Mapping Between
Extended Package for Voice Over IP (VoIP) Applications, Version 1.3, 3-November-2014
and
NIST SP 800-53 Revision 4

Important Caveats

- **Product vs. System.** The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 1, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 4, 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.
- **SA-4(7).** Perhaps it is needless to say, but 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, 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 4 Control**		**Comments and Observations**
Security Requirements for VoIP Applications (TOE)				
FCS_CKM_EXT.2(1)	**Cryptographic Key Storage**	IA-5	**Authenticator Management**	A conformant TOE has the ability to protect authenticator content using PKI.

		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to meet the storage portion of this control through the use of secure platform storage for key data.
FCS_SRTP_EXT.1	**Secure Real-Time Transport Protocol**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will ensure the confidentiality and integrity of data in transit using SRTP.
		SC-8 (1)	**Transmission Confidentiality and Integrity:** Cryptographic or Alternate Physical Protection	The specific mechanism used by the TOE to secure data in transit is the use of a cryptographic channel.
		SC-13	**Cryptographic Protection**	A conformant TOE will use an SRTP implementation that uses NSA-approved and FIPS-validated cryptography in order to secure data in transit.
		SC-19	**Voice over Internet Protocol**	A conformant TOE will implement SRTP to carry VoIP traffic, which allows the organization to satisfy this control (but is not sufficient to meet the control on its own).
FDP_VOP_EXT.1	**Voice Over IP Data Protection**	N/A	N/A	A conformant TOE will ensure that VoIP data is only transmitted when the TSF is in a state that is authorized to do so. There are no specific controls that are satisfied by this behavior.
FIA_SIPC_EXT.1	**Session Initiation Protocol (SIP) Client**	IA-2	**Identification and Authentication (Organizational Users)**	The TOE has the ability to enforce user authentication for SIP registration.

		IA-5	**Authenticator Management**	A conformant TOE has the ability to protect authenticator content using PKI.
		IA-5(1)	**Authenticator Management:** Password-Based Authentication	A compliant TOE has the ability to condition stored passwords.
		SC-19	**Voice over Internet Protocol**	A compliant TOE has the ability to control access to VoIP functions through the use of a password for SIP registration.
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 STIGs or other organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE; the security control assessor must review what has been selected in the Security Target and determine what additional support is provided, if any.
FPT_TUD_EXT.1	**Trusted Update**	CM-8	**Information System Component Inventory**	FPT_TUD_EXT.1.1 supports obtaining the TOE version number, which supports the component inventory on the software side.
FTP_ITC.1(1)	**Inter-TSF Trusted Channel:** SDES-SRTP	SC-8(1)	**Transmission Confidentiality and Integrity**	A conformant TOE uses SDES-SRTP to ensure the confidentiality and

				integrity of data in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic or Alternate Physical Protection	The method used to secure data in transit involves cryptographic protection.
		SC-11	**Trusted Path**	A conformant TOE will allow a user to establish a trusted path from the TOE to a remote VoIP application.
		SC-19	**Voice over Internet Protocol**	A conformant TOE will implement SRTP to carry VoIP traffic, which allows the organization to satisfy this control (but is not sufficient to meet the control on its own).
Security Functional Requirements for VoIP Client Applications or Client Platforms				
FCS_CKM.1(1)	**Cryptographic Key Generation:** Asymmetric Keys	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE may provide a key generation function in support of the key lifecycle process.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	If the TOE is responsible for this functionality (as opposed to its underlying platform), it will implement the key generation function using asymmetric keys.
FCS_CKM.1(2)	**Cryptographic Key Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE may provide a key generation function in support of the key lifecycle process.

