Mapping Between

PP-Module for Authentication Servers, Version 1.0, 2023-01-25

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 or 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 certain controls, but typically satisfaction also requires the implementation of operational procedures. Further, given that systems are typically the product of the 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.
- **Granularity of SFRs versus controls**. It is important to remember that the Security Functional Requirements (SFRs) and the Security and Privacy Controls (controls) are at completely different levels of abstraction. SFRs can be very low level, specifying internal characteristics and behaviors of given functions. Even when broader, SFRs are restricted to a specific product. Controls, on the other hand, are very high level, specifying both technical behavior and processes for the whole system, broadly across the large number of devices, components, and products that make up the system and achieve the overall mission. A low-level SFR may contribute in some small way toward the satisfaction of a control, but it rarely satisfies the control in isolation and should not be interpreted as doing so. More often, the combination of SFRs that define the security functionality of a product may serve to support just a single control, and looking at the finer level of detail may not be as useful, such as the low-level details of protocol implementations. When looking at these mappings, it is important to remember the differences in levels of abstraction; in particular, it is important not to read more into an SFR to control mapping than a contribution of some level of support.
- **IA-2, IA-3, IA-5, IA-8, IA-9**. The primary purpose of an authentication server is to authenticate a user, service, or IT entity that attempts to access a protected network. An authentication server product therefore supports the enforcement of IA-3 in general at a high level, as well as one or more of IA-2, IA-8, or IA-9, depending on whether the TOE authenticates organizational users, non-organizational users, or services. Regardless of the usage of the authentication server, it will also play a role in enforcing the technical controls of IA-5 by ensuring the confidentiality of authenticators. 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 these controls and relevant sub-controls are the behaviors that the authentication server is intended to address.
- **SA-4(7)**. Generally, 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 implement trusted communications only supports SC-8 to the extent that the TOE's implementation of EAP-TLS as required by the PP-Module is consistent with the mechanisms the organization is required to use for confidentiality and integrity of data in transit. 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.
- **PP-Module**. A TOE that conforms to this PP-Module will also conform to either the Application Software Protection Profile (App PP) or collaborative Protection Profile for Network Devices (NDcPP) by definition. Therefore, the TOE will satisfy additional security controls not referenced here through its conformance to one of those PPs. This PP-Module refines some of the Base-PP requirements to ensure consistency between the applicable PP and the PP-Module, but this does not affect the security controls that satisfying those requirements is intended to address.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
Mandatory Requirements (presented alphabetically)				
FAU_GEN.1/AuthSvr	**Audit Data Generation (Authentication Server)**	AU-2	**Event Logging**	A conformant TOE can generate audit records for various events.
		AU-3	**Content of Audit Records**	A conformant TOE will ensure that audit records include date, type, outcome, and subject identity data.
		AU-12	**Audit Record Generation**	The TOE can generate audit logs, as well as control which events are logged, satisfying this control.
FCO_NRO.1	**Selective Proof of Origin**	AU-10	**Non-repudiation**	A conformant TOE supports non-repudiation through its ability to generate evidence of origin for RADIUS Access-Request packets.
		AU-10(1)	**Non-repudiation:** Association of Identities	A conformant TOE supports this control through its ability to maintain associations between RADIUS Access-Requests and the NAS from which they originate.
		AU-10(2)	**Non-repudiation:** Validate Binding of Information Producer Identity	A conformant TOE supports this control by having a mechanism for verifying proof of origin for Access-Request packets.
FCO_NRR.1	**Selective Proof of Receipt**	AU-10	**Non-repudiation**	A conformant TOE supports enforcement of this control by providing proof of receipt for RADIUS Access-Request packets.
		AU-10(1)	**Non-repudiation:** Association of Identities	A conformant TOE supports this control by providing a receipt of a RADIUS Access-Request that identifies the TOE as the valid recipient of it.
FCS_CKM.3	**Cryptographic Key Access**	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

