NIST SP 800-53 Revision 4 Mapping: Protection Profile for Application Software Version 1.0 2014-10-15

Introduction

Several of the NIST SP 800-53/CNSS 1253 controls are either fully or partially addressed by compliant TOEs. This section outlines the requirements that are addressed, and can be used by certification personnel to determine what, if any, additional testing is required when the TOE is incorporated into its operational configuration.

General Caveats

- A protection profile describes the security characteristics of a given product; the Risk Management Framework and the NIST SP 800-53 controls are designed for systems. A product, in isolation, can never satisfy a control for an overall system – at minimum, there needs to be assurance that supporting operational policies and practices are in place. At best, a product can support an overall system in satisfying the control.

- There are no general controls in NIST SP 800-53 regarding what make an application acceptable for use – that determination appears to be left up to organizations and organizational policy. The closest notion is that of having a whitelist (or blacklist) of approved (or disapproved) applications.

- There is an interesting implication if this profile is issued: For those organizations where SA-4(7) is mandatory, this profile could be required for every potential COTS IA and IA-enabled application, because CNSSP 11 requires evaluation against a profile if a profile for that technology type exists.

- Note that the application itself, as part of its designed functionality, may support satisfaction of a NIST SP 800-53 control. Given that the profile itself is agnostic regarding the application functionality and purpose, this mapping must be similarly agnostic.

- Just as Common Criteria SFRs differ based on the completion of assignments and selections, so to do NIST SP 800-53 controls. An underlying assumption in the statement of support is that the assignments (or supporting policies) are completed in congruent fashions. In other words, if the SFR is calling for the use of a particular algorithm for a particular cryptographic function, then the assignment in SC-13 is completed to call for that same algorithm for the same cryptographic function.

- A flaw in the approach taken by many of the newer PPs is to view the SFRs as divisible – that is, some elements (the individual "The TSF shall" statements, xxx_xxx.1.x) can be present or no, with assurance activities for each. The Common Criteria, on the other hand, considers the SFRs to be the indivisible unit (e.g., FAU_GEN.1). This document only maps to the level of the whole SFR. Also note that most of the functional requirements are not drawn from the "stock" Common Criteria.

Base Security Functional and Assurance Requirements

Common Criteria Version 3.x SFR/SAR		**NIST SP 800-53 Revision 4 Control** † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		**Comments and Observations**
FCS_RBG_EXT.1	**Cryptographic Support (FCS)** Random Bit Generation Services • Application [uses no DRBG functionality, invokes platform-provided DRBG functionality, implements DRBG functionality] for its cryptographic operations.	This control supports no NIST SP 800-53 controls: • If it is completed to use no DBRG functionality, it is unrelated to any control as there are no controls that either call for the use or non-use of random number generators. • If it is completed to use either platform-provided or internally-implemented DBRGs, then it has a relation to cryptography. However, the support for control satisfaction (and thus, potentially SC-13) would be in the SFRs that actually call out the cryptographic requirements.		
FCS_STO_EXT.1	**Cryptographic Support (FCS)** Storage of Secrets • Application [doesn't store any credentials, invokes the functionality provided by the platform to securely store [list of credentials], implements functionality to securely store [list of credentials]] to non-volatile memory.	**Note:** There are three situations related to this control: 1. If the application does not handle credentials, it does not support any credential handling controls. 2. If the application handles credentials but does not store them, it still requires to protect the credentials during transit (addressed by other controls) 3. If the application stores credentials (however it does it), then the following controls are supported:		
		IA-5	**Authenticator Management** Organization manages information system authenticators by… • […] • Protecting authenticator content from unauthorized disclosure and modification • […]	Protecting persistent credentials (secret keys, PKI private keys, or passwords) is a form of protecting authenticator content.
		IA-5(1)	**Authenticator Management** | Password-Based Authentication Information system, for password-based authentication… • […] • Stores and transmits only encrypted representations of passwords • […]	Supports only storing encrypted representations. (Use of cryptography is implied by the placement under FCS)

