## Mapping Between

# Collaborative Protection Profile for Network Devices, Version 2.0, 05-May-2017

### 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 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 Ver	rsion 3.x SFR	Supports Enforcement of NIST SP 800-53 Revision 4 Control		Comments and Observations
FAU_GEN.1	Audit Data Generation	AU-2	Auditable Events	A conformant TOE has the ability to 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	A conformant TOE will
	110 5	Audit Records	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	A conformant TOE will
		Audit Records:	generate audit
		Additional Audit	information for some
		Information	auditable events beyond
			what is mandated in
			AU-3. This may or may
			not be sufficient to
			satisfy this control
			based on the additional
			audit information
			required by the
			organization. The TOE
			supports the
			control if its auditable
			control II its auditable
			with the assignments
			chosen for the control
			and if the TOF's audit
			log is part of the overall
			system's auditing.
	AU-12	Audit	A conformant TOE has
		Generation	the ability to 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/enable the generation of specific audit records (which would typically be expressed in CC as FAU_SEL.1).
FAU_GEN.2	<u>User Identity</u> <u>Association</u>	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.
FAU_STG_EXT.1	<u>Protected</u> <u>Audit Event</u> <u>Storage</u>	AU-4	Audit Storage Capacity	A conformant TOE allocates some amount of local storage for audit data. It can be used to support the enforcement of this control if the amount of storage is consistent with the assignment chosen for the control.
		AU-4(1)	Audit Storage Capacity: Transfer to Alternate Storage	A conformant TOE has the ability to logically transmit audit data to a location in its Operational Environment. While this SFR requires the TSF to store generated audit data on the TOE, a minimum storage size or retention period is not specified Therefore a

		1
		storage of audit data is
		limited or transitory.
AU-5	Response to	A conformant TOE has
	Audit	the ability to react in a
	Processing	specific manner when
	Failures	the allocated audit
		storage space is full.
		Depending on the
		actions taken by the
		TOE when this occurs
		and on the assignments
		chosen for this control,
		the TOE can be used to
		support the enforcement
		of either or both parts of
		the control.
AU-5(2)	Kesponse to	A conformant TOE has
	Audit	the ability to react in a
	Processing	specific manner when
	Fanures: Real-	the allocated audit
	Time Alerts	storage space is full. A
		comornant TOE may
		of this control
		depending on the
		behavior specified in the
		ST and the assignments
		chosen for this control
$\Delta U_{-5}(4)$	Response to	A conformant TOE has
110-5(4)	Audit	the ability to react in a
	Processing	specific manner when
	Failures:	the allocated audit
	Shutdown on	storage space is full. A
	Failure	conformant TOE may
		support the enforcement
		of this control,
		depending on the
		behavior specified in the
		ST and the assignments
		chosen for this control.
AU-9	Protection of	A conformant TOE has
	Audit	the ability to prevent
	Information	unauthorized
		modification and
		deletion of audit
		records.
AU-9(2)	Protection of	A conformant TOE
	Audit	must be able to transmit
	Information:	audit data to a logically
	Audit Backup on	remote location. It can

FCS_CKM.1	<u>Cryptographic</u> <u>Key</u> <u>Generation</u>	SC-12	Separate Physical Systems/Compon ents Cryptographic Key Establishment and	be used to support the enforcement of this control if the recipient of the audit data is physically remote from the TOE. The ability of the TOE to generate asymmetric keys satisfies the key generation portion of
		SC-12(3)	Management Cryptographic Key Establishment and Management: Asymmetric Keys	this control. A conformant TOE's ensures that generated asymmetric keys provide an appropriate level of security.
FCS_CKM.2	<u>Cryptographic</u> <u>Key</u> <u>Establishment</u>	SC-12	Cryptographic Key Establishment and Management	A conformant TOE supports this control by providing a key establishment function.
		SC-12(3)	Cryptographic Key Establishment and Management: Asymmetric Keys	A conformant TOE supports the production of asymmetric keys by providing a key establishment function.
FCS_CKM.4	Cryptographic Key Destruction	SC-12	Cryptographic Key Establishment and Management	A conformant TOE has the ability to securely destroy cryptographic keys.
FCS_COP.1/DataEncry ption	<u>Cryptographic</u> <u>Operation</u> (AES Data <u>Encryption/De</u> <u>cryption)</u>	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/SigGen	Cryptographic Operation (Signature Generation and Verification)	SC-13	Cryptographic Protection	A conformant TOE has the ability to perform cryptographic signing using NSA-approved and FIPS-validated algorithms.

