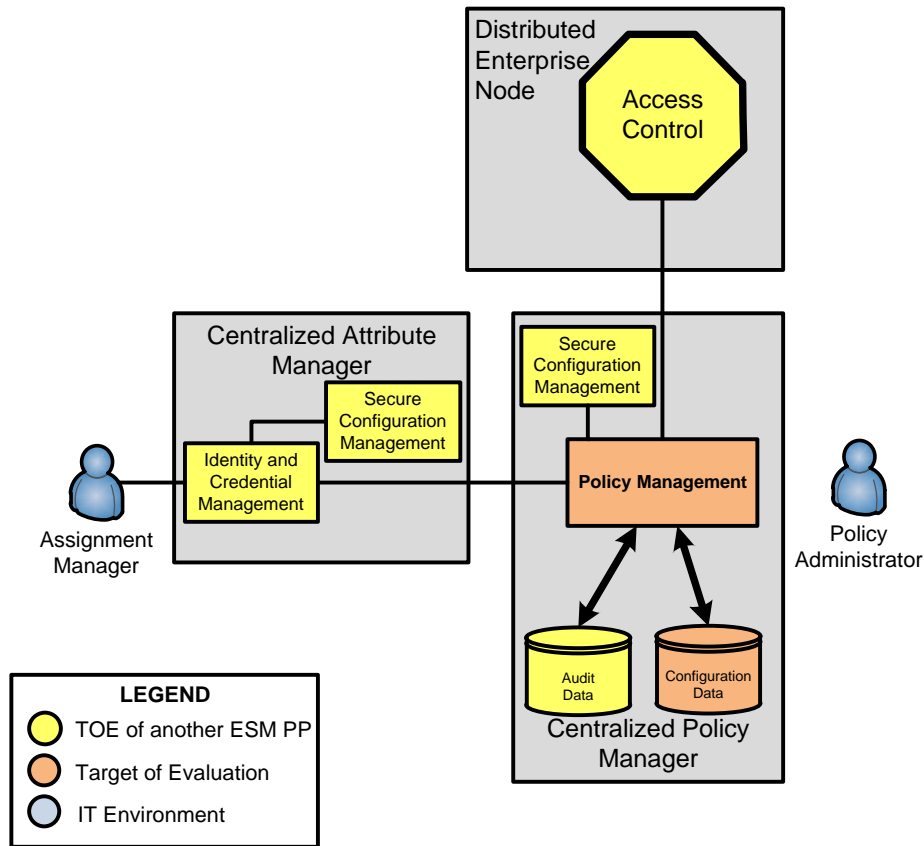


Figure 1. Context for Protection Profile

1.4 Compliant Targets of Evaluation

The purpose of a Policy Management product is to serve as a trusted source for policy information that is ultimately consumed by one or more Access Control products. These policies will determine what resources should be protected in the Operational Environment, what subjects are allowed to access these resources, and what set of operations this access is allowed to encompass. The PP does not prescribe any specific format used for access control; any of Mandatory Access Control (MAC), Discretionary Access Control (DAC), Role-Based Access Control (RBAC), Attribute-Based Access Control (ABAC), or other policies can be defined if they are capable of defining the desired access control mechanism.

A TOE that conforms to this PP may be able to define policies that control access to any

of a wide variety of resources. It is the responsibility of the Security Target (ST) author to clearly indicate what resources are protected and what attributes are used to determine how access is allowed or denied. The ST must also indicate the Access Control products that are able to consume the policies defined by the TOE and the other ESM products that may provide the TOE with organizational data for use in defining policies.

The TOE may be deployed as hardware or software, as a redundant distributed system, or as a single agent that resides on a server or network boundary device. Note that operational environment objectives may not be claimed as being met by the TOE due to the nature of strict compliance. For common cases where operational environment objectives may be satisfied by ESM Policy 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 to 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 policy management in an ESM setting. The Standard Protection Profile for ESM Access Control defines a number of technology types against which access control can be enforced. For each of these technology types, a minimum set of objects is defined to ensure that policies can define access control in sufficient detail. An ST that claims conformance to this PP should identify all applicable technology types for which it is able to define policies. These policies should then be described in sufficient detail to demonstrate how the requirements for the corresponding Access Control products are met by their contents.

Regardless of the technology type, it is essential for a product claiming conformance to an ESM Protection Profile to handle subjects and attributes that are **organizationally defined**. 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). In addition, a Policy Management product must be able to enforce its own internal access control so

that only authorized subjects are able to write policies and configure Access Control products.

A product that claims conformance to this PP is also expected to provide the ability to transmit its own identity to Access Control products and receive receipts of policy data that are generated by these products. This is mandated so that Access Control products have assurance that they are receiving policy data from a genuine source and so that Policy Management products have assurance that their specified policies have been received by the appropriate Access Control product.

1.6 Related Protection Profiles

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

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

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 - describes the Protection Profile's relationships with other standards so that the TOE's applicability to certification and accreditation efforts can be quickly identified.
- Appendix C - Defines 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 - Describes the conventions used in the document.
- Appendix E - Defines the terminology used in the document.
- Appendix F - Provides the formal PP identification information.

2 Conformance Claims

2.1 CC Conformance Claims

This Protection Profile is compliant with *Common Criteria for Information Technology Security Evaluation*, CCMB-2009-07-004, Version 3.1 Revision 3 July 2009.

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

2.2 PP Conformance Claim

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

2.3 Package Conformance Claim

This Protection Profile claims a package of EAL1 augmented.

2.4 ST Conformance Requirements

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

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

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

3 Threats

The following sections enumerate the threats that exist for 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 Policy 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 distribute policies to be enforced to remote Access Control products. It may receive user attributes or session data 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, 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 Policy Creation

If the TSF does not provide sufficient measures to determine who is trying to use it and define authorizations based on this identity data, there will not be assurance that policies are complete and accurate. A poorly designed or implemented authentication function will allow an attacker to illegitimately access the TSF and attempt to perform management functions. 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 create policies, the resulting compromise of the integrity of the organization's access control policies is the same.

[T.UNAUTH]

3.4 Weak Policies

The Standard Protection Profile for Enterprise Security Management Access Control specifies a variety of technology types and the minimum sets of subjects, objects, operations, and attributes in order to define sufficiently detailed policies for each technology type. A Policy Management product must be capable of creating policies that provide the same level of detail that a compatible Access Control product can consume. An insufficiently detailed policy is an ineffective access control mechanism because it either allows unintended activity or incorrectly restricts legitimate usage.

[T.WEAKPOL]

3.5 Contradictory Policy Data

An access control policy can potentially contain many different complex rules that permit and forbid access to various objects. A consequence of this is that a policy may contain rules that contradict one another. For example, a rule may exist that allows a particular user the ability to run a particular program on a host while another rule in the same policy may exist that forbids all members of a group that user belongs to from running the same program. If a policy that contains such a contradiction is consumed by an Access Control product, it may create an unpredictable result.

[T.CONTRADICT]

3.6 False Updates

When an Access Control product receives what appears to be updated policy information from the TOE, the Access Control product must have some assurance of the authenticity of the policy and the identity of the sender. If the communications channel is not sufficiently protected or the mechanism by which the TOE provides a guarantee of a

policy's integrity is not sufficiently robust, an attacker who is aware of the syntax used to transmit a policy may be able to forge an arbitrarily fake one and have an Access Control product consume it. If this occurs, an Access Control product may be configured to enforce a permissive fake policy that allows unauthorized access, to enforce a restrictive fake policy that prevents legitimate activities from being performed, or to consume an incorrectly formatted policy and either terminate or allow an attacker access to memory space within the system on which the Access Control product resides.

[T.FORGE]

3.7 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]

4 Security Objectives

4.1 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))

4.2 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))

4.3 Administrator Authorization

Policy Administrators will be designated by the TSF to be given various responsibilities

for managing the TOE and creating policies. The TSF will have its own internal method of enforcing controlled access so that no actions can be performed against it unless the subject is identified, authenticated, and authorized.

(O.AUTH: FIA_UAU.2, FIA_UID.2, FIA_USB.1, FMT_MSA.1(1), FMT_SMR.1, FTP_TRP.1)

4.4 Policy Definition

The primary purpose of the TOE is to create sufficiently detailed policies to enforce robust access control against one or more types of technology. Therefore, it is expected that the TSF will be able to manage, at minimum, policy attributes that are consistent with the corresponding technology type(s) described in the User Data Protection requirements in the Standard Protection Profile for Enterprise Security Management Access Control. In addition, the TSF will be able to detect or prevent inconsistencies in the application of policies so that policies are unambiguously defined. Finally, the TOE must also be able to uniquely identify policies it creates so that it can be used to determine what policies are being implemented by remote products. The TSF may optionally define (and subsequently serve as an authoritative source for) subject and/or object attributes that can be subsequently used to define policies. For example, in conjunction with the definition of a mandatory access control policy, the TOE may provide the capability to define security labels as an object attribute, clearances as a subject attribute, and distribute policies that define authorized access based on these labels.

(O.CONSISTENT, O.POLICY: ESM_ACD.1, ESM_ATD.1 (optional), ESM_ATD.2 (optional), FMT_MSA.1(2), FMT_MSA.3, FMT_MSA_EXT.5, FMT_SMF.1)

4.5 Dependent Product Configuration

In addition to being responsible for providing policies to be consumed by Access Control products, the TOE must be able to configure the behavior of the functions of these products. This includes the configuration of what events they audit, what policies they enforce, and how they react in the event of a failure state or lack of connectivity.