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
		IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • […] • Enforces authorized access to the corresponding private key; • […]	Supports only storing encrypted representations. (Use of cryptography is implied by the placement under FCS)
		SC-12	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Protecting the key supports key management.
FDP_DEC_EXT.1	**User Data Protection (FDP)** Access to Platform Resources • Application provides user awareness of its intent to access [no hardware resources, network connectivity, camera, microphone, location services, NFC, USB, Bluetooth, [additional hardware resources]] • Application provides user awareness of its intent to access [no system-wide information repositories, address book, calendar, call lists, system logs, [additional system-wide information repositories]] • Application only seeks access to those resources for which it has provided a justification to access. • Application restricts network communication to [no network communication, user-initiated communication for [list of functions for which the user can initiate network communication], respond to [list of remotely-initiated communication] , [list of application-initiated network communication]]. • Application [doesn't transmit PII over a network , requires user approval before executing [list of	IP-1	**Consent** Organization… • Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; • Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; • Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and • Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.	Requiring user approval before transmitting PII is a form of consent, and thus supports IP-1.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	functions that transmit PII over a network]] .	**Note:** In general, there are no controls requiring *user* awareness of what a particular application accesses. With respect to documentation of what resources are used, the following control is supported through documentation:		
		SA-4(1)	**Acquisition Process** | Functional Properties of Security Controls • Organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	Arguably, describing the platform resources that the application access is part of the description of the functional properties of the application, and hence providing that description for the application.
		Note: FDP_DEC_EXT.1.4, which talks about restricting network communication, arguably is a form of managed boundary access, thus supporting the following control:		
		SC-7	**Boundary Protection** Information system… • Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system • Implements subnetworks for publicly accessible system components that are [*physically; logically*] separated from internal organizational networks • Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	Although not a firewall, the notion that the application may restrict network communication to specific functions or specific remotely initiated functions is a form of managed access control, and thus SC-7 is supported.
		Note: Depending on the completion of the control, the following enhancements may be supported:		
		SA-4(9)	**Acquisition Process** | Functions / Ports / Protocols / Services in Use • Organization requires the developer of the information system, system component, or information system service to identify early in the system development life cycle, the functions, ports, protocols, and services intended for organizational use.	If the application is describing network connectivity, or use of NFC, Bluetooth, or other similar protocols, it would fall under the description of planned functions, ports, protocols, and services in use.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
		SC-15	**Collaborative Computing Devices** Information system… • Prohibits remote activation of collaborative computing devices with the following exceptions: [*exceptions where remote activation is to be allowed*]; • Provides an explicit indication of use to users physically present at the devices.	If the application identifies use of the camera or microphone, it supports satisfaction of this control by identifying that the system needs to ensure the control is appropriately addressed. **However, it does not meet the control because it does not require an explicit indicate of use of those components**.
		SC-42	**Sensor Capability and Data** Information system… • Prohibits the remote activation of environmental sensing capabilities with the following exceptions: [*exceptions where remote activation of sensors is allowed*]; • Provides an explicit indication of sensor use to [*class of users*].	If the application identifies use of the camera, microphone, or location services, it supports satisfaction of this control by identifying that the system needs to ensure the control is appropriately addressed. **However, it does not meet the control because it does not require an explicit indicate of use of those components**.
FDP_DAR_EXT.1	**User Data Protection (FDP)** Storage Of Sensitive Application Data • Application [invokes platform-provided functionality to encrypt sensitive data stored, implements functionality to encrypt sensitive data stored, not store any sensitive data] in non-volatile memory.	SC-28	**Protection of Information at Rest** • Information system protects the [*(one or more): confidentiality; integrity*] of [*information at rest*].	Assuming the SFR is completed to address sensitive data (i.e., the last option of no sensitive data is not chosen) and the control is completed in a congruent manner, the implementation of the SFR supports the control.
		SC-28(1)	**Protection of Information at Rest** | Cryptographic Protection • Information system implements cryptographic mechanisms to prevent unauthorized disclosure and modification of [*information*] on [*information system components*].	Assuming the SFR is completed to address sensitive data (i.e., the last option of no sensitive data is not chosen) and the control is completed in a congruent manner, the implementation of the SFR supports the control.
FMT_MEC_EXT.1	**Security Management (FMT)** Supported Configuration Mechanism • Application invokes the mechanisms recommended by the platform vendor for storing and setting configuration options.	**No Correspondence**. There are no controls dealing with how configuration options are set. CM-6 does address ensuring the option's values are in accordance with specified organizational guidance (i.e., STIGs), and there is a preference that SCAP support is present, but that is as close as NIST SP 800-53 comes.		

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FMT_CFG_EXT.1	**Security Management (FMT)** Secure by Default Configuration • Application only provides enough functionality to set new credentials when configured with default credentials or no credentials. • Application is configured by default with file permissions which protect it and its data from unauthorized access.	CM-6	**Configuration Settings** Organization… • Establishes and documents configuration settings for information technology products employed within the information system using [*security configuration checklists*] that reflect the most restrictive mode consistent with operational requirements; • Implements the configuration settings; • […]	The SFR would seem to support configuration in the most restrictive mode, although to support the control, those settings would have to be congruent with settings established by the organization. **Note:** One might think the SFR supports AC-3 (Access Enforcement); however the SFR has nothing to do with the actual enforcement of policy, only the settings of permissions. A similar argument would apply to AC-6 (Least Privilege).
		SA-4(5)	**Acquisition Process** | System / Component / Service Configurations Organization requires the developer of the information system, system component, or information system service to: • Deliver the system, component, or service with [*security configurations*] implemented; • Use the configurations as the default for any subsequent system, component, or service reinstallation or upgrade.	The SFR would seem to support this, depending on how the control is completed as the default configuration.
FMT_SMF.1	**Specification of Management Functions** Specification of Management Functions • Product is of performing the following management functions: [no management functions, enable/disable the transmission of any information describing the system's hardware, software, or configuration , enable/disable the transmission of any PII, enable/disable transmission of any application state (e.g. crashdump) information, enable/disable network backup functionality to [*list of enterprise or commercial cloud backup systems*] , [*list of other management functions to be provided by the TSF*]].	**Unclear Correspondence**. In general, due to its system orientation, there are few controls in NIST SP 800-53 devoted to specifically required management functionality. Further, given the nature of the assignment here (e.g., it could be completed to require no management functions), the SFR does not *apriori* satisfy any control. The following controls might be supported, depending on how the SFR is completed:		
		RA-5(4)	**Vulnerability Scanning** | Discoverable Information • Organization determines what information about the information system is discoverable by adversaries and subsequently takes [*corrective actions*].	If the SFR is completed to address transmission of information describing the system's hardware, software, or configuration, it would appear to support hiding information about the system from adversaries. **Note:** There is a similar control, SA-7(16), related to boundary devices hiding information. In general, this completion goes to any control that addresses hiding or

