Mapping Between

PP for Peripheral Sharing Device, Version 4.0, 19-July-2019

and

NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System**. The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 2, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context.** Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.
- **AC-4.** The primary purpose of a peripheral sharing device is to enforce logical separation between information flows in support of AC-4 generally, and AC-4(21) and AC-4(22) in particular. Any other security controls a peripheral sharing device helps to satisfy is in support of that over-arching purpose (i.e. the security requirements are intended to ensure that enforcement of AC-4 and relevant sub-controls cannot be subverted).
- **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.
- **Limited device functionality.** Peripheral sharing devices are typically isolated from other systems aside from those they are directly connected to. As a result, they generally do not have sophisticated auditing, I&A, or management functionality. For example, a peripheral sharing device's audit mechanism may only have a limited set of records that may only be retrieved on demand; such a device may not meet organizational requirements for automatic logging to a centralized repository. Similarly, a peripheral sharing device's I&A mechanism may be limited to local password-based authentication of a limited number of pre-defined user identities; there should not be an expectation that an organizational user's role and identity are carried over to such a device because a network interface from it to a third-party authentication server may not exist.
- **System context of supported controls.** For a conformant TOE to support these controls in the context of an information system, the selections and assignments completed in the TOE's Security Target must be congruent with those made for the supported controls. For example, the TOE's ability to generate audit records only supports AU-2 to the extent that the TOE's audit records are included in the set of "organization-defined auditable events" assigned by that control. The security control assessor must compare the TOE's functional claims to the behavior required for the system to determine the extent to which the applicable controls are supported.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
TOE Security Functional Requirements				
FDP_APC_EXT.1	**Active PSD Connections**	AC-4(21)	**Information Flow Enforcement:** Physical or Logical Separation of Information Flows	A conformant TOE supports this control by ensuring that communications through the TOE between a connected computer and all connected peripherals are routed only to the interfaces selected by the user.
FDP_PDC_EXT.1	**Peripheral Device Connection**	AC-4	**Information Flow Enforcement**	A conformant TOE supports this control by ensuring that only a well-defined set of authorized peripherals can transfer information to/from computers that are connected to the TOE.
FDP_RIP_EXT.1	**Residual Information Protection**	SC-4	**Information in Shared System Resources**	A conformant TOE does not maintain residual user data so that there is no risk of unintended disclosure or transmission of this data outside of its intended destination.
FDP_SWI_EXT.1	**PSD Switching**	AC-4(21)	**Information Flow Enforcement:** Physical or Logical Separation of Information Flows	A conformant TOE supports this control by ensuring that communications through the TOE between a connected computer and all connected peripherals are routed only to the interfaces selected by the user.
FPT_FLS_EXT.1	**Failure with Preservation of Secure State**	SC-24	**Fail in Known State**	A conformant TOE supports this control by failing into a known state when defined failures occur.
FPT_NTA_EXT.1	**No Access to TOE**	AC-3	**Access Enforcement**	A conformant TOE enforces access controls that prevent unauthorized access to system functions and data.
FPT_PHP.1	**Passive Detection of Physical Attack**	PE-3(5)	**Physical Access Control:** Tamper Protection	A conformant TOE supports this control by implementing a mechanism to create evidence of physical tampering.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FPT_TST.1	**TSF Testing**	SI-6	**Security and Privacy Function Verification**	A conformant TOE supports part (a) of this control by implementing a self-test mechanism to ensure the correct behavior of certain TOE functions.
FPT_TST_EXT.1	**TSF Testing**	SI-6	**Security and Privacy Function Verification**	A conformant TOE supports part (c) of this control by implementing a notification mechanism in the event of a failed self-test.
Optional Requirements				
FAU_GEN.1	**Audit Data Generation**	AU-2	**Event Logging**	A conformant TOE supports this control to the extent that it has the ability to generate log records. However, it may not fully address the control since the control expects organizational coordination of logging functions and the TOE may not have an external interface that supports this.
		AU-3	**Content of Audit Records**	A conformant TOE supports this control by enumerating the events for which it generates audit records and the information that these records contain.
		AU-12	**Audit Record Generation**	A conformant TOE supports this control by implementing an audit generation function.
FIA_UAU.2	**User Authentication Before Any Action**	AC-14	**Permitted Actions without Identification or Authentication**	A conformant TOE supports this control by preventing the execution of management functions prior to user authentication.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE supports this control by providing a mechanism to authenticate users to its own management interface. Note that a conformant

