Mapping Between
PP-Module for Enterprise Session Controller (ESC), Version 1.0, 2020-11-19
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.
- **AC-4.** The primary purpose of an ESC product is to broker voice and video over IP (VVoIP) communications. This has an access control aspect by determining when such communications are authorized. This supports the implementation of AC-4 at a general level. 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 AC-4 and relevant sub-controls are the behaviors that ESC is intended to address.
- **SA-4(7).** Generally, satisfaction of any NIAP PP 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, a conformant TOE claims multiple iterations of FAU_GEN.1 for security audit data generation. However, this is not a guarantee that the auditing capabilities provided by the TSF will align fully with organizational policies for what information must be audited. 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 the collaborative Protection Profile for Network Devices (NDcPP) by definition. Therefore, the TOE will satisfy additional security controls not referenced here through its conformance to that PP. This PP-Module refines some of the NDcPP requirements to ensure consistency between the 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		Comments and Observations
Mandatory Requirements (presented alphabetically)				
FAU_GEN.1/CDR	**Audit Data Generation (Call Detail Record)**	AU-2	**Event Logging**	A conformant TOE can generate call detail records, which are a form of audit record. The TOE supports the enforcement of the control if these records 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 call detail 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 call detail 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 can generate call detail records, which are a type of audit log. The TOE supports the enforcement of parts (a) and (c) of the control if its auditable events are consistent with the assignments chosen

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				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 conformant TOE because the PP does not define functionality to suppress or enable the generation of specific audit records (which would typically be expressed in CC as FAU_SEL.1).
FAU_GEN.1/Log	**Audit Data Generation (System Log)**	AU-2	**Event Logging**	A conformant TOE can 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 3.1R5 SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
		AU-12	**Audit Record Generation**	A conformant TOE can 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 conformant TOE because the PP does not define functionality to suppress or enable the generation of specific audit records (which would typically be expressed in CC as FAU_SEL.1).
FAU_SAR.1/Log	**Log Audit Review (System Log)**	AU-7	**Audit Record Reduction and Report Generation**	A conformant TOE supports this control by implementing a mechanism to review audit data.
FAU_STG.1/CDR	**Protected Audit Trail Storage (Call Detail Record)**	AU-9	**Protection of Audit Information**	A conformant TOE can prevent unauthorized modification and deletion of audit records.
FAU_VVR_EXT.1	**Recording Voice and Video Call Data**	AU-3(1)	**Content of Audit Records:** Additional Audit Information	**(selection-dependent)** A conformant TOE may be able to generate voice or video records of user calls for the purpose of auditing system activity, depending on the selections made.
FDP_IFC.1	**Subset Information Control**	AC-4	**Information Flow Enforcement**	A conformant TOE supports this control by defining an information flow control policy that determines the circumstances in which it will allow a connection to be established between two VVoIP endpoints.
FDP_IFF.1	**Simple Security Attributes**	AC-4	**Information Flow Enforcement**	A conformant TOE supports this control by enforcing the information flow

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				control policy defined by FDP_IFC.1.
FDP_RIP.1	**Subset Residual Information Protection**	SC-4	**Information in Shared Resources**	A conformant TOE supports this control by ensuring that residual information is not present on the system following a factory reset or wipe.
FIA_UAU.2/TC	**User Authentication before Any Action (Telecommunications Devices)**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by ensuring that telecommunications devices are authenticated to the TOE before allowing them to interface with it.
FIA_UAU.2/VVoIP	**User Authentication before Any Action (VVoIP Endpoints)**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by ensuring that VVoIP endpoints are authenticated to the TOE before allowing them to interface with it.
FMT_CFG_EXT.1	**Secure by Default Configuration**	AC-3	**Access Enforcement**	A conformant TOE supports this control through its default implementation of file permissions that protect the application binaries and data from unauthorized access.
		AC-6	**Least Privilege**	A conformant TOE is implemented such that its default file system permissions restrict its access to only the subjects that need to interact with it.
		IA-5	**Authenticator Management**	If the TOE includes a default credential, part (e) of this control is satisfied because the credential must be changed on first use. This also satisfies part (b) of the control as the changed credential is an 'initial authenticator.' Note however that there are no PP requirements for the composition of authenticators, so part (b) is only satisfied if the

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				administrator follows organizational guidance when specifying this.
FMT_SMF.1/ESC	**Specification of Management Functions (ESC)**	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.
FPT_FLS.1	**Failure with Preservation of a Secure State**	SC-24	**Fail in Known State**	A conformant TOE supports this control by failing in a known state when any of the failures identified in the SFR occur.
FTP_ITC.1/ESC	**Inter-TSF Trusted Channel (ESC Communications)**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE can ensure the confidentiality and integrity of signaling communications between itself and other telecommunications devices.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The TOE supports a cryptographic method of protecting external communications.
Strictly Optional Requirements (presented alphabetically)				
This PP-Module has no optional requirements.				
Objective Requirements (presented alphabetically)				
This PP-Module has no objective requirements.				
Implementation-Based Requirements (presented alphabetically)				
FPT_TUD_EXT.1/VVoIP	**Trusted Update (VVoIP Endpoints)**	CM-14	**Signed Components**	**(selection-dependent)** If the TOE supports the ability to deliver updates to registered VVoIP

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
				endpoints, it may have the ability to use a digital signature algorithm to assert the authenticity and integrity of these updates, depending on the selections made.
		SI-2	**Flaw Remediation**	If the TOE supports the ability to deliver updates to registered VVoIP endpoints, this mechanism can be used to remedy any flaws that are present in VVoIP software or firmware.
		SI-7	**Software, Firmware, and Information Integrity**	If the TOE supports the ability to deliver updates to registered VVoIP endpoints, it can assert the integrity of the updates it delivers.
		SI-7(1)	**Software, Firmware, and Information Integrity:** Integrity Checks	If the TOE supports the ability to deliver updates to registered VVoIP endpoints, it can assert the integrity of the updates it delivers.
Selection-Based Requirements (presented alphabetically)				
FAU_SEL.1	**Selective Audit**	AU-12	**Audit Record Generation**	A conformant TOE can support part (b) of this control by providing a mechanism to determine the set of auditable events that result in the generation of audit records.
FAU_STG.1/VVR	**Protected Audit Trail Storage (Voice/Video Recording)**	AU-9	**Protection of Audit Information**	A conformant TOE can prevent unauthorized modification and deletion of call detail records.
FAU_VVR_EXT.2	**Generation of Voice and Video Recordings**	AU-11	**Audit Record Retention**	A conformant TOE supports this control by implementing mechanisms to retain and identify audit records of voice and video calls in an accessible format.