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
				concealing information about the system configuration.
		IP-1	**Consent** Organization… • Provides means, where feasible and appropriate, for individuals to authorize the collection, use, maintaining, and sharing of personally identifiable information (PII) prior to its collection; • Provides appropriate means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use, dissemination, and retention of PII; • Obtains consent, where feasible and appropriate, from individuals prior to any new uses or disclosure of previously collected PII; and • Ensures that individuals are aware of and, where feasible, consent to all uses of PII not initially described in the public notice that was in effect at the time the organization collected the PII.	If the SFR is completed to manage transmission of PII, it would appear to support IP-1.
		CP-9	**Information System Backup** Organization… • Conducts backups of user-level information contained in the information system [*frequency consistent with recovery time and recovery point objectives*]; • Conducts backups of system-level information contained in the information system [*frequency consistent with recovery time and recovery point objectives*]; • Conducts backups of information system documentation including security-related documentation [*frequency consistent with recovery*	If the SFR is completed to permit management of network backup functionality, it would appear to support CP-9.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			time and recovery point objectives]; • Protects the confidentiality, integrity, and availability of backup information at storage locations.	
FPT_API_EXT.1	**Protection of the TSF (FPT)** Use of Supported Services and APIs • Application only uses supported platform APIs	**No Correspondence**. There are no controls dealing with what interfaces applications use. Such a requirement is too low-level for NIST SP 800-53.		
FPT_AEX_EXT.1	**Protection of the TSF (FPT)** Anti-Exploitation Capabilities • Application does not request to map memory at an explicit address except for [*list of explicit exceptions*] . • Application [does not allocate any memory region with both write and execute permissions , allocates memory regions with write and execute permissions for only [*list of functions performing just-in-time compilation*]] . • Application is compatible with security features provided by the platform vendor. • Application does not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so. • Application is compiled with stack-based buffer overflow protection enabled.	SA-4(3)	**Acquisition Process** | Development Methods / Techniques / Practices • Organization requires the developer of the information system, system component, or information system service to demonstrate the use of a system development life cycle that includes [*state-of-the-practice system/security engineering methods, software development methods, testing / evaluation / validation techniques, and quality control processes*].	Depending on how the control is completed, the SFR may support use of *state-of-the-practice system/security engineering methods.*
		SA-8	**Security Engineering Principles** • Organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	Following the properties described in the SFR supports satisfaction of SA-8, as they are all security engineering principles.
		SI-16	**Memory Protection** • Information system implements [*security safeguards*] to protect its memory from unauthorized code execution.	The techniques in the SFR support memory protection.
FPT_TUD_EXT.1	**Protection of the TSF (FPT)** Integrity for Installation and Update • Application [provides the ability, leverages the platform] to check for updates and patches to the application software. • Application is distributed using the format of the platform-supported package manager.	CM-5(3)	**Access Restrictions for Change** | Signed Components • Information system prevents the installation of [*software and firmware components*] without verification that the component has been digitally signed using a certificate that is	The SFR supports the digital signature aspect of this.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	• Application is packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events. • Application does not download, modify, replace or update its own binary code. • Application [provides the ability, leverages the platform] to query the current version of the application software. • Application installation package and its updates are digitally signed such that its platform can cryptographically verify them prior to installation.		recognized and approved by the organization.	
		SI-2	**Flaw Remediation** Organization… • […] • Installs security-relevant software and firmware updates within [*time period*] of the release of the updates; • […]	The ability to check for updates, combined with appropriate procedures, supports the installation aspect of this.
		Note: Many of the aspects of this SFR are below the level of the NIST SP 800-53 or note addressed by the controls, as they are specific to a particular application or component, as opposed to a system-level control.		
FPT_LIB_EXT.1	**Protection of the TSF (FPT)** Use of Third Party Libraries • Application is packaged with only [*list of third-party libraries*].	CM-7(5)	**Least Functionality** | Authorized Software / Whitelisting Organization… • Identifies [*software programs authorized to execute on the information system*]; • Employs a deny-all, permit-by-exception policy to allow the execution of authorized software programs on the information system • Reviews and updates the list of authorized software programs [*frequency*].	This SFR might be viewed as supporting whitelisting of components. However, the control is focused on programs, whereas the SFR is at the level of third-party libraries.
FTP_DIT_EXT.1	**Trusted Path/Channel (FTP)** Protection of Data in Transit • Application [does not transmit any data, does not transmit any sensitive data, encrypts all transmitted sensitive data with [*at least one of: HTTPS, TLS, DTLS*], encrypts all transmitted data with [*at least one of: HTTPS, TLS, DTLS*]] between itself and another trusted IT product.	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	Assuming the SFR is completed to indicate that sensitive transmitted information is protected, this control would be supported.
		SC-8(1)	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical*	Assuming the SFR is completed to indicate that sensitive transmitted information is protected, this control would be supported (given the protocols specified).