FCS_COP.1/Hash	Cryptographic Operation (Hash Algorithm)	SC-13	Cryptographic Protection	A conformant TOE has the ability to perform cryptographic hashing using NSA-approved and FIPS-validated algorithms.
FCS_COP.1/KeyedHash	<u>Cryptographic</u> <u>Operation</u> (Keyed Hash <u>Algorithm)</u>	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	<u>Random Bit</u> <u>Generation</u>	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.
FIA_AFL.1	Authentication Failure Management	AC-7	Unsuccessful Logon Attempts	The TOE has the ability to detect when a defined number of unsuccessful authentication attempts occur and take some corrective action.
FIA_PMG_EXT.1	Password Management	IA-5(1)	Authenticator Management: Password-Based Authentication	A conformant TOE will have the ability to enforce some minimum password complexity requirements, although they are not identical to CNSS or DoD requirements or to those specified in part a of this control.
FIA_UIA_EXT.1	<u>User</u> <u>Identification</u> <u>and</u> <u>Authentication</u>	AC-14	Permitted Actions Without Identification of Authentication	A conformant TOE will define a list of actions that are permitted prior to authentication.
FIA_UAU_EXT.2	Password- <u>Based</u> <u>Authentication</u>	IA-5(1)	Authenticator Management: Password-Based Authentication	A conformant TOE will have the ability to authenticate users with a password-based authentication mechanism.
FIA_UAU.7	<u>Protected</u> <u>Authentication</u> <u>Feedback</u>	IA-6	Authenticator Feedback	The TOE is required to provide obscured feedback to the user while authentication is in progress.

FMT_MOF.1/ManualU pdate	<u>Management</u> of Security <u>Functions</u> <u>Behavior</u>	AC-3 AC-3(7)	Access Enforcement Access Enforcement: Role-Based Access Control	A conformant TOE will not permit application of a TOE update unless proper authorization is provided. A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	Least Privilege	A conformant TOE enforces least privilege by restricting the users that are able to perform manual updates of the TOE software/firmware.
FMT_MTD.1/ CoreData	<u>Management</u> of TSF Data	AC-3	Access Enforcement	A conformant TOE will not permit manipulation of its stored data unless proper authorization is provided
		AC-3(7)	Access Enforcement: Role-Based Access Control	A conformant TOE will restrict access to management functionality to members of a certain role.
		AC-6	Least Privilege	A conformant TOE enforces least privilege by restricting the users that are able to manage TSF data.
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 organizational requirements. Specific additional controls may be supported depending on the functionality claimed by the TOE.

FMT_SMR.2	Restrictions on Security Roles	AC-2(7)	Account Management: Role-Based Schemes	A conformant TOE has the ability to associate users with roles, in support of part a of the control.
FPT_APW_EXT.1	Protection of Administrator Passwords	IA-5(6)	Authenticator Management: Protection of Authenticators	A conformant TOE must have the ability to securely store passwords and any other credential data it uses.
FPT_SKP_EXT.1	<u>Protection of</u> <u>TSF Data</u>	SC-12	Cryptographic Protection	A conformant TOE will ensure that secret key and keying material data are not stored in plaintext except in specific cases where appropriate.
FPT_TST_EXT.1	<u>TSF Testing</u>	SI-6	Security Function Verification	A conformant TOE will run automatic tests to ensure correct operation of its own functionality.
		SI-7	Software, Firmware, and Information Integrity	One of the self-tests the TOE may perform is an integrity test of its own software and/or firmware.
FPT_TUD_EXT.1	<u>Trusted</u> <u>Update</u>	CM-5(3)	Access Restrictions for Change: Signed Components	A conformant TOE requires that updates to itself include integrity measures. Depending on the selection made in the SFR, this may include a digital signature.
		SI-7(1)	Software, Firmware and Information Integrity: Integrity Checks	A conformant TOE has the ability to verify the integrity of updates to itself.
FPT_STM_EXT.1	<u>Reliable Time</u> <u>Stamps</u>	AU-8	Time Stamps	A conformant can generate and use time stamps addresses the actions defined in this control.
		AU-8(1)	<b>Time Stamps:</b> Synchronization with Authoritative Time Source	A conformant TOE may have the ability to synchronize with an NTP server in its Operational

