Mapping Between collaborative PP-Module for Biometric enrolment and verification – for unlocking the device - [BIOPP-Module], Version 1.1, 12-September-2022 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.
- **Granularity of SFRs vs controls.** It is important to remember that the Security Functional Requirements (SFRs) and the Security and Privacy Controls (Controls) are at completely different levels of abstractions. SFRs can be very low level, specifying internal characteristics and behaviors of given functions. Even when broader, SFRs are restricted to a specific product. Controls, on the other hand, are very high level, specifying both technical behavior and processes for the system writ large, broadly across the large number of devices, components and products that make up the system and achieve the overall mission. A low-level SFR may contribute in some small way towards the satisfaction of a control, but it rarely satisfies the control in isolation and should not be interpreted as doing so. More often, the combination of SFRs that define the security functionality of a product may serve to support just a single control, and looking at the finer level of detail may not be as useful, such as the low-level details of protocol implementations. When looking at these mappings, it is important to remember the differences in levels of abstraction; in particular, it is important not to read more into an SFR to Control mapping than a contribution of some level of support.
- **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.
- **IA-2 and IA-5.** The primary purpose of this PP-Module is to define requirements that relate to the use of biometric data as an authenticator. Therefore, a TOE that conforms to this PP-Module is expected to satisfy IA-5 controls related to the generation, use, and secure storage of biometric authenticators. This data is used as a way to identify and authenticate the user to whom the data belongs, which supports IA-2 at a high level as

well. Specific additional controls may be satisfied by individual SFRs.

- **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.
- **PP-Module vs Base-PP.** This is a PP-Module, which extends a Protection Profile (Base-PP) by defines new security functionality for it. A TOE that conforms to this PP-Module must also conform to the Base-PP as well. The security control mapping for the Base-PP must also be considered to determine the extent to which a conformant TOE supports the implementation of organizational security controls.

Common Criteria Version 3.x SFR		NIST SP 800-53 Revision 5 Control		Comments and Observations
Mandatory Requirements (presented alphabetically)				
FIA_MBE_EXT.1	**Biometric enrolment**	IA-2(1)	**Identification and Authentication (Organizational Users):** Multi-Factor Authentication to Privileged Accounts	A conformant TOE provides a mechanism for registering a biometric authentication factor by using a non-biometric authentication factor.
		IA-2(2)	**Identification and Authentication (Organizational Users):** Multi-Factor Authentication to Non-Privileged Accounts	A conformant TOE provides a mechanism for registering a biometric authentication factor by using a non-biometric authentication factor.
		IA-5	**Authenticator Management**	A conformant TOE provides a mechanism to verify the identity of the individual enrolling in the biometric system as specified in part (a) of the control.
FIA_MBE_EXT.2	**Quality of biometric templates for biometric enrolment**	IA-5(12)	**Authenticator Management:** Biometric Authentication Performance	A conformant TOE supports this control by enforcing a quality standard for biometric samples.
FIA_MBV_EXT.1	**Biometric verification**	IA-2	**Identification and Authentication (Organizational Users)**	A conformant TOE provides a biometric verification mechanism to process an individual's biometric sample.
		IA-5(12)	**Authenticator Management:** Biometric Authentication Performance	A conformant TOE provides a biometric verification mechanism that does not exceed the FMR, FAR, FNMR, and FRR established confidence levels.
FIA_MBV_EXT.2	**Quality of biometric samples for biometric verification**	IA-5(12)	**Authenticator Management:** Biometric Authentication Performance	A conformant TOE uses only biometric samples measured against a quality metric standard.
FPT_BDP_EXT.1	**Biometric data processing**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE transmits plaintext biometric data between the capture sensor and the SEE isolated from the main computer operating system on the TSF in

				runtime.
		SC-39(1)	**Process Isolation:** Hardware Separation	A conformant TOE supports this control by ensuring that biometric data is processed in a physically separate execution environment.
FPT_PBT_EXT.1	**Protection of biometric template**	IA-5	**Authenticator Management**	A conformant TOE supports part (g) of this control by ensuring that the biometric authentication template is protected from unauthorized access.
		IA-5(6)	**Authenticator Management:** Protection of Authenticators	A conformant TOE supports this control by implementing additional protection mechanisms for the biometric authentication template.
Optional Requirements (presented alphabetically)				
FIA_MBE_EXT.3	**Presentation attack detection for biometric enrolment**	IA-5(17)	**Authenticator Management:** Presentation Attack Detection for Biometric Authenticators	A conformant TOE supports this control by implementing a mechanism to detect presentation attack attempts.
FIA_MBV_EXT.3	**Presentation attack detection for biometric verification**	IA-5(17)	**Authenticator Management:** Presentation Attack Detection for Biometric Authenticators	A conformant TOE supports this control by implementing a quantifiably strong presentation attack detection mechanism.
Objective Requirements (presented alphabetically)				
This PP-Module has no objective requirements.				
Implementation-based Requirements (presented alphabetically)				
This PP-Module has no implementation-based requirements.				
Selection-based Requirements (presented alphabetically)				
This PP-Module has no selection-based requirements.				