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			safeguards].	
ADV_FSP.1	**Functional Specification** Security-Enforcing Functional Specification • Developer provides a functional specification and a tracing from the functional specification to the SFRs. • Functional specification: 1. Describe the purpose and method of use for each SFR-enforcing and SFR-supporting interface. 2. Identifies all parameters associated with each SFR-enforcing and SFR-supporting interface. 3. Provides rationale for the implicit categorisation of interfaces as SFR-non-interfering. • Tracing demonstrates that the SFRs trace to interfaces in the functional specification. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. • Evaluator determines that the functional specification is an accurate and complete instantiation of the SFRs.	SA-4(1)	**Acquisition Process** | Functional Properties of Security Controls • Organization requires the developer of the information system, system component, or information system service to provide a description of the functional properties of the security controls to be employed.	The ADV_FSP family provides information about functional interfaces. The SA-4(1) control requires describing the functionality (i.e., security capability, functions, or mechanisms) visible at the interfaces of the controls and specifically exclude functionality and data structures internal to the operation of the controls.
		SA-4(2)	**Acquisition Process** | Design / Implementation Information for Security Controls • Organization requires the developer of the information system, system component, or information system service to provide design and implementation information for the security controls to be employed that includes: [*(one or more): security-relevant external system interfaces; high-level design; low-level design; source code or hardware schematics; [design/implementation information]*] at [*level of detail*].	The ADV_FSP family provides information about functional interfaces. The SA-4(2) control requires design and implementation information; it should be completed to require them at the level of the security-relevant external system interfaces. **Note**: There is no requirement that requires separation of interfaces into security-enforcing, security non-enforcing, security non-interfering, etc.
AGD_OPE.1	**Operational User Guidance** Operational User Guidance • Developer provides operational user guidance. • Operational user guidance: 1. Describes, for each user role, the user-accessible functions and privileges that should be controlled in a secure processing environment, including appropriate warnings. 2. Describes, for each user role, how to use the available interfaces provided by the	SA-5	**Information System Documentation‡** Organization… • Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. Effective use and maintenance of security functions/mechanisms;	AGD_OPE is the combined requirement for administrator and user documentation.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	product in a secure manner. 3. Describes, for each user role, the available functions and interfaces, in particular all security parameters under the control of the user, indicating secure values as appropriate. 4. For each user role, clearly presents each type of security-relevant event relative to the user-accessible functions that need to be performed, including changing the security characteristics of entities under the control of the product. 5. Identifies all possible modes of operation of the product (including operation following failure or operational error), their consequences and implications for maintaining secure operation. 6. For each user role, describes the security measures to be followed in order to fulfill the security objectives for the operational environment as described in the ST. 7. Is written to be clear and reasonable. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence.		3. Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; • Obtains user documentation for the information system, system component, or information system service that describes: 1. User-accessible security functions/mechanisms and how to effectively use those security functions / mechanisms; 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner; 3. User responsibilities in maintaining the security of the system, component, or service; • [⋮]	
		Note: NIST SP 800-53 parallels the CC v2 approach, which distinguished administrator and user documentation (AGD_USR, AGD_ADM). CC v3 combined these into a single SAR, reflecting the situation that some products do not have non-administrative users.		
AGD_PRE.1	**Preparative Procedures** Preparative Procedures • Developer provides the product including its preparative procedures. • Preparative procedures: 1. Describe all the steps necessary for secure acceptance of the delivered product in accordance with the developer's delivery procedures. 2. Describe all the steps necessary for secure installation of the product and for the secure preparation of the operational environment in accordance with the security objectives for the operational environment as described in the ST. • Evaluator confirms that the	SA-5	**Information System Documentation ‡** Organization… • Obtains administrator documentation for the information system, system component, or information system service that describes: 1. Secure configuration, installation, and operation of the system, component, or service; 2. [⋮] • [⋮]	AGD_PRE.1 calls for describing all the steps necessary for secure acceptance and secure delivery. The control calls for documentation or secure configuration and installation.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	information provided meets all requirements for content and presentation of evidence. • Evaluator applies the preparative procedures to confirm that the product can be prepared securely for operation.			
ALC_CMC.1	**CM Capabilities** Labeling of the TOE • Developer provides the product and a reference for the product. • The product is labelled with its unique reference. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence.	CM-9	**Configuration Management Plan ‡** Organization develops, documents, and implements a configuration management plan for the information system that… • […] • Establishes a process for identifying configuration items throughout the system development life cycle and for managing the configuration of the configuration items; • […]	At the product level, identification of the configuration items would include identification of the product with a unique reference.
ALC_CMS.1	**CM Scope** TOE CM Coverage • Developer provides a configuration list for the TOE. • Configuration list includes the following: the TOE itself; and the evaluation evidence required by the SARs. • Configuration list uniquely identifies the configuration items. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence.	CM-3(6)*	**Configuration Change Control** | Cryptography Management • Organization ensures that cryptographic mechanisms used to provide [*security safeguards*] are under configuration management.	At the product level, if the cryptographic mechanisms providing the safeguards are part of the TOE, they would be covered by CM.
		CM-9	**Configuration Management Plan ‡** Organization develops, documents, and implements a configuration management plan for the information system that… • […] • Defines the configuration items for the information system and places the configuration items under configuration management;. • […]	This addresses defining the configuration items and the CM system. Note that ALC_CMC focuses on the *product*, whereas CM-9 focuses on the *system*.
		SA-10	**Developer Configuration Management ‡** Organization requires the developer of the information system, system component, or information system service to: • […] • Document, manage, and control the integrity of changes to [*configuration*	ALC_CMS captures the "[*configuration items under configuration management*]"

