Mapping Between

Standard Protection Profile for Enterprise Security Management, Access Control, Version 2.1, 2013-10-24

and

NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System**. The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 2, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context.** Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.
- **AC-3, SC-7(10), PL-9**. The primary purpose of an ESM Access Control product is either to allow or reject user access attempts to protected resources, in support of AC-3, or to prevent the transmission of data matching certain characteristics from leaving the system, in support of SC-7(10). The product is also intended to fulfill PL-9 at a high level since the notion of enterprise security management expects a centralized policy configuration that is enforced against all organizational users and assets rather than be configured on a per-user or per-system basis. Individual SFRs may relate to other security controls to ensure the secure implementation of the functions that are performed in support of this, but the reader should be aware that those are all implemented in support of ensuring the proper implementation of AC-3 for the specific resources that the TOE protects.
- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP or PP-Configuration supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE's Security Target must be congruent with those made for the supported controls. For example, the TOE's ability to generate audit records only supports AU-2 to the extent that the TOE's audit records are included in the set of "organization-defined auditable events" assigned by that control. The security control assessor must compare the TOE's functional claims to the behavior required for the system to determine the extent to which the applicable controls are supported.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
TOE Security Functional Requirements				
ESM_EID.2	**Reliance on Enterprise Identification**	IA-2 -or- IA-8	**Identification and Authentication (Organizational Users)** **-or-** **Identification and Authentication (Non-Organizational Users)**	A conformant TOE supports this control by implementing or invoking a mechanism to identify users so that appropriate access control policies can be enforced. These users may be from inside or outside the organization.
FAU_GEN.1	**Audit Data Generation**	AU-2	**Event Logging**	A conformant TOE has the ability to generate audit records for various events. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data. The TOE supports the enforcement of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		AU-12	**Audit Record Generation**	A conformant TOE has the ability to generate audit logs. The TOE supports the enforcement of parts (a) and (c) of the control if its auditable events are consistent with the assignments chosen for the control and if the TOE's audit log is part of the overall system's auditing.
FAU_SEL.1	**Selective Audit**	AU-12	**Audit Record Generation**	A conformant TOE supports part (b) of this control by implementing a mechanism to determine the events that cause audit records to be generated.
FAU_STG.1	**Protected Audit Trail Storage (Local Storage)**	AU-9	**Protection of Audit Information**	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records.
		AU-9(6)	**Protection of Audit Information:** Read-Only Access	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records. If the TOE prevents this by preventing all modification and deletion of audit records (i.e., there is no 'authorized' ability to do this), it can be used to support the enforcement of this control.
FAU_STG_EXT.1	**External Audit Trail Storage**	AU-4(1)	**Audit Log Storage Capacity:** Transfer to Alternate Storage	A conformant TOE has the ability to logically transmit audit data to a location in its Operational Environment. While this SFR requires the TSF to store generated audit data on the TOE, a minimum storage size or retention period is not specified. Therefore, a TOE may support the enforcement of this control if the local storage of audit data is limited or transitory.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		AU-9	**Protection of Audit Information**	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records.
		AU-9(2)	**Protection of Audit Information:** Store on Separate Physical Systems or Components	A conformant TOE must be able to transmit audit data to a logically remote location. It can be used to support the enforcement of this control if the recipient of the audit data is physically remote from the TOE.
FCO_NRR.2	**Enforced Proof of Receipt**	AU-10	**Non-Repudiation**	A conformant TOE supports this control by generating proof of receipt of an access control policy to the originator of that policy. This allows the originator of that policy to affirm that the TOE is enforcing the desired policy.
FDP_ACC.1	**Access Control Policy**	AC-3	**Access Enforcement**	A conformant TOE supports this control by defining an access control policy that determines whether actions are allowed based on the subject/object/operation of the action.
FDP_AFC.1	**Access Control Functions**	AC-3	**Access Enforcement**	A conformant TOE supports this control by enforcing access control rules specified by the configured access control policy.
FMT_MOF.1(1)	**Management of Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE will not permit configuration of its functionality unless proper authorization is provided.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to manage TOE functionality.
FMT_MOF.1(2)	**Management of Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE will not permit configuration of its functionality unless proper authorization is provided.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				the users that are able to manage TOE functionality.
FMT_MSA.1	**Management of Security Attributes**	AC-3	**Access Enforcement**	A conformant TOE will not permit configuration of its security attributes unless proper authorization is provided.
		AC-6	**Least Privilege**	A conformant TOE enforces least privilege by restricting the users that are able to manage TOE security attributes.
FMT_MSA.3	**Static Attribute Initialization**	SA-8(23)	**Security and Privacy Engineering Principles:** Secure Defaults	This SFR requires the TOE to have the ability to enforce a restrictive posture by default with respect to access control enforcement.
FMT_SMF.1	**Specification of Management Functions**	CM-6	**Configuration Settings**	A conformant TOE may satisfy one or more optional capabilities defined in this SFR. In general, a conformant TOE will satisfy this control to the extent that the TOE provides a method to configure its behavior in accordance with organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE.
FMT_SMR.1	**Security Roles**	AC-2(7)	**Account Management:** Privileged User Accounts	A conformant TOE has the ability to associate a Policy Management product acting on behalf of an administrator with a privileged role that allows for its configuration to be changed.
FPT_APW_EXT.1	**Protection of Stored Credentials**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to administrative credentials, which supports the control to the extent that such a repository is identified by the organization as requiring restricted access.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		IA-5	**Authenticator Management**	A conformant TOE protects authentication data from unauthorized disclosure, in support of part (g) of this control.
FPT_FLS_EXT.1	**Failure of Communications**	SC-17	**Fail-Safe Procedures**	A conformant TOE supports this control by enforcing known behavior in the event of a communications failure.
FPT_RPL.1	**Replay Protection**	AC-17(10)	**Remote Access:** Authenticate Remote Commands	A conformant TOE supports this control by implementing a mechanism to prevent the acceptance of replayed configuration instructions.
FPT_SKP_EXT.1	**Protection of Secret Key Parameters**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE restricts access to the key storage repository, which supports this control if such a repository is identified by the organization as requiring restricted access.
		IA-5	**Authenticator Management**	If the stored key data includes an authenticator (such as an SSH private key), a conformant TOE protects authentication data from unauthorized disclosure, in support of part (g) of this control.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by protecting stored cryptographic data. If that cryptographic data includes authentication data, it supports IA-5 part (g) as well.
FRU_FLT.1	**Degraded Fault Tolerance**	SI-17	**Fail-Safe Procedures**	A conformant TOE supports this control by enforcing known behavior in the event of a communications failure.
FTP_ITC.1	**Inter-TSF Trusted Channel**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocol(s) used to establish trusted