(O.MANAGE: FAU_SEL_EXT.1, FMT_MOF_EXT.1, FMT_MSA.1(2), FMT_SMF.1)

4.6 Secure Distribution of Policies

For the reasons described in Section 3.2, it is important that policies should be protected from disclosure. Similarly, the ability for an attacker to modify a policy or administrative commands in transit would pose a risk to the security of protected assets. As a result, the TSF is expected to establish trusted channels to identified and authenticated end points and distribute policies that are protected from modification and disclosure. The TSF should also provide evidence of its own identity for use in the secure establishment of these trusted channels.

(O.ACCESSID, O.AUTH, O.DISTRIB, O.EAVES, O.INTEGRITY, O.SELFID: ESM_ACT.1, 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), FIA_UID.2, FIA_UAU.2, FTP_ITC.1(1), FTP_ITC.1(2), FTP_TRP.1)

4.7 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

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

5.1 Class ESM: Enterprise Security Management

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

5.1.1 ESM_ACD Access Control Policy Definition

Family Behavior

The requirements of this family ensure that the TSF will have the ability to authoritatively define access control policies for use in an ESM deployment.

Component Leveling

There is only one component in this family, ESM_ACD.1. ESM_ACD.1, access control policy definition, requires the TSF to be able to define access control policies for consumption by external Access Control products.

5.1.1.1 ESM_ACD.1 Access Control Policy Definition

The ESM_ACD family defines requirements for defining access control policies. This allows other ESM products to enforce their own security functions by utilizing this attribute data. The ESM_ACD.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to define policies that govern the behavior of products that reside external to the TOE.

Hierarchical to: No other components

Dependencies: No dependencies

ESM_ACD.1.1 The TSF shall provide the ability to define access control

policies for consumption by one or more compatible Access Control products.

ESM_ACD.1.2 Access control policies defined by the TSF must be capable of containing the following:

- a. Subjects: *[assignment: list of subjects that can be used to make an access control decision and the source from which they are derived]*; and
- b. Objects: *[assignment: list of objects that can be used to make an access control decision and the source from which they are derived]*; and
- c. Operations: *[assignment: list of operations that can be used to make an access control decision and the source from which they are derived]*; and
- d. Attributes: *[assignment: list of attributes that can be used to make an access control decision and the source from which they are derived]*

ESM_ACD.1.3 The TSF shall associate unique identifying information with each policy.

Management: ESM_ACD.1

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

- a) Creation and modification of policies.

Audit: ESM_ACD.1

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

- a) Minimal: Creation and modification of policies.

5.1.2 ESM_ACT Access Control Policy Transmission

Family Behavior

The requirements of this family ensure that the TSF will have the ability to transfer defined access control policies to other ESM products.

Component Leveling

There is only one component in this family, ESM_ACT.1. ESM_ACT.1, access control policy transmission, requires the TOE to transmit access control policy data defined by ESM_ACD.1 to compatible and authorized ESM products external to the TSF under conditions defined by the ST author.

5.1.2.1 ESM_ACT.1 Access Control Policy Transmission

The ESM_ACT family defines requirements for transmitting enterprise policy attributes. This allows other ESM products to enforce their own security functions by utilizing attribute data defined by the TSF. The ESM_ACT.1 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to distribute access control policy data to external entities.

| | |
|------------------|--|
| Hierarchical to: | No other components |
| Dependencies: | ESM_ACD.1 Access Control Policy Definition |
| ESM_ACT.1.1 | The TSF shall transmit policies to compatible and authorized Access Control products under the following circumstances: <u>[selection: choose one or more of: immediately following creation of a new or updated policy, at a periodic interval, at the request of a compatible Secure Configuration Management product, <i>[assignment: other circumstances]</i>]</u> . |

Management: ESM_ACT.1

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

- a) Specification of the access control policy data to be transmitted.
- b) Specification of the circumstances under which this data is transmitted.
- c) Specification of the destinations to which this data is transmitted.

Audit: ESM_ACT.1

The following actions should be auditable if ESM ACT.1 Access control policy transmission is included in the PP/ST:

- a) Minimal: Transmission of identity and credential data to external processes or repositories.

5.1.3 ESM_ATD Attribute Definition

Family Behavior

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

Component Leveling

There are two components in this family, ESM_ATD.1 and ESM_ATD.2, that are not hierarchical to each other. ESM_ATD.1, object attribute definition, requires the TSF to be able to define some set of policy-related object attributes. ESM_ATD.2, subject attribute definition, requires the TSF to be able to define some set of policy-related subject attributes³. In both cases, these attributes are expected to be subsequently associated with controlled entities in the Operational Environment for use in handling access control. Examples of object attributes include security labels for use in mandatory access control (MAC) environments and protection levels that can be associated with web pages that reside within an organization's intranet. Examples of subject attributes include clearances or MAC ranges that would be associated with defined identities.

5.1.3.1 ESM_ATD.1 Object Attribute Definition

The ESM_ATD.1 component defines requirements for specification of object attributes. This allows other ESM products to enforce their own security functions by utilizing attribute data defined by the TSF. The ESM_ATD.1 requirements have been added

³ In other words, attributes relevant to policies enforced by the access control component. Subjects may have additional attributes that are related to identity and credentials. The ability to manage of subject attributes is optional in the Policy Management component; a system designer may choose to provide that capability within the Identity and Credential Management component.

because CC Part 2 lacks a requirement for the ability of the TSF to define attributes that are associated with objects that reside in the Operational Environment.

Hierarchical to: No other components

Dependencies: No dependencies

ESM_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual objects: [**assignment: *list of security attributes***].

ESM_ATD.1.2 The TSF shall be able to associate security attributes with individual objects.

Management: ESM_ATD.1

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

- a) Definition of object attributes.
- b) Association of attributes with objects.

Audit: ESM_ATD.1

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

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

5.1.3.2 ESM_ATD.2 Subject Attribute Definition

The ESM_ATD.2 component defines requirements for specification of subject attributes. This allows other ESM products to enforce their own security functions by utilizing attribute data defined by the TSF. In particular, subject attributes might be maintained by an Identity Management component and consumed by the Access Control component. The ESM_ATD.2 requirements have been added because CC Part 2 lacks a requirement for the ability of the TSF to define attributes that are associated with subjects that reside in the Operational Environment.

Hierarchical to: No other components

- Dependencies: No dependencies
- ESM_ATD.2.1 The TSF shall maintain the following list of security attributes belonging to individual subjects: [**assignment: list of security attributes**].
- ESM_ATD.2.2 The TSF shall be able to associate security attributes with individual subjects.

Management: ESM_ATD.2

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

- a) Definition of subject attributes.
- b) Association of attributes with subjects.

Audit: ESM_ATD.2

The following actions should be auditable if ESM_ATD.2 Subject attribute definition is included in the PP/ST:

- a) Minimal: Definition of subject attributes.
- b) Minimal: Association of attributes with subjects.

5.2 Class FAU: Security Audit

5.2.1 FAU_SEL_EXT.1 External Selective Audit

The FAU_SEL_EXT.1 family defines requirements for defining the auditable events on an external IT entity. Auditable events refer to the situations that trigger audit data to be written as audit data defined in FAU_GEN.1. The FAU_SEL_EXT.1 requirement has been added because CC Part 2 lacks a selectable audit requirement that demonstrates the ability of the TSF to define the auditable events for a specific external entity.

- Hierarchical to: No other components.
- Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

FAU_SEL_EXT.1.1 The TSF shall be able to select the set of events to be

audited by an ESM Access Control product from the set of all auditable events based on the following attributes:

- a. [selection: object identity, user identity, subject identity, host identity, event type]; and
- b. [*assignment: list of additional attributes that audit selectivity is based upon*]

Management: FAU_SEL_EXT.1

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

- a) Specification of the external IT entity that will be configured by the TSF.
- b) Specification of the auditable events for an external IT entity.

Audit: FAU_SEL_EXT.1

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

- a) Minimal: Changes to the set of events that are defined as auditable by the external entity.

5.2.2 FAU_STG_EXT.1 External Audit Trail Storage

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

⁴ FAU_STG.1 could have been treated as an optional requirement in Appendix C -Architectural Variations and Additional Requirements. 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

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] unauthorised modifications to the stored audit records in the TOE-internal audit trail.

SFR mandates protected audit storage and transmission, while still supporting an “all-in-one” product that combines ESM capabilities.

Management: FAU_STG_EXT.1

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

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

Audit: FAU_STG_EXT.1

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

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

5.3 Class FCS: Cryptographic Support

5.3.1 FCS_CKM_EXT.4 Cryptographic Key Zeroization

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

Hierarchical to: No other components

Dependencies: No dependencies

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

Management: FCS_CKM_EXT.4

There are no management actions foreseen.

Audit: FCS_CKM_EXT.4

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

- a) Basic: Failure of the key zeroization process.

5.3.2 FCS_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 FMT: Security Management

5.4.1 FMT_MOF_EXT.1 External Management of Functions Behavior

The FMT_MOF family defines the ability of the TSF to manage the behavior of its own functions. FMT_MOF_EXT extends this capability by defining requirements for managing the behavior of the functions of an external IT entity. In this case, the external IT entity to be managed is an ESM Access Control product. The FMT_MOF_EXT.1 requirement has been added because CC Part 2 lacks a requirement that demonstrates the ability of the TSF to manage functions of entities that are external to the TSF.

