Mapping Between

Network Device Collaborative Protection Profile (NDcPP)/Application Software Protection Profile (App PP) Extended Package (EP) for Authentication Servers, Version 1.0, 2015-08-07

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.
- **IA-2, IA-3, IA-8.** The primary purpose of an authentication server is to authenticate an entity (user 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 both of IA-2 and IA-8, depending on whether the users authenticated by the TOE are part of the organization that operates it. 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).** 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 implement trusted communications on its TLS interfaces supports SC-8 and related controls for those interfaces only; it cannot enforce protection of data in transit for non-TLS protocols that are outside of its own boundary.
- **Extended Package.** A TOE that conforms to this Extended Package will also conform to the collaborative Protection Profile for Network Devices (NDcPP) or Application Software Protection Profile (App PP) by definition. Therefore, the TOE will satisfy additional security controls not referenced here through its conformance to either of those PPs. This Extended Package refines

some of the NDcPP or App PP requirements to ensure consistency between the PP and the Extended Package, but this does not affect the security controls that satisfying those requirements is intended to address. Additionally note that when the TOE conforms to the App PP, there are additional SFRs that must be claimed as part of conformance to this EP; these SFRs, and their relevant control mappings, are included below.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
App PP Additional Requirements				
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.
		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. Part (b) is not satisfied by a

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				conformant TOE because the PP does not define functionality to suppress/enable the generation of specific audit records (which would typically be expressed in CC as FAU_SEL.1).
FMT_SMR.2	**Restrictions on Security Roles**	AC-2(7)	**Account Management:** Privileged User Accounts	A conformant TOE has the ability to associate users with roles, in support of part (a) of the control.
FPT_TST_EXT.1	**TSF Testing**	SI-6	**Security and Privacy Function Verification**	A conformant TOE will run automatic tests to ensure correct operation of its own functionality.
		SI-7	**Software, Firmware, and Information Integrity**	One of the self-tests the TOE may perform is an integrity test of its own software or firmware.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	One of the self-tests the TOE may perform is an integrity test of its own software or firmware.
TOE Security Functional Requirements				
FCO_NRO.1	**Selective Proof of Origin**	AU-10	**Non-Repudiation**	A conformant TOE enforces 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.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		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_EAP-TLS_EXT.1	**Extended: Extensible Authentication Protocol – Transport Layer Security (EAP-TLS)**	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 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	**Extended: RADIUS**	IA-2 -or- IA-3 -or- IA-8	**Identification and Authentication (Organizational Users)** **-or-** **Device Identification and Authentication** **-or-** **Identification and Authentication (Non-Organizational Users)**	A conformant TOE has the ability to perform RADIUS authentication, which can be used for both user (whether organizational or not) and device authentication.
FIA_PSK_EXT.1	**Extended: Pre-Shared Key Composition**	IA-5	**Authenticator Management**	A conformant TOE uses pre-shared keys as a type of authenticator and will ensure their strength and confidentiality, which supports parts (c) and (g) of the control.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
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	**Inter-TSF Trusted Channel**	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				
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.
Selection-Based Requirements				
FCS_EAP-TLS_EXT.1.7	**EAP-TLS Protocol**	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_RADSEC_EXT.1	**Extended: RadSec**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by implementing a mechanism

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				to authenticate peer devices.
		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.
Objective Requirements				
This EP has no objective requirements.				