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				the organization as requiring restricted access.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE can securely store cryptographic keys.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE can securely store cryptographic keys.
FCS_EAP-TLS_EXT.1	**EAP-TLS Protocol**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE can 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 EAP-TLS supports a cryptographic method of protecting data in transit.
		SC-13	**Cryptographic Protection**	A conformant TOE supports this control if the control's assignment defines the cryptography implemented by the TSF as appropriate for the information system.
FCS_RADIUS_EXT.1	**Authentication Protocol**	IA-2 -or- IA-3 -or- IA-8 -or- IA-9	**Identification and Authentication (Organizational Users)** **-or-** **Device Identification and Authentication** **-or-** **Identification and Authentication (Non-Organizational Users)** **-or-**	A conformant TOE can perform RADIUS authentication, which can be used for any of user (whether organizational or not), device, or service authentication.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Service Identification and Authentication	
FCS_STG_EXT.1	**Cryptographic Key Storage**	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.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE can securely store cryptographic keys.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE can securely store cryptographic keys.
FIA_AFL.1/AuthSvr	**Authentication Failure Handling (Claimant)**	AC-7	**Unsuccessful Logon Attempts**	The TOE can detect when a defined number of unsuccessful authentication attempts occurs and take some corrective action.
FIA_UAU.6	**Re-Authenticating**	IA-11	**Re-authentication**	A conformant TOE supports this control by enforcing re-authentication of the administrator when certain conditions are met.
FIA_X509_EXT.1/ AuthSvr	**X.509 Certification Validation (Claimant)**	IA-3	**Device Identification and Authentication**	A conformant TOE uses X.509 certificates to perform device authentication of distributed TOE components.
		IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	The TOE uses X.509 certificate authentication between distributed components to establish cryptographically-secured communications between them. Establishment of these channels may require bidirectional (mutual) authentication.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE can validate certificate path and status, which satisfies this control.
		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	The TOE's use of X.509 certificates to authenticate distributed components ensures that it will include the functionality needed to validate certificate authorities.
FMT_SMF.1/AuthSvr	**Specification of Management Functions (Authentication Server)**	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.
FTA_TSE.1	**TOE Session Establishment**	AC-2(11)	**Account Management:** Usage Conditions	A conformant TOE supports this control by ensuring that user authentication requests are only accepted as valid if administrator-defined usage conditions are met.
FTP_ITC.1/NAS	**Inter-TSF Trusted Channel (Relying Party Communications)**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE can 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 (presented alphabetically)				
No optional requirements.				

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
Objective Requirements (presented alphabetically)				
No objective requirements.				
Implementation-Based Requirements (presented alphabetically)				
No implementation-based requirements.				
Selection-Based Requirements (presented alphabetically)				
FCS_RADSEC_EXT.1	**RadSec**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by implementing a mechanism to authenticate peer devices.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE can 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.
FIA_HOTP_EXT.1	**HMAC-Based One-Time Password Pre-Shared Keys**	IA-5	**Authenticator Management**	A conformant TOE uses hash-based pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (h) of this control.
FIA_PSK_EXT.1	**Pre-Shared Key Usage**	N/A	**N/A**	This SFR does not support any security controls on its own; it only functions as a stub to allow the TOE vendor to specify the types of pre-shared keys that are supported, which determines which of

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				FIA_HOTP_EXT.1, FIA_PSK_EXT.2, FIA_PSK_EXT.3, and FIA_TOTP_EXT.1 are claimed.
FIA_PSK_EXT.1/ AuthSvr	**Pre-Shared Key Usage (Claimant Authentication)**	N/A	**N/A**	This SFR does not support any security controls on its own; it only functions as a stub to allow the TOE vendor to specify the context in which the TOE uses pre-shared keys and the types of pre-shared keys that are used.
FIA_PSK_EXT.2	**Generated Pre-Shared Keys**	IA-5	**Authenticator Management**	A conformant TOE uses generated pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (h) of this control.
FIA_PSK_EXT.3	**Password-Based Pre-Shared Keys**	IA-5	**Authenticator Management**	A conformant TOE uses password-based pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (h) of this control.
FIA_TOTP_EXT.1	**Time-Based One-Time Password Pre-Shared Keys**	IA-5	**Authenticator Management**	A conformant TOE uses time-based pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (h) of this control. Note also that time-based pre-shared keys implicitly support part (f) of this control since they are only valid for a given period.