				Environment, satisfying this control.
FTA_SSL_EXT.1	<u>TSF-Initiated</u> <u>Session</u> <u>Locking</u>	AC-11	Session Locking	A conformant TOE may have the ability to lock an idle local interactive session, depending on the selection made in the SFR.
		AC-11(1)	Session Locking: Pattern Hiding	Depending on how the lock function is implemented, a conformant TOE may have the ability to obfuscate the display when in the locked state.
		AC-12	Session Termination	A conformant TOE may have the ability to terminate an idle local interactive session, depending on the selection made in the SFR.
FTA_SSL.3	<u>TSF-Initiated</u> <u>Termination</u>	AC-2(5)	Account Management: Inactivity Logout	A conformant TOE will have the ability to log out after a period of inactivity.
		AC-12	Session Termination	A conformant TOE will have the ability to terminate an idle remote interactive session.
FTA_SSL.4	<u>User-Initiated</u> <u>Termination</u>	AC-12(1)	Session Termination: User-Initiated Logouts / Message Displays	A conformant TOE has the ability to terminate an active session upon user request.
FTA_TAB.1	Default TOE Access Banners	AC-8	System Use Notification	A conformant TOE displays an advisory warning to the user prior to authentication.
FTP_ITC.1	Inter-TSF Trusted Channel	IA-3(1) SC-8	Device Identification and Authentication: Cryptographic Bidirectional Authentication Transmission Confidentiality and Integrity	A conformant TOE may support the enforcement of this control if the protocol(s) used to establish trusted communications uses mutual authentication. 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 or Alternate Physical Protection	The TOE supports a cryptographic method of protecting data in transit.
FTP_TRP.1/Admin	<u>Trusted Path</u>	IA-3(1)	Device Identification and Authentication: Cryptographic Bidirectional Authentication	A conformant TOE may support the enforcement of this control if the protocol(s) used to establish trusted communications uses mutual authentication.
		SC-8(1)	Transmission Confidentiality and Integrity: Cryptographic For Alternate Physical Protection	A conformant TOE will have the ability to prevent unauthorized disclosure of information and also detect modification to that information.
		SC-11	Trusted Path	The TOE establishes a trusted communication path between remote users and itself.
<b>Optional Requirements</b>	1			
FAU_STG.1	<u>Protected</u> <u>Audit Trail</u> <u>Storage</u>	AU-9	Protection of Audit Information	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records.
		AU-9(6)	Protection of Audit Information: Read Only Access	A conformant TOE has the ability to prevent unauthorized modification and deletion of audit records. If the TOE prevents this by preventing all modification and deletion of audit records (i.e., there is no 'authorized' ability to do this), it can be used to support the

				enforcement of this
	~		-	control.
FAU_STG_EXT.2/	Counting Lost	AU-5	Response to	A conformant TOE has
LocSpace	<u>Audit Data</u>		Audit	the ability to count the
			Processing	amount of audit data
			Failures	that is lost by audit
				processing failures. This
				may be used to support
				the enforcement of this
				control if such an action
				is consistent with the
				assignment specified in
		A T T 7	<b>b</b>	part b of the control.
FAU_STG.3/	Action in Case	AU-5	Response to	A conformant TOE will
LocSpace	of Possible		Audit	have the ability to
	<u>Audit Data</u>		Processing	generate a warning if
	Loss		Failures	local audit storage space
				is exhausted. This may
				on foresement of part a of
				this control if the
				mothed of issuing the
				warning qualifies as an
				'alert'
		$\Delta U 5(1)$	<b>D</b> ocnonco to	A conformant TOF will
		AU-3(1)	Audit	have the ability to
			Processing	generate a warning if
			Failures: Audit	local audit storage space
			Storage Capacity	is exhausted. This may
			storage capacity	be used to support the
				enforcement of this
				control if the TOE's
				behavior is consistent
				with the assignments
				chosen for this control
				(e.g., since the SFR
				applies when audit
				storage space is fully
				exhausted the final
				assignment must be
				ʻ100%').
FIA_X509_EXT.1/ITT	<u>Certificate</u>	IA-3	Device	A conformant TOE uses
	<u>Validation</u>		Identification	X.509 certificates to
			and	perform device
			Authentication	authentication of
				distributed TOE
			<b>D</b> :	components.
		IA-3(1)	Device	The TOE uses X.509
			Identification	certificate authentication
		1	ana	between distributed