Hierarchical to: No other components.

Dependencies: FMT_SMF.1 Specification of management functions
FMT_SMR.1 Security roles

FMT_MOF_EXT.1.1 The TSF shall restrict the ability to query the behavior of, modify the functions of Access Control products: audited events, repository for remote audit storage, Access Control SFP, policy version being implemented, Access Control SFP behavior to enforce in the event of communications outage, [**assignment: *other functions***] to [**assignment: *the authorized identified roles***].

Management: FMT_MOF_EXT.1

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

- a) Specification of the external IT entity that will be configured by the TSF.
- b) Configuration of the functions of the specified external entities.

Audit: FMT_MOF_EXT.1

There are no auditable events foreseen. The activities defined by this requirement are a subset of the management functions specified in FMT_SMF.1. Because of this, auditing of all management functions that are specified in FMT_SMF.1 is sufficient to address the auditing of FMT_MOF_EXT.1.

5.4.2 FMT_MSA_EXT.5 Consistent Security Attributes

The FMT_MSA family defines the ability of the TSF to manage security attributes. FMT_MSA_EXT extends this capability by defining additional requirements for how these attributes can be managed. FMT_MSA_EXT.5 requires the TSF to enforce the notion of consistent attributes. The ST author must define what constitutes inconsistent attributes and what behavior the TSF exhibits when such inconsistencies are detected. If the TSF is implemented in a manner that prevents inconsistencies rather than merely detecting them, this can also be indicated. The FMT_MSA_EXT.5 requirement has been added because CC Part 2 lacks a requirement for defining inconsistent attributes and how the TSF acts to prevent or detect their use.

Hierarchical to: No other components.

Dependencies: FMT_MOF_EXT.1 External Management of Functions Behavior

FMT_MSA_EXT.5.1 The TSF shall [selection: identify the following internal inconsistencies within a policy prior to distribution: *[assignment: non-empty list of inconsistencies]*; only permit definition of unambiguous policies].

FMT_MSA_EXT.5.2 The TSF shall take the following action when an inconsistency is detected: [selection: issue a prompt for an administrator to manually resolve the inconsistency, *[assignment: other action]*].

Management: FMT_MSA_EXT.5

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

- a) Specification of inconsistent data to be detected or prevented by the TSF.
- b) Specification of actions to be taken by the TSF when inconsistent data is detected.

Audit: FMT_MSA_EXT.5

There are no auditable events foreseen. The activities defined by this requirement are a subset of the management functions specified in FMT_SMF.1. Because of this, auditing of all management functions that are specified in FMT_SMF.1 is sufficient to address the auditing of FMT_MSA_EXT.5.

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_ACD.1 | Access Control Policy Definition |
| ESM_ACT.1 | Access Control Policy Transmission |
| ESM_ATD.1 (optional) | Object attribute definition <i>(as defined in Appendix C.1.1)</i> |
| ESM_ATD.2 (optional) | Subject attribute definition <i>(as defined in Appendix C.1.2)</i> |
| FAU_GEN.1 | Audit Data Generation |
| FAU_SEL_EXT.1 | External Selective Audit |
| FAU_STG_EXT.1 | External Audit Trail Storage |
| FCS_CKM.1 (optional) | Cryptographic Key Generation (for asymmetric keys) <i>(as defined in Appendix C.4.1 if the TOE provides cryptographic functionality)</i> |
| FCS_CKM_EXT.4 (optional) | Cryptographic Key Zeroization <i>(as defined in Appendix C.4.2 if the TOE provides cryptographic functionality)</i> |
| FCS_COP.1(1) (optional) | Cryptographic Operation (for data encryption/decryption) <i>(as defined in Appendix C.4.3 if the TOE provides cryptographic functionality)</i> |
| FCS_COP.1(2) (optional) | Cryptographic Operation (for cryptographic signature) <i>(as defined in Appendix C.4.4 if the TOE provides cryptographic functionality)</i> |

| Functional Component | |
|-----------------------------|--|
| FCS_COP.1(3) (optional) | Cryptographic Operation (for cryptographic hashing) <i>(as defined in Appendix C.4.5 if the TOE provides cryptographic functionality)</i> |
| FCS_COP.1(4) (optional) | Cryptographic Operation (for keyed-hash message authentication) <i>(as defined in Appendix C.4.6 if the TOE provides cryptographic functionality)</i> |
| FCS_RBG_EXT.1 (optional) | Extended: Cryptographic operation (Random Bit Generation) <i>(as defined in Appendix C.4.7 if the TOE provides cryptographic functionality)</i> |
| 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 |
| FIA_USB.1 | User-Subject Binding |
| FMT_MOF_EXT.1 | External Management of Functions Behavior |
| FMT_MSA.1(1) | Management of Security Attributes (internal attributes) |
| FMT_MSA.1(2) | Management of Security Attributes (external attributes) |
| FMT_MSA.3 | Static Attribute Initialization |
| FMT_MSA_EXT.5 | Consistent Security Attributes |
| FMT_SMF.1 | Specification of Management Functions |
| FMT_SMR.1 | Security Management Roles |
| FPT_STM.1 (optional) | Reliable Time Stamps <i>(as defined in Appendix C.2.1)</i> |
| FTA_SSL_EXT.1 (optional) | TSF-initiated Session Locking and Termination |

| Functional Component | |
|----------------------|---|
| | <i>(optional – defined in Appendix C.3)</i> |
| FTA_SSL.3 (optional) | TSF-initiated termination <i>(optional – defined in Appendix C.3)</i> |
| FTA_SSL.4 (optional) | User-initiated termination <i>(optional – defined in Appendix C.3)</i> |
| FTA_TAB.1 | TOE Access Banner |
| FTA_TSE.1 (optional) | TOE Session Establishment <i>(optional – defined in Appendix C.3)</i> |
| 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_ACD.1 Access Control Policy Definition

| | |
|------------------|--|
| Hierarchical to: | No other components. |
| ESM_ACD.1.1 | The TSF shall provide the ability to define access control policies for consumption by one or more compatible Access Control products. |
| ESM_ACD.1.2 | Access control policies defined by the TSF must be capable of containing the following: Subjects: <i>[assignment: list of subjects that can be used to make an access control decision and the source from which they are derived]</i> ; and <i>Application Note:</i> <i>Example source for subject data would be a compatible Identity and Credential Management product.</i> Objects: <i>[assignment: list of objects that can be used to make an access control decision and the source from which they are derived]</i> ; and <i>Application Note:</i> <i>A host-based example source for objects would be the operating system of the host on which those objects reside.</i> Operations: <i>[assignment: list of operations that can be used to make an access control decision and the source from which they are derived]</i> ; and <i>Application Note:</i> <i>A host-based example source for operations would be the operating system of the host on which those objects reside.</i> Attributes: <i>[assignment: list of attributes that can be used</i> |

to make an access control decision and the source from which they are derived]

Application Note: Example source for attribute data would be a compatible Identity and Credential Management product or the TOE itself. Optional SFRs to define object and/or subject attributes may be found in Appendix C.1.

Application Note: The intent of this requirement is to ensure that if the TSF is compatible with an Access Control product, then it must be able to produce policies that take advantage of the full range of that product's features. For example, if the TSF claims to be compatible with a particular Host-Based Access Control product but can only write policies that control file access, then the TSF is not capable of sufficiently utilizing the features of that Access Control product.

ESM_ACD.1.3 The TSF shall associate unique identifying information with each policy.

Application Note: This requirement exists so that the TOE is able to subsequently determine what policy is being implemented by any Access Control product that consumes a policy it creates.

Dependencies: No dependencies

Assurance Activity:

The evaluator must do the following:

- *Verify that the ST identifies compatible Access Control products*
- *Verify that the ST describes the scope and granularity of the entities that define policies (subjects, objects, operations, attributes)*
- *Review STs for the compatible Access Control products and verify that there is correspondence between the policies the TOE is capable of creating and the policies the Access Control products are capable of consuming*

- *Verify that the design documentation indicates how policies are identified*

The evaluator will test this capability by using the TOE to create a policy that utilizes the full range of subjects, objects, operations, and attributes and sending it to a compatible Access Control product for consumption. The evaluator will then perform actions that are mediated by the Access Control product in order to confirm that the policy was applied appropriately. The evaluator will also verify that a policy identifier is associated with a transmitted policy by querying the policy that is being implemented by the Access Control product.

ESM_ACT.1 Access Control Policy Transmission

Hierarchical to: No other components.

ESM_ACT.1.1 The TSF shall transmit policies to compatible and authorized Access Control products under the following circumstances: [selection: choose one or more of: immediately following creation of a new or updated policy, at a periodic interval, at the request of a compatible Secure Configuration Management product, **assignment: other circumstances**]].

Application Note: This requirement exists to provide some assurance that up-to-date policies will be implemented.

