Mapping Between

Application Software Extended Package for Email Clients, Version 2.0, 2015-06-18

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 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 EP will also conform to Protection Profile for Application Software (App PP) by definition. Therefore, the TOE will satisfy additional security controls not referenced here through its conformance to that PP. The EP does not modify any of the App PP requirements, so it does not affect the security controls that satisfying those requirements is intended to address.
- **TOE vs OE implementation.** Many SFRs in this PP describe functionality that may be implemented either by the TOE itself or through TSF implication of a similarly-validated component in its operational environment (i.e., a general-purpose operating system). Those SFRs that may be implemented in this manner are denoted with an asterisk (*).

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
TOE Security Functional Requirements				
FCS_SMIME_EXT.1	**Secure/Multipurpose Internet Mail Extensions (S/MIME)**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports this control by requiring encrypting the sending or receiving to as part of the S/MIME protocol.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports this control by requiring encrypting the sending or receiving to as part of the S/MIME protocol.
FCS_CKM_EXT.3	**Protection of Key and Key Material**	AC-3(11)	**Access Enforcement:** Restrict Access to Specific Information Types	A conformant TOE supports this control by ensuring that if any secret keys are stored on the host OS platform, access to them is restricted by key wrapping such that unauthorized subjects cannot view or invoke the key. Note that the control only applies to any keys stored by the TOE on its host platform; the SFR does not require the TOE to interface with a larger organizational key storage repository.
		IA-5	**Authenticator Management**	If the stored key data includes an authenticator such as private keys (and associated certificates) for signature and for encryption as part of the S/MIME protocol), a conformant TOE protects authentication data from unauthorized disclosure, in support of part (g) of this control.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the enforcement of this control by storing cryptographic data in a manner that prevents its unauthorized access.
FCS_CKM_EXT.4*	**Cryptographic Key Destruction**	SC-12	**Cryptographic Key**	A conformant TOE or the platform has the

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Establishment and Management	ability to securely destroy cryptographic keys.
FCS_KYC_EXT.1*	**Key Chaining**	SC-12	**Cryptographic Key Establishment and Management**	The ability of a conformant TOE to maintain a key chain through some combination of its own mechanisms or platform ones satisfies the key access portion of this control.
		SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key wrapping using NSA approved and FIPS validated algorithms, depending on selections made.
		SC-28(3)	**Protection of Information at Rest:** Cryptographic Keys	A conformant TOE supports this control by ensuring that the confidentiality of key data at rest is protected through the use of a key chain to encrypt stored keys, either implemented by the TSF or through reliance on a platform mechanism.
FCS_IVG_EXT.1	**Initialization Vector Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of IVs as needed ensures that generated cryptographic keys have sufficient strength.
FDP_NOT_EXT.1	**Notification of S/MIME Status**	N/A	**N/A**	There are no relevant security controls for this behavior as no control exists for making a user aware of potential malicious activity. SI-4 relates to notification of potential malicious activity administrators, but that does not apply to this case. This SFR relates to user notification as a mechanism to reduce the risk that the user inadvertently triggers malicious activity against the system.
FDP_SMIME_EXT.1	**S/MIME**	SC-8	**Transmission Confidentiality and Integrity**	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 protect email data when in transit.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports this control by using a cryptographic mechanism for the protection of email data in transit.
		SC-28	**Protection of Information at Rest**	A conformant TOE supports this control by implementing a mechanism to protect email data at rest when it has reached its destination.
		SC-28(1)	**Protection of Information at Rest:** Cryptographic Protection	A conformant TOE supports this control by implementing a cryptographic mechanism to protect data at rest.
FIA_X509_EXT.3	**Authentication and Encryption**	CM-14	**Signed Components**	A conformant TOE has the ability to prevent the installation of software if the associated code signing certificate is invalid or missing.
		IA-5(2)	**Authenticator Management:** Public Key-Based Authentication	A conformant TOE has the ability to validate certificate path and status for certificates used in authentication, which satisfies this control.
		SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports this control by implementing a mechanism to ensure that a communications channel will not be established If the confidentiality and integrity of data in transit cannot be assured.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE uses X.509 certificates to enforce the establishment of trusted communications using a cryptographic method.
		SC-23	**Session Authenticity**	A conformant TOE supports this control by requiring the use of X.509v3 certificates as