			A 41 4 <sup>2</sup> 4 <sup>2</sup>	· · · · · · · · · · · · · · · · · · ·
			Authentication:	components to establish
			Cryptographic	cryptographically-
			Bidirectional	secured communications
			Authentication	between them.
				Establishment of these
				channels may require
				bidirectional (mutual)
				authentication.
		IA-5(2)	Authenticator	A conformant TOE has
			Management:	the ability to validate
			PKI-Based	certificate path and
			Authentication	status which satisfies
			Autointication	this control
		SC 22(5)	C	The TOE's use of $\mathbf{Y}$ 500
		SC-25(5)	Session	The TOE's use of X.309
			Authenticity:	certificates to
			Allowed	authenticate distributed
			Certificate	components ensures that
			Authorities	it will include the
				functionality needed to
				validate certificate
				authorities.
FIA_X509_EXT.1/	Certificate	SC-23	Session	Depending on the
ITT	Validation		Authenticity	TOE's use of trusted
				communications
				channels, it may use
				X.509 certificate
				validation in support of
				session authentication
		SC-23(5)	Session	If the TOF uses X 509
		50 25(5)	Authenticity.	certificates as part of
			Allowed	session authentication it
			Cortificato	will include the
			Authoritics	functionality needed to
			Autionities	runctionality needed to
				vandate certificate
	N			authorities.
FM1_MOF.1/Services	Management	AC-3	Access	A conformant TOE will
	of Security		Enforcement	not permit starting and
	Functions			stopping of services
	<b>Behavior</b>			unless proper
				authorization is
				provided.
		AC-3(7)	Access	A conformant TOE will
			Enforcement:	restrict access to
			Role-Based	management
			Access Control	functionality to
				members of a certain
				role.
		AC-6	Least Privilege	A conformant TOE
				enforces least privilege
				by restricting the users

		1		
				that are able to start and
	M4			stop services.
FMT_MTD.1/	Management	AC-3	Access	A conformant TOE will
CryptoKeys	of 1SF Data		Enforcement	not permit manipulation
				of cryptographic data
				unless proper
				authorization is
				provided.
		AC-3(7)	Access	A conformant TOE will
			<b>Enforcement:</b>	restrict access to
			Role-Based	management
			Access Control	functionality to
				members of a certain
				role.
		AC-6	Least Privilege	A conformant TOE
			8	enforces least privilege
				by restricting the users
				that are able to interact
				with cryptographic data.
FPT ITT 1	Basic Internal	SC-8	Transmission	A conformant TOE will
	TSF Data	200	Confidentiality	support this control by
	Transfer		and Integrity	providing a protected
	Protection			communication channel
	<u>1100000000</u>			between remote
				distributed TOF
				components
		SC-8(1)	Transmission	A conformant TOE will
		50 0(1)	Confidentiality	use cryptographic
			and Integrity:	methods to protect data
			Cryptographic or	in transit between
			Alternate	different parts of the
			Physical	TOF
			Protection	IOL.
ETD TDD 1/Loin	Trusted Path	ΙΔ_3	Device	A conformant TOF
		1A-3	Identification	supports the
			and	anforcement of this
			Authoritoption	control by providing a
			Authentication	registration mechanism
				that allows distributed
				TOE components to
				identify and authenticate
				themselves to the other
		<b>CC</b> 9	<b>T</b> • •	themselves to the other.
		50-0	I Fallshillssion	A contornant TOE Will
			confidentiality	support enforcement of
			and integrity	uns control by
				providing a protected
				communication channel
				between remote
				distributed TOE
1		1	1	components as a method

