Mapping Between
Functional Package for Transport Layer Security (TLS), Version 1.1, 12-February-2019
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.
- **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 5 Control**		**Comments and Observations**
Mandatory Requirements				
FCS_TLS_EXT.1	**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	A conformant TOE uses TLS as 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.
Optional Requirements				
This Package has no optional requirements.				
Selection-Based Requirements				
FCS_TLSC_EXT.1	**TLS Client Protocol**	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.
FCS_TLSC_EXT.2	**TLS Client Support for Mutual Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications and provides its own client certificate to the peer, 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.
FCS_TLSC_EXT.4	**TLS Client Support for Renegotiation**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-13	**Cryptographic Protection**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
FCS_TLSC_EXT.5	**TLS Client Support for Supported Groups Extension**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports the enforcement of additional permutations

				of TLS through the behavior enforced by this SFR.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-13	**Cryptographic Protection**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
FCS_TLSS_EXT.1	**TLS Server Protocol**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE provides a server certificate to a TLS client 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.
FCS_TLSS_EXT.2	**TLS Server Support for Mutual Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications and provides its own server certificate to the peer, 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.
FCS_TLSS_EXT.4	**TLS Server Support for Renegotiation**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-13	**Cryptographic Protection**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
FCS_DTLSC_EXT.1	**DTLS Client Protocol**	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.
FCS_DTLSC_EXT.2	**DTLS Client Support for Mutual Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications and provides its own client certificate to the peer, 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.
FCS_DTLSS_EXT.1	**DTLS Server Protocol**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE provides a server certificate to a DTLS client 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:**	The TOE supports a cryptographic method of protecting data in transit.

			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_DTLSS_EXT.2	**Server Support for Mutual Authentication**	IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications and provides its own server certificate to the peer, 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.
Objective Requirements				
FCS_TLSC_EXT.3	**TLS Client Support for Signature Algorithms Extension**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports the enforcement of additional permutations of TLS through the

				behavior enforced by this SFR.
		SC-13	**Cryptographic Protection**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
FCS_TLSS_EXT.3	**TLS Server Support for Signature Algorithms Extension**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.
		SC-13	**Cryptographic Protection**	A conformant TOE supports the enforcement of additional permutations of TLS through the behavior enforced by this SFR.