Mapping Between

PP-Module for User Authentication Devices, Version 1.0, 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_FIL_EXT.1/UA	**Device Filtering (User Authentication Devices)**	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_PDC_EXT.2/UA	**Authorized Devices (User Authentication Devices)**	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_PDC_EXT.4	**Supported Authentication Device**	N/A	**N/A**	This SFR specifies whether the TOE has its own internal authentication device or if it has a peripheral USB port that allows a third-party device to be connected to it. It exists as its own SFR only to determine whether FDP_TER_EXT.2 must be claimed by the TOE and therefore does not satisfy any controls on its own.
FDP_PWR_EXT.1	**Powered By Computer**	N/A	**N/A**	A conformant TOE ensures that it is only powered through its own dedicated power interface and cannot be powered by a USB connection to a powered computer. There is no applicable control that this behavior supports.
FDP_TER_EXT.1	**Session Termination**	AC-12	**Session Termination**	A conformant TOE supports this control by enforcing termination of an active user session when the element used to authenticate the session has been removed from the TOE.
FDP_UAI_EXT.1	**User Authentication Isolation**	AC-4(21)	**Information Flow Enforcement:** Physical or Logical Separation of Information Flows	A conformant TOE supports this control by isolating information flows related to user authentication from

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				other data flows within the TOE boundary.
Optional Requirements				
This PP-Module has no objective requirements.				
Selection-Based Requirements				
FDP_TER_EXT.2	**Session Termination of Removed Devices**	AC-12	**Session Termination**	A conformant TOE supports this control by enforcing termination of an active user session when the device used to facilitate the authentication of the session is disconnected from the TOE.
FDP_TER_EXT.3	**Session Termination upon Switching**	AC-12	**Session Termination**	A conformant TOE supports this control by enforcing termination of an active user session when the TOE is switched off of the computer where the session is active.
Objective Requirements				
This PP-Module has no objective requirements.				