				to transmit registration
				information.
		SC-8(1)	Transmission	A conformant TOE will
			Confidentiality	use cryptographic
			and Integrity:	methods to protect
			Cryptographic or	initial registration data
			Alternate	transmitted between
			Physical	different parts of the
			Protection	TOE.
FCO_CPC_EXT.1	Component	AC-4	Information	A conformant TOE
	Registration		Flow	supports the
	Channel		Enforcement	enforcement of this
	<b>Definition</b>			control by providing a
				registration mechanism
				that is used as a
				condition for distributed
				TOE components to
				establish information
				flow between them.
Selection-Based Requiren	nents			
FCS_DTLSC_EXT.1	<b>DTLS Client</b>	IA-5(2)	Authenticator	The TOE requires peers
	<b>Protocol</b>		Management:	to possess a valid
			PKI-Based	certificate before
			Authentication	establishing trusted
				communications,
				supporting this control.
		SC-8	Transmission	A conformant TOE has
			Confidentiality	the ability to ensure the
			and Integrity	confidentiality and
				integrity of information
				transmitted between the
				TOE and another trusted
				IT product.
		SC-8(1)	Transmission	The TOE supports a
			Integrity:	cryptographic method of
			Cryptographic or	protecting data in
			Alternate	transit.
			Physical	
			Protection	
		SC-13	Cryptographic	The TOE provides
			Protection	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	IA-5(2)	Authenticator	The TOE requires peers
	Protocol –		Management:	to possess a valid
	with		PKI-Based	certificate before
	Authentication		Authentication	establishing trusted
				communications and
				provides its own client
				certificate to the peer,
				supporting this control.
		SC-8	Transmission	A conformant TOE has
			Confidentiality	the ability to ensure the
			and Integrity	confidentiality and
				integrity of information
				transmitted between the
				TOE and another trusted
				IT product.
		SC-8(1)	Transmission	The TOE supports a
			Integrity:	cryptographic method of
			Cryptographic or	protecting data in
			Alternate	transit.
			Physical	
			Protection	
		SC-13	Cryptographic	The TOE provides
			Protection	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	IA-5(2)	Authenticator	The TOE provides a
	<b>Protocol</b>		Management:	server certificate to a
			PKI-Based	TLS client before
			Authentication	establishing trusted
				communications,
				supporting this control
		SC-8	Transmission	A conformant TOE has
			Confidentiality	the ability to ensure the
			and Integrity	confidentiality and
				integrity of information
				transmitted between the
				TOE and another trusted
				IT product.
		SC-8(1)	Transmission	The TOE supports a
			Integrity:	cryptographic method of
			Cryptographic or	protecting data in
			Alternate	transit.
			Physical	
		1	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	DTLS Server Protocol with <u>Mutual</u> Authentication	IA-5(2)	Authenticator Management: PKI-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 Integrity: Cryptographic or Alternate Physical 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_HTTPS_EXT.1	HTTPS Protocol	IA-5(2)	Authenticator Management: PKI-Based Authentication	A conformant TOE may support the implementation of PKI- based authentication by validating peer certificates as part of the authentication process.

		SC-8	Transmission	A conformant TOE has
			Confidentiality	the ability to ensure the
			and Integrity	confidentiality and
			87	integrity of information
				transmitted between the
				TOE and another trusted
				11 product.
		SC-8 (1)	Transmission	The TOE supports a
			Confidentiality	cryptographic method of
			and Integrity:	protecting data in
			Cryptographic or	transit.
			alternate	
			protection	
		SC-13	Cryntographic	The TOE provides
		50 15	Protection	cryptographic methods
			rottenon	to socure data in transit
				which may action
				which may satisfy
				organization-defined
				uses if the functionality
				claimed by the TSF is
				consistent with
				organizational
				requirements.
FCS_IPSEC_EXT.1	<b>IPsec Protocol</b>	IA-5(2)	Authenticator	A conformant TOE
			Management:	implements peer
			PKI-Based	authentication for IPsec.
			Authentication	
		SC-8	Transmission	A conformant TOE
		500	Confidentiality	implements IPsec as a
			and Integrity	method of ensuring
			and mugnity	confidentiality and
				integrity of data in
				transit
		CC 9(1)	<b>T</b>	transit.
		SC-0(1)	I ransmission	The TOE's use of IPsec
			miegrity:	provides a
			Cryptographic or	cryptographic means to
			Alternate	protect data in transit.
			Physical	
			Protection	
		SC-13	Cryptographic	The TOE provides
			Protection	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
1		1		requirements.

FCS SSHC EXT.1	SSH Client	AC-17(2)	Remote Access:	The SSH client protocol
	Protocol		Protection of	implemented by the
			Confidentiality/In	TOE provides
			tegrity Using	confidentiality and
			Encryption	integrity for remote
				access.
		IA-2	Identification and	A conformant TOE may use its SSH client
			Authentication	functionality to interact
			(Organizational	with a remote system on
			Users)	behalf of an
				organizational user.
		IA-3	Device	A conformant TOE may
			Identification	use its SSH client
			and	functionality to establish
			Authentication	a static or as-needed
				connection to a specific
				remote device that is
				authenticated using a
				public key and/or X.509
				certificate (instead of an
				administrator-supplied
				credential), which
				supports this control.
		SC-8	Transmission	A conformant TOE has
			Confidentiality	the ability to ensure the
			and Integrity	confidentiality and
				integrity of information
				TOE and another trusted
				I DE and another it usied
		SC-8(1)	Transmission	The TOE's use of SSH
		50-0(1)	Integrity.	supports a cryptographic
			Cryptographic or	method of protecting
			Alternate	data in transit.
			Physical	
			Protection	
		SC-13	Cryptographic	The TOE provides
			Protection	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_SSHS_EXT.1	SSH Server	AC-17(2)	Remote Access:	The SSH client protocol
	<b>Protocol</b>		Protection of	implemented by the
			Confidentiality/In	TOE provides