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_ACD.1 Access control policy definition

Assurance Activity:

The evaluator shall review the operational guidance to determine how to create and update policies, and the circumstances under which new or updated policies are transmitted to consuming ESM products (and how those circumstances are managed, if applicable). The evaluator shall obtain a compatible Access Control product, and following the procedures in the operational guidance for both the Policy Manager and

the Access Control product, create a new policy and ensure that the new policy defined in the Policy Manager is transmitted and installed successfully in the Access Control product, in accordance with the circumstances defined in the SFR. In other words, (a) if the selection is completed to transmit after creation of a new policy, then the evaluator shall create the new policy and ensure that, after a reasonable window for transmission, the new policy is installed; (b) if the selection is completed to transmit periodically, the evaluator shall create the new policy, wait until the periodic period has passed, and then confirm that the new policy is present in the Access Control component; or (c) if the section is completed to transmit upon the request of a compatible Secure Configuration Management component, the evaluator shall create the policy, use the Secure Configuration Management component to request transmission, and the confirm that the Access Control component has received and installed the policy. 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 policy, and then repeat the previous procedure to ensure that the updated policy is transmitted to the Access Control component in accordance with the SFR-specified circumstances. Lastly, as updating a policy encompasses deletion of a policy, the evaluator shall repeat the process a third time, this time deleting the policy to ensure it is removed as an active policy from the Access Control component.

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

6.1.3 Class FAU: Security Audit

FAU_GEN.1 Audit Data Generation

Hierarchical to: No other components.

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- a) Start-up and shutdown of the audit functions; and
- b) All auditable events identified in Table 3 for the [not specified] level of audit; **and**

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

Table 3. Auditable Events

| Component | Event | Additional Information |
|-----------------------------|--|--|
| ESM_ACD.1 | Creation or modification of policy | Unique policy identifier |
| ESM_ACT.1 | Transmission of policy to Access Control products | Destination of policy |
| ESM_ATD.1 (optional) | Definition of object attributes. | Identification of the attribute defined. |
| ESM_ATD.1 (optional) | Association of attributes with objects. | Identification of the object and the attribute. |
| ESM_ATD.2 (optional) | Definition of subject attributes. | Identification of the attribute defined. |
| ESM_ATD.2 (optional) | Association of attributes with subjects. | Identification of the subject and the attribute. |
| FAU_SEL_EXT.1 | All modifications to audit configuration | None |
| 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 |

Standard Protection Profile for Enterprise Security Management Policy Management

| Component | Event | Additional Information |
|-----------------------------|---|--|
| | | signed/verified. |
| FCS_COP.1(3) (optional) | Failure of hashing function. | Cryptographic mode of operation, name/identifier of object being hashed. |
| FCS_COP.1(4) (optional) | Failure in Cryptographic Hashing for Non-Data Integrity. | Cryptographic mode of operation, name/identifier of object being hashed. |
| FCS_RBG_EXT.1 (optional) | Failure of the randomization process. | None |
| 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 |
| FIA_USB.1 | Successful and unsuccessful binding of user attributes to a subject | None |
| FMT_MSA.1 | All modifications of security attributes | None |
| FMT_MSA.3 | All modifications of the initial values of security attributes | Attribute modified, modified value |
| FMT_SMF.1 | Use of the management functions | Management function performed |

| Component | Event | Additional Information |
|--------------|--|---|
| FMT_SMR.1 | Modifications to the members of the management roles | None |
| 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 |
| 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.

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_SEL_EXT.1 External selective audit

Hierarchical to: No other components.

FAU_SEL_EXT.1.1 The TSF shall be able to select the set of events to be audited by an ESM Access Control product from the set of all auditable events based on the following attributes:

- a) [selection: object identity, user identity, subject identity, host identity, event type]; and
- b) [*assignment: list of additional attributes that audit selectivity is based upon*]

Application Note: This requirement is for the ability of the TOE to configure the auditing function of an Access Control product. This is a complement to the FAU_SEL.1 requirement included in the Access Control Protection Profile.

Dependencies: FAU_GEN.1 Audit data generation
FMT_MTD.1 Management of TSF data

Assurance Activity:

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

The evaluator shall test this capability by configuring a compatible Access Control product to have:

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

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

enabled events are recorded by the Access Control product.

FAU_STG_EXT.1 External audit trail storage

Hierarchical to: No other components.

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

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

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] 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 use an external repository for audit storage. The evaluator shall also check the operational guidance in order to determine that a discussion on the interface to this repository is provided, including how the connection to it is established, how data is passed to it, and what happens when a connection to the repository is lost and subsequently re-established.

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

6.1.4 Class FCS: Cryptographic Support

The cryptographic requirements for the TOE can either be implemented by the TSF or by reliance on non-ESM Operational Environment components. The expectation is that the TSF is able to utilize a suite of cryptographic algorithms that have been previously validated rather than forcing vendors to implement their own unique and redundant cryptographic capabilities. The ST should clearly indicate what cryptographic capabilities

are used by the TSF. 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 Class FIA: Identification and Authentication

FIA_AFL.1 Authentication failure handling

Hierarchical to: No other components

FIA_AFL.1.1 The TSF shall detect when [selection: [assignment: *positive integer number*], an administrator configurable positive integer within [assignment: *range of acceptable values*]] unsuccessful authentication attempts occur related to [assignment: *list of authentication events*].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [selection: met, surpassed], the TSF shall [assignment: *list of actions*].

Dependencies: FIA_UAU.1 Timing of authentication

Assurance Activity:

The evaluator shall check the 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. 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*
 - 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 in order to determine how the TOE determines whether a 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.

FIA_USB.1 User-subject binding

Hierarchical to: No other components.

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **[assignment: list of user security attributes]**.

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[assignment: rules for the initial association of attributes]**.

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[assignment: rules for the changing of attributes]**.

Dependencies: FIA_ATD.1 User attribute definition

Assurance Activity:

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

The evaluator shall test this capability by configuring the TSF to accept user information from external sources as defined by the ST. The evaluator shall then perform authentication activities using these methods and validate that authentication is successful in each instance. Based on the defined privileges assigned to each of the subjects, the evaluator shall then perform various management tests in order to determine that the user authorizations are consistent with their externally-defined

attributes and the configuration of the TSF's access control policy. For example, if a user who is defined in an LDAP repository belongs to a certain group and the TSF is configured such that members of that group only have read-only access to policy information, the evaluator shall authenticate to the TSF as that user and verify that as a subject under the control of the TSF that they do not have write access to policy information. This verifies that the aspects of the user's identity data that are pertinent to how the TSF treats the user are appropriately taken from external sources and utilized in order to determine what the user is able to do.

6.1.6 Class FMT: Security Management

FMT_MOF_EXT.1 External management of functions behavior

Hierarchical to: No other components.

FMT_MOF_EXT.1.1 The TSF shall restrict the ability to query the behavior of, modify the functions of Access Control products: *audited events, repository for remote audit storage, Access Control SFP, policy version being implemented, Access Control SFP behavior to enforce in the event of communications outage, [assignment: other functions] to [assignment: the authorized identified roles].*

Application Note: This requirement primarily pertains to the ability of the TSF to manage the behavior of an Access Control product. This is the complement to the FMT_MOF.1 requirement included in the Access Control Protection Profile.

Dependencies: FMT_SMF.1 Specification of management functions

FMT_SMR.1 Security roles

Assurance Activity:

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

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

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

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

Once this has been done, the evaluator shall reconfigure the TOE and Policy Management product such that the Policy Management product is no longer authorized

to configure the TOE. The evaluator shall then attempt to use the Policy Management product to configure the TOE and observe that it is either disallowed or that the option is not even present.

FMT_MSA.1(1) Management of security attributes (internal attributes)

Hierarchical to: No other components.

FMT_MSA.1.1(1) The TSF shall restrict the ability to [selection: change default, query, modify, delete, ***assignment: other operations***] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles].

Application Note: This iteration must include the following attributes at minimum:

- *Attributes that define the TSF's own access control policy; and*
- *Attributes that define the TSF's connection to other ESM products and environmental repositories*

Assurance Activity:

The evaluator shall review the ST and operational guidance to determine that it describes how the TSF maintains its own access control internally (i.e. "if I'm an administrator on the PM TOE, how do I say who my users are, what AC products they can control, and to what extent can they control those AC products"). The evaluator shall perform testing to confirm that described behaviors exhibit the documented semantics (i.e. set up a new user, give them privileges, log in and see that those privileges were granted, change some attributes that will affect their privileges, log back in and see that those privileges have been changed).

The evaluator shall also review the ST and operational guidance to determine how the TOE is associated with ESM Access Control products. The evaluator shall verify how the TOE discovers AC products in the operational environment and how it is recognized as the valid controller of those products. The evaluator shall confirm this behavior with

testing. One approach to doing this is to place the TOE and two compatible AC products on the same network. The evaluator shall follow the documented configuration steps such that one of the AC products is associated with the TOE. The evaluator shall then confirm that they now have the ability to manage only that AC product. The evaluator shall capture traffic and replaying it against the other AC product and confirm that it has no effect.

The evaluator shall review the ST and operational guidance to determine if there are any other defined internal security attributes. If there are, the evaluator shall verify that they can be configured in the manner specified by the evidence, and that their configuration has the effect defined in the evidence.

FMT_MSA.1(2) Management of security attributes (external attributes)

FMT_MSA.1.1(2) The TSF shall restrict the ability to [selection: change default, query, modify, delete, ***assignment: other operations***] the security attributes [assignment: list of security attributes] to [assignment: the authorised identified roles].

Application Note: This iteration must include the following attributes at minimum:

- *Attributes that define policies that are exported to other ESM Access Control products*

Application Note: This SFR has been broken up into two iterations for clarity. The first iteration defines the security attributes managed by the TSF that are subsequently used by the TSF. The second iteration defines the security attributes managed by the TSF that pertain to access control policies that are transmitted to external Access Control products.