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			items under configuration management]; • [⋮]	
		Note: This is a *developer* process – a missing area in SA. Installation of remediated flaws is SI-2.		
ALC_TSU_EXT.1	**Life Cycle** Timely Security Updates • Developer provides a description in the TSS of how timely security updates are made to the TOE. Application developers must support updates to their products for purposes of fixing security vulnerabilities. • Developer provides a description in the TSS of how users are notified when updates change security properties or the configuration of the product. • Developer includes the process for creating and deploying security updates for the TOE software. • Developer expresses the time window as the length of time, in days, between public disclosure of a vulnerability and the public availability of security updates to the TOE. • Developer includes the mechanisms publicly available for reporting security issues pertaining to the TOE. The reporting mechanism could include web sites, email addresses, as well as a means to protect the sensitive nature of the report (e.g., public keys that could be used to encrypt the details of a proof-of-concept exploit). • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence.	SA-10	**Developer Configuration Management ‡** Organization requires the developer of the information system, system component, or information system service to: • [⋮] • Track security flaws and flaw resolution within the system, component, or service and report findings to [*personnel*].	Part of providing security updates is the implication that flaws are being tracked and updated. The SAR supports tracking of flaws and flaw resolution.
		SA-11	**Developer Security Testing and Evaluation ‡** Organization requires the developer of the information system, system component, or information system service to: • [⋮] • Implement a verifiable flaw remediation process; • Correct flaws identified during security testing/evaluation.	Part of providing security updates is the implication that flaws are being tracked and updated. The SAR supports tracking of flaws and flaw resolution.
		SI-2	**Flaw Remediation** Organization… • Identifies, reports, and corrects information system flaws; • Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; • Installs security-relevant software and firmware updates within [*time period*] of the release of the updates; • Incorporates flaw remediation into the organizational configuration management process.	Although the SAR focuses more on the release of the updates, having the updates released supports SI-2.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
ATE_IND.1	**Independent Testing** Independent Testing – Conformance • Developer provides the product for testing. • The product shall be suitable for testing. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. • Evaluator tests a subset of the TSF to confirm that the TSF operates as specified.	CA-2	**Security Assessments** Organization… • Develops a security assessment plan that describes the scope of the assessment including: (1) Security controls and control enhancements under assessment; (2) Assessment procedures to be used to determine security control effectiveness; and (3) Assessment environment, assessment team, and assessment roles and responsibilities; • Assesses the security controls in the information system and its environment of operation [*frequency*] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security requirements; • Produces a security assessment report that documents the results of the assessment • Provides the results of the security control assessment to [*individuals or roles*].	Independent testing *at the product level* supports testing of the overall system. As such, the *product-level* test plan can support the system-level test plans in terms of eliminating test redundancy, and the results of testing can feed into the system results.
		CA-2(1)	**Security Assessments** | Independent Assessors • Organization employs assessors or assessment teams with [*level of independence*] to conduct security control assessments.	Assessment teams for ATE_IND are drawn from NIAP-approved CCTLs that are independent from the developer. However, the CCTLs may not meet the *level of independence* dictated by the SCA.
AVA_VAN.1	**Vulnerability Analysis** Vulnerability Survey • Developer provides the product for testing. • The product is suitable for testing. • Evaluator confirms that the information provided meets all requirements for content and presentation of evidence. • Evaluator performs a search of	CA-2(2)	**Security Assessments** | Specialized Assessments • Organization includes as part of security control assessments, [*frequency*], [*announced; unannounced*], [*(one or more): in-depth monitoring; vulnerability scanning; malicious user testing; insider threat assessment; performance/load testing;*	If the assignment in CA-2(2) is completed to include a public domain search and subsequent testing of any potential vulnerabilities identified, then AVA_VAN.1 addresses CA-2(2) *at the product level*. **Note:** Vulnerability testing at the product level does not ensure the product integrated