			togrity Using	confidentiality and
			En a marti a n	confidentiality and
			Encryption	integrity for remote
				access.
		IA-2	Identification	A conformant TOE
			and	provides SSH server
			Authentication	functionality that
			(Organizational	enforces identification
			Users)	and authentication of
			()()	organizational users
				attempting to access the
				TSE
		60.9	<b>T</b>	131.
		SC-8	Transmission	A conformant TOE has
			Integrity	the ability to ensure the
				confidentiality and
				integrity of information
				transmitted between the
				TOE and another trusted
				IT product.
		SC-8(1)	Transmission	The TOE's use of SSH
		~ /	Integrity:	enforces a cryptographic
			Cryptographic or	method of protecting
			Alternate	data in transit
			Dhysical	data in transit.
			Physical	
		60.12	Protection	
		SC-13	Cryptographic	The TOE provides
			Protection	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 FXT 1	TLS Client	IA-5(2)	Authenticator	The TOE requires peers
	Protocol	11 5(2)	Management:	to possess a valid
	<u>1100000</u>		PKI_Based	certificate before
			Authentication	establishing trusted
			Aumentication	
				communications,
		00.0		supporting this control.
		SC-8	Transmission	A conformant TOE has
			Confidentiality	the ability to ensure the
			and Integrity	confidentiality and
				integrity of information
				transmitted between the
				TOE and another trusted
				IT product.
		SC-8(1)	Transmission	The TOE supports a
		, í	Integrity:	cryptographic method of
			Cryptographic or	

			Alternate	protecting data in
			Physical	transit.
			Protection	
		SC-13	Cryptographic	The TOE provides
			Protection	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 TISC FXT 2	TI S Client	$IA_{-5}(2)$	Authenticator	The TOF requires peers
TED_TEDC_EXT.2	Protocol with	11 5(2)	Management.	to possess a valid
	Authentication		PKI_Based	certificate before
	Automication		Authentication	establishing trusted
			Autoniteation	communications and
				provides its own client
				certificate to the peer
				supporting this control
		SC 9	Transmission	A conformant TOE has
		SC-0	1 ransmission Confidentiality	A comomiant TOE has
			ond Integrity	approximation in the second se
			and integrity	integrity of information
				transmitted between the
				TOE and another trusted
				TOE and another trusted
			<b>T</b> • •	
		SC-8(1)		The TOE supports a
			Integrity:	cryptographic method of
			Cryptographic or	protecting data in
			Alternate	transit.
			Physical	
		SC 12	Protection Crumta granhia	The TOE meetides
		SC-15	Cryptographic	The TOE provides
			Protection	to soowe date in transit
				which may satisfy
				which may satisfy
				uses if the functionality
				claimed by the TCF is
				consistent with
				organizational
				requirements
ECS TISS EVT 1	TI S Sarvar	$IA_{-5}(2)$	Authenticator	The TOE provides a
rcs_1Lss_EA1.1	<u>ILS Server</u> Protocol	14-3(2)	Aumenticator Monogoment	server certificate to a
	<u>1 1010C01</u>		DKI Based	TIS client before
			Authentication	establishing trusted
				communications
				supporting this control
			1	supporting this control.