Dependencies: [FDP_ACC.1 Subset access control, or
FDP_IFC.1 Subset information flow control]
FMT_SMR.1 Security roles

FMT_SMF.1 Specification of Management Functions

Assurance Activity:

The evaluator shall review the ST in order to determine that it specifies the operations that can be managed by the TSF. For example, the TSF must have the ability to create policies. The data that can comprise these policies should be defined in the ST. The evaluator shall then check the operational guidance in order to determine that it defines a set of managed attributes consistent with the ST and the TSF mechanisms by which these attributes can be manipulated.

The evaluator shall test this capability by performing, for each defined attribute and operation, an operation on the TSF that manipulates the attribute. They should also verify that the mechanism of session establishment is defined so that it's understood how permissions to operate the TSF come to be assigned to users who provide a collection of external identification and authentication information to it.

FMT_MSA.3 Static attribute initialization

Hierarchical to: No other components.

FMT_MSA.3.1 The TSF shall enforce the [**assignment: access control SFP(s)**] to provide restrictive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**assignment: the authorized identified roles**] to specify alternative initial values to override the default values when an object or information is created.

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

Assurance Activity:

The evaluator shall review the operational guidance in order to determine that it defines what the default values are for managed attributes. The evaluator shall test this capability by performing activities against the TSF that involve the instantiation of new

security attributes and verifying that the default values are consistent with the description in the guidance and that they can collectively be described in the manner defined by the ST.

FMT_MSA_EXT.5 Consistent security attributes

Hierarchical to: No other components.

FMT_MSA_EXT.5.1 The TSF shall [selection: identify the following internal inconsistencies within a policy prior to distribution: ***[assignment: non-empty list of inconsistencies]***; only permit definition of unambiguous policies].

Application Note: The most common expected type of inconsistency is the case where one part of a policy allows a subject access to an object and another part denies the same subject access to the same object.

Application Note: If the TOE's policy management engine defines an unambiguous hierarchical method of implementing a policy such that no contradictions occur, the ST author indicates that non unambiguous policies can be defined. If this is the case, it is expected that the TSS or operational guidance provides an overview of how contradictory policy is prevented by the TOE.

FMT_MSA_EXT.5.2 The TSF shall take the following action when an inconsistency is detected: [selection: issue a prompt for an administrator to manually resolve the inconsistency, ***[assignment: other action]***].

Application Note: If the TOE's policy management engine defines an unambiguous hierarchical method of implementing a policy such that no contradictions occur, FMT_MSA_EXT.5.2 is vacuously satisfied as it is impossible to have inconsistencies to detect.

Dependencies: FMT_MOF_EXT.1 External Management of Functions Behavior

Assurance Activity:

The evaluator shall review the operational guidance in order to determine that it explains what potential contradictions in policy data may exist. For example, a policy could potentially contain two rules that permit and forbid the same subject from accessing the same object. Alternatively, the TOE may define an unambiguous hierarchy that makes it impossible for contradictions to occur.

The evaluator shall test this capability by defining policies that contain the contradictions indicated in the operational guidance and observing if the TSF responds by detecting the contradictions and reacting in the manner prescribed in the ST. If the TSF behaves in a manner that prevents contradictions from occurring, the evaluator shall review the operational guidance in order to determine if the mechanism for preventing contradictions is described and if this feature is communicated to administrators. This feature should be tested in conjunction with a compatible Access Control product; in other words, if the TOE has a mechanism that prevents contradictions (for example, if a deny rule always supersedes an allow rule), then correct enforcement of such a policy by a compatible Access Control product is both a sufficient and a necessary condition for demonstrating the effectiveness of this mechanism.

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: ***[assignment: list of management functions to be provided by the TSF]***.

Application Note: Management functions listed in Table 4 below must be claimed by Security Target author where applicable.

Application Note: Security Target authors may, and are encouraged to, add additional security relevant operations, objects, and security attributes to the table. Additional objects may be

added to existing operations and additional security attributes may be added to existing objects.

Dependencies: No dependencies.

Table 4. Management Functions within the TOE

| Requirement | Management Activities |
|----------------------|--|
| ESM_ACD.1 | Creation of policies |
| ESM_ACT.1 | Transmission of policies |
| ESM_ATD.1 (optional) | Definition of object attributes. Association of attributes with objects. |
| ESM_ATD.2 (optional) | Definition of subject attributes. Association of attributes with subjects. |
| FAU_SEL_EXT.1 | Configuration of auditable events for defined external entities |
| FAU_STG_EXT.1 | Configuration of external audit storage location |
| FIA_AFL.1 | Configuration of authentication failure threshold value, configuration of actions to take when threshold is reached, execution of restoration to normal state following threshold action (if applicable) |
| FIA_SOS.1 | Management of the metric used to verify secrets |
| FIA_UAU.2 | Management of authentication data for both interactive users and authorized IT entities |
| FIA_UID.2 | Management of user identities for both interactive users and authorized IT entities |
| FIA_USB.1 | Definition of default subject security attributes, modification of subject security attributes |
| FMT_MOF_EXT.1 | Configuration of the behavior of other ESM products |
| FMT_MSA.1 | Management of sets of subjects that can interact with security |

| Requirement | Management Activities |
|---------------|---|
| | attributes, Management of rules by which security attributes inherit specified values |
| FMT_MSA.3 | Managing the subjects that can specify initial values, Managing the permissive or restrictive setting of default values for a given access control SFP, Management of rules by which security attributes inherit specified values |
| FMT_MSA_EXT.5 | Configuration of what policy inconsistencies the TSF should identify and how the TSF should respond if any inconsistencies are detected (if applicable) |
| FMT_SMR.1 | Management of the users that belong to a particular role |
| FTA_TAB.1 | Maintenance of the banner |
| 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 and 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 *Policy Administrator* to refer to an individual who is authorized to write and distribute access control policies. 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 “*Policy Administrator*”.

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_MSA.1(1).

6.1.7 Class FTA: TOE Access

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. If the banner is not displayed by default, the evaluator shall

configure the TOE in accordance with the operational guidance in order to enable its display. The evaluator shall then attempt to access the TOE and verify that a TOE banner exists. If applicable, the evaluator will also attempt to utilize the functionality to modify the TOE access banner as per the standards defined in FMT_SMF.1 and verify that the TOE access banner is appropriately updated.

6.1.8 Class FTP: Trusted Paths/Channels

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

Hierarchical to: No other components.

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

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

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

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

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

communications to authentication server, etc.).

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check the operational guidance in order to determine the mechanism by which secure communications are enabled. The evaluator shall also check the TSS, operational guidance, and other provided evidence to determine 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 operational guidance, ST, and any available design documentation to see how cryptography is utilized and to verify that the functions used have been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national standard for the nation in which the evaluation is being conducted.*

The evaluator shall test this capability by enabling secure communications on the TOE and placing a packet sniffer on the local network. They shall then use the TOE to perform actions that require communications to all trusted IT products with which it communicates and observe the captured packet traffic that is directed to or from the TOE to ensure that their contents are obfuscated.

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

Hierarchical to: No other components.

FTP_ITC.1.1(2) **Refinement:** The TSF shall *use* [assignment: *FCS-specified service*] *in providing a trusted* communication channel between itself and *authorized IT entities* that is logically distinct from other communication channels and provides assured identification of its end points and

detection of the modification of data.

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

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 policy data, [assignment: other functions]***.

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

Dependencies: No dependencies.

Assurance Activity:

The evaluator shall check the operational guidance in order to determine the mechanism by which secure communications are enabled. The evaluator shall also check the TSS, operational guidance, and other available evidence to determine 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 operational guidance, ST, and any available design documentation to see how cryptography is utilized and to verify that the functions used have been validated by FIPS 140-2 (if evaluating in the United States or Canada) or an equivalent national standard for the nation in which the evaluation is being conducted.

The evaluator shall test this capability by enabling secure communications on the TOE and placing a packet sniffer on the local network. They shall then use the TOE to perform actions that require communications to all trusted IT products with which it communicates and observe the captured packet traffic that is directed to or from the TOE to ensure that their contents are obfuscated.

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

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

6.1.9 Unfulfilled Dependencies

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

- | | |
|-----------|--|
| FDP_ACC.1 | This SFR is an unfulfilled dependency on FMT_MSA.1. It has not been included because a formal access control SFP for determining administrator authorities is not required by the PP. FMT_MSA.1 should be applied in the same manner as FMT_MOF.1. Rather than applying a specific access control SFP to defining authorizations to manage security attributes, restricting it to assigned roles or other logical grouping of users is sufficient for this PP. |
| FIA_ATD.1 | This SFR is an unfulfilled dependency on FIA_USB.1. It has not been included because the ESM Policy Management product is expected to <i>utilize</i> user security attributes rather than <i>define</i> them. Any attributes that can be used to define policies should already be defined by a compatible Identity and Credential Management product; if not, they may be defined by the ESM_ATD components. |
| 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 are a formal instantiation of the Security Objectives. The PP draws from EAL1 the Security Assurance Requirements (SARs) to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

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

6.2.1 Class ADV: Development

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

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

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 invocable 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 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 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 6.1. The Assurance Activities identify the minimum testing activities associated with these components. The evaluator produces a test report documenting the plan for and results of testing, as well as coverage arguments focused on the platform/TOE combinations that are claiming conformance to this PP.