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	public domain sources to identify potential vulnerabilities in the product. • Evaluator conducts penetration testing, based on the identified potential vulnerabilities, to determine that the product is resistant to attacks performed by an attacker possessing Basic attack potential.		*[other forms of security assessment]*].	into the complete system is configured correctly, nor does it ensure there are no other integration flaws.
		CA-8	**Penetration Testing** • Organization conducts penetration testing [*frequency*] on [*information systems or system components*].	AVA_VAN.1.3E supports CA-8 with respect to testing on the product.
		SA-11(2)	**Developer Security Testing and Evaluation** | Threat and Vulnerability Analyses • Organization requires the developer of the information system, system component, or information system service to perform threat and vulnerability analyses and subsequent testing/evaluation of the as-built system, component, or service.	AVA_VAN requires that there be a vulnerability analysis performed.
		Note:* RA-3 and SA-11(5) were included in the mapping published in NIST SP 800-53 Revision 4. Upon further reflection, the mappings to RA-3 and SA-11(5) are erroneous. RA-3 is risk assessment, including the likelihood and magnitude of harm, from attacks. It is not the determination of vulnerabilities. Risk assessment can only be done in the context of a particular mission and installation. As for SA-11(5), under the Common Criteria, it is the *evaluator*, not the *developer*, that performs vulnerability assessment.		

Optional Requirements

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FCS_TLSC_EXT.1	Cryptographic Support (FCS) TLS Client Protocol • [1.4] Application supports mutual authentication using X.509v3 certificates.	IA-2	**Identification and Authentication (Organizational Users)** • Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	Mutual authentication using certificates (PKI authentication) authentication supports IA-2 and IA-8

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
		IA-8	**Identification and Authentication (Non-Organizational Users)** • Information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	Mutual authentication using certificates (PKI authentication) authentication supports IA-2 and IA-8
		SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Whether this control is satisfied depends on the implementation method for meeting the SFR. At the SFR level, this can be addressed either through refinement of the SFR, or through appropriate specifications in the TSS that would indicated FDP_ITT is implemented through FCS operations.
		SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches fo r TLS.
		SC-23 †	**Session Authenticity** • Information system protects the authenticity of communications sessions.	TLS is used for communication sessions.

Selection-Based Requirements

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FCS_RBG_EXT.2	**Cryptographic Support (FCS)** Random Bit Generation from Application • Application performs all deterministic random big generation in accordance with [NIST SP 800-90A algorithms, FIPS 140-2 Annex C algorithms] • Application seeds the algorithm by an entropy source that …	**Note**: Unclear. This might fit within SC-12 and key generation, but it could also be below the level of any existing NIST control.		
FCS_RBG_EXT.2	**Cryptographic Support (FCS)** Cryptographic Key Generation Services • Application [generates no asymmetric cryptographic keys, invokes platform-provided functionality for asymmetric key generation, implements asymmetric key generation] .	**No Correspondence.** If the product does not generate asymmetric cryptographic keys, then no controls are supported. If the asymmetric keys are generated by the platform, then it is the platform that supports the controls (SC-12, SC-12(1)), not the application. If the application implements asymmetric key generation, the support is addressed with the SFRs implementing the key generation.		
FCS_CKM.1	**Cryptographic Support (FCS)** Cryptographic Key Generation • Application generates asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm [[RSA schemes] using cryptographic key sizes of [2048-bit or greater] that meet the following: [FIPS PUB 186-4, ANSI X9.31-1998, Section 4.1], [ECC schemes] using [“NIST curves” P-256, P-384 and [selection: P-521 , no other curves]] that meet the following: [FIPS PUB 186-4], [FFC schemes] using cryptographic key sizes of [2048-bit or greater] that meet the following: [FIPS PUB 186-4]] .	SC-12†	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Assignment must be completed congruent with the SFR completion, and the completed control must agree with the completed control in the System Security Plan for the system under analysis.
		SC-12(3)†	**Cryptographic Key Establishment and Management** | Asymmetric Keys Organization produces, controls, and distributes asymmetric cryptographic keys using [NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user’s private key].	FCS_CKM.1(1) calls for asymmetric key in accordance with the NIST process; as NSA developed the PP, it is by implication an NSA-approved technology and process.
FCS_CKM.2	**Cryptographic Support (FCS)** Cryptographic Key Establishment	**Note:** If the control is completed to invoke platform functionality, it is actually the platform that supports the following controls with respect to key establishment (usage is a different story, but usage of cryptography is addressed by other SFRs).		