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				communications uses mutual authentication.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
Optional Requirements				
ESM_DSC.1	**Object Discovery**	AU-13	**Monitoring for Information Disclosure**	A conformant TOE supports this control by implementing a mechanism to discover data that may be subject to unauthorized disclosure and taking some corrective action in response.
FCS_CKM.1	**Cryptographic Key Generation (for Asymmetric Keys)**	SC-12	**Cryptographic Key Establishment and Management**	The ability of the TOE to generate asymmetric keys satisfies the key generation portion of this control.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE ensures that generated asymmetric keys provide an appropriate level of security.
FCS_CKM_EXT.4	**Cryptographic Key Zeroization**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_COP.1(1)	**Cryptographic Operation (for Data Encryption/Decryption)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(2)	**Cryptographic Operation (for Cryptographic Signature)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1(3)	**Cryptographic Operation (for Cryptographic Hashing)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform cryptographic hashing using NSA-approved and FIPS-validated algorithms.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FCS_COP.1(4)	**Cryptographic Operation (for Keyed-Hash Message Authentication)**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform keyed-hash message authentication using NSA-approved and FIPS-validated algorithms.
FCS_HTTPS_EXT.1	**HTTPS**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE may support the implementation of PKI-based authentication by validating peer certificates as part of the authentication process.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8 (1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_IPSEC_EXT.1	**IPsec**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE implements peer authentication for IPsec.
		SC-7(5)	**Boundary Protection:** Deny by Default - Allow by Exception	A conformant TOE's IPsec implementation includes a default-deny posture in its SPD.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements IPsec as a method of ensuring confidentiality and integrity of data in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:**	The TOE's use of IPsec provides a cryptographic means to protect data in transit.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Cryptographic Protection	
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_RBG_EXT.1	**Cryptographic Operation (Random Bit Generation)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of an appropriate DRBG ensures that generated keys provide an appropriate level of security.
FCS_SSH_EXT.1	**SSH**	AC-17(2)	**Remote Access:** Protection of Confidentiality and Integrity Using Encryption	The SSH client protocol implemented by the TOE provides confidentiality and integrity for remote access.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE may use its SSH client functionality to interact with a remote system on behalf of an organizational user.
		IA-3	**Device Identification and Authentication**	A conformant TOE may use its SSH client functionality to establish a static or as-needed connection to a specific remote device that is authenticated using a public key or X.509 certificate (instead of an administrator-supplied credential), which supports this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE's use of SSH supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FCS_TLS_EXT.1	**TLS**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications, supporting this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	The TOE provides cryptographic methods to secure data in transit, which may satisfy organization-defined uses if the functionality claimed by the TSF is consistent with organizational requirements.
FPT_FLS.1	**Failure with Preservation of a Secure State**	SC-24	**Fail in Known State**	A conformant TOE supports this control by enforcing known behavior in the event of its own failure.
FTA_TSE.1	**TOE Session Establishment**	AC-2(11)	**Account Management:** Usage Conditions	A conformant TOE supports this control by enforcing usage conditions that prevent otherwise valid subjects from accessing objects that are protected by the TSF.
Selection-Based Requirements				
No selection-based requirements defined.				
Objective Requirements				
No objective requirements defined.				