Developer action elements:

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

Content and presentation elements:

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

Evaluator action elements:

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

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

Assurance 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 |
|---|--|--|
| <p>A.ESM – The TOE will be able to establish connectivity to other ESM products in order to share security data.</p> | <p>OE.AUDIT – The Operational Environment will provide a remote location for storage of audit data.</p> | <p>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.</p> |
| | <p>OE.PROTECT – One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets.</p> | <p>If the TOE does not provide policy data to at least one Access Control product, then there is no purpose to its deployment.</p> |
| <p>A.MANAGE – There will be one or more competent individuals assigned to install, configure, and operate the TOE.</p> | <p>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.</p> | <p>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.</p> |

| | | |
|---|---|---|
| | <p>OE.INSTAL – Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a secure manner.</p> | <p>If administrators are able to ensure the secure setup and operation of the TOE, it's assumed that they are competent.</p> |
| | <p>OE.PERSON – Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.</p> | <p>If proper care is taken for the selection and training of administrators, then there is an expectation that they will subsequently perform their duties.</p> |
| <p>A.USERID – The TOE will receive identity data from the Operational Environment.</p> | <p>OE.USERID – The Operational Environment must be able to identify a user requesting access to the TOE.</p> | <p>The expectation of an ESM product is that it is able to utilize organizationally-maintained identity data that resides in the Operational Environment.</p> |

Table 7. Policies, Threats, Objectives, and Rationale

| Policies/Threats | Objectives | Rationale |
|---|---|---|
| <p>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.</p> | <p>O.BANNER – The TOE will display an advisory warning regarding use of the TOE.</p> | <p>FTA_TAB.1</p> <p>The requirement for the TOE to display a banner is sufficient to ensure that this policy is implemented.</p> |

| | | |
|---|--|---|
| <p>T.ADMIN_ERROR – An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.</p> | <p>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.</p> | <p>This objective requires the TOE to have designated administrators for the configuration of the TOE, that allows the TOE some assurance that the TOE will be managed and configured consistently.</p> |
| | <p>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.</p> | <p>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.</p> |
| | <p>OE.PERSON – Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.</p> | <p>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.</p> |
| <p>T.CONTRADICT – A careless administrator may create a policy that contains contradictory rules for access control enforcement resulting in a security policy that does not have unambiguous enforcement rules.</p> | <p>O.CONSISTENT – The TSF will provide a mechanism to identify and rectify contradictory policy data.</p> | <p>FMT_MSA_EXT.5</p> <p>The ability of the TSF to detect inconsistent data and to provide the ability to correct any detected inconsistencies will ensure that only consistent policies are transmitted to Access Control products for consumption.</p> |

| | | |
|--|--|--|
| <p>T.EAVES – A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.</p> | <p>O.DISTRIB – The TOE will provide the ability to distribute policies to trusted IT products using secure channels.</p> | <p>ESM_ACT.1 FTP_ITC.1(1)</p> <p>The TOE will leverage third-party cryptographic tools to generate CSPs for usage within the product and its sensitive connections. The TOE will be expected to use appropriate CSPs for the encryption, hashing, and authentication of data sent over trusted channels to external products and between TOE components in the event of a multiple-box deployment.</p> |
| | <p>O.EAVES – The TOE will either leverage a third-party cryptographic suite or contain the ability to utilize cryptographic algorithms to secure the communication channels to and from itself.</p> | <p>FTP_ITC.1(1) 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</p> <p>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.</p> |

| | | |
|--|---|---|
| <p>T.FORGE – A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product.</p> | <p>O.ACCESSID – The TOE will contain the ability to validate the identity of other ESM products prior to distributing data to them.</p> | <p>FTP_ITC.1(1)</p> <p>Requiring an Access Control product to provide proof of its identity prior to the establishment of a trusted channel from the TOE will reduce the risk that the TOE will disclose authentic policies to illegitimate sources. This reduces the risk of policies being examined for reconnaissance purposes.</p> |
| | <p>O.AUTH – The TOE will provide a mechanism to examine human and IT entity user identity data from the Operational Environment and determine the extent to which the claimed identity should be able to perform TSF management functions.</p> | <p>FIA_UAU.2 FIA_UID.2</p> <p>The Policy Management product is expected only to exchange policy information with authorized and identified external IT entities.</p> |
| | <p>O.INTEGRITY – The TOE will contain the ability to assert the integrity of policy data.</p> | <p>FTP_ITC.1(2)</p> <p>Providing assurance of integrity of policy data sent to the Access Control product allows for assurance that the policy the Access Control product receives is the policy that was intended for it.</p> |

| | | |
|--|---|--|
| | <p>O.SELFID – The TOE will be able to confirm its identity to the ESM deployment upon sending data to other processes within the ESM deployment.</p> | <p>FTP_ITC.1(1)</p> <p>Requiring the TOE to provide proof of its identity prior to the establishment of a trusted channel with an Access Control product will help mitigate the risk of the Access Control product consuming a forged policy.</p> |
|--|---|--|

| | | |
|---|---|---|
| <p>T.UNAUTH – A malicious user could bypass the TOE’s identification, authentication, and authorization mechanisms in order to utilize the TOE’s management functions.</p> | <p>O.AUDIT – The TOE will provide measures for generating security relevant events that will detect access attempts to TOE-protected resources by users.</p> | <p>FAU_GEN.1 FAU_STG_EXT.1 FPT_STM.1 (optional)</p> <p>The Policy Management product will only allow properly identified users to perform actions. The Policy Management product will also be required to generate audit logs for each security-relevant action performed by users of the TOE. In addition, the TOE must provide some functionality to review audited events locally such that malicious actions can be determined. The TOE must also provide functionality to offload audited event data to an Audit Manager ESM component or other external repository. Appropriate accountability for actions performed on the TOE can aid in the detection of and mitigate the impact of unauthorized actions.</p> |
|---|---|---|

| | | |
|--|---|--|
| | <p>O.AUTH – The TOE will provide a mechanism to examine human and IT entity user identity data from the Operational Environment and determine the extent to which the claimed identity should be able to perform TSF management functions.</p> | <p>FIA_UAU.2 FIA_UID.2 FIA_USB.1 FMT_MSA.1(1) FMT_SMR.1 FTP_TRP.1</p> <p>The Policy Management product is required to have its own access control policy defined to allow authorized users and disallow unauthorized users specific management functionality within the product. Doing so requires the user to be successfully identified and authenticated and to have an established session such that the user session contains their applicable subjects.</p> |
| | <p>O.MANAGE – The TOE will provide the ability to manage the behavior of trusted IT products using secure channels.</p> | <p>FAU_SEL_EXT.1 FMT_MOF_EXT.1 FMT_MSA.1(2) FMT_SMF.1</p> <p>The TSF is required to include the ability to configure the auditable events for, at minimum, a compatible Access Control product. This helps ensure that relevant audit data is being recorded throughout the ESM deployment.</p> |

| | | |
|--|--|---|
| <p>T.WEAKIA - A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.</p> | <p>O.ROBUST - The TOE will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.</p> | <p>FIA_AFL.1 FIA_SOS.1 FTA_TSE.1 (optional) FTA_SSL_EXT.1 (optional) FTA_SSL.3 (optional) FTA_SSL.4 (optional)</p> <p>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 handling, it decreases the number of individual guesses an attacker can make.</p> |
| <p>T.WEAKPOL – A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity.</p> | <p>O.POLICY – The TOE will provide the ability to generate policies that are sufficiently detailed to satisfy the Data Protection requirements for one or more technology types in the Standard Protection Profile for Enterprise Security Management Access Control.</p> | <p>ESM_ACD.1 ESM_ATD.1 (optional) ESM_ATD.2 (optional) FMT_MSA.1(2) FMT_MSA.3 FMT_SMF.1</p> <p>The Policy Management product must provide the ability to define policies. These policies must be robust, and they must be restrictive by default. This will ensure that strong policies are created that are capable of utilizing the full set of access control functions of compatible products.</p> |

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.USERID | The TOE will receive identity data from the Operational Environment. |

8.1.2 Physical Assumptions

No physical assumptions are prescribed in this Protection Profile 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. |

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.CONDTRADICT | A careless administrator may create a policy that contains contradictory rules for access control enforcement. |
| T.EAVES | A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data. |
| T.FORGE | A malicious user may exploit a weak or nonexistent ability for the TOE to provide proof of its own identity in order to send forged policies to an Access Control product. |
| T.UNAUTH | A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly utilize the TOE's management functions. |
| T.WEAKPOL | A Policy Administrator may be incapable of using the TOE to define policies in sufficient detail to facilitate robust access control, causing an Access Control product to behave in a manner that allows illegitimate activity or prohibits legitimate activity. |
| T.WEAKIA | A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials. |

8.3 Organizational Security Policies

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

Table 11. Organizational Security Policies

| Assumption Name | Assumption Definition |
|-----------------------|--|
| P.BANNER ⁶ | 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.

