Mapping Between

Protection Profile for Application Software, Version 1.2, 22-April-2016

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 protect data at rest only supports SC-28(1) to the extent that the data that any sensitive data that is encrypted as per FDP_DAR_EXT.1 is included in the set of "organization-defined information at rest" 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 Application Software				
FCS_RBG_EXT.1	**Random Bit Generation Serices**	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_STO_EXT.1	**Storage of Credentials**	IA-5	**Authenticator Management**	A conformant TOE will protect authenticator data from unauthorized modification or disclosure.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A compliant TOE will have the ability to store and protect user credentials at rest, either within its own boundary or in the Operational Environment.
FDP_DEC_EXT.1	**Access to Platform Resources**	AC-6	**Least Privilege**	A compliant TOE will have the minimum level of access to system resources required to implement its functionality.
FDP_NET_EXT.1	**Network Communications**	AC-3	**Access Enforcement**	A compliant TOE will only access network resources for which it is authorized.
		AC-6	**Least Privilege**	A compliant TOE will have the minimum level of access to network resources required to implement its functionality.
FDP_DAR_EXT.1	**Encryption of Sensitive Application Data**	SC-13	**Cryptographic Protection**	If the TOE provides its own capability to encrypt sensitive data, it will perform symmetric encryption and decryption using NSA-approved and FIPS-validated algorithms to do so.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A compliant TOE will have the ability to store sensitive data in secure encrypted storage, either within its own boundary or in the Operational Environment.
FMT_MEC_EXT.1	**Supported Configuration Mechanism**	N/A	N/A	This SFR defines the ability of the TOE to be deployed in an environment where an OS platform is used in

				accordance with vendor guidance. This means that the TOE can exist in an organization that satisfies CM-2 but the presence of the TOE does not assist in the enforcement or satisfaction of the control.
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.
FMT_CFG_EXT.1	**Secure by Default Configuration**	IA-5(5)	**Authenticator Management:** Change Authenticators Prior to Delivery	The TOE does not allow for the use of default authenticators to perform management functions; if a default authenticator is provided it only grants sufficient functionality for an administrator to change it.
FPR_ANO_EXT.1	**User Consent for Transmission of Personally Identifiable Information**	AC-3	**Access Enforcement**	A conformant TOE supports access enforcement by ensuring that only authorized transmission of personally

				identifiable information will be performed.
FPT_API_EXT.1	**Use of Supported Services and API's**	SA-15(5)	**Development Process, Standards, and Tools:** Attack Surface Reduction	The TOE developer is required to use only documented platform APIs, which reduces the attack surface of the TSF to known components.
FPT_AEX_EXT.1	**Anti-Exploitation Capabilities**	SI-16	**Memory Protection**	A conformant TOE may provide measures to ensure that the underlying platform's memory is protected against unauthorized code execution. The extent to which the control is satisfied depends on both the organizational safeguards that are used to mitigate this and the specific countermeasures that are used by the TOE.
FPT_TUD_EXT.1	**Integrity for Installation and Update**	SI-2	**Flaw Remediation**	To prevent the software from being out of date and vulnerable to flaws, a conformant TOE will provide the ability to update its components through the underlying OS platform.
		SI-2(5)	**Flaw Remediation:** Automatic Software/Firmware Updates	A conformant TOE must be able to enforce automatic updates to ensure the software is up date.
FPT_LIB_EXT.1	**Use of Third Party Libraries**	SA-15(5)	**Development Process, Standards, and Tools:** Attack Surface Reduction	A conformant TOE supports the enforcement of this control because enumerating the third party libraries used by the TOE reduces the attack surface of the TSF to known components.