		0.0.0	<b>m</b> • •	
		SC-8	I ransmission	A conformant TOE has
			Confidentiality	the ability to ensure the
			and Integrity	confidentiality and
				integrity of information
				transmitted between the
				TOE and another trusted
				IT product
		$SC_{-8}(1)$	Transmission	The TOF supports a
		50 0(1)	Intogrity.	cryptographic method of
			Counte complia con	eryptographic method of
			Alternate	protecting data in
			Alternate	transit.
			Physical	
			Protection	
		SC-13	Cryptographic	The TOE provides
			Protection	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	IA-5(2)	Authenticator	The TOE requires peers
	<b>Protocol with</b>		Management:	to possess a valid
			0	
	Mutual		PKI-Based	certificate before
	<u>Mutual</u> Authentication		PKI-Based Authentication	certificate before establishing trusted
	<u>Mutual</u> <u>Authentication</u>		PKI-Based Authentication	certificate before establishing trusted communications and
	<u>Mutual</u> <u>Authentication</u>		PKI-Based Authentication	certificate before establishing trusted communications and provides its own server
	<u>Mutual</u> <u>Authentication</u>		PKI-Based Authentication	certificate before establishing trusted communications and provides its own server certificate to the peer.
	<u>Mutual</u> <u>Authentication</u>		PKI-Based Authentication	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control
	<u>Mutual</u> <u>Authentication</u>	<u>SC-8</u>	PKI-Based Authentication	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control.
	<u>Mutual</u> <u>Authentication</u>	SC-8	PKI-Based Authentication Transmission	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the
	<u>Mutual</u> <u>Authentication</u>	SC-8	PKI-Based Authentication Transmission Confidentiality and Integrity	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and
	<u>Mutual</u> <u>Authentication</u>	SC-8	PKI-Based Authentication Transmission Confidentiality and Integrity	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information
	<u>Mutual</u> <u>Authentication</u>	SC-8	PKI-Based Authentication Transmission Confidentiality and Integrity	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the
	<u>Mutual</u> <u>Authentication</u>	SC-8	PKI-Based Authentication Transmission Confidentiality and Integrity	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the
	<u>Mutual</u> <u>Authentication</u>	SC-8	PKI-Based Authentication Transmission Confidentiality and Integrity	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted
	<u>Mutual</u> <u>Authentication</u>	SC-8	PKI-Based Authentication Transmission Confidentiality and Integrity	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product.
	<u>Mutual</u> <u>Authentication</u>	SC-8 SC-8(1)	PKI-Based Authentication Transmission Confidentiality and Integrity Transmission	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product. The TOE supports a
	<u>Mutual</u> <u>Authentication</u>	SC-8 SC-8(1)	PKI-Based Authentication Transmission Confidentiality and Integrity Transmission Integrity:	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product. The TOE supports a cryptographic method of
	<u>Mutual</u> <u>Authentication</u>	SC-8 SC-8(1)	PKI-Based Authentication Transmission Confidentiality and Integrity Transmission Integrity: Cryptographic or	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product. The TOE supports a cryptographic method of protecting data in
	<u>Mutual</u> <u>Authentication</u>	SC-8 SC-8(1)	PKI-Based Authentication Transmission Confidentiality and Integrity Transmission Integrity: Cryptographic or Alternate	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product. The TOE supports a cryptographic method of protecting data in transit.
	<u>Mutual</u> <u>Authentication</u>	SC-8 SC-8(1)	PKI-Based Authentication Transmission Confidentiality and Integrity Transmission Integrity: Cryptographic or Alternate Physical	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product. The TOE supports a cryptographic method of protecting data in transit.
	<u>Mutual</u> <u>Authentication</u>	SC-8 SC-8(1)	PKI-Based Authentication Transmission Confidentiality and Integrity Transmission Integrity: Cryptographic or Alternate Physical Protection	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product. The TOE supports a cryptographic method of protecting data in transit.
	<u>Mutual</u> <u>Authentication</u>	SC-8 SC-8(1) SC-13	PKI-Based Authentication Transmission Confidentiality and Integrity Transmission Integrity: Cryptographic or Alternate Physical Protection Cryptographic	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product. The TOE supports a cryptographic method of protecting data in transit.
	<u>Mutual</u> <u>Authentication</u>	SC-8 SC-8(1) SC-13	PKI-Based Authentication Transmission Confidentiality and Integrity Transmission Integrity: Cryptographic or Alternate Physical Protection Cryptographic Protection	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product. The TOE supports a cryptographic method of protecting data in transit.
	<u>Mutual</u> <u>Authentication</u>	SC-8 SC-8(1) SC-13	PKI-Based Authentication Transmission Confidentiality and Integrity Transmission Integrity: Cryptographic or Alternate Physical Protection Cryptographic Protection	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product. The TOE supports a cryptographic method of protecting data in transit. The TOE provides cryptographic methods to secure data in transit
	<u>Mutual</u> <u>Authentication</u>	SC-8 SC-8(1) SC-13	PKI-Based Authentication Transmission Confidentiality and Integrity Transmission Integrity: Cryptographic or Alternate Physical Protection Cryptographic Protection	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product. The TOE supports a cryptographic method of protecting data in transit. The TOE provides cryptographic methods to secure data in transit which may satisfy
	<u>Mutual</u> <u>Authentication</u>	SC-8 SC-8(1) SC-13	PKI-Based Authentication Transmission Confidentiality and Integrity Transmission Integrity: Cryptographic or Alternate Physical Protection Cryptographic Protection	certificate before establishing trusted communications and provides its own server certificate to the peer, supporting this control. A conformant TOE has the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another trusted IT product. The TOE supports a cryptographic method of protecting data in transit. The TOE provides cryptographic methods to secure data in transit which may satisfy organization-defined