⁶ 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

| TOE Security Obj. | TOE Security Objective Definition |
|--------------------------|---|
| O.ACCESSID | The TOE will contain 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 examine human and IT entity user identity data received from the Operational Environment and determine the extent to which the claimed identity should be able to perform TSF management functions. |
| O.BANNER | The TOE will display an advisory warning regarding use of the TOE. |
| O.CONSISTENT | The TSF will provide a mechanism to identify and rectify contradictory policy data. |
| O.DISTRIB | The TOE will provide the ability to distribute policies to trusted IT products using secure channels. |
| O.MANAGE | The TOE will provide the ability to manage the behavior of trusted IT products using secure channels. |
| O.EAVES | The TOE will either leverage a third-party cryptographic suite or contain the ability to utilize cryptographic algorithms to secure the communication channels to and from itself. |
| O.INTEGRITY | The TOE will contain the ability to assert the integrity of policy data. |
| O.POLICY | The TOE will provide the ability to generate policies that are sufficiently detailed to satisfy the Data Protection requirements for one or more technology types in the Standard Protection Profile for Enterprise Security Management Access Control. |
| 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 data to other processes within the ESM deployment. |

8.4.2 Security Objectives for the Operational Environment

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

Table 13. Security Objectives for the Operational Environment

| Environmental Security Obj. | Environmental Security Objective Definition |
|------------------------------------|---|
| OE.ADMIN | There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE. |
| OE.AUDIT | The Operational Environment will provide a remote location for storage of audit data. |
| OE.INSTAL | Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a secure manner. |
| OE.PERSON | Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE. |
| OE.PROTECT | One or more ESM Access Control products will be deployed in the Operational Environment to protect organizational assets. |
| OE.USERID | The Operational Environment must be able to identify a user requesting access to the TOE. |

Appendix A - Supporting Tables and References

A.1 References

- (1) Booz Allen Hamilton, Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 1.x, forthcoming
- (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

| Acronym | Definition |
|---------|--|
| ABAC | Attribute-Based Access Control |
| CC | Common Criteria |
| CM | Configuration Management |
| DAC | Discretionary Access Control |
| ESM | Enterprise Security Management |
| IT | Information Technology |
| LDAP | Lightweight Directory Access Protocol |
| MAC | Mandatory Access Control |
| NIST | National Institute of Standards and Technology |
| OE | Operational Environment |
| OS | Operating System |
| OSP | Organizational Security Policy |
| PM | Policy Management |
| PP | Protection Profile |
| RBAC | Role-Based Access Control |
| SAR | Security Assurance Requirement |

| Acronym | Definition |
|----------------|---------------------------------|
| SCM | Secure Configuration Management |
| SFP | Security Function Policy |
| SFR | Security Functional Requirement |
| ST | Security Target |
| TSF | TOE Security Function |
| TFSI | TOE Security Function Interface |

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

| CC SFR/SAR | NIST 800-53 Control | | Comments and Observations |
|---|--|------|---|
| Common Criteria Version 3.x Security Functional Requirements (SFRs) and PP extended SFRs | | | |
| ESM_ACD.1 | Access Control Policy Definition Access Control Policy Definition | AC-2 | Account Management specifying access privileges Partial. ESM_ACD.1 provides the TOE the ability to define access control policies that can be subsequently enforced by Access Control products. This provides the access privilege specification aspect of AC-2. |
| | | AC-3 | Access Enforcement System enforces authorizations Partial. Although AC-3 focuses on the enforcement, critical to enforcement is the ability to define the policy to be enforced. |

Standard Protection Profile for Enterprise Security Management Policy Management

| CC SFR/SAR | | NIST 800-53 Control | | Comments and Observations |
|----------------------|--|--|--|---|
| | | AC-3(3) | Access Enforcement Non-discretionary access control | Partial. This control defines the subject, objects, and operations to be controlled by this policy. |
| | | AC-3(4) | Access Enforcement Discretionary access control | Partial. This control defines the subject, objects, and operations to be controlled by this policy. |
| | | Note: The presumption is that ESM_ACD is roughly parallel to the FDP_ACC and FDP_IFC controls, in that they define the policy that is enforced elsewhere. | | |
| ESM_ACT.1 | Access Control Policy Transmission Access Control Policy Transmission | AC-2 | Account Management specifying access privileges | Partial. ESM_ACD.1 provides the TOE the ability to transmit access control policies that can be subsequently enforced by Access Control products. This provides the access privilege specification aspect of AC-2. |
| ESM_ATD.1 (optional) | Attribute Definition Object Attribute Definition | AC-3 | Access Enforcement System enforces authorizations | Partial. This control defines the object attributes critical to policy enforcement. |
| | | AC-3(3) | Access Enforcement Non-discretionary access control | Partial. This control defines the object attributes critical to policy enforcement. |
| | | AC-3(4) | Access Enforcement Discretionary access control | Partial. This control defines the object attributes critical to policy enforcement. |
| ESM_ATD.2 (optional) | Attribute Definition Subject Attribute Definition | AC-2 | Account Management specifying access privileges | Partial. This control defines the subject attributes critical to policy enforcement. |
| | | AC-3 | Access Enforcement System enforces authorizations | Partial. This control defines the subject attributes critical to policy enforcement. |
| | | AC-3(3) | Access Enforcement Non-discretionary access control | Partial. This control defines the subject attributes critical to policy enforcement. |
| | | AC-3(4) | Access Enforcement Discretionary access control | Partial. This control defines the subject attributes critical to policy enforcement. |

Standard Protection Profile for Enterprise Security Management Policy Management

| CC SFR/SAR | | NIST 800-53 Control | | Comments and Observations |
|------------|---|--|---|---|
| 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. |
| | | 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. | | |

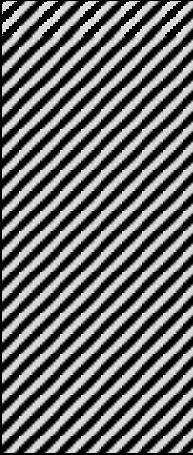
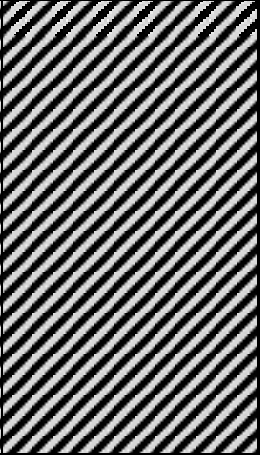
Standard Protection Profile for Enterprise Security Management Policy Management

| CC SFR/SAR | | NIST 800-53 Control | | Comments and Observations |
|---|--|---------------------|---|---|
| FAU_SEL_EXT.1 | Security Audit Event Selection External Selective Audit | AU-12 | Audit Generation Generate and pre-select on [components] | Partial. FAU_SEL.1 goes to item b of the AU-12 control. |
| 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.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). | | | | |
| FCS_COP.1(1) FCS_COP.1(2) FCS_COP.1(3) FCS_COP.1(4) (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 <i>not</i> 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. | | | | |

Standard Protection Profile for Enterprise Security Management Policy Management

| CC SFR/SAR | | NIST 800-53 Control | | Comments and Observations |
|-----------------------------|--|---------------------|---|--|
| 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. |

Standard Protection Profile for Enterprise Security Management Policy Management

| CC SFR/SAR | | NIST 800-53 Control | | Comments and Observations |
|---------------|--|---|--|---|
| FIA_USB.1 | User-Subject Binding User-Subject Binding |  |  | No Mapping. This SFR requires that the TSF associate particular user attributes with subjects, and enforces a set of rules when initially assigning or changing those attributes. AC-16 addresses the binding of attributes to information, but not explicitly to subjects in the same sense as FIA_USB.1. |
| FMT_MOF_EXT.1 | Management of Functions in TSF Management of External Security Functions Behavior | AC-3(3) | Access Enforcement Non-discretionary access control | Partial. Restriction of management functions to particular roles is at least a partial implementation of RBAC. |
| FMT_MSA.1(1) | Management of Security Attributes Management of Security Attributes (Internal Attributes) | SI-9 | Information Input Restrictions Restricts ability to input information to authorized persons | Partial. The SFR would seem to imply this control, although the SFR is much more specific. |
| FMT_MSA.1(2) | Management of Security Attributes Management of Security Attributes (External Attributes) | SI-9 | Information Input Restrictions Restricts ability to input information to authorized persons | Partial. The SFR would seem to imply this control, although the SFR is much more specific. |

Standard Protection Profile for Enterprise Security Management Policy Management

| CC SFR/SAR | | NIST 800-53 Control | | Comments and Observations |
|---------------|---|---------------------|---|---|
| FMT_MSA.3 | <p><u>Management of Security Attributes</u> Static Attribute Initialization</p> | [Hatched Area] | | <p>No Mapping. There appears to be no control corresponding to this SFR. The SFR requires the TOE to provide [selection, choose one of: restrictive, permissive, [assignment: other property]] default values for security attributes that are used to enforce the security policy, as well as allowing the [assignment: the authorised identified roles] to specify alternative initial values to override the default values when an object or information is created.</p> |
| FMT_MSA_EXT.5 | <p><u>Management of Security Attributes</u> Consistent Security Attributes</p> | [Hatched Area] | | <p>No Mapping. This SFR requires the TSF to define consistent security attributes for access control policies and take action when inconsistencies are detected. There are no specific controls that require defined attributes to be consistent.</p> |
| FMT_SMF.1 | <p><u>Specification of Management Functions</u> Specification of Management Functions</p> | [Hatched Area] | | <p>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.</p> |
| FMT_SMR.1 | <p><u>Security Management Roles</u> Security Roles</p> | AC-2(7) | Account Management Role-based schemes | <p>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.</p> |