FTP_DIT_EXT.1	**Protection of Data in Transit**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE ensures the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic or Alternate Physical Protection	The use of the protocols specified in the SFR ensures the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
		SC-11	**Trusted Path**	The TOE may establish a trusted communication path between remote users and itself.
ADV_FSP.1	**Basic Functional Specification**	SA-4(1)	**Acquisition Process:** Functional Properties of Security Controls	A conformant TOE will provide a functional specification as part of the Security Target which describes the security functionality of each external interface.
AGD_OPE.1	**Operational User Guidance**	SA-5	**Information System Documentation**	The TOE includes guidance documentation that is reviewed as part of the evaluation includes operational instructions.
AGD_PRE.1	**Preparative Procedures**	SA-5	**Information System Documentation**	The TOE includes guidance documentation that is reviewed as part of this evaluation defines installation and preparation procedures.
ALC_CMC.1	**Life-Cycle Support**	SA-10	**Developer Configuration Management**	The evaluation of a conformant a TOE will demonstrate that it provides a unique identification for itself, which can be used as an input to a developer configuration management system.
ALC_CMS.1	**TOE CM Coverage**	SA-10	**Development Configuration Management**	The evaluation of a conformant a TOE will demonstrate that it

				provides a configuration list for its own components, which can be used as an input to a developer configuration management system.
ALC_TSU_EXT.1	**Timely Security Updates**	MA-6(1)	**Timely Maintenance:** Preventive Maintenance	A conformant TOE includes a description of how timely security updates must be applied for the purpose of preventative maintenance.
		SI-2	**Flaw Remediation**	To prevent the software from being out of date and vulnerable to flaws, a conformant TOE will provide the ability to update its components on a timely basis.
ATE_IND.1	**Independent Testing - Conformance**	CA-2	**Security Assessments**	A conformant TOE will have a security assessment performed against it.
		CA-2(1)	**Security Assessments:** Independent Assessors	A conformant TOE will be evaluated by an independent assessor as part of the evaluation process.
AVA_VAN.1	**Vulnerability Survey**	CA-2(2)	**Security Assessments:** Specialized Assessments	**Partial.** A conformant TOE will have a vulnerability scan performed against it as a specialized assessment method.
		CA-8	**Penetration Testing**	Penetration testing is performed on a conformant TOE to determine that it is resistant to attacks.
		RA-3	**Risk Assessment**	**Partial.** As part of the evaluation, a conformant TOE will be tested for its resistance against vulnerabilities that meet a given risk level as determined by the PP authors.
		SA-11(2)	**Developer Security Testing**	**Partial.** The Protection Profile defines threats

			and Evaluation: Threat and Vulnerability Analyses	for a given technology type that a conformant TOE is expected to mitigate. Partial match because the TOE developer may not conduct this assessment prior to independent evaluators.
		SA-11(5)	**Developer Security Testing and Evaluation:** Penetration Testing/ Analysis	**Partial.** The Protection Profile mandates that a conformant TOE be subjected to relevant penetration testing. Partial match because the TOE developer may not perform this activity prior to independent evaluators.
Optional Requirements				
FCS_CKM.1(2)	**Cryptographic Symmetric Key Generation**	SC-12(2)	**Cryptographic Key Establishment and Management:** Symmetric Keys	A conformant TOE has the ability to produce symmetric keys in accordance with organization-defined requirements.
FCS_TLSC_EXT.2	**TLS Client Protocol**	IA-3(1)	**Device Identification and Authentication:** Cryptographic Bidirectional Authentication	A TOE that supports TLS mutual authentication may enforce bidirectional device authentication, depending on the external interfaces provided by the TSF.
		IA-5(2)	**Authenticator Management:** PKI-Based Authentication	The TOE requires peers to possess a valid certificate before establishing trusted communications, satisfying this control.
Selection-Based Requirements				
FCS_RBG_EXT.2	**Random Bit Generation from Application**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to generate keys using pseudo-random inputs in accordance with organization-defined requirements.

