Mapping Between
PP-Module for Bluetooth, Version 1.0,
2021-04-15
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 and 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 specific controls, but typically satisfaction also requires the implementation of operational procedures; furthermore, 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 whether the control is satisfied in the overall system context.
- **Granularity of SFRs versus 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 abstraction. 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 whole system, 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 toward 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; particularly, it is important not to read more into an SFR to control mapping than a contribution of some level of support.
- **AC-18.** The primary purpose of this PP-Module is to define implementation requirements for Bluetooth. Therefore, a product implementing Bluetooth supports the enforcement of AC-18 at a high level. Individual SFRs may relate to other security controls to ensure the secure implementation of the functions that are performed in support of this, but the reader should be aware that AC-18 is the behavior that Bluetooth is intended to address.
- **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.
- **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.** A TOE that conforms to this PP-Module will also conform to either the Protection Profile for Mobile Device Fundamentals (MDF PP) or the Protection Profile for General Purpose Operating Systems (GPOS PP) by definition. Therefore, the TOE will satisfy additional security controls not referenced here through its conformance to one of these Base-PPs. This PP-Module refines some of the Base-PP requirements to ensure consistency between the claimed Base-PP and the PP-Module, but this does not affect the security controls that satisfying those requirements is intended to address.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
Additional Requirements (MDF PP Base)				
FMT_SMF_EXT.1/BT	**Specification of Management Functions**	CM-6	**Configuration Settings**	A conformant TOE may satisfy one or more optional 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. Specific additional controls may be supported depending on the functionality claimed by the TOE.
Additional Requirements (GPOS PP Base)				
FMT_MOF_EXT.1/BT	**Management of Security Functions Behavior**	AC-3	**Access Enforcement**	A conformant TOE supports this control by providing access control restrictions to various functions. Note that the extent of support depends on the extent to which this behavior is captured in the organizational access control policies defined by AC-1.
		AC-3(7)	**Access Enforcement:** Role-Based Access Control	A conformant TOE supports this control by providing different role-based levels of management functionality to users, administrators, and MDM.
		AC-6	**Least Privilege**	A conformant TOE supports the concept of least privilege by limiting device management functions to only the roles that are needed to perform them.
		AC-6(1)	**Least Privilege:** Authorize Access to Security Functions	A conformant TOE will enforce access restrictions such that users are not granted excessive administrative privileges to manage the TSF.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		AC-6(10)	**Least Privilege:** Prohibit Non-Privileged Users from Executing Privileged Functions	A conformant TOE supports this control by defining some management functionality as privileged such that ordinary users cannot perform these functions.
FMT_SMF_EXT.1/BT	**Specification of Management Functions**	CM-6	**Configuration Settings**	A conformant TOE may satisfy one or more optional 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. Specific additional controls may be supported depending on the functionality claimed by the TOE.
Mandatory Requirements				
FAU_GEN.1/BT	**Audit Data Generation (Bluetooth)**	AU-2	**Event Logging**	A conformant TOE can 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	**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.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		AU-3(1)	**Content of Audit Records:** Additional Audit Information	A conformant TOE will generate audit information for some auditable events beyond what is mandated in AU-3. This may or may not be sufficient to satisfy this control based on the additional audit information required by the organization. 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 can generate audit logs. 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.
FCS_CKM_EXT.8	**Bluetooth Key Generation**	AC-18(1)	**Wireless Access:** Authentication and Encryption	A conformant TOE supports the encryption portion of this control by supporting the functionality needed for Bluetooth communications to be encrypted.
		SC-12	**Cryptographic Key Establishment and Management**	A conformant TOE supports the key generation function of this control, specifically as it relates to Bluetooth keys.
FIA_BLT_EXT.1	**Bluetooth User Authorization**	AC-18	**Wireless Access**	A conformant TOE supports this control by providing restrictions on Bluetooth pairing, assuming the organization's policies include such restrictions.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		AC-18(1)	**Wireless Access:** Authentication and Encryption	A conformant TOE supports the authentication portion of this control by requiring the user to authenticate any remote device before Bluetooth pairing can occur.
FIA_BLT_EXT.2	**Bluetooth Mutual Authentication**	AC-18(1)	**Wireless Access:** Authentication and Encryption	A conformant TOE supports the authentication portion of this control by requiring mutual authentication between itself and a remote Bluetooth device prior to allowing wireless access.
		IA-3	**Device Identification and Authentication**	A conformant TOE will require mutual authentication with a remote Bluetooth device prior to establishing a link to it.
FIA_BLT_EXT.3	**Rejection of Duplicate Bluetooth Connections**	AC-18(1)	**Wireless Access:** Authentication and Encryption	A conformant TOE supports the authentication portion of this control by disallowing duplicate Bluetooth device addresses to authenticate to the TOE.
		IA-3	**Device Identification and Authentication**	A conformant TOE will require a Bluetooth device to be uniquely identified prior to attempting to authenticate it.
FIA_BLT_EXT.4	**Secure Simple Pairing**	AC-18(1)	**Wireless Access:** Authentication and Encryption	A conformant TOE supports the authentication portion of this control by using SSP to establish Bluetooth connectivity.
		IA-3	**Device Identification and Authentication**	A conformant TOE may use SSP as part of performing device authentication, depending on the remote logical interfaces provided by the TSF.
FIA_BLT_EXT.6	**Trusted Bluetooth Device User Authorization**	AC-18	**Wireless Access**	A conformant TOE supports this control by requiring explicit user authorization for devices to gain access to Bluetooth profiles.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
		IA-9	**Service Identification and Authentication**	A conformant TOE supports service identification because it can authorize or limit access to specific services through its associated Bluetooth profiles.
FIA_BLT_EXT.7	**Untrusted Bluetooth Device User Authorization**	AC-18	**Wireless Access**	A conformant TOE supports this control by requiring explicit user authorization for devices to gain access to Bluetooth profiles.
		IA-9	**Service Identification and Authentication**	A conformant TOE supports service identification because it can authorize or limit access to specific services through its associated Bluetooth profiles.
FTP_BLT_EXT.1	**Bluetooth Encryption**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will support this control by providing a protected communication channel over the Bluetooth interface.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The protected communications implemented by the TOE use cryptographic methods to secure data in transit.
FTP_BLT_EXT.2	**Persistence of Bluetooth Encryption**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE will support this control by providing a protected communication channel over the Bluetooth interface.
		SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	The protected communications implemented by the TOE use cryptographic methods to secure data in transit.
FTP_BLT_EXT.3/BR	**Bluetooth Encryption Parameters (BR/EDR)**	SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports this control by ensuring that the protected channel uses a minimum cryptographic key strength to secure data in transit.

Common Criteria Version 3.1R5 SFR		NIST SP 800-53 Revision 5 Control Supports		Comments and Observations
Optional Requirements				
This PP-Module has no optional requirements.				
Objective Requirements				
FIA_BLT_EXT.5	**Bluetooth Secure Connections**	SC-8	**Transmission Confidentiality and Integrity**	A conformant TOE supports this control by ensuring the confidentiality and integrity of data transmitted over the Bluetooth interface.
Implementation-Based Requirements				
This PP-Module has no implementation-based requirements.				
Selection-Based Requirements				
FTP_BLT_EXT.3/LE	**Bluetooth Encryption Parameters (LE)**	SC-8(1)	**Transmission Confidentiality and Integrity:** Cryptographic Protection	A conformant TOE supports this control by ensuring that the protected channel uses a minimum cryptographic key strength to secure data in transit.