Standard Protection Profile for Enterprise Security Management Policy Management

| CC SFR/SAR | | NIST 800-53 Control | | Comments and Observations |
|--------------------------|---|---------------------|--|--|
| | | 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_STM.1 (optional) | <u>Time Stamps</u> 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) | <u>Session Locking and Termination</u> 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) | <u>Session Locking and Termination</u> 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. |

Standard Protection Profile for Enterprise Security Management Policy Management

| CC SFR/SAR | | NIST 800-53 Control | | Comments and Observations |
|---|---|--|--|---|
| 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. |
| FTA_TSE.1 (optional) | TOE Session Establishment TOE Session Establishment | | | No Mapping. This SFR requires that the TOE be able to deny session establishment based on [assignment: attributes]. This is too broad to map to a NIST SP 800-53 Revision 3 control. |
| 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 | ST Introduction ST Introduction | | | No Mapping. This SAR deals with format and structure of the Security Target, a description of the |

Standard Protection Profile for Enterprise Security Management Policy Management

| CC SFR/SAR | | NIST 800-53 Control | | Comments and Observations |
|---|---|---------------------|--|--|
| EAL5 EAL6 EAL7 | | | | functional and assurance requirements of the product to be evaluated. |
| ASE_CCL.1 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7 | <u>Conformance Claims</u> 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 | <u>Security Problem Definition</u> 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 | <u>Security Objectives</u> Security Objectives for the Operational Environment | | | No Mapping. This SAR deals with format and structure of the Security Target, a description of the functional and assurance requirements of the product to be evaluated. |
| ASE_OBJ.2 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7 | <u>Security Objectives</u> 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 | <u>Extended Components Definition</u> 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. |

Standard Protection Profile for Enterprise Security Management Policy Management

| CC SFR/SAR | | NIST 800-53 Control | | Comments and Observations |
|--|--|---------------------|--|--|
| 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 EAL1 EAL2 EAL3 EAL4 EAL5 EAL6 EAL7 | TOE Summary Specification TOE Summary Specification | SA-4(1) | Acquisitions Acquisition documents describe functional properties of security controls to support analysis/test | Partial. The TSS in the ST describes <i>how</i> 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 | Partial. The ADV_FSP family |

Standard Protection Profile for Enterprise Security Management Policy Management

| CC SFR/SAR | | NIST 800-53 Control | | Comments and Observations |
|---|--|---|--|--|
| | | | Documents describe security-relevant external interfaces to support analysis/test | 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 <i>product</i> , whereas CM-9 is focused on the <i>system</i> . |
| | | 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 <i>product</i> , whereas CM-9 is focused on the <i>system</i> . |
| | | SA-10 | Developer Configuration Management | Partial. ALC_CMS captures some of the developer |

Standard Protection Profile for Enterprise Security Management Policy Management

| CC SFR/SAR | | NIST 800-53 Control | | Comments and Observations |
|-------------------|---|--|--|--|
| | | | Developer has configuration management during development; flaw tracking | 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. |
| | | <p>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.</p> <p>Note: ATE_IND.1 only has independent oversight for a portion of the test suite.</p> | | |
| AVA_VAN.1 EAL1 | Vulnerability Analysis Vulnerability Survey | CA-2(2) | Security Assessments [announced/unannounced] security testing (e.g., penetration testing) | Partial. This addresses the requirement to conduct penetration testing. |
| | | RA-3 | Risk Assessment Conduct/document/review risk assessments | Partial. Conceivably, part of a risk assessment is doing a survey of vulnerabilities. Note that the CC does not imply formal vulnerability scanning, which is RA-5. |
| | | SA-11(2) | Developer Security Testing Developer vulnerability analysis | Partial. AVA_VAN requires that there be a vulnerability analysis performed. |
| | | <p>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</p> | | |

Standard Protection Profile for Enterprise Security Management Policy Management

| CC SFR/SAR | NIST 800-53 Control | Comments and Observations |
|------------|---------------------|---------------------------|
| | | vulnerability assessment. |

Appendix C - Architectural Variations and Additional Requirements

C.1 Attribute Definition

At minimum, this Protection Profile requires a conformant TOE to be able to define and distribute access control policies. Policies may require subject and/or object attributes in order to facilitate sufficiently granular access control for an enterprise. The ESM must therefore include the capability to define and maintain subject and/or object attribute data. Definition of attributes may be handled through the Policy Management component, or they may be handled by the Standard Protection Profile for ESM Identity and Credential Management. The SFRs in this section should be used if subject or object attribute definition capabilities are to be part of the Policy Management component. If a TOE claiming conformance to this PP does not include this capability, then it must be compatible with an Identity and Credential Management product that does.

C.1.1 ESM_ATD.1 Object attribute definition

Hierarchical to: No other components.

ESM_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual objects: [**assignment: list of security attributes**].

ESM_ATD.1.2 The TSF shall be able to associate security attributes with individual objects.

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

Dependencies: No dependencies.

Assurance Activity:

The evaluation team must determine through the evaluation of design documents how exactly to generate and utilize object data within the TOE. The evaluation team must then generate this information through normal TOE functionality that will apply the data to a

desired object or set of objects. The evaluation team 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 evaluation team should attempt to perform actions against the object with both positive and negative expected results.

In addition to this inclusion, the following augmentations should be made to existing SFRs as currently prescribed by the PPs:

- FMT_MSA.1 must be assumed to apply to object security attributes in addition to subject attributes.

C.1.2 ESM_ATD.2 Subject attribute definition

Hierarchical to: No other components.

ESM_ATD.2.1 The TSF shall maintain the following list of security attributes belonging to individual subjects: [**assignment: list of security attributes**].

ESM_ATD.2.2 The TSF shall be able to associate security attributes with individual subjects.

Application Note: Subject security attributes refer to attributes that may ultimately factor into an access control decision and are associated with active entities under the access control policy.

Dependencies: No dependencies.

Assurance Activity:

The evaluation team must determine through the evaluation of design documents how exactly to create subjects and utilize subject data within the TOE. The evaluation team must then generate this information through normal TOE functionality that will apply the data to a desired subject. The evaluation team 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 evaluation team should attempt to perform actions by the subject against defined objects

with both positive and negative expected results.

In addition to this inclusion, the following augmentations should be made to existing SFRs as currently prescribed by the PPs:

- FMT_MSA.1 must be assumed to apply to subject security attributes in addition to object attributes.

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 monotonically 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:

- lock the session – clear or overwrite display

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

- terminate the session

] after an Authorized Administrator specified time period of inactivity.

Dependencies: No dependencies

Assurance Activity:

The evaluator shall 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 in 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 (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. 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
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 \leq 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 | A mechanism put in place to allow or deny the execution of defined operations requested by defined subjects to be performed against defined objects or the result achieved by employing such a mechanism. |
| Attribute-Based Access Control | A means of access control that is based upon the attributes of a user rather than the rights of a user. An example would be a system that grants access to specific resources if a user is an engineer and denies access to the same resources if the user is a contractor. |
| Authorized Administrator | A term synonymous with “Administrator”, used because some Common Criteria SFRs use the specific terminology. |
| Consume | The act of an Access Control product receiving a policy, parsing it, and storing it in a manner such that it can be used to enforce access control |
| Discretionary Access Control | A means of access control based on authorizations issued to a subject by virtue of their identity or group membership. |
| Enterprise Security Management | Systems and personnel required to order, create, disseminate, modify, suspend, and terminate security management controls |
| Identity and Credential Management Product | An ESM product that contains the primary functionality to store and manage identities and credentials within an ESM deployment for the purposes of identification and authentication. |
| Mandatory Access Control | A means of access control based on the notion that all subjects and objects within an enterprise are associated with one or more hierarchical labels. The dominance relationship assigned to these labels determines if access is permitted. |
| 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 |

Standard Protection Profile for Enterprise Security Management Policy Management

| Term | Definition |
|---|---|
| | TOE is installed. |
| Policy | A collection of rules that determine how the Access Control SFP is instantiated. These rules define the conditions under which defined subjects are allowed to perform defined operations against defined objects. |
| Policy Administrator | Within the context of the PP, this refers to one or more individuals who are responsible for using the TOE to generate and distribute policies. |
| Policy Enforcement Point | A component of an Enterprise Security Management that is responsible for applying the Access Control SFP to all relevant behavior in an enterprise. Synonymous with the Access Control product referred to within this PP. |
| Policy Management product | An application that is responsible for creating policies that are consumed by the Policy Enforcement Point. These policies may be created through automated mechanisms, by manual administrative input, or by some combination of the two. This is the TOE as defined within this PP. |
| Role-Based Access Control | A means of access control that authorizes subject requests based on the roles to which they are assigned and the authorizations that are associated with those roles. |
| Secure Configuration Management Product | A product with the capability to alter the configuration of an ESM component and/or the ability to provision systems that reside in the Operational Environment |
| TOE Administrator | Within the context of the PP this refers to the one or more individuals who are responsible for setting up the TOE, using the Policy Management product to define policies the TOE consumes, and reviewing audit data the TOE generates. |
| User | A blanket term for a generic user of the TOE; any entity that is identified and authenticated to the Policy Management product. |

Appendix F - Identification

Title: Standard Protection Profile for Enterprise Security Management Policy Management

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

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

Version: PP Version 1.4

Keywords: enterprise security, enterprise security management, policy management, security management

Evaluation Assurance Level (EAL): EAL 1 augmented