Mapping Between

PP-Module for Host Agent, Version 1.0, 2020-10-23

and

NIST SP 800-53 Revision 5

Important Caveats

- **Product vs. System**. The Common Criteria is designed for the evaluation of products; the Risk Management Framework (NIST SP 800-37 Revision 2, DOD 8510.01) and associated control/control interpretations (NIST SP 800-53 Revision 5, CNSSI № 1253) are used for the assessment and authorization of mission systems. **Products cannot satisfy controls outside of the system context.** Products may support a system satisfying particular controls, but typically satisfaction also requires the implementation of operational procedures; further, given that systems are typically the product of integration of multiple products configured to meet mission requirements, an overall system assessment is required to determine if the control is satisfied in the overall system context.
- **SA-4(7).** Perhaps it is needless to say, but satisfaction of any NIAP PP or PP-Configuration supports system satisfaction of SA-4(7), which is the implementation of CNSSP № 11.
- **Limited device functionality.** A Host Agent is a generic type of application that is capable of collecting configuration and behavioral information about the system it runs on, reporting that back to a central server, and potentially applying some configuration back to the system it runs on to control some aspect of that system's behavior. Specific security functionality is dependent on the purpose of the Host Agent, which is dependent on other PP-Modules that the TOE claims conformance to. The Host Agent as an abstract entity is not deployed to address a particular security control; it has security functionality that supports certain controls being enforced, but its primary purpose depends on the specific type of Host Agent that it is.
- **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				
FAU_GEN.1/HA	**Audit Data Generation**	AU-2	**Event Logging**	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

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				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 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.
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	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.
		AU-12	**Audit Record Generation**	A conformant TOE has 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-Module does not define functionality to suppress or enable the generation of specific audit records (which would

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				typically be expressed in CC as FAU_SEL.1).
FAU_STO_EXT.1	**Audit Data Storage**	AU-9	**Protection of Audit Information**	A conformant TOE shall store audit events using the platform-provided mechanism.
FDP_NET_EXT.2	**Network Communications**	AC-3	**Access Enforcement**	A conformant TOE automatically limits its network activities to the specific resources for which it is authorized.
FHA_HAD_EXT.1	**Host Agent Declaration**	N/A	**N/A**	This requirement defines the 'type' of product the TOE is with regards to other functionality. Any relevant security controls are supported by the other SFRs that are included in the TOE boundary based on claims made here.
FMT_SMF.1/HA	**Specification of Management Functions (Configuration of Host Agent)**	CM-6	**Configuration Settings**	A conformant TOE may satisfy the 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.
FMT_UNR_EXT.1	**User Unenrollment Prevention**	AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE shall permit authorized users to unenroll the Host Agent with the ESM system and prevent unprivileged users of the platform from unenrolling the Host Agent with the ESM system.
		AC-6(10)	**Least Privilege:** Prohibit Non-Privileged Users from Executing Privileged Functions	A conformant TOE shall prevent unprivileged users of the platform from unenrolling the Host Agent with the ESM system.
Optional Requirements				
This PP-Module has no optional requirements.				
Selection-Based Requirements				

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
FHA_CHA_EXT.1	**Cache Host Agent Collected Data**	AU-5(5)	**Response to Audit Logging Process Failures**: Alternate Audit Logging Capabilities	A conformant TOE shall cache and manage collected data for a period of more than 72 hours on either persistent or non-persistent storage if the trusted channel is not available.
FHA_COL_EXT.1	**Collected Audit**	AU-2	**Event Logging**	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(1)	**Content of Audit Records:** Additional Audit Information	A conformant TOE shall be capable of collecting endpoint data.
FTP_DIT_EXT.2	**Protection of Data in Transit for Peer-to-Peer Host Agents**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports the ability to ensure the confidentiality and integrity of information transmitted between the TOE and another Host Agent.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE protects data in transit between peer components using a cryptographic channel.
Objective Requirements				
FMT_POL_EXT.1	**Trusted Policy Update**	AU-10	**Non-Repudiation**	A conformant Host Agent or Host Agent Platform will only accept policies or commands that are digitally signed as verification as being sent by the ESM Server.
		SC-13	**Cryptographic Protection**	A conformant TOE relies on digital signatures to validate the authenticity and integrity of policy data sent to it. Note that this function may be implemented by the TOE itself, or the TOE may rely

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
				on its underlying platform to implement it.
		SI-7	**Software, Firmware, and Information Integrity**	A conformant TOE relies on digital signatures to validate the integrity of data sent to it. Note that this function may be implemented by the TOE itself, or the TOE may rely on its underlying platform to implement it.