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				TOE likely implements only a rudimentary authentication function because it is isolated from other organizational systems and therefore will likely not enforce sub-controls. Also note that while the TOE is accessed by organizational users, the TOE's authentication mechanism is likely exclusive to the TOE and is therefore not tied back to any centrally maintained user identity.
FIA_UID.2	**User Identification Before Any Action**	AC-14	**Permitted Actions without Identification or Authentication**	A conformant TOE supports this control by preventing the execution of management functions prior to user authentication.
		IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE supports this control by providing a mechanism to authenticate users to its own management interface. Note that a conformant TOE likely implements only a rudimentary authentication function because it is isolated from other organizational systems and therefore will likely not enforce sub-controls. Also note that while the TOE is accessed by organizational users, the TOE's authentication mechanism is likely exclusive to the TOE and is therefore not tied back to any centrally maintained user identity.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FMT_MOF.1	**Management of Security Functions Behavior**	AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE supports this control by ensuring that the TOE's management functions are only accessible to members of authorized roles. Note that the TOE may only have a rudimentary management interface that only has one or two pre-defined roles, so there is likely no connection between TOE management accounts and role assignments to organizational users.
FMT_SMF.1	**Specification of Management Functions**	N/A	**N/A**	While this SFR is typically associated with CM-6, a peripheral sharing device only has a rudimentary management interface with minimal configuration options that do not rise to the level of relevance to an organizational configuration policy. To the extent that the TOE's management functionality supports any security controls, conformance to the KM or UA module and a claim of configurable device filtration for either of those peripheral types could support AC-4.
FMT_SMR.1	**Security Roles**	AC-2(7)	**Account Management:** Role-based Schemes	A conformant TOE supports this control by defining a role-based mechanism to control access to management functions.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE supports this control by ensuring that the TOE's management functions are only accessible to members of authorized roles. Note that the TOE may only have a

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				rudimentary management interface that only has one or two pre-defined roles, so there is likely no connection between TOE management accounts and role assignments to organizational users.
FPT_STM.1	**Reliable Time Stamps**	AU-8	**Time Stamps**	A conformant TOE supports this control by implementing a reliable system clock. Note that due to the rudimentary nature of the TOE it is not likely that its time function is synchronized to an authoritative organizational source.
FDP_RIP_EXT.2	**Purge of Residual Information**	CP-10	**System Recovery and Reconstitution**	A conformant TOE supports this control because claiming this SFR asserts that the TOE has a factory reset function, which allows the TOE to be restored to a known state from some set of unknown or failure states. Note however that certain failure states may not be recoverable by an administrator, such as a triggering of the TOE's tamper response mechanism when FPT_PHP.3 is claimed.
		SC-4	**Information in Shared System Resources**	A conformant TOE supports this control by implementing a factory reset function that purges system and user data and prevents its unintentional disclosure.
FPT_PHP.3	**Resistance to Physical Attack**	PE-3(5)	**Physical Access Control:** Tamper Protection	A conformant TOE supports this control by implementing a mechanism to respond to detected physical tampering.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
Selection-Based Requirements				
FDP_SWI_EXT.2	**PSD Switching Methods**	SC-2	**Separation of System and User Functionality**	A conformant TOE supports this control by ensuring that peripheral user devices cannot be used to perform the system function of switching channel selection unless a guard is implemented.
		AC-4(21)	**Information Flow Enforcement:** Physical or Logical Separation of Information Flows	A conformant TOE supports this control by enforcing the behavior that connected peripherals will only interact with a connected computer through express user action.
FTA_CIN_EXT.1	**Continuous Indications**	AC-4(21)	**Information Flow Enforcement:** Physical Separation of Information Flows	A conformant TOE supports this control by providing an indication of system activity. Note that the indication itself does not relate to the control being enforced; it only relates to the control to the extent that it makes the user aware of the current behavior of the TOE's information flow enforcement function.
Objective Requirements				
This PP has no objective requirements.				