		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	If the TOE is responsible for this functionality (as opposed to its underlying platform), it will implement the key generation function using asymmetric keys.
FCS_CKM_EXT.4	**Cryptographic Key Material Destruction (Key Material)**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_COP.1(1)	**Cryptographic Operation:** 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 hashing 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 signing using NSA-approved and FIPS-validated algorithms.
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_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_TLS_EXT.1	**Transport Layer Security**	IA-5(2)	**Authenticator Management:**	The TOE requires peers to possess a valid certificate before

			PKI-Based Authentication	establishing trusted communications, satisfying this control.
		SC-8	**Transmission Integrity**	A conformant TOE will use TLS to provide confidentiality and integrity to data in transit.
		SC-8(1)	**Transmission Integrity:** Cryptographic or Alternate Physical Protection	The TOE's use of TLS to secure data in transit is a cryptographic method of protection.
		SC-13	**Cryptographic Protection**	The TOE's implementation of TLS uses NSA-approved and FIPS-validated cryptographic algorithms to establish the trusted channel.
FIA_X509_EXT.1	**X509 Certificate Validation**	IA-5(2)	**Authenticator Management:** PKI-Based Authentication	A conformant TOE has the ability to certificate path and status, which satisfies this control.
		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	A conformant TOE specifies what CA's are allowed when validating certificates as part of the establishment of VoIP sessions.
FIA_X509_EXT.2	**X509 Certificate Use and Management**	CM-5(3)	**Access Restrictions for Change:** Signed Components	A conformant TOE may have the ability to ensure that any software updates have a valid signature.
		IA-2	**Identification and Authentication**	A conformant TOE has the ability to perform X.509 certificate authentication.
		SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE may use X.509 certificates in order to verify the integrity of the TSF.
FMT_SMF.1	**Specification of Management Functions**	N/A	N/A	The existence of management functions does not satisfy any security controls on its own. The security

				functions that are manageable are mapped to individual controls based on the SFRs defined by those functions. Depending on how this SFR is completed in the ST, it may support various functions (in particular, tying them to support of AC-6 for that function).
FPT_TST_EXT.1	**TSF Self Test**	SI-7(1)	**Software, Firmware and Information Integrity:** Integrity Checks	The TOE has the ability to verify the integrity of the boot chain prior to execution.
		SI-7(6)	**Software, Firmware and Information Integrity:** Cryptographically-Validated Integrity	A conformant TOE has the ability to implement cryptographic mechanisms to detect unauthorized change to its own executable code.
FPT_TUD_EXT.1	**Trusted Update**	CM-5(3)	**Access Restrictions for Change:** Signed Components	A conformant TOE has the ability to require a signed update.
		SI-2	**Flaw Remediation**	A conformant TOE has the ability to remedy implementation flaws through software updates.
		SI-7(1)	**Software, Firmware and Information Integrity:** Integrity Checks	The TOE has the ability to verify the integrity of updates to itself.
FTP_ITC.1(2)	**Inter-TSF Trusted Channel:** TLS/SIP	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE has the ability to secure the confidentiality and integrity of communications with a SIP server.

		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic or Alternate Physical Protection	The TOE uses cryptographic protection to ensure the confidentiality and integrity of data in transit.
Optional Requirements				
N/A	**N/A**	**N/A**	**N/A**	**N/A**
Selection-based Requirements				
FIA_X509_EXT.2 (1)	**X509 Authentication**	SI-7(15)	**Software, Firmware, and Information Integrity:** Code Authentication	A conformant TOE will ensure that malicious code will not be installed and/or executed through the enforcement of code signing certificates.
Objective Requirements				
FAU_GEN.1	**Audit Data Generation**	AU-2	**Audit Events**	A conformant TOE supports part (a) of this control by providing the ability to generate records of auditable events.
		AU-3	**Content of Audit Records**	A conformant TOE supports this control by ensuring that generated audit records include the date and time of the event, type of the event, subject identity, and the outcome of the event.
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	A conformant TOE satisfies this control by including additional information in audit records as needed based on the type of event being recorded.
		AU-12	**Audit Generation**	A conformant TOE has the ability to generate auditable events defined by AU-2, satisfying this control.

FAU_SEL.1	**Selective Audit**	AU-12	**Audit Generation**	A conformant TOE has the ability to 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.
FTP_ALT_EXT.1	**Trusted Channel Alert**	SI-4(5)	**Information System Monitoring:** System-Generated Alerts	A conformant TOE will automatically alert the user if their communications are unsecured, which may be an indication of potential compromise.