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	• Application [invokes platform-provided functionality , implement functionality] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [RSA-based key establishment schemes] that meets the following: [NIST Special Publication 800-56B, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography"] and [[Elliptic curve-based key establishment schemes] that meets the following: [NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"] , [Finite field-based key establishment schemes] that meets the following: [NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"] , No other schemes].	SC-12†	**Cryptographic Key Establishment and Management** • Organization establishes and manages cryptographic keys for required cryptography employed within the information system in accordance with [*requirements for key generation, distribution, storage, access, and destruction*].	Assignment must be completed congruent with the SFR completion, and the completed control must agree with the completed control in the System Security Plan for the system under analysis.
		SC-12(3)†	**Cryptographic Key Establishment and Management** | Asymmetric Keys Organization produces, controls, and distributes asymmetric cryptographic keys using [NSA-approved key management technology and processes; approved PKI Class 3 certificates or prepositioned keying material; approved PKI Class 3 or Class 4 certificates and hardware security tokens that protect the user's private key].	FCS_CKM.1(1) calls for asymmetric key in accordance with the NIST process; as NSA developed the PP, it is by implication an NSA-approved technology and process.
FCS_COP.1(1)	**Cryptographic Support (FCS)** Cryptographic Operation - Encryption/Decryption • Application performs encryption/decryption in accordance with a specified cryptographic algorithm AES-CBC (as defined in NIST SP 800-38A) mode; and [AES-GCM (as defined in NIST SP 800-38D), no other modes] and cryptographic key sizes 128-bit key sizes and [256-bit key sizes, no other key sizes] .	SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
		Note: FCS_COP.1(1) may also be viewed as supporting SC-8 and SC-8(1), or SC-28, depending upon the purposes for which the encryption is used.		
FCS_COP.1(2)	**Cryptographic Support (FCS)** Cryptographic Operation - Hashing • Application performs [***cryptographic hashing***] in accordance with SHA-1 and [SHA-256, SHA-384, SHA-512, no other algorithms] and message digest sizes 160 and [256, 384, 512, no other message digest sizes] bits that meet the following: FIPS Pub 180-4.	SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
FCS_COP.1(3)	**Cryptographic Support (FCS)** Cryptographic Operation - Signing • Application performs cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm [RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 4, ECDSA schemes using "NIST curves" P-256, P-384 and [P-521, no other curves] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5] .	SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
		Note: FCS_COP.1(2) may also be viewed as supporting AU-10, but that support really depends upon the purpose for which the digital signatures are used. Provision of a digital signature service does not *apriori* give non-repudiation.		
FCS_COP.1(4)	**Cryptographic Support (FCS)** Cryptographic Operation - Keyed-Hash Message Authentication • Application performs keyed-hash message authentication in accordance with a specified cryptographic algorithm HMAC-SHA-256 and [SHA-1, SHA-384, SHA-512, no other algorithms] with key sizes [*key size (in bits) used in HMAC*] and message digest sizes 256 and [160, 384, 512, no other size] bits that meet the following: FIPS Pub 198-1 The Keyed-Hash Message Authentication Code and FIPS Pub 180-4 Secure Hash Standard.	SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	The assignment in the SFR must be completed to include all the cryptographic operations, algorithms, key sizes, and standards specified in the iterations of the FCS_COP.1 SFR.
FCS_TLSC_EXT.1	**Cryptographic Support (FCS)** TLS Client Protocol • [1.1] Application [invokes platform-provided TLS 1.2, implements TLS 1.2 (RFC 5246)] supporting the following ciphersuites: Mandatory Ciphersuites: TLS_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246 Optional Ciphersuites: [TLS_RSA_WITH_AES_256_CBC_SHA as defined in RFC 5246, TLS_DHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 5246, TLS_DHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC	IA-2	**Identification and Authentication (Organizational Users)** • Information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	Mutual authentication using certificates (PKI authentication) authentication supports IA-2 and IA-8
		IA-8	**Identification and Authentication (Non-Organizational Users)** • Information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	Mutual authentication using certificates (PKI authentication) authentication supports IA-2 and IA-8