				claimed by the TSF is
				consistent with
				organizational
		<b>1 1 1 1 1</b>		requirements.
FIA_X509_EXT.1/Rev	<u>Certificate</u>	IA-5(2)	Authenticator	A conformant TOE has
	Validation		Management:	the ability to validate
			PKI-Based	certificate path and
			Authentication	status, which satisfies
			<b>a</b> .	this control.
		SC-23	Session	Depending on the
			Authenticity	IOE's use of trusted
				communications
				$\mathbf{X}_{500}$ continues
				A.509 certificate
				validation in support of
		SC(22(5))	Section	If the TOE uses V 500
		SC-23(3)	Authonticity	cartificates as part of
			Allowed	session authentication it
			Certificate	will include the
			Authorities	functionality needed to
			rumonnes	validate certificate
				authorities.
FIA X509 EXT.2	Certificate	IA-2	Identification	A conformant TOE has
	Authentication		and	the ability to identify
			Authentication	and authenticate
				organizational users
				using X.509 certificates.
FIA_X509_EXT.3	<b>Certificate</b>	IA-5(2)	Authenticator	A conformant TOE
	<b>Requests</b>		Management:	supports this control in
			PKI-Based	part by providing an
			Authentication	interface to generate
				certificate signing
				requests.
FPT_TST_EXT.2	Self-Tests	SI-7(12)	Software,	A conformant TOE
	Based on		Firmware, and	ensures the integrity of
	Certificates		Information	its own functions prior
			Integrity:	to execution.
			Varification	
EPT TUD EXT 2	Trusted	CM 5(3)		A conformant TOF
ITI_IOD_EXI.2	<u>Indetes</u> Resed	CIVI-3(3)	Restrictions for	supports the
	on Certificates		Change Signed	enforcement of this
	on certificates		Components	control through the use
			Componento	of code signing
				certificates for software
				updates.
		SI-7(15)	Software.	A conformant TOE's
		× - /	Firmware, and	use of a code signing
			Information	certificate for software

				1
			Integrity: Code	updates supports the
			Authentication	enforcement of this
				control
EMT MOE 1/	Managamant	$\Lambda C 3$	Access	A conformant TOF will
	of Society	AC-J	ALLESS Enforcement	not normit anobling of
AutoUpdate	of Security		Enforcement	not permit enabling of
	Functions			automatic updates
	<b>Behaviour</b>			unless proper
				authorization is
				provided.
		AC-3(7)	Access	A conformant TOE will
		,	Enforcement:	restrict access to
			Role-Based	management
			Access Control	functionality to
			Access Control	functionality to
				members of a certain
				role.
		AC-6	Least Privilege	A conformant TOE
				enforces least privilege
				by restricting the users
				that are able to
				configure automatic
				undates
		SI 2(5)	Flow	A conformant TOE will
		51-2(3)		A conformant TOE will
			Remediation:	nave the ability to have
			Automatic	software or firmware
			Software/	updates be configured to
			Firmware	occur automatically.
			Updates	
FMT MOF.1/Functions	Management	AC-3	Access	A conformant TOE will
	of Security		Enforcement	not permit management
	Functions		Linorcement	of audit behavior unless
	Pahoviour			proper outhorization is
	Denaviour			proper autionization is
				provided.
		AC-3(/)	Access	A conformant TOE will
			Enforcement:	restrict access to
			Role-Based	management
			Access Control	functionality to
				members of a certain
				role.
		AC-6	Least Privilege	A conformant TOF
			Least I I VIICge	anforcas lasst privilage
				by most most in a the most
				by restricting the users
				that are able to
				configure audit
				behavior