FCS_CKM_EXT.1	**Cryptographic Key Generation Services**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE may provide a key generation function.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE may have the ability to generate asymmetric cryptographic keys. This SFR addresses the control with respect to key generation.
FCS_CKM.1(1)	**Cryptographic Asymmetric Key Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE provides a key generation function.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE has the ability to generate asymmetric cryptographic keys. This SFR addresses the control with respect to key generation.
FCS_CKM.2	**Cryptographic Key Establishment**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE provides a key establishment function.
		SC-12(3)	**Cryptographic Key Establishment and Management:** Asymmetric Keys	A conformant TOE has the ability to perform key establishment for asymmetric cryptographic keys. This control satisfies this SFR with respect to key establishment.
FCS_COP.1(1)	**Cryptographic Operation – 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 - Hashing**	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 - Signing**	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 – Keyed-Hash Message Authentication**	SC-13	**Cryptographic Protection**	**Partial.** A conformant TOE has the ability to perform keyed-hash message authentication using NSA-approved and FIPS-validated algorithms.
FCS_TLSC_EXT.1	**TLS Client Protocol**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements TLS as a method of ensuring confidentiality and integrity of data in transit.
		SC-8(1)	**Transmission Integrity:** Cryptographic or Alternate Physical Protection	The TOE's use of TLS provides a cryptographic means to protect data in transit.
		SC-13	**Cryptographic Protection**	A conformant TOE's use of specific ciphersuites to establish a TLS channel allows it to conform with NSA standards.
FCS_TLSC_EXT.4	**TLS Client Protocol**	SC-13	**Cryptographic Protection**	A conformant TOE's use of specific NIST curves in the establishment of a TLS session allows it to conform with NSA standards.
FCS_TLSS_EXT.1	**TLS Server Protocol**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE implements TLS as a method of ensuring confidentiality and integrity of data in transit.

		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic or Alternate Physical Protection	The TOE's use of TLS provides a cryptographic means to protect data in transit.
		SC-13	**Cryptographic Protection**	A conformant TOE's use of specific ciphersuites to establish a TLS channel allows it to conform with NSA standards.
FCS_DTLS_EXT.1	**DTLS Implementation**	SC-8(1)	**Transmission Integrity:** Cryptographic or Alternate Physical Protection	The ability of a conformant TOE to implement DTLS with a range of mandatory and optional ciphersuites ensures the confidentiality and integrity of data and transit.
		SC-13	**Cryptographic Protection**	A conformant TOE's use of DTLS to secure data in transit allows it to conform with NSA standards.
FCS_HTTPS_EXT.1	**HTTPS Protocol**	SC-8(1)	**Transmission Integrity:** Cryptographic or Alternate Physical Protection	The ability of a conformant TOE to implement HTTPS using TLS 1.2 ensures the confidentiality and integrity of data and transit.
		SC-13	**Cryptographic Protection**	A conformant TOE's use of HTTPS to secure data in transit allows it to conform with NSA standards.
FIA_X509_EXT.1	**X.509 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	**Session Authenticity**	Depending on the TOE's use of trusted communications channels, it may use X.509 certificate validation in support of session authentication.

		SC-23(5)	**Session Authenticity:** Allowed Certificate Authorities	If the TOE uses X.509 certificates as part of session authentication, it will include the functionality needed to validate certificate authorities.
FIA_X509_EXT.2	**X.509 Certificate Authentication**	IA-2	**Identification and Authentication**	A conformant TOE has the ability to identify and authenticate organizational users using X.509 certificates.
		IA-3	**Device Identification and Authentication**	A conformant TOE may use X.509 certificate authentication as part of performing device authentication, depending on the remote logical interfaces provided by the TSF.
Objective Requirements				
FCS_TLSC_EXT.3	**TLS Client Protocol**	SC-13	**Cryptographic Protection**	A conformant TOE's use of specific hash algorithms in the establishment of a TLS session allows it to conform with NSA standards.
FPT_API_EXT.2	**Use of Supported Services and APIs**	SA-15(5)	**Development Process, Standards, and Tools:** Attack Surface Reduction	The TOE developer is required to parse only certain types of data, which reduces the attack surface of the TSF to known components.
FPT_IDV_EXT.1	**Software Identification and Versions**	N/A	N/A	The use of SWID tags to identify the TOE does not satisfy any particular security control.