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	5246, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA as defined in RFC 4492, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA as defined in RFC 4492, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA as defined in RFC 4492, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA as defined in RFC 4492, TLS_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5246, TLS_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246, TLS_DHE_RSA_WITH_AES_128_CBC_ SHA256 as defined in RFC 5246, TLS_DHE_RSA_WITH_AES_256_CBC_ SHA256 as defined in RFC 5246, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289, no other ciphersuite] . • [1.2] Application verifies that the presented identifier matches the reference identifier according to RFC 6125. • [1.3] Application only establishes a trusted channel if the peer certificate is valid. • [1.5] Application presents the supported Elliptic Curves Extension in the Client Hello with the following NIST curves: [secp256r1, secp384r1, secp521r1] and no other curves.	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Whether this control is satisfied depends on the implementation method for meeting the SFR. At the SFR level, this can be addressed either through refinement of the SFR, or through appropriate specifications in the TSS that would indicated FDP_ITT is implemented through FCS operations.
		SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches fo r TLS.
		SC-23 †	**Session Authenticity** • Information system protects the authenticity of communications sessions.	TLS is used for communication sessions.
FCS_DTLS_EXT.1	**Cryptographic Support (FCS)** DTLS Implementation • Application implements the DTLS protocol in accordance with DTLS 1.2 (RFC 6347). • Application implements the	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
	requirements in TLS (FCS_TLSC_EXT.1) for the DTLS implementation, except where variations are allowed according to DTLS 1.2 (RFC 6347). • Application does not establish a trusted communication channel if the peer certificate is deemed invalid.	SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Whether this control is satisfied depends on the implementation method for meeting the SFR. At the SFR level, this can be addressed either through refinement of the SFR, or through appropriate specifications in the TSS that would indicated FDP_ITT is implemented through FCS operations.
		SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches fo r DTLS.
		SC-23 †	**Session Authenticity** • Information system protects the authenticity of communications sessions.	DTLS is used for communication sessions.
FCS_HTTPS_EXT.1	**Cryptographic Support (FCS)** HTTPS Protocol • Application implements the HTTPS protocol that complies with RFC 2818. • Application implements HTTPS using TLS (FCS_TLSC_EXT.1). • Application notifies the user and [not establish the connection , request application authorization to establish the connection , no other action] if the peer certificate is deemed invalid.	SC-8	**Transmission Confidentiality and Integrity** • Information system protects the [*(one or more): confidentiality; integrity*] of transmitted information.	The assignment in SC-8 should be completed to correspond with the requirement for protection from disclosure / modification in the SFR.
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	Whether this control is satisfied depends on the implementation method for meeting the SFR. At the SFR level, this can be addressed either through refinement of the SFR, or through appropriate specifications in the TSS that would indicated FDP_ITT is implemented through FCS operations.
		SC-13 †	**Cryptographic Protection** • Information system implements [*cryptographic uses and type of cryptography required for each use*] in accordance with applicable federal laws … and standards.	This would specific the specific encryption approaches fo r HTTPS.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
		SC-23 †	**Session Authenticity** • Information system protects the authenticity of communications sessions.	HTTPS is used for communication sessions.
FIA_X509_EXT.1	**Identification and Authentication (FIA)** X.509 Certificate Validation • Application validates certificates in accordance with the following rules… • Application only treats a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.	IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; • Enforces authorized access to the corresponding private key; • Maps the authenticated identity to the account of the individual or group; • Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	Addresses the certificate validation portion of IA-5(2).**Note that this does not address all of IA-5(2).**
FIA_X509_EXT.2	**Identification and Authentication (FIA)** X.509 Certificate Authentication • Application uses X.509v3 certificates as defined by RFC 5280 to support authentication for [HTTPS , TLS , DTLS]. • When the application cannot establish a connection to determine the validity of a certificate, application [allows the administrator to choose whether to accept the certificate in these cases , accepts the certificate , does not accept the certificate] .	CM-5(3)	**Access Restrictions for Change** | Signed Components • Information system prevents the installation of [*software and firmware components*] without verification that the component has been digitally signed using a certificate that is recognized and approved by the organization.	This SFR supports the use of digital certificates for code signing.
		IA-5(2)	**Authenticator Management** | PKI-Based Authentication Information system, for PKI-based authentication… • Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information; • Enforces authorized access to the corresponding private key;	This SFR supports the use of digital certificates for authentication.

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects		Comments and Observations
			• Maps the authenticated identity to the account of the individual or group; • Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information via the network.	
		SC-8(1) †	**Transmission Confidentiality and Integrity** | Cryptographic or Alternate Physical Protection • Information system implements cryptographic mechanisms to [*prevent unauthorized disclosure of information; detect changes to information*] during transmission unless otherwise protected by [*alternative physical safeguards*].	This SFR supports SC-8(1), as the protocols cited require certificate validation and provide transmission security.

Objective Requirements

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects	Comments and Observations
FCS_TLSC_EXT.1	**Cryptographic Support (FCS)** TLS Client Protocol • [1.6] Application present the signature_algorithms extension in the Client Hello with the supported_signature_algorithms value containing the following hash algorithms: [selection: SHA256, SHA384, SHA512] and no other hash algorithms.	**Note:** This additional element does not change the basic controls supported by the SFR.	
FPT_API_EXT.1	**Protection of the TSF (FPT)** Use of Supported Services and APIs • [1.2] Application [uses platform-provided libraries, does not implement functionality] for parsing [assignment: list of formats parsed that are included	**No Correspondence**. There are no controls dealing with what interfaces applications use. Such a requirement is too low-level for NIST SP 800-53.	

Common Criteria Version 3.x SFR/SAR		NIST SP 800-53 Revision 4 Control † indicates mapping depends on SFR selections, assignments, or implementation * Indicates control does not directly implement control, but supports implementation of the control ‡ indicates control text has been condensed to relevant aspects	Comments and Observations
	in the IANA MIME media types]		
FPT_IDV_EXT.1	**Protection of the TSF (FPT)** Software Identification and Versions • Application includes SWID tags that comply with the minimum requirements for SWID tag from ISO/IEC 19770-2:2009 standard.	**No Correspondence**. NIST SP 800-53 has no controls related to the specific mechanism used for software identification.	