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				defined by RFC 5280 to support encryption and authentication for S/MIME.
		SI-7(15)	**Software, Firmware, and Information Integrity:** Code Authentication	A conformant TOE prevents the installation of code if the code signing certificate is deemed invalid.
FMT_MOF_EXT.1	**Management of Functions Behavior**	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_AON_EXT.1	**Support for Only Trusted Add-ons**	CM-14	**Signed Components**	A conformant TOE supports this control by ensuring that add-ons are not supported unless explicitly trusted, which is achieved through the add-on's use of a digital signature.
FTP_ITC_EXT.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				
FCS_CKM_EXT.5	**Cryptographic Key Derivation (Password/Passphrase Conditioning)**	IA-5	**Authenticator Management**	A conformant TOE protects the authenticator content from unauthorized disclosure and modification as identified in part (g) of the control.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		IA-5(1)	**Authenticator Management:** Password-Based Authentication	A conformant TOE protects stored passwords using an approved salted key derivation function as identified in part (d) of the control.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to perform Password-based Key Derivation Functions.
FCS_SAG_EXT.1	**Cryptographic Salt Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of salts as needed ensures that generated cryptographic keys have sufficient strength.
FCS_NOG_EXT.1	**Cryptographic Nonce Generation**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE's use of nonces as needed ensures that generated cryptographic keys have sufficient strength.
FDP_NOT_EXT.2	**Notification of URI**	SN/A	**N/A**	There are no relevant security controls for this behavior as no control exists for making a user aware of potential malicious activity. SI-4 relates to notification of potential malicious activity administrators, but that does not apply to this case. This SFR relates to user notification as a mechanism to reduce the risk that the user inadvertently triggers malicious activity against the system.
FDP_PST_EXT.1	**Storage of Persistent Information**	N/A	**N/A**	This SFR requires the TOE to be able to operate in a way that minimizes the persistent information that it needs to store so as to limit the potential for unauthorized access to that information. There are no security controls that this behavior applies to specifically.
FDP_REN_EXT.1	**Rendering of Message Content**	CM-7(2)	**Least Functionality:**	A conformant TOE enforces this control by operating in a plaintext-mode mode

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Prevent Program Execution	which disables the rendering and execution of automatic downloading, rendering and execution of images, external resources and embedded objects such as HTML or JavaScript objects. The applicability of this control is dependent on the extent to which the selections made for the TOE in the SFR aligns with the assignments made for the organization in the control.
		SC-18	**Mobile Code**	A conformant TOE defines acceptable and unacceptable mobile code and mobile code technologies.
Selection-Based Requirements				
FCS_COP_EXT.2	**Key Wrapping**	SC-13	**Cryptographic Protection**	A conformant TOE has the ability to perform key wrapping using NSA approved and FIPS validated algorithms.
FCS_SMC_EXT.1	**Key Combining**	SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE has the ability to perform submask combining in support of key generation functions.
FIA_SASL_EXT.1	**Simple Authentication and Security Layer (SASL)**	IA-3	**Device Identification and Authentication**	A conformant TOE supports this control by implementing SASL as an authentication mechanism.
FPT_AON_EXT.2	**Trusted Installation and Update for Add-ons**	CM-14	**Signed Components**	A conformant TOE requires that updates to its add-ons include integrity measures. Depending on the selection made in the SFR, this may include a digital signature. Note that the SFR also prohibits the automatic installation of add-ons but there are no controls that this behavior applies to.
		SI-7(1)	**Software, Firmware, and Information**	A conformant TOE has the ability to verify the integrity

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
			Integrity: Integrity Checks	of any add-ons that are installed on top of it.
Objective Requirements				